Technical Guide:

FileVault Encryption, Bootstrap Token, Volume Ownership, Local Administrator Password Solution (LAPS) on macOS with Jamf Pro for Texas A&M

Table of Contents

Introduction

This document provides a comprehensive guide for IT professionals on how to manage FileVault encryption, Bootstrap Token, Volume Ownership, and Local Administrator Password Solution (LAPS) on macOS devices using Jamf Pro. These features are critical for ensuring the security and proper management of macOS devices within an organization.

FileVault Encryption

FileVault is a built-in encryption feature on macOS that secures data at rest by encrypting the entire disk. This ensures that unauthorized users cannot access the data without the correct login credentials.

Steps to Enable FileVault Encryption with Jamf Pro

1. **Open Jamf Pro Console**: Log in to your Jamf Pro console.
2. **Create a FileVault Configuration Profile**: Navigate to "Computers" > "Configuration Profiles" and create a new profile.
3. **Configure FileVault Settings**: In the profile, go to the "Security & Privacy" payload and configure the FileVault settings. You can choose to enable FileVault, set a recovery key, and specify additional options.
4. **Deploy the Profile**: Assign the profile to the target devices and deploy it. The devices will prompt users to enable FileVault upon the next login.
5. **Monitor Encryption Status**: Use Jamf Pro to monitor the encryption status of the devices and ensure compliance.

Important Considerations

- **Recovery Key Management**: Jamf Pro can escrow the recovery keys, ensuring they are securely stored and accessible when needed.
- **User Management**: Ensure that all users who need access to the encrypted disk are enabled for FileVault through Jamf Pro.

Bootstrap Token

The Bootstrap Token is a feature introduced in macOS Catalina (10.15) that allows for the automatic granting of Secure Tokens to mobile and local accounts created by MDM solutions.

Steps to Manage Bootstrap Token with Jamf Pro

1. **Check Secure Token Status**: Use the command `sudo fdesetup list -extended` to list users with Secure Tokens.
2. **Check Bootstrap Token Status**: Use the command `sudo profiles status -type bootstraptoken` to check if a profile has a Bootstrap Token.
3. **Generate Bootstrap Token**: If a user has a Secure Token, you can generate a Bootstrap Token using the command `sudo profiles install -type bootstraptoken`.
4. **Escrow Bootstrap Token**: Ensure that the Bootstrap Token is escrowed to your MDM solution for future use.

Remediations: Escrowing the Bootstrap Token from Apple UEM

- **Attempt to escrow the bootstrap token using Policy**

1. **Technician Login**: The technician should log into the device using their credentials.
2. **Run the Escrow Bootstrap Token Policy**: This can be found in the Self-Service Application and will be scoped to devices needing remediation.
3. **Policy information**: The policy can be found under the name **"Escrow Bootstrap Token"** or run from terminal as an admin user. The terminal command would be "**sudo jamf policy -event escrowBootStrap"**.
4. **Select Account with Secure Token**: When prompted, select the account with a Secure Token.
5. **Enter Credentials**: Use the credentials from the Jamf Pro inventory record for that device or other known user account with correct password.
6. **Policy Validation**: The policy should give dialog prompts letting the end user know if the process was successful or not.
7. **Restart and Login**: Once the script is completed and was successful, restart the device and log in with the technician's credentials.
8. **Verify Volume Ownership and Secure Token**: Ensure that Volume Ownership and Secure Token are issued to the logged-in user. This can be verified in Jamf.

Verify Jamf Pro Computer Inventory Record

1. **Check Jamf Pro Inventory:** Once the Bootstrap token or Secure Token has been escrowed to Jamf Pro for the device. Verify the inventory record has been updated.
2. **Where to verify:** In Jamf Pro, you can click the menu on the left and click Computer > Search Inventory > and in the top search bar enter the device serial number. (Make sure the drop down next to the search bar is set to '*Computers*'
3. **Device Inventory:** Once you have found the device. You can locate the Devices Extension Attributes updated by Jamf Pro. The Extension Attributes we are verifying are: **SecureToken Users** and **Volume Owners.** They are located here under the individual devices Inventory Record: Inventory > User and Location.
4. **Extension Attributes:** The two Extensions Attributes mentioned in step 3 (**SecureToken Users** and **Volume Owners)** will show the current end user with Volume Ownership and Secure token access.
5. **No Information Found:** If the two Extension Attributes do not have any information or usernames. Try running a Health Check from the Support Hub or Self-Service Application. You can also open the Terminal Application and run this command in an elevated state as administrator: "**sudo jamf recon".** This will attempt to update the device's inventory record in Jamf Pro.

Scenarios

- **User with Secure Token but no Bootstrap Token**: Generate a Bootstrap Token using the Secure Token status.
- **User without Secure Token but another user has it**: Pass the Secure Token from the existing user to the intended user, then generate the Bootstrap Token.
- **No Users with Secure Token**: Re-enroll the device to generate a new Secure Token upon re-enrollment.
- **Unable to Add User for Secure Token**: If no users have a Bootstrap Token and the password is unknown. The device will have to be wiped and re-imaged to create a new token.

Secure Token Troubleshooting

As a basic overview, Secure Tokens and Bootstrap Tokens are leveraged in this order: Secure Token >> Bootstrap Token. Secure Tokens allow us to generate a Bootstrap Token. Bootstrap Tokens are mostly used for mass action Apple Silicon macOS updates. To update M1 macOS machines without user interaction, ensure that there is a Bootstrap Token to do so. Bootstrap Tokens are generated based on Secure Token status.

Initial Checks with Terminal.app

- **List Users with Secure Tokens**: `sudo fdesetup list -extended`
- **Check Bootstrap Token Status**: `sudo profiles status -type bootstraptoken`

Scenarios

1. **Scenario A - Intended User has Secure Token, but not a Bootstrap Token**
    - Generate Bootstrap Token for the user based on Secure Token status with Terminal:

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

4. **Scenario B - Intended User does not have Secure Token or Bootstrap Token, but another User on the computer does have a Secure Token (Scripting)**
    - This can be saved as a file and ran.
    - Pass Secure Token from the Secure Token holding user to the intended user:

```
#!/bin/bash
currentUser=$(who | grep "console" | cut -d" " -f1)
userPwd=$(osascript << EOF
text returned of (display dialog "Updating password for $currentUser. Please enter your new password" default answer "xxxxxxxxx" buttons {"OK"} default button 1 with hidden answer)
EOF
  )
  echo "Enabling Secure token for $currentUser"
  sysadminctl -adminUser $4 -adminPassword $5 -secureTokenOn $currentUser -password $userPwd
```

    - Generate Bootstrap Token based on Secure Token status with Terminal:

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

15. **Scenario C - No Users on the computer have a Secure Token**
    - Re-enroll the device to generate a new Secure Token upon re-enrollment.

- Special note: When generating a new user after re-enrollment, ensure that the account is NOT being modified in the PreStage, and the username does not match any management account(s) being deployed in the PreStage. If unsure of the current Management Account name, check Settings > Global Management > User-Initiated Enrollment > macOS > Management Account.

Volume Ownership

Volume Ownership is a concept introduced with macOS Big Sur (11.0) and Apple Silicon Macs. It ensures that the user who sets up the Mac is granted ownership of the volume, allowing them to perform software updates and other administrative tasks.

Steps to Manage Volume Ownership with Jamf Pro

1. **Verify Volume Ownership**: Ensure that the primary user has volume ownership by checking their Secure Token status.
2. **Assign Volume Ownership**: If the primary user does not have volume ownership, use the Bootstrap Token to grant it.
3. **Re-enroll Device**: If necessary, re-enroll the device to reset volume ownership and Secure Token status.

Important Considerations

- **Secure Token Requirement**: Volume ownership is tied to the Secure Token status of the user.
- **MDM Integration**: Ensure that your MDM solution supports Bootstrap Token and Secure Token management.

Troubleshooting Common Issues

FileVault Encryption

1. **Unsupported File System**: FileVault works only with the APFS (Apple File System) format. If you encounter an unsupported file system, back up your data and reformat the drive to APFS.
2. **Insufficient Disk Space**: Ensure you have ample free disk space before enabling FileVault. Insufficient space can prevent encryption from starting.
3. **Admin Account Permissions**: Verify that the admin account you're using has full administrative privileges.

Bootstrap Token

1. **Secure Token Status**: Use the command with Terminal: `sudo fdesetup list -extended` to list users with Secure Tokens. If no users have a Secure Token, re-enroll the device to generate a new Secure Token upon re-enrollment.
2. **Escrow Issues**: Ensure that the Bootstrap Token is properly escrowed to your MDM solution. Use the command with Terminal: `sudo profiles status -type bootstraptoken` to check the status.
3. **Password Issues**: If you encounter issues with passing Secure Tokens, ensure that the correct admin credentials are used in scripts and policies.

Volume Ownership

1. **Secure Token Requirement**: Volume ownership is tied to the Secure Token status of the user. Verify that the primary user has a Secure Token.
2. **Re-enrollment**: If volume ownership issues persist, re-enroll the device to reset volume ownership and Secure Token status.

Local Administrator Password Solution (LAPS)

The Local Administrator Password Solution (LAPS) is Jamf's implementation of a managed local administrator password solution. LAPS allows you to use Jamf Pro to automatically store, rotate, and view the randomized password of a managed local administrator account. This functionality is available in the Jamf Pro API and the Jamf Pro interface.

Steps to Implement LAPS with Jamf Pro

1. **Enable LAPS in Jamf Pro**: Navigate to the Jamf Pro console and enable LAPS in the Jamf Pro API.
2. **View Managed Local Administrator Accounts**: After enabling LAPS, you can view managed local administrator accounts and passwords in the Jamf Pro interface. Viewing a LAPS password automatically triggers password rotation according to your LAPS settings.
3. **Monitor LAPS Events**: All LAPS events, including password viewing and rotation, are logged. To view a list of events, navigate to the computer's inventory record, click the "History" tab, and then click the "Managed Local Administrator Account History" category.

Important Considerations

- **Password Rotation**: Ensure that password rotation settings are configured according to your organization's security policies.
- **Audit Logs**: Regularly review audit logs to monitor LAPS events and ensure compliance.

Best Practices for Using Jamf Pro

1. **Automated MDM Enrollment**: Utilize automated MDM enrollment for zero-touch deployment of macOS, iOS, and tvOS devices. This ensures a seamless and efficient setup process for end users.
2. **Regular Updates**: Keep Jamf Pro and all managed devices up to date with the latest software versions and security patches. This helps to mitigate vulnerabilities and ensures optimal performance.
3. **Role-Based Access Control**: Implement role-based access control (RBAC) to manage permissions and access levels within Jamf Pro. This ensures that users have the appropriate level of access based on their roles and responsibilities.
4. **Advanced Searches and Reporting**: Leverage advanced searches and reporting capabilities in Jamf Pro to monitor device compliance, generate insights, and create alerts for specific conditions.
5. **Integration with Other Tools**: Integrate Jamf Pro with other tools such as Power BI for deeper data analysis and visualization. This enhances the ability to make data-driven decisions.
6. **Compliance Monitoring**: Use pre-built compliance checks and customizable threat detection rules to ensure that devices adhere to organizational security policies.
7. **User Training and Documentation**: Provide comprehensive training and documentation for end users and IT staff to ensure they are familiar with Jamf Pro features and best practices.

References

- **Local Administrator Password Solution for Jamf Pro**: Local Administrator Password Solution
- **Jamf Pro Documentation**: Jamf Pro Documentation
- **Apple Documentation**: Apple Token and Volume Ownership Documentation

Conclusion

Managing FileVault encryption, Bootstrap Token, Volume Ownership, Local Administrator Password Solution (LAPS) on macOS is essential for maintaining the security and integrity of devices within an organization. By following the steps outlined in this document and leveraging Jamf Pro, IT professionals can ensure that macOS devices are properly encrypted and managed.
