Apple Device Administrators' Meeting
12.06.18

macOS 10.13 Spring Update: UAMDM, UAKEL and Secure Token

Context:

Want to allow current Orchard Mac users to upgrade to macOS 10.13

Want to allow new Macs running macOS 10.13 to join Orchard

Desktops and laptops

Support macOS 10.12 back to 10.10

Software using Kernel Extensions (kexts)

FileVault 2 encryption

Bound to AD and create mobile user

UAMDM

User Approved Mobile Device Management

Introduced macOS 10.13.2

Grants MDM system additional security privileges

Manage kernel extension loading (UAKEL)

Depends on enrolment method - imaging / user-driven / DEP

No automated or remote approval

Resources:

https://support.apple.com/en-us/HT208019

https://simplemdm.com/2017/11/01/user-approved-mdm-enrollment/

https://derflounder.wordpress.com/2018/03/30/detecting-user-approved-mdm-using-the-profiles-command-line-tool-on-macos-10-13-4/

https://www.jamf.com/jamf-nation/discussions/27653/summary-of-macos-10-13-4-information-and-links

UAKEL

User Approved Kernel Extension Loading

Protect system from malicious code

Consent to each kext on first load

Any user can consent

To manage need
1) UAMDM
2) Configuration Profile to whitelist kexts using Team ID and Bundle ID

Resources:

https://support.apple.com/en-us/HT208019

https://derflounder.wordpress.com/2018/04/12/whitelisting-third-party-kernel-extensions-using-profiles/

Secure Token

Undocumented user account attribute

Introduced 10.13

Required for FileVault but behaviour not clear

Should be granted to first user to log into GUI but patchy (AD / mobile users)

Can be passed down or granted by user who has Secure Token him/herself

Resources:

https://derflounder.wordpress.com/2018/01/20/secure-token-and-filevault-on-apple-file-system/

Demo: 10.13.5 VM

The Moving Target

1) Which 10.13.x to upgrade to and support for new enrollments?

UAMDM
“Auto-accepted until 10.13.3 but DEP-only enrolments from then on.”

Secure Token
“In 10.13.4 beta, mobile users prompted for admin credentials to add Secure Token whether encrypted or not.”

2) MDM limitations
Profiles for kext whitelist and FileVault escrow not supported until jamf 10.

Resources:

https://www.jamf.com/jamf-nation/discussions/27653/summary-of-macos-10-13-4-information-and-links [note on mobile accounts in first post]

Where we are with UAMDM

Accepted automatically when upgrading to 10.13.5, for DEP and user-driven enrollments
- imaging still to test

Non-DEP enrollments at 10.13.5 need manual UAMDM approval

jamf PRO 10.3 may have a workaround
https://www.jamf.com/jamf-nation/discussions/26435/macos-10-13-2-and-user-approved-mdm-enrollment#responseChild163342

Where we are with UAKEL

Kernel extensions installed prior to 10.13.4 automatically approved

Use custom settings to build whitelisting profile (to test)

Cannot blanket whitelist, need specific Team ID and Bundle IDs

Resources:

https://derflounder.wordpress.com/2018/04/12/whitelisting-third-party-kernel-extensions-using-profiles/

https://support.zuludesk.com/hc/en-us/articles/115004701513-Whitelist-Kernel-Extensions

Where we are with Secure Token

Admin with Secure Token can manage FileVault

FileVault enabled users can still unlock without Secure Token

Mobile users on upgrade to 10.13.5 get Secure Token

For new enrolments on 10.13.5, the initial user gets Secure Token
- still to test where first login is AD user

If no user has Secure Token, rerun Setup Assistant

Resources:

https://derflounder.wordpress.com/2018/01/20/secure-token-and-filevault-on-apple-file-system/

Command Line Bonuses

Note: tested on 10.13.5.

MDM enrollment status, including UAMDM status

```
profiles status -type enrollment
```

Returns:

```
Enrolled via DEP: No / Yes
MDM enrollment: No / Yes / Yes (User Approved)
```

Determine Team ID and Bundle IDs for kexts in order to whitelist them

```
cbeard-10-13p5:~ root# sqlite3 /var/db/SystemPolicyConfiguration/
KextPolicy
SQLite version 3.19.3 2017-06-27 16:48:08
Enter ".help" for usage hints.
sqlite> SELECT * FROM kext_policy;
2H5GFH3774|com.sophos.kext.oas|0|Sophos|4
2H5GFH3774|com.sophos.nke.swi|0|Sophos|4
sqlite> .quit
```

https://grahamgilbert.com/blog/2017/09/11/enabling-kernel-extensions-in-high-sierra/

Resources on using spctl and Recovery to approve kexts

https://pikeralpha.wordpress.com/2017/08/29/user-approved-kernel-extension-loading/

https://www.idelta.info/archives/secure-kernel-extension-loading-in-macos-high-sierra/

Determine if a user has Secure Token (will work via SSH)

```
sysadminctl -secureTokenStatus <username>
```

Grant Secure Token to another user

Need to be logged in as admin with Secure Token and know password of recipient user

```
sysadminctl interactive -secureTokenOn <recipient-user> -password -
```

Rerun Setup Assistant (eg. to create a new admin account with Secure Token)

```
rm -r /var/db/.AppleSetupDone
reboot now
```