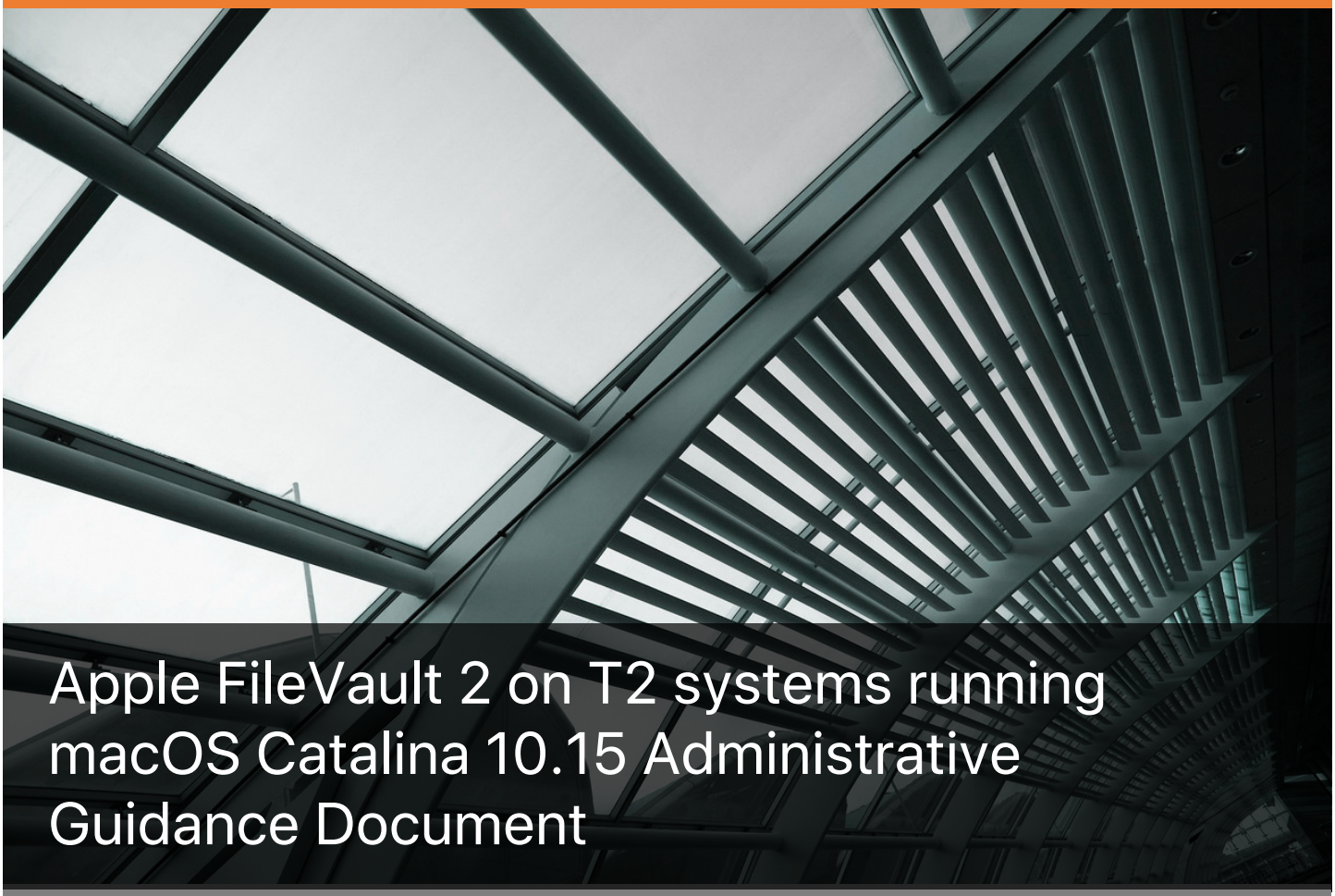


# Apple FileVault 2 on T2 systems running macOS Catalina 10.15 Administrative Guidance Document

Prepared By:
Acumen Security, LLC
www.acumensecurity.net

Prepared for: Apple
One Apple Park Way
Cupertino, CA 95014

Document Version: 0.8
Date: April 19, 2021

## Table of Contents

Revision History

| Version | Date | Description |
|---|---|---|
| 0.1 | 10/29/2020 | Initial draft |
| 0.2 | 11/24/2020 | Updated based on internal review. |
| 0.3 | 01/05/2021 | Updated based on vendor feedback. |
| 0.4 | 01/06/2021 | Updated based on vendor feedback. |
| 0.5 | 03/18/2021 | Updated based on vendor feedback. |
| 0.6 | 03/19/2021 | Updated based on internal review. |
| 0.7 | 03/24/2021 | Updated based on internal review. |
| 0.8 | 04/19/2021 | Updated based on comments. |

**Trademarks:**

Apple's trademarks applicable to this document are listed in https://www.apple.com/legal/intellectual-property/trademark/appletmlist.html. Other company, product, and service names may be trademarks or service marks of others.

## Abbreviations:

The following table provides a list of abbreviations used throughout this document.

| Term | Full Form |
|---|---|
| TOE | Target of Evaluation |
| FDE | Full Drive Encryption |
| EE | Encryption Engine |
| AA | Authorization Acquisition |
| OS | Operating System |
| ROM | Read Only Memory |
| UEFI | Unified Extensible Firmware Interface |
| eSPI | Enhanced Serial Peripheral Interface |
| DFU | Device Firmware Upgrade |
| DEK | Data Encryption Key |
| VPN | Virtual Private Network |
| CC | Common Criteria |
| TLS | Transport Layer Security |
| RSA | Rivest-Shamir-Adleman public-key cryptosystem |
| SIP | System Integrity Protection |
| APFS | Apple File System |
| HFS | Hierarchical File System |
| NVRAM | Non-volatile Random-Access Memory |
| PRAM | Parameter Random Access Memory |
| AES | Advanced Encryption Standard |
| HMAC | Hash-based Message Authentication Code |
| SHA | Secure Hash Algorithm |
| BEV | Border Encryption Value |

# 1 Administrative Guidance Document Introduction

This Common Criteria guidance document contains configuration information needed to configure and administer Apple FileVault 2 on T2 Systems running on macOS Catalina 10.15. The TOE type is an authorization and encryption engine product. It satisfies all the criteria to meet the collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 2.0 + Errata 20190201 [FDE EE v2.0e] and collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition Version 2.0 + Errata 20190201 [FDE AA v2.0e]. The information contained in this document is intended for Administrators who are responsible for the configuration and management of the TOE.

## 1.1 TOE Overview

The TOE is a full drive encryption product which supports both authorization acquisition and the encryption engine. The TOE is Unix-based Operating System (OS) which leverages the Apple T2 security chip (T2 security chip) to perform the full disk encryption. The OS core is a POSIX compliant OS built on top of the XNU kernel with standard Unix facilities available from the command line interface.

### 1.1.1 TOE Product Type

The TOE type is an authorization and encryption engine product. It satisfies all of the criterion to meet the collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 2.0 + Errata 20190201 [FDE EE v2.0e] and collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition Version 2.0 + Errata 20190201 [FDE AA v2.0e].

## 1.2 TOE Description

### 1.2.1 Evaluated Configuration

The TOE is comprised of both software and hardware. The TOE hardware consists of the Apple T2 Security Chip which is a custom silicon for the Mac. It contains the Secure Enclave coprocessor which provides security related functionality for all the EE functionality (i.e., other than encryption/decryption of storage data) and all of the cryptographic functionality for AA (i.e., PBKDF2). The Password Acquisition component (AA) is the pre-boot component on the disk and captures the user password and passes it to the T2/SEP. The T2 provides a dedicated AES crypto engine built into the Direct Memory Access (DMA) path between the storage and main memory of the host platform. The T2 chip is placed in the data path between the Intel chip and the storage, enabling it to encrypt/decrypt all data flowing between these two components.

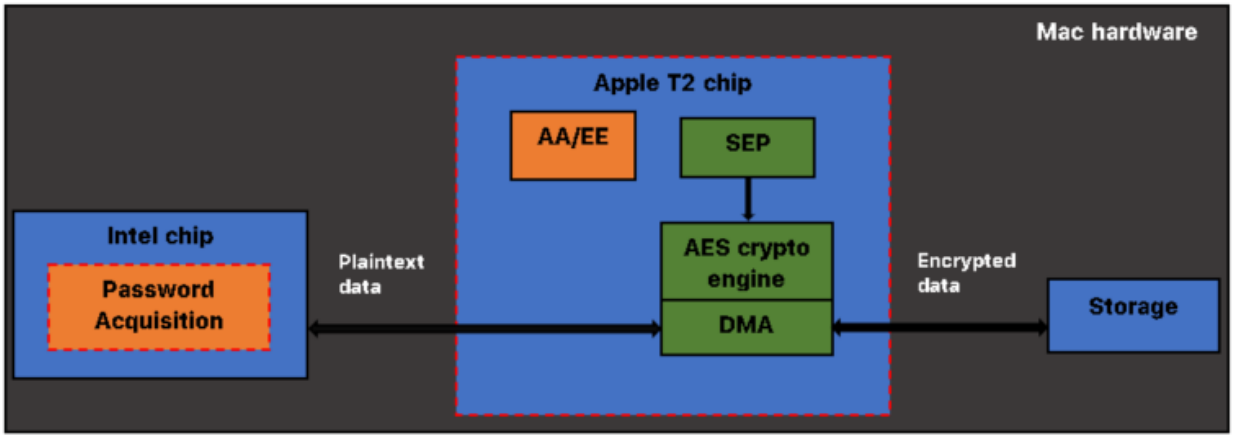



**Figure 1: Major components of the TOE within red border**

The TOE also supports secure connectivity with an Apple update server as described in Table 1 below:

| Sr. No | Component | Required | Usage/Purpose Description for TOE performance |
|---|---|---|---|
| 1 | Apple update server | Yes | Provides the ability to download authentic signed updates. |

**Table 1: IT Environment Components**

Table 2 below provides a list of supported platforms:

| Device | Year | Intel Processor | Apple T2 Chip |
|---|---|---|---|
| iMac Pro<br><br>Model: A1862<br>Reference: iMac Pro1,1 | Late 2017 | Intel Xeon W-2140B (Skylake) | |
| iMac Pro<br><br>Model: A1862<br>Reference: iMac Pro1,1 | Late 2017 | Intel Xeon W-2150B (Skylake) | |
| iMac Pro<br><br>Model: A1862<br>Reference: iMac Pro1,1 | Late 2017 | Intel Xeon W-2170B (Skylake) | |
| iMac Pro<br><br>Model: A1862<br>Reference: iMac Pro1,1 | Late 2017 | Intel Xeon W-2191B (Skylake) | |

| Device | Year | Intel Processor | Apple T2 Chip |
|---|---|---|---|
| Mac mini<br><br>Model: A1993<br>Reference: Macmini8,1 | 2018 | Intel Core i5-8500B (Coffee Lake) | Apple T2 (ARM64)<br><br>Processor T2 (processor family arm64) from Apple family: arm64 manufacturer: Apple series: T Series Software: TxFW 10.15 |
| Mac mini<br><br>Model: A1993<br>Reference: Macmini8,1 | 2018 | Intel Core i7-8700B (Coffee Lake) | |
| MacBook Pro<br><br>Model: A1989<br>Reference: MacBookPro15,2 | Mid 2018 | Intel Core i5-8279U (Coffee Lake) | |
| MacBook Pro<br><br>Model: 1989<br>Reference: MacBookPro15,2 | Mid 2018 | Intel Core i5-8259U (Coffee Lake) | |
| MacBook Pro<br><br>Model: A1990<br>Reference: MacBookPro15,1 | Mid 2018 | Intel Core i7-8750H (Coffee Lake) | |
| MacBook Pro<br><br>Model: A1989<br>Reference: MacBookPro15,2 | Mid 2018 | Intel Core i7-8559U (Coffee Lake) | |
| MacBook Pro<br><br>Model: A1990<br>Reference: MacBookPro15,3 | Mid 2018 | Intel Core i7-8850H (Coffee Lake) | |
| MacBook Pro<br><br>Model: A1990<br>Reference: MacBookPro15,1 | Mid 2018 | Intel Core i9-8950HK (Coffee Lake) | |
| MacBook Pro<br><br>Model: A1990<br>Reference: MacBookPro15,3 | Mid 2018 | Intel Core i9-8950HK (Coffee Lake) | |
| MacBook Air<br><br>Model: A1932<br>Reference: MacBookAir8,1 | Late 2018 | Intel Core i5-8210Y (Amber Lake) | Apple T2 (ARM64)<br><br>Processor T2 (processor family arm64) from Apple |
| MacBook Air<br><br>Model: A1932<br>Reference: MacBookAir8,2 | 2019 | Intel Core i5-8210Y (Amber Lake) | |

| Device | Year | Intel Processor | Apple T2 Chip |
|---|---|---|---|
| Mac Pro<br><br>Model: A1991<br>Reference: Mac Pro7,1 | 2019 | Intel Xeon W-3223 (Cascade Lake) | family: arm64<br>manufacturer: Apple<br>series: T Series<br>Software: TxFW 10.15 |
| Mac Pro<br><br>Model: A1991<br>Reference: Mac Pro7,1 | 2019 | Intel Xeon W-3235 (Cascade Lake) | |
| Mac Pro<br><br>Model: A1991<br>Reference: Mac Pro7,1 | 2019 | Intel Xeon W-3245 (Cascade Lake) | |
| Mac Pro<br><br>Model: A1991<br>Reference: Mac Pro7,1 | 2019 | Intel Xeon W-3265M (Cascade Lake) | |
| Mac Pro<br><br>Model: A1991<br>Reference: Mac Pro7,1 | 2019 | Intel Xeon W-3275M (Amber Lake) | |
| MacBook Pro<br><br>Model: A1989<br>Reference: MacBookPro15,2 | 2019 | Intel Core i5-8279U (Amber Lake) | Apple T2 (ARM64)<br><br>Processor T2 (processor family arm64) from Apple family: arm64 manufacturer: |
| MacBook Pro<br><br>Model: A2159<br>Reference: MacBookPro15,4 | 2019 | Intel Core i5-8257U (Amber Lake) | |
| MacBook Pro<br><br>Model: A1990<br>Reference: MacBookPro15,1 | 2019 | Intel Core i7-9750H (Coffee Lake) | |
| MacBook Pro<br><br>Model: A1989<br>Reference: MacBookPro15,2 | 2019 | Intel Core i7-8569U (Coffee Lake) | |
| MacBook Pro<br><br>Model: A2159<br>Reference: MacBookPro15,4 | 2019 | Intel Core i7-8557U (Coffee Lake) | |
| MacBook Pro:<br><br>Model: A2141<br>Reference: MacBookPro16,1 | 2019 | Intel Core i7-9750H (Coffee Lake) | |

| Device | Year | Intel Processor | Apple T2 Chip |
|---|---|---|---|
| MacBook Pro<br><br>Model: A1990<br>Reference: MacBookPro15,1 | 2019 | Intel Core i9-9880H (Coffee Lake) | Apple<br>series: T Series<br>Software: TxFW 10.15 |
| MacBook Pro<br><br>Model: A1990<br>Reference: MacBookPro15,1 | 2019 | Intel Core I9-9980HK (Coffee Lake) | |
| MacBook Pro<br><br>Model: A1990<br>Reference: MacBookPro15,3 | 2019 | Intel Core i9-9880H (Coffee Lake) | |
| MacBook Pro<br><br>Model: A2141<br>Reference: MacBookPro16,1 | 2019 | Intel Core i9-9880H (Coffee Lake) | Apple T2 (ARM64)<br><br>Processor T2 (processor family arm64) from Apple family: arm64 manufacturer: Apple<br>series: T Series<br>Software: TxFW 10.15 |
| MacBook Pro<br><br>Model: A2141<br>Reference: MacBookPro16,1 | 2019 | Intel Core i9-9980HK (Coffee Lake) | |
| MacBook Pro<br><br>Model: A2141<br>Reference: MacBook Pro16,4 | 2019 | Intel Core i7-9750H (Coffee Lake) | |
| MacBook Pro<br><br>Model: A2141<br>Reference: MacBook Pro16,4 | 2019 | Intel Core i9-9880H (Coffee Lake) | |
| MacBook Pro<br><br>Model: A2141<br>Reference: MacBook Pro16,4 | 2019 | Intel Core i9-9980HK (Coffee Lake) | |
| iMac<br><br>Model: A2115<br>Reference: iMac20,1 | 2019 | Intel Core i5-10500 (Ice Lake) | |
| Mac Pro (rack)<br><br>Model: A2304<br>Reference: MacPro7,1 | 2019 | Intel Xeon W-3275M (Cascade Lake) | |
| Mac Pro (rack)<br><br>Model: A2304<br>Reference: MacPro7,1 | 2019 | Intel Xeon W-3265M (Cascade Lake) | |

| Device | Year | Intel Processor | Apple T2 Chip |
|---|---|---|---|
| Mac Pro (rack)<br><br>Model: A2304<br>Reference: MacPro7,1 | 2019 | Intel Xeon W-3245<br>(Cascade Lake) | |
| Mac Pro (rack)<br><br>Model: A2304<br>Reference: MacPro7,1 | 2019 | Intel Xeon W-3235<br>(Cascade Lake) | |
| Mac Pro (rack)<br><br>Model: A2304<br>Reference: MacPro7,1 | 2019 | Intel Xeon W-3223<br>(Cascade Lake) | Apple T2 (ARM64)<br><br>Processor T2 (processor family arm64) from Apple family: arm64 manufacturer: Apple series: T Series Software: TxFW 10.15 |
| MacBook Air<br><br>Model: A2179<br>Reference: MacBook Air9,1 | 2020 | Intel Core i5-1030NG7<br>(Ice Lake) | |
| MacBook Air<br><br>Model: A2179<br>Reference: MacBook Air9,1 | 2020 | Intel Core i7-1060NG7<br>(Ice Lake) | |
| MacBook Pro<br><br>Model: A2289<br>Reference: MacBook Pro16,3 | 2020 | Intel Core i5-8257U<br>(Coffee Lake) | |
| MacBook Pro<br><br>Model: A2289<br>Reference: MacBook Pro16,3 | 2020 | Intel Core i7-8557U<br>(Coffee Lake) | |
| MacBook Pro<br><br>Model: A2251<br>Reference: MacBook Pro16,2 | 2020 | Intel Core i5-1037NG7<br>(Ice Lake) | |
| MacBook Pro<br><br>Model: A2251<br>Reference: MacBook Pro16,2 | 2020 | Intel Core i7-1068NG7<br>(Ice Lake) | |
| iMac<br><br>Model: A2115<br>Reference: iMac20,1 | 2020 | Intel Core i5-10600<br>(Ice Lake) | |
| iMac<br><br>Model: A2115<br>Reference: iMac20,1 | 2020 | Intel Core i7-10700K<br>(Ice Lake) | |

| Device | Year | Intel Processor | Apple T2 Chip |
|---|---|---|---|
| iMac<br><br>Model: A2115<br>Reference: iMac20,1 | 2020 | Intel Core i9-10910<br>(Coffee Lake) | |
| iMac<br><br>Model: A2115<br>Reference: iMac20,2 | 2020 | Intel Core i7-10700K<br>(Ice Lake) | |
| iMac<br><br>Model: A2115<br>Reference: iMac20,2 | 2020 | Intel Core i9-10910<br>(Coffee Lake) | |

**Table 2: Platform specifications**

Note: The Apple T2 security chip is the same exact same chip across all Intel Mac platforms. All processing for cryptography related to FileVault 2 (FDE) is performed using the Apple T2 / SEP rather than the Intel chipset, so the Intel processors or their microarchitectures play no role in the processing (encryption/decryption) and the management of those keys for data under FileVault 2.

### 1.2.2 Physical Boundaries

The TOE is comprised of both hardware and software running on the listed platforms as indicated in Table 2. The Encryption Engine (EE) is instantiated on the T2 chip. The AA is instantiated on both the Intel chip (Password Acquisition) and the T2. It contains the Secure Enclave coprocessor which provides security related functionality for all the EE functionality (i.e., other than encryption/decryption of storage data) and all of the cryptographic functionality for AA (i.e., PBKDF2). The Password Acquisition component (AA) is the pre-boot component on the disk and captures the user password and passes it to the T2/SEP. The T2 provides a dedicated AES crypto engine built into the Direct Memory Access (DMA) path between the storage and main memory of the host platform.

## 1.3 TOE Delivery

The evaluated TOE is a delivered as a pre-installed OS on an Apple Mac with a T2 security chip. Digitally signed and verifiable updates to the TOE can be downloaded from: https://support.apple.com/downloads/macos

## 1.4 TOE Self-Tests

The TOE is designed to perform all required self-tests without the need for any TOE configuration changes. If any of the self-tests fail, the TOE will immediately shut down and prevent any attempted use of the unverified TOE.

### 1.4.1 Software/Firmware Integrity Tests

The OS (Catalina build 19H15) includes the firmware for the T2. Hence 19H15 identifies both the OS and the T2 security chip firmware.

All other TOE firmware and software integrity tests are performed using digital signature

verification prior to any execution of the corresponding code.

When a Mac computer with the Apple T2 security chip is turned on, the chip executes code from read-only memory known as Boot ROM. The Boot ROM code contains the Apple Root CA public key, which is used to verify that the iBoot bootloader is signed by Apple's private key before allowing it to load. This immutable code, referred to as the hardware root of trust, is laid down during chip fabrication and is audited for vulnerabilities and implicitly trusted. This is the first step in the chain of trust. iBoot verifies the kernel and kernel extension code on the T2 security chip, which subsequently verifies the Intel UEFI firmware. The UEFI firmware and the associated signature are initially available only to the T2 security chip.

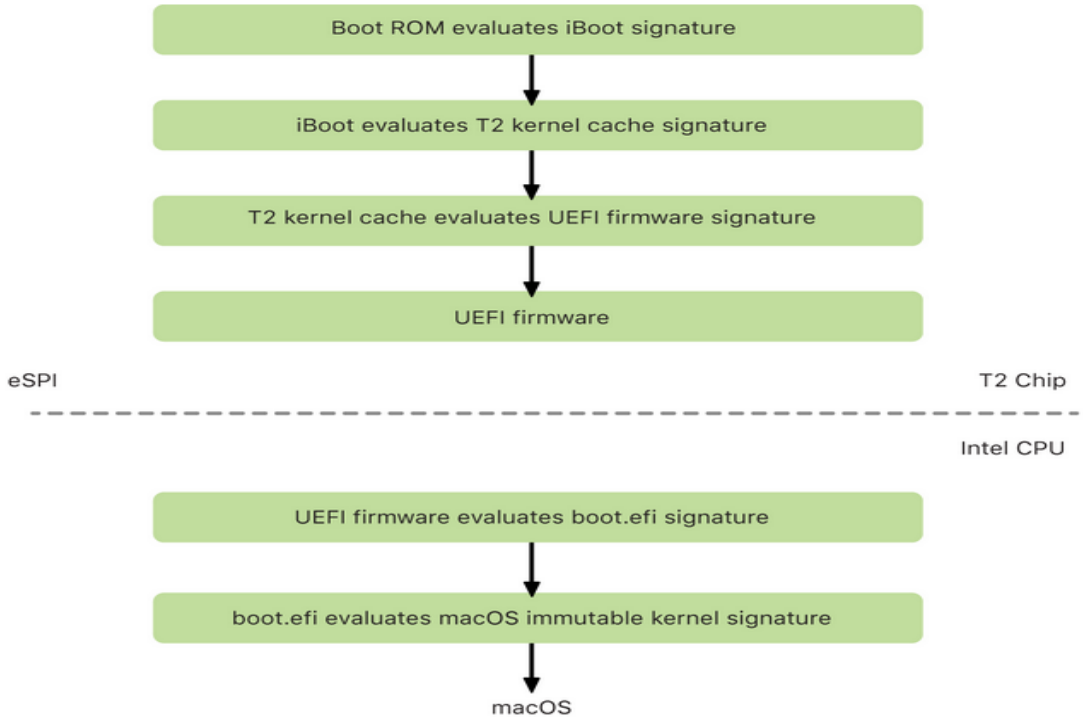



Figure 2: TOE Boot Sequence

After verification, the UEFI firmware image is mapped into a portion of the T2 security chip memory. This memory is made available to the Intel CPU through the enhanced Serial Peripheral Interface (eSPI). When the Intel CPU first boots, it fetches the UEFI firmware through eSPI from the integrity-checked, memory-mapped copy of the firmware located on the T2 security chip.

The evaluation of the chain of trust continues on the Intel CPU, with the UEFI firmware evaluating the signature for boot.efi, which is the macOS bootloader. The Intel-resident macOS secure boot signatures are stored in the same Image4 format used for iOS, iPadOS, and T2 security chip secure boot, and the code that parses the Image4 files is the same hardened code from the current iOS and iPadOS secure boot implementation. Boot.efi in turn verifies the

signature of a new file, called immutablekernel. When secure boot is enabled, the immutablekernel file represents the complete set of Apple kernel extensions required to boot macOS. The secure boot policy terminates at the handoff to the immutablekernel, and after that, macOS security policies (such as System Integrity Protection and signed kernel extensions) take effect. If there are any errors or failures in this process, the Mac enters macOS Recovery mode[1].

For further information refer to the Apple Platform Security Guide[2].

[1] macOS Recovery mode on Intel-based Macs: https://support.apple.com/en-us/HT201314
[2] Apple Platform Security Guide: https://support.apple.com/guide/security/boot-process-sec5d0fab7c6/1/web/1

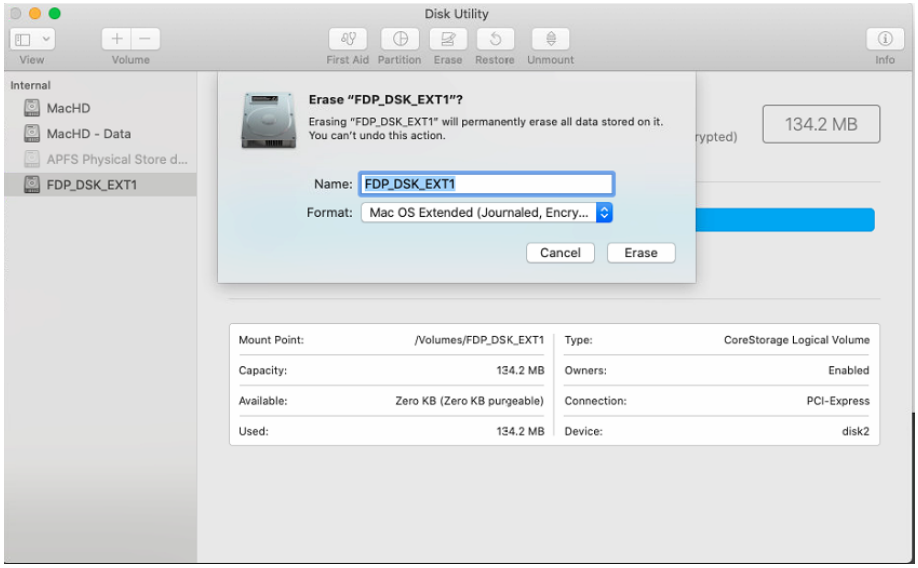
# 2 Prerequisites for Installation

The user should ensure that compatible hardware is available before installing the TOE. The TOE cannot be installed on non-Apple products nor it can be installed as a virtual instance. The TOE can be installed on any one or all the above hardware platforms; refer to Section 1.2 for a complete list of supported hardware platforms.

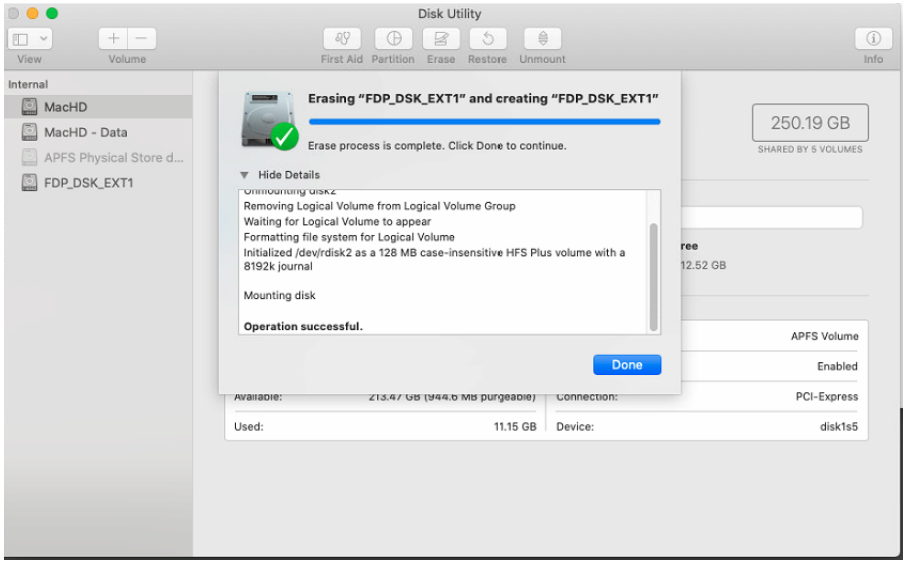
## 2.1 TOE Management Functions

The TOE allows an authorized user to perform the management functions as below:

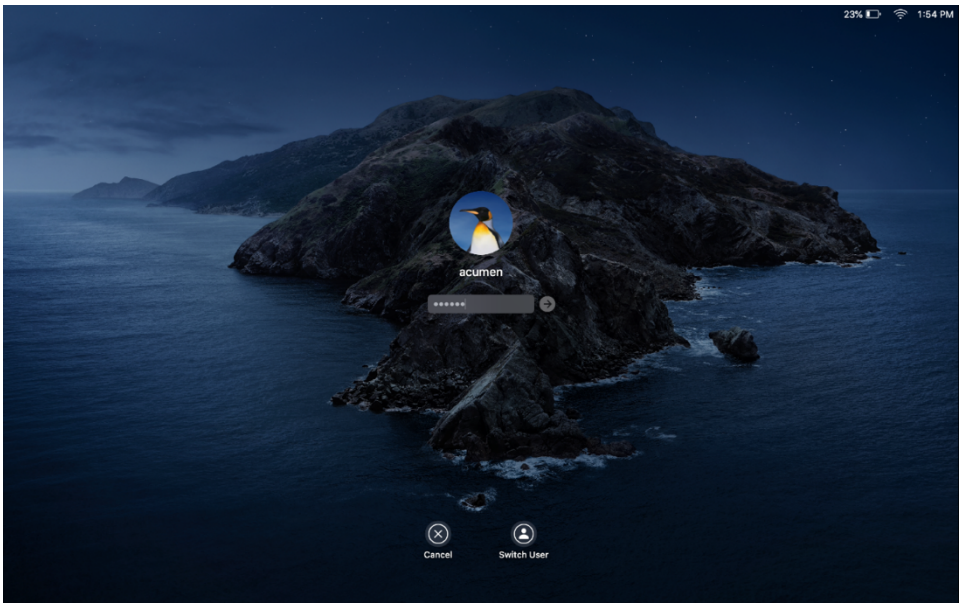
- Forward a command to the Encryption Engine (EE) to change and cryptographically erase the Device Encryption Key or DEK.
    - Open the Disk Utility application, and select the disk to be encrypted. In this case, the name of the disk was set to FDP_DSK_EXT1 drive.
    - Note: FDP_DSK_EXT1 is an example disk name.
    - Then select “Mac OS Extended (Journaled, Encrypted)”.
    - Click Erase.



- Click on Done.

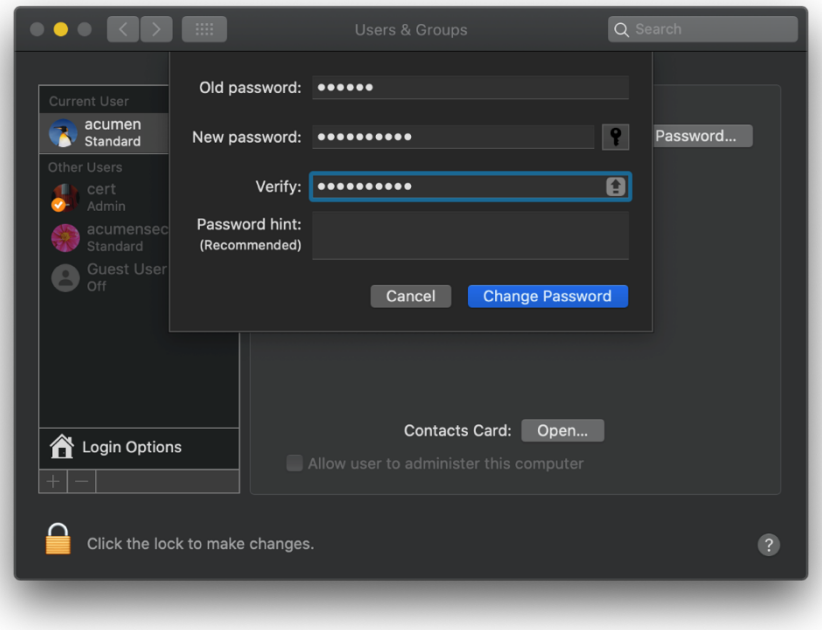



- Allowing authorized users to change authorization factors such as a user password.
  - Login to the macOS as an authorized user:



- Navigate to System Preferences -> Users & Groups.


- Select the appropriate user (i.e., in this case acumen) and click on Change Password.




- Initiate the macOS software update (refer to Section 4).

# 3 Installation of the Apple macOS Catalina 10.15

macOS and the T2 security chip are pre-installed on the supported hardware platforms as mentioned above. Should the need arise, the user can manually download and re-install and/or update macOS on the supporting hardware.

Note: The user cannot update the Apple T2 security chip.

It is recommended to take a back-up of the macOS before updating the the macOS. Refer Section 4 for detailed installation steps. The TOE implements an anti-rollback feature that prevents the user from downgrading the macOS software version to an earlier version. This feature helps avoid rollback attacks.

## 3.1 Clean Installation Steps for Apple macOS Catalina 10.15

Before installing/re-installing the macOS, the user should backup the user data to a media (e.g. hard drive) and keep the media in a safe and secure location such as a locker/safe. The macOS Catalina 10.15 can be installed in different ways as described below.

## 3.2 Install the TOE from Apple Website

- macOS update(s) can be downloaded from the website below: https://support.apple.com/downloads/macos
- After downloading, double click on macOSUpdXXX.dmg file, where XXX = actual macOS Catalina version.
- Before updating, the TOE will verify the downloaded file using a digital signature verification.
- If the digital signature verification is successful, the TOE will proceed to installing the update. Occasional TOE reboots are normal during the installation.
- If the digital signature verification is unsuccessful, the TOE will not proceed with the update/installation process.
- The TOE will reboot after the update is successfully installed.

## 3.3 Reinstall the TOE

- On the TOE, choose Apple menu > Restart.
    - Immediately after the TOE reboots, do one of the following:
    - Install the latest version of the TOE from the Internet: Press and hold Option-Command-R until a spinning globe appears, then release the keys.
    - Reinstall your computer's original version of macOS from the Internet: Press and hold Shift-Option-Command-R until a spinning globe appears, then release the keys.
    - Reinstall the TOE from the built-in recovery disk on your computer:
    - Press and hold Command-R until the Utilities window appears.
- Select Reinstall macOS, then click continue.

- Follow the onscreen instructions. In the pane where you select a disk, select your current macOS disk (in most cases, it's the only one available).
- For additional information and support about reinstalling the TOE, refer macOS User Guide[3].

[3] macOS User Guide: https://support.apple.com/guide/mac-help/reinstall-macos-mchlp1599/10.15/mac/10.15

# 4 Check Software Updates

macOS updates can be downloaded manually from the following website: https://support.apple.com/downloads. The installation of authentic macOS updates is covered in Section 4.

## 4.1 Installing Updates

Authentic macOS and software application update(s) can be downloaded from https://support.apple.com/downloads. Once an update(s) is downloaded, the user can initiate the installation of that update in the following manner:

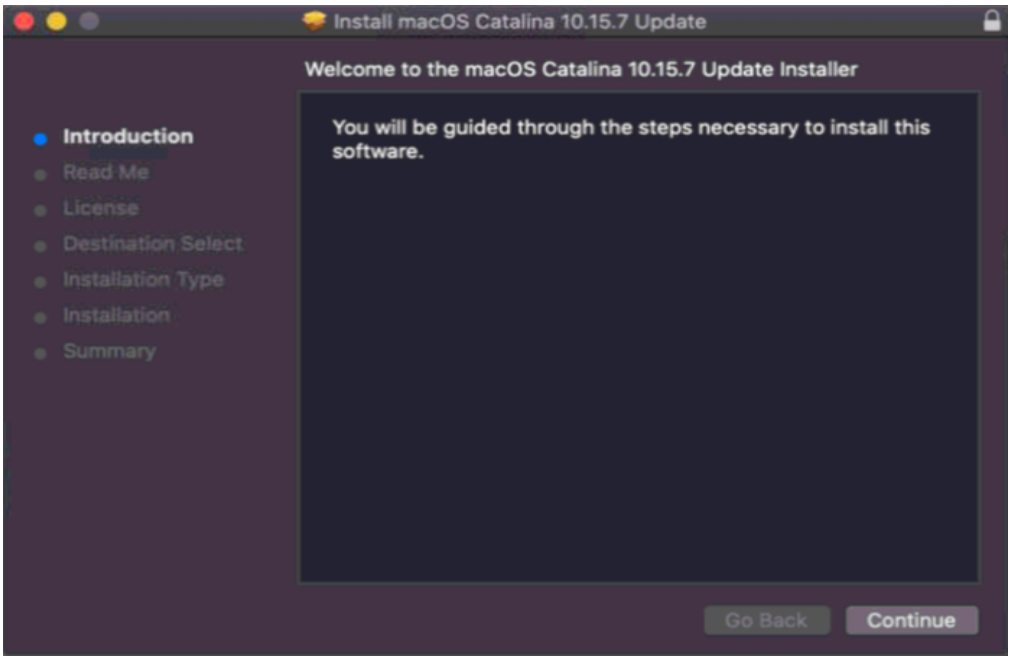
- Update(s) can be downloaded from the website below: https://support.apple.com/downloads according to the user requirement(s).
- Double click on the downloaded update.
- The TOE verifies the integrity of the software update by performing an RSA 2048-bit digital signature verification.
- After the digital signature verification is successful the TOE will install the update.
- If the digital signature verification fails, the TOE will warn the user that the digital signature verification failed and will not install the update. The TOE then terminates the update process.

Note: macOS may occasionally reboot itself during the update process. This behavior is not uncommon. Software Application updates may or may not require the macOS to reboot.

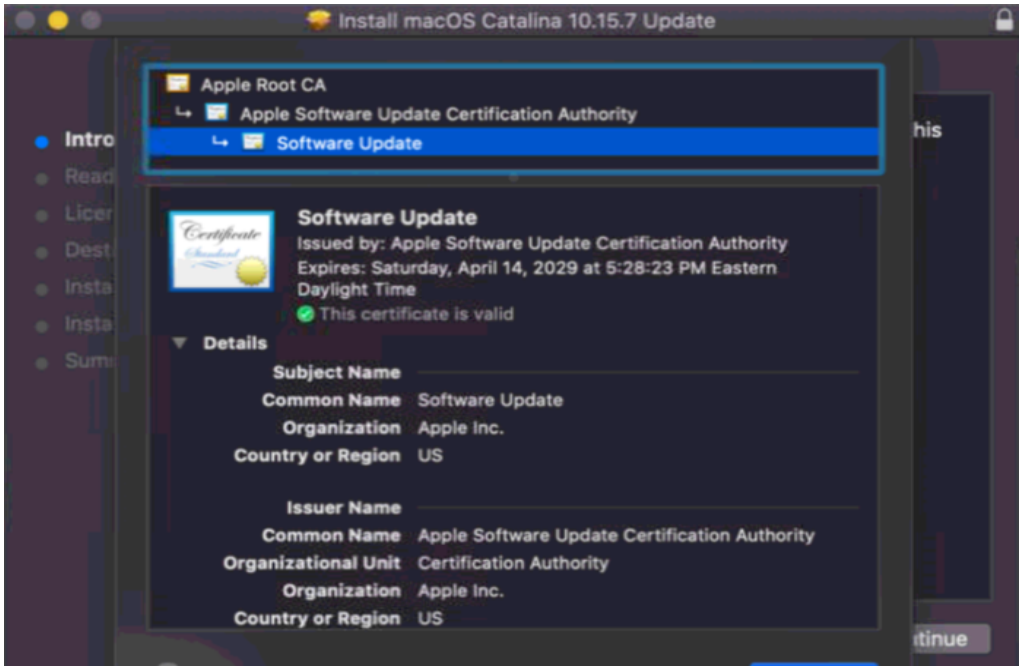
## 4.2 Installing OS updates

- Download the appropriate macOS update(s) from https://support.apple.com/downloads according to the user requirements.
- In this case, "macOSUpd10.15.7.dmg" was downloaded and installed. Before installing the update, the macOS performs a digital signature verification as shown below:


- After successful digital signature verification, the macOS will proceed with the installation.

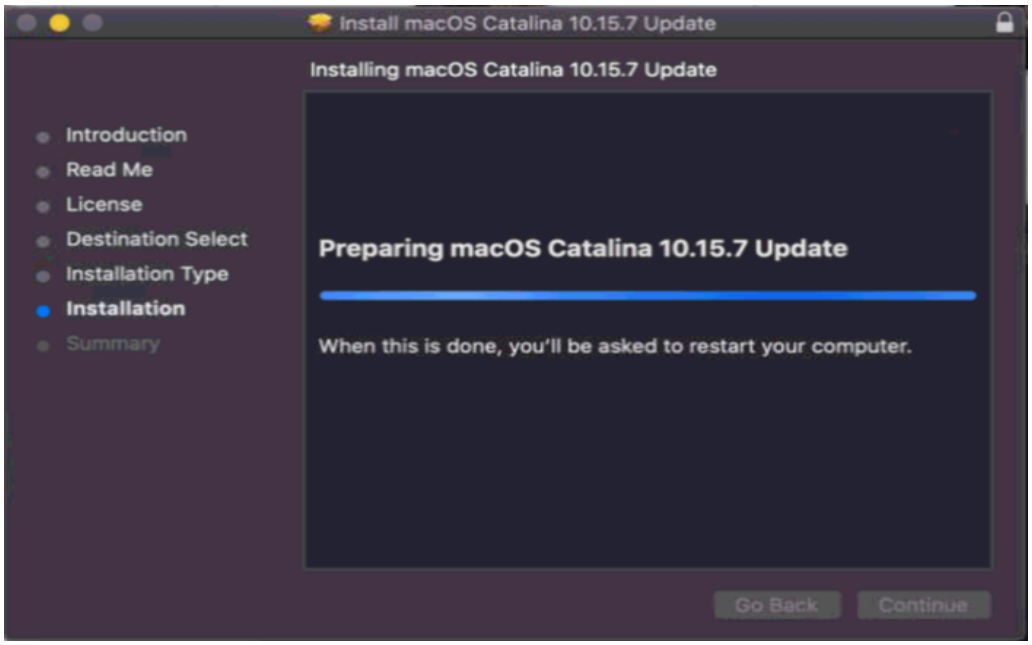



- Additionally, the user can click on the "lock icon" in the upper right-hand corner of the installer window to verify the digital signature as shown below. This approach can be used to verify digital signature on any installer.

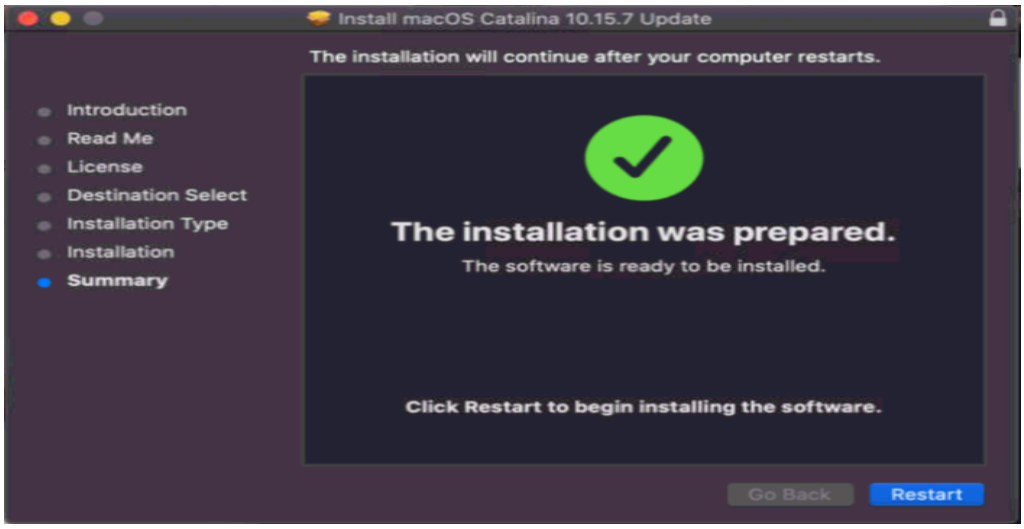



- macOS will prompt the user to install the OS update. If the user does not want to install the update, then the user can simply close the window and the macOS will not be updated.

- The macOS will first prepare the update for installation.




- After the update is prepared for installation, macOS will display the message "The installation was prepared". Click on Restart to start the installation process. macOS will reboot once the update is successfully installed.




- The user can verify the updated version of the macOS (i.e., in this case macOS Catalina 10.15.7) by navigating to "Apple Symbol".
    - "About This Mac" -> "Overview"

# 5 TOE Startup Security Utility

Startup Security Utility is a replacement to the previous Firmware Password Utility. On Mac computers with an Apple T2 security chip, it handles a larger set of security policy settings. The utility is accessible by booting into recovery OS and selecting Startup Security Utility from the Utilities menu. The advantage of putting critical system security policy controls (such as secure boot or System Integrity Protection (SIP) in the recovery OS is that the entire OS is integrity checked. This ensures that any attacker code that has broken into the Mac cannot trivially impersonate the user for purposes of further disabling security policies.

Critical policy changes now require authentication, even in recovery mode. This feature is available only on Mac computers containing the T2 security chip. When the Startup Security Utility is first opened, it prompts the user to enter an administrator password from the primary macOS installation associated with the currently booted macOS Recovery. If no administrator exists, one must be created before the policy can be changed. The T2 security chip requires that the Mac computer is currently booted into macOS Recovery and that an authentication with a Secure Enclave backed credential has occurred before such a policy change can be made. Security policy changes have two implicit requirements. macOS Recovery must:

- Be booted from a storage device directly connected to the T2 security chip, because partitions on other devices do not have Secure Enclave backed credentials bound to the internal storage device.
- Reside on an Apple File System (APFS) based volume because there is support only for storing the Authentication in Recovery credentials sent to the Secure Enclave on the "Pre-boot" APFS volume of a drive. Hierarchical File System (HFS) plus-formatted volumes can't use secure boot.

This policy is only shown in Startup Security Utility on Mac computers with an Apple T2 security chip. Although most use cases should not require changes to the secure boot policy, administrators are ultimately in control of their device's settings, and may choose, depending on their needs, to disable or downgrade the secure boot functionality on their Mac.

Secure boot policy changes made from within this app apply only to the evaluation of the chain of trust being verified on the Intel processor. The option "Secure boot the T2 security chip" is always in effect.

The secure boot policy can be configured to one of three settings: Full Security, Medium Security, and No Security. No Security completely disables secure boot functionality on the Intel processor and allows the user to boot from any supported and allowed boot media. More information can be found here: https://support.apple.com/guide/mac-help/what-is-the-startup-security-utility-on-mac-mchlf5346320/10.15/mac/10.15

## 5.1 Mac startup key combinations:

To use any of these key combinations, press and hold the keys immediately after pressing the power button to turn on your Mac, or after your Mac begins to restart. Keep holding until the

described behavior occurs.

- **Command (⌘)-R:** Start up from the built-in macOS Recovery, system. Or use Option-Command-R or Shift-Option-Command-R to start up from macOS Recovery over the Internet. macOS Recovery installs different versions of macOS, depending on the key combination you use while starting up. If your Mac is using a firmware password, you are prompted to enter the password.
- **Option (⌥) or Alt:** Start up to Startup Manager which allows you to choose other available startup disks or volumes. If your Mac is using a firmware password, you are prompted to enter the password.
- **Option-Command-P-R:** Reset NVRAM or PRAM. If your Mac is using a firmware password, it ignores this key combination or starts up from macOS Recovery.
- **Shift (⇧):** Start up in safe mode. Disabled when using a firmware password.
- **D:** Start up to the Apple Diagnostics utility. Or use Option-D to start up to this utility over the Internet. Disabled when using a firmware password.
- **N:** Start up from a NetBoot server, if your Mac supports network startup volumes. To use the default boot image on the server, hold down Option-N instead. Disabled when using a firmware password.
- **Command-S:** Start up in single-user mode. Disabled in macOS Mojave or later, or when using a firmware password.
- **T:** Start up in target disk mode. Disabled when using a firmware password.
- **Command-V:** Start up in verbose mode. Disabled when using a firmware password.
- **Eject** (⏏) or **F12** or **mouse button** or **trackpad button:** Eject removable media, such as an optical disc. Disabled when using a firmware password.

#### 5.1.1.1 If a Key Combination Does Not Work

- If a key combination does not work at startup, one of these solutions might help:
- Be sure to press and hold all keys in the combination together, not one at a time.
- Shut down your Mac. Then press the power button to turn on your Mac. Then press and hold the keys as your Mac starts up.
- Wait a few seconds before pressing the keys, to give your Mac more time to recognize the keyboard as it starts up. Some keyboards have a light that flashes briefly at startup, indicating that the keyboard is recognized and ready for use.
- If you are using a wireless keyboard, plug it into your Mac, if possible. Or use your built-in keyboard or a wired keyboard. If you're using a keyboard made for a PC, such as a keyboard with a Windows logo, try a keyboard made for Mac.
- If you're using Boot Camp to start up from Microsoft Windows, set Startup Disk to start up from macOS instead. Then shut down or restart and try again.

Note: Remember that some key combinations are disabled when your Mac is using a firmware password.

# 6 TOE Cryptographic Operation Hashing, Encryption and Decryption

For disk encryption, the TOE uses AES data encryption and AES decryption using AES in XTS mode that meet the following: AES as specified in ISO/IEC18033-3 and XTS as specified in IEEE 1619. The key size supported is 256-bits. The TOE supports key encryption and decryption using AES algorithm as specified in ISO/IEC 18033-3. The modes supported are CBC, as specified in ISO/IEC 10116 and GCM, as specified in ISO/IEC 19772. The key size supported is 256 bits.

The TOE performs deterministic random bit generation services according to NIST SP 800-90A using CTR_DRBG (AES).

The TOE performs cryptographic message authentication using HMAC-SHA-256 and the TOE supports the following hashing algorithms: SHA-256.

Note: The TOE supports AES data encryption and AES decryption by default and no configuration is required.

# 7 Key Destruction

The TOE erases cryptographic keys and key material from volatile memory by performing a single overwrite of zeroes and/or by removal of power to the memory. The TOE erases cryptographic keys and key material from non-volatile memory by performing a single overwrite of zeroes. The erase operation is performed by the SEP and is not configurable by a user. There are no circumstances that do not conform to the key destruction requirement (e.g. sudden unexpected power loss).

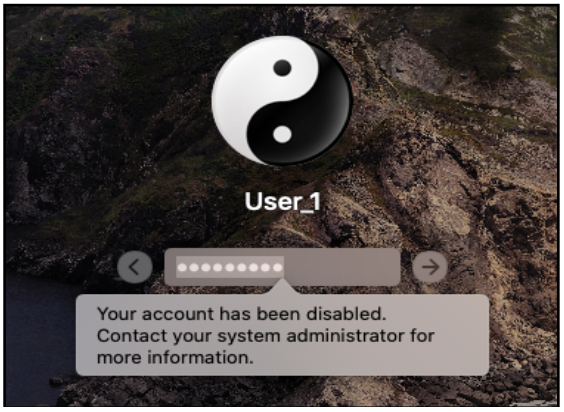
# 8 Validation of Cryptographic Elements

The Unlock key is defined as the Border Encryption Value. It is derived from the Hardware Unique ID or UID and the user passcode. macOS requires the validation of the BEV prior to allowing access to TSF data after exiting a compliant power saving state and it will block validation after 10 consecutive failed validation attempts.

The macOS can be configured for password validation as below:

```
cert@mac-mini-i5-8500B ~ % sudo pwpolicy -u User_1 -setpolicy "MaxFailedLoginAttempts=10"
Password:
Setting policy for User_1
cert@mac-mini-i5-8500B ~ %
```

After ten consecutive failed authentication attempts, macOS blocks the validation attempts by disabling the user account.



# 9 Enable Full Disk Encryption

Starting with macOS X 10.13 and a Mac computer with an Apple T2 Security Chip, Macs use built-in, always-on hardware encryption capability to secure all data at rest. On Mac computers with the Apple T2 Security Chip, internal volume encryption automatically leverages the AES-XTS Encryption Engine, and DMA hardware security capabilities of the chip. After a user enables FileVault on a Mac, their credentials are required to cryptographically unlock volumes during the boot process.

Without valid login credentials, the internal APFS volume (in macOS 10.15, this includes the System and Data volumes) remains encrypted and is protected from unauthorized access even if the physical storage device is removed and connected to another computer. Internal volume encryption on a Mac with the T2 security chip is implemented by constructing and managing a hierarchy of keys and builds on the hardware encryption technologies built into the chip. This hierarchy of keys is designed to simultaneously achieve four goals.

This hierarchy of keys is designed to simultaneously achieve four goals:

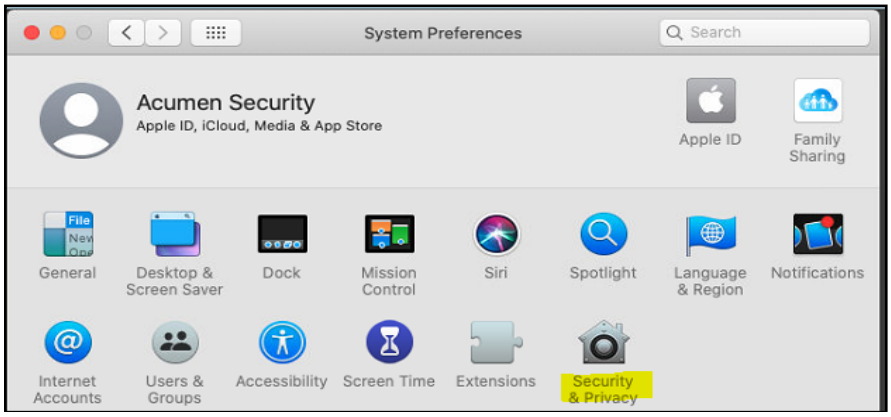
- Require the user's password for decryption.
- Protect the system from a brute-force attack directly against storage media removed from Mac.
- Provide a swift and secure method for wiping content via deletion of necessary cryptographic material.
- Enable users to change their password (and in turn the cryptographic keys used to protect their files) without requiring re-encryption of the entire volume.

On Mac computers with the T2 security chip, all FileVault 2 key handling occurs in the Secure Enclave; encryption keys are never exposed to the Intel CPU. All APFS volumes are created with a volume key by default. Volume and metadata contents are encrypted with this volume key, which is wrapped with the class key. The class key is protected by a combination of the user's password and the hardware UID when FileVault 2 is turned on. This protection is the default on Mac computers with the T2 security chip.

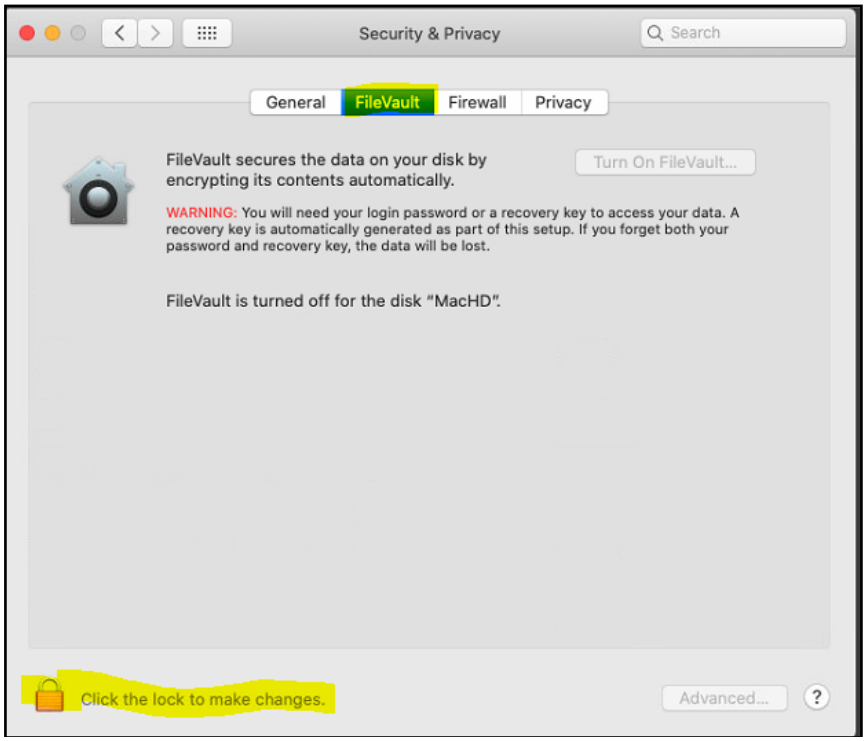
Note: Encryption of removable storage devices does not utilize the security capabilities of the T2 security chip, and its encryption is performed in the same manner as Mac computers without the T2 security chip.

The user can enable/disable FileVault as shown below:

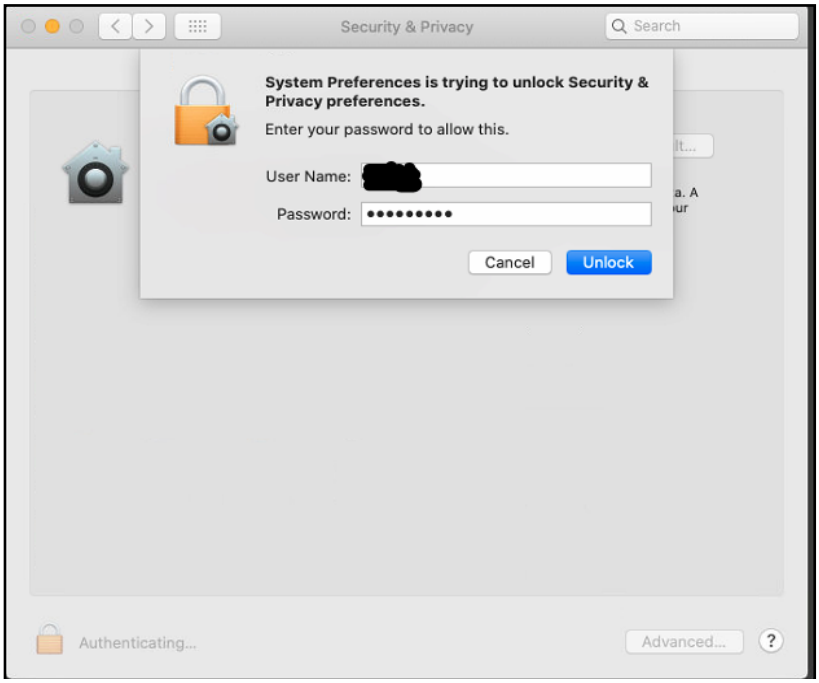
- Open System Preferences and click on Security & Privacy



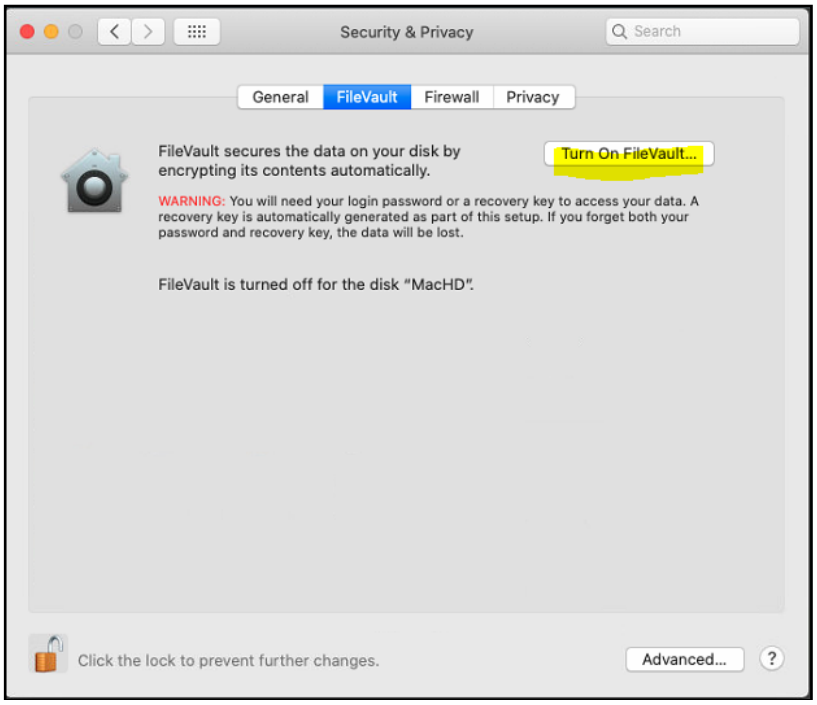

- Click on FileVault and then click the lock to make changes and enter Administrator credentials.



- Enter Administrator credentials to unlock.




- To enable FileVault, click on Turn On FileVault.



- To disable FileVault, click on Turn Off FileVault.

# 10 Authorization Factors

The TOE supports password as the authorization factor. Passwords of up to 256 characters are supported and can be comprised of any combination of upper-case characters, lower case characters, numbers, and any other 8-bit special character.

The TOE performs password based key derivation function in accordance with NIST SP 800-132. It leverages the HMAC-SHA-256 algorithm with 50,000 iterations and the UID as the “purpose” value as defined in Appendix A.2.1 of SP 800-132.

The TOE supports the following power saving state: G2(S5)- soft off, also recognized as Shutdown. The TOE can enter G2(S5)-soft off power saving state by the user selecting the Shutdown option on the TOE host device. To resume from a compliant power state, the user must re-authenticate to the TOE by using a correct username and password.

# 11 Password Policy

The TOE supports a password length of minimum 8 characters including letters (upper- and lower-case), numbers, and special symbols. To apply a password policy the policy command uses the setaccountpolicies subcommand. This subcommand sets (replaces) the account polices for the specified user. If no user is specified, it sets the global account policies. This subcommand takes one argument: the path of the XML file containing the policies. To import a global policy, it must be saved in a file (e.g. policy_file) and imported by typing the following command in Terminal:

**sudo pwpolicy -setaccountpolicies [path to policy_file]**

The following is an example of the text for a password policy that will configure the minimum password length to 8, minimum special characters to 2, minimum numeric characters to 2, minimum upper and lower case characters to 2 (each), and sets the timeout between failed password attempts to 60 seconds and the maximum limit of authentication attempts to 3 until lockout:

```
<?xml version=“1.0” encoding=“UTF-8”?>
<plist version =“1.0”>
<dict>
    <key>policyCategoryPasswordContent</key>
    <array>
            <dict>
            <key>policyContent</key>
                <string>policyAttributePassword
matches '.{8,}+'</string>
            <key>policyIdentifier</key>
                <string>Has at least 8 characters</string>
            <key>policyParameters</key>
                <dict>
                <key>minimumLength</key>
                    <integer>8</integer>
                </dict>
            </dict>
            <dict>
            <key>policyContent</key>
                <string>policyAttributePassword matches '(.*[^a-zA-
Z0- 9].*){2,}+'</string>
            <key>policyIdentifier</key>
                <string>Has at least 2
special character</string>
            <key>policyParameters</key>
```

```
                <dict>
                <key>minimumSymbols</key>
                        <integer>2</integer>
                </dict>
        </dict>
        <dict>
        <key>policyContent</key>
                <string>policyAttributePassword matches
'(.*[0-9].*){2,}+'</string>
        <key>policyIdentifier</key>
                <string>Has at least 2 numbers</string>
        <key>policyParameters</key>
                <dict>
                <key>minimumNumericCharacters</key>
                        <integer>2</integer>
                </dict>
        </dict>
        <dict>
        <key>policyContent</key>
                <string>policyAttributePassword matches
'(.*[A-Z].*){2,}+'</string>
        <key>policyIdentifier</key>
                <string>Has at least 2 upper
case letters</string>
        <key>policyParameters</key>
                <dict>
                <key>minimumAlphaCharacters</key>
                        <integer>2</integer>
                </dict>
        </dict>
        <dict>
        <key>policyContent</key>
                <string>policyAttributePassword matches
'(.*[a-z].*){2,}+'</string>
        <key>policyIdentifier</key>
                <string>Has at least 2 lower
case letters</string>
        <key>policyParameters</key>
                <dict>
                <key>minimumAlphaCharactersLowerCase</key>
                        <integer>2</integer>
                </dict>
        </dict>
```

```
                <dict>
                <key>policyContent</key>
                        <string>(policyAttributeFailedAuthentications
    &lt; policyAttributeMaximumFailedAuthentications) OR
    (policyAttributeCurrentTime &gt
    (policyAttributeLastFailedAuthenticationTime +
    autoEnableInSeconds))</string>
                <key>policyIdentifier</key>
                        <string>Authentication Lockout</string>
                <key>policyParameters</key>
                        <dict>
                        <key>autoEnableInSeconds</key>
                                <integer>60</integer>
        <key>policyAttributeMaximumFailedAuthentications</key>
                                <integer>3</integer>
                        </dict>
                </dict>
    </array>
    </dict>
</plist>
```

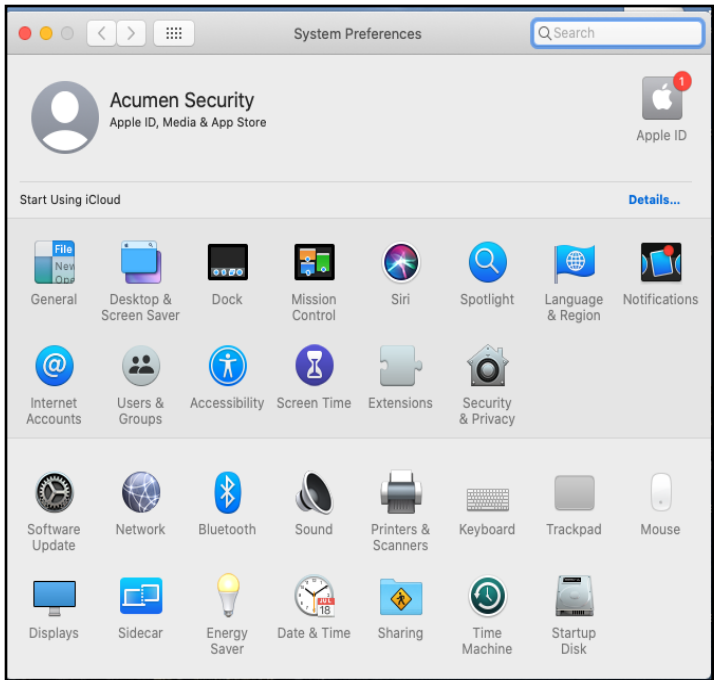
Any of the integer values in the above text can be modified to update the policy to the desired values. The number of failed authentication attempts is configurable within the range of 1-50 attempts. The following steps are then performed to import and apply the policies:

1. The XML text is saved in a text file. For this example, the file is titled “policy_file” and is saved to the Desktop of the Mac.
2. Open Terminal.
3. Enter the following command in Terminal: sudo pwpolicy -setaccountpolicies ~/Desktop/policy_file.
4. Enter the administrator password when prompted.
5. When the password is entered correctly you will see “Setting global account policies”. This indicates that the policy has been accepted.

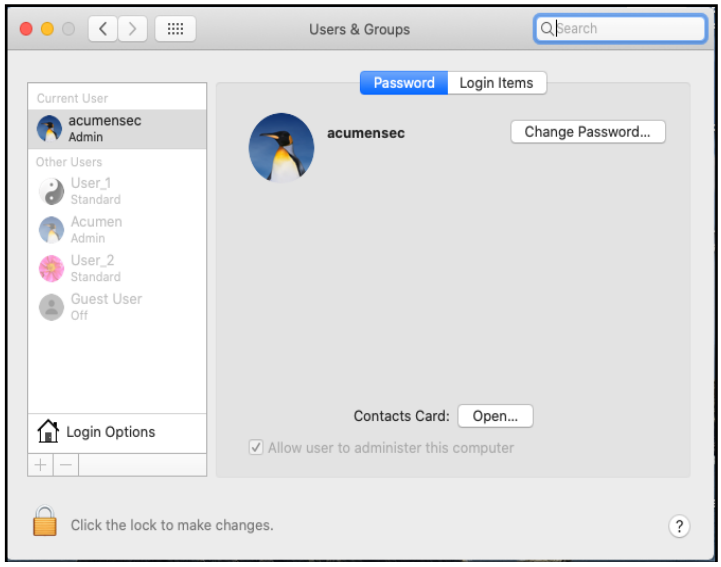
# 12 Creating User Accounts

The process of creating/adding a new user is shown below:

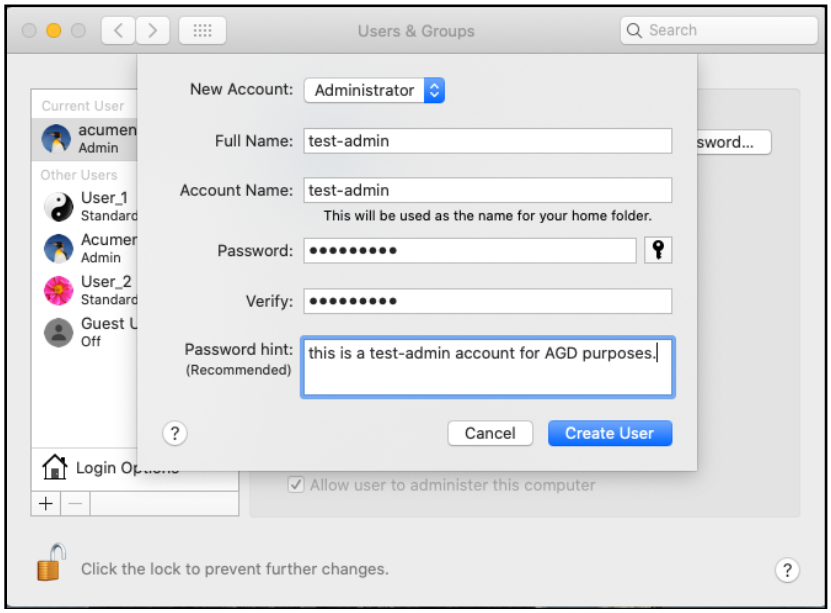
- Start System Preferences application:



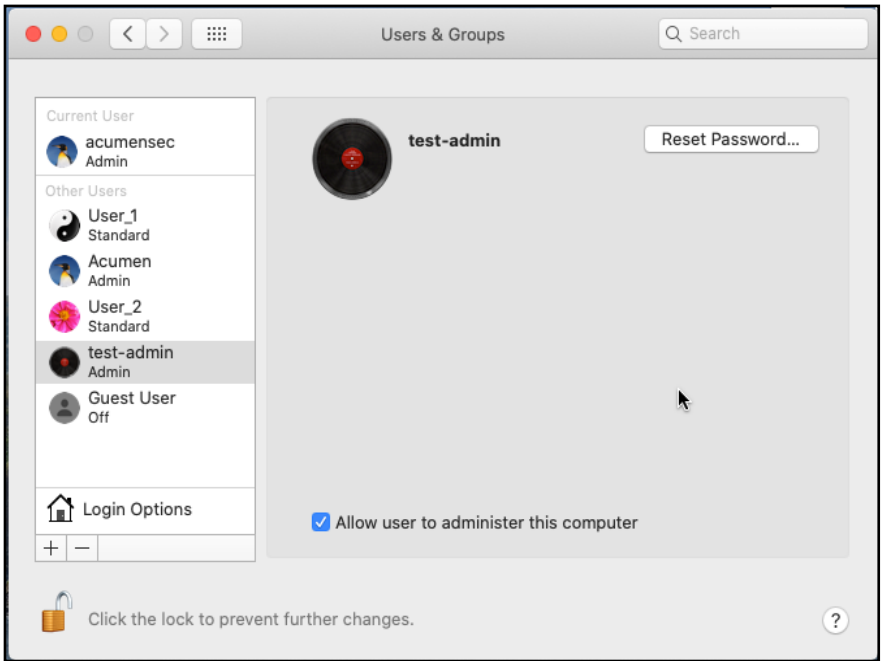

- Select Users & Groups:



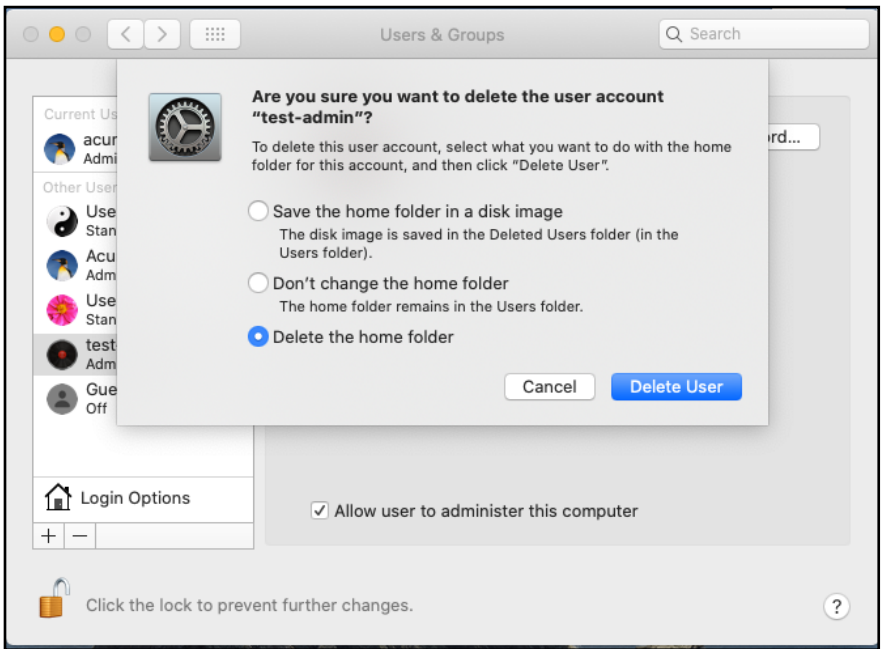
- Click on the lock to make changes and enter your current login password.
- Then click on + symbol and add a new user as shown below:



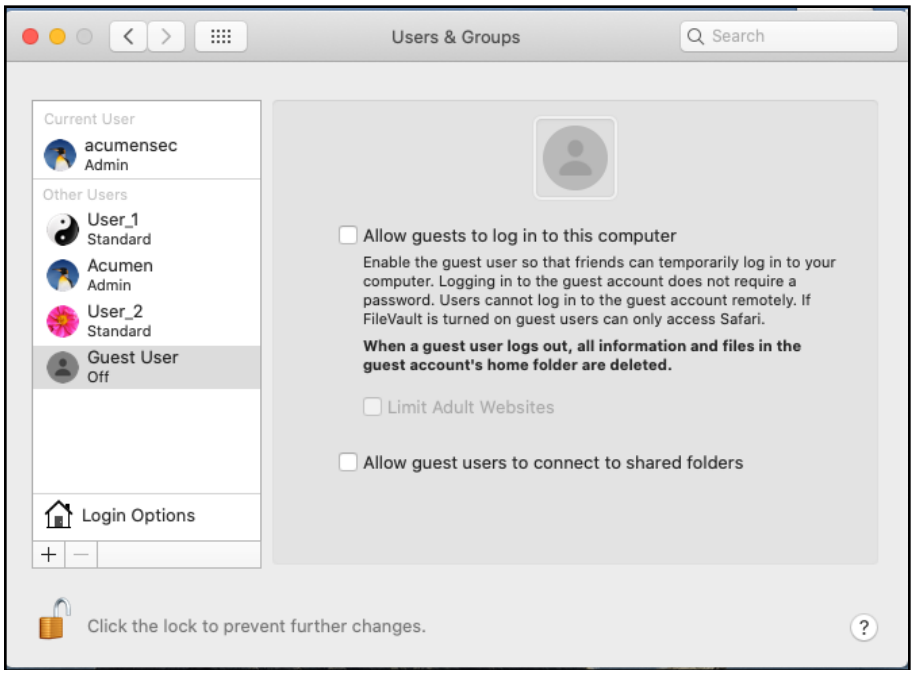

- Click on Create User.
- After clicking on Create, a new user test-admin is added to the TOE with Administrator privileges.



- To delete a user, click on – symbol and click on Delete.



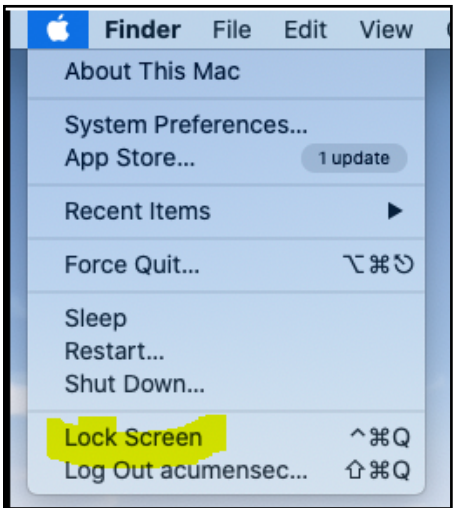

- After deleting the user, the TOE looks like below:



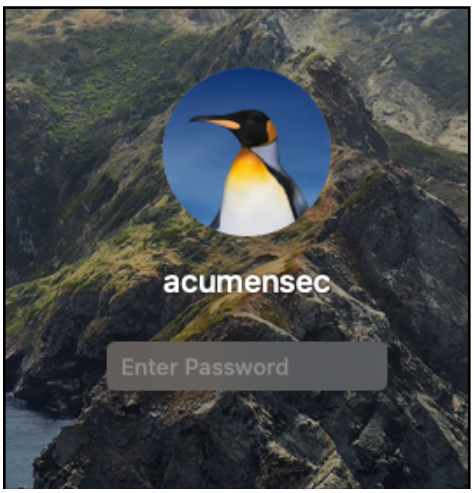
## 12.1 Locking an Account

The TOE allows the user to lock a user account as shown below:

- Click on Apple symbol and then click on Lock Screen.




- The TOE will now lock the screen for the currently signed in User.
- After locking, the TOE screen looks like below:

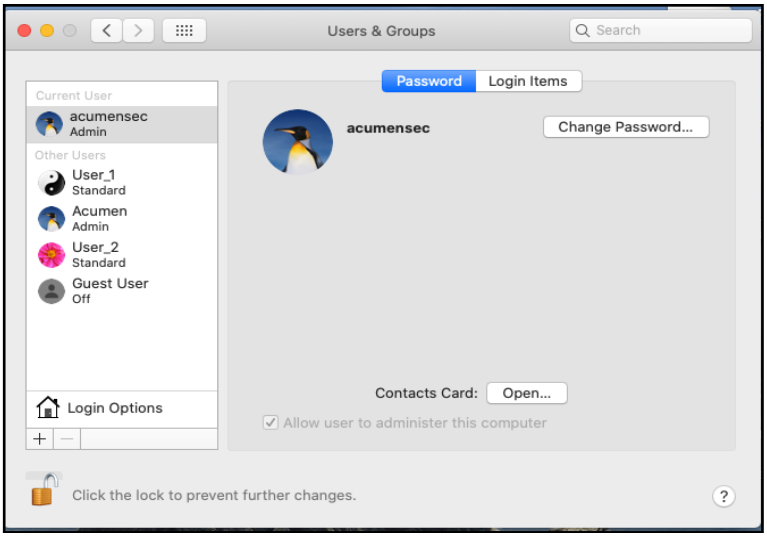


## 12.2 Changing User Passwords

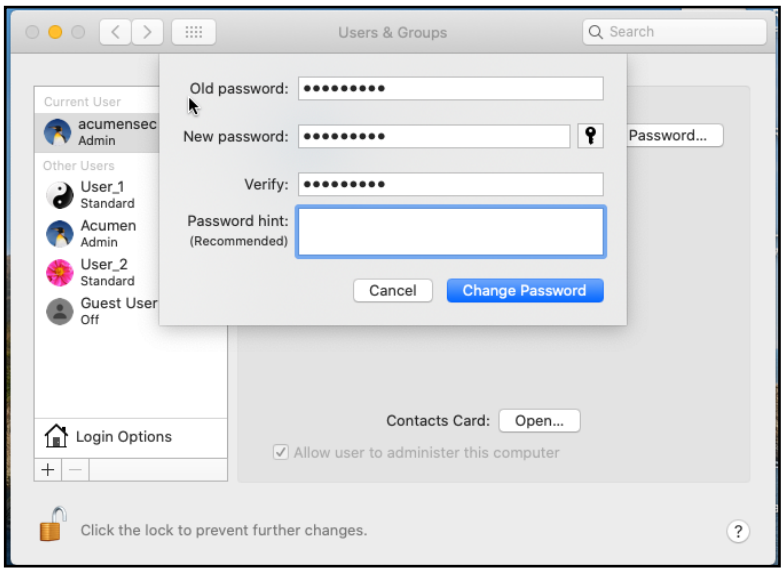
The TOE allows the User to change their existing password.

### 12.2.1 Change user password after authenticating to macOS

- Open System Preferences and click on Users & Groups.



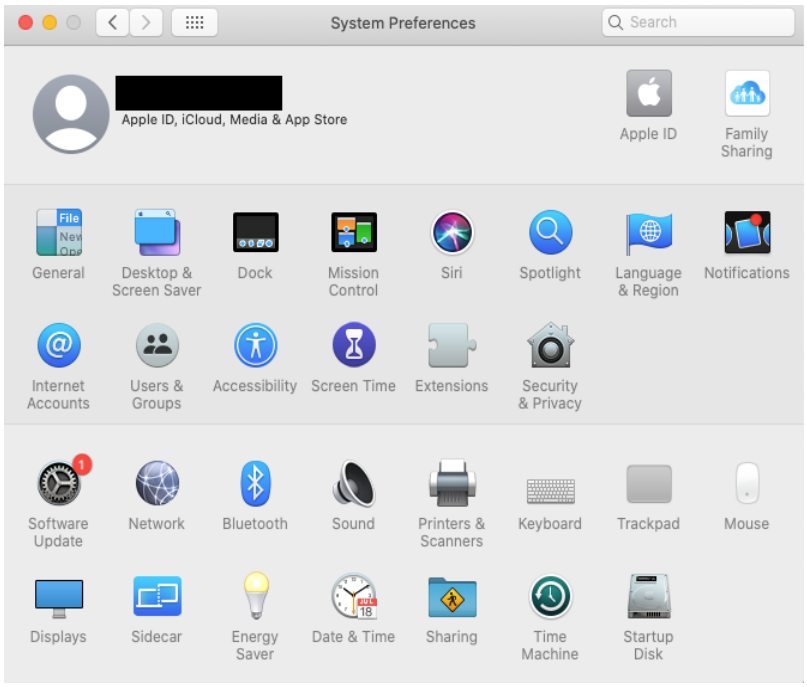

- Click on Change Password and the new password will be enforced by the TOE.



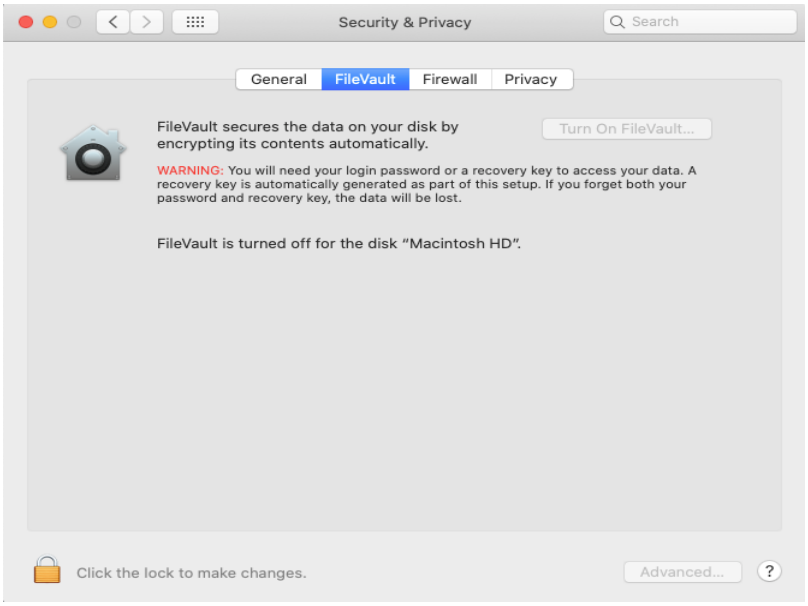
### 12.2.2 Change user password using a recovery key

A recovery key is a randomly generated 28-character code that the user can use to reset their password. The recovery key is generated during the FileVault enabling process and manually saved by the user. The recovery key is never stored in the TOE. If FileVault is disabled and re-enabled, a new recovery key is generated. The steps below explain how to set a recovery key and how to reset the user password using the recovery key.

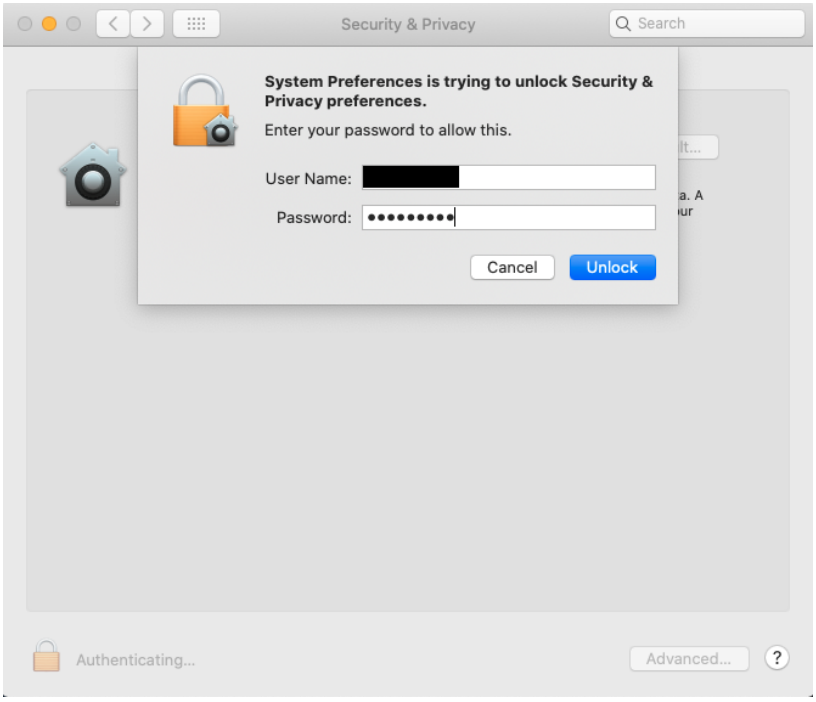
- Open System Preferences



- Open Security & Privacy, click on FileVault and then click on “Click the lock to make changes”

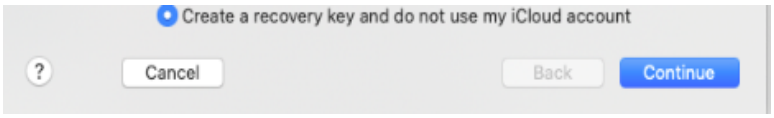



- Enter credentials. Note: User Name is intentionally blurred below.



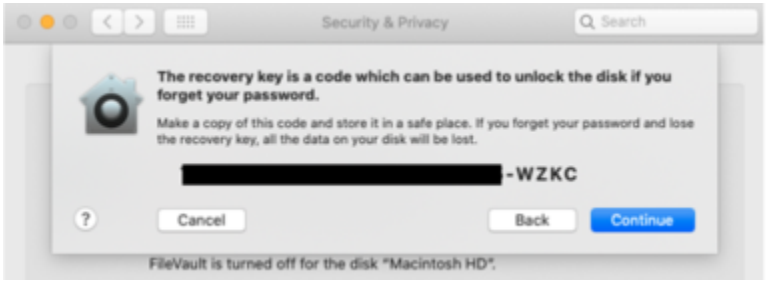
- After unlocking, click on “Turn On FileVault”


- Click on Continue to create a recovery key

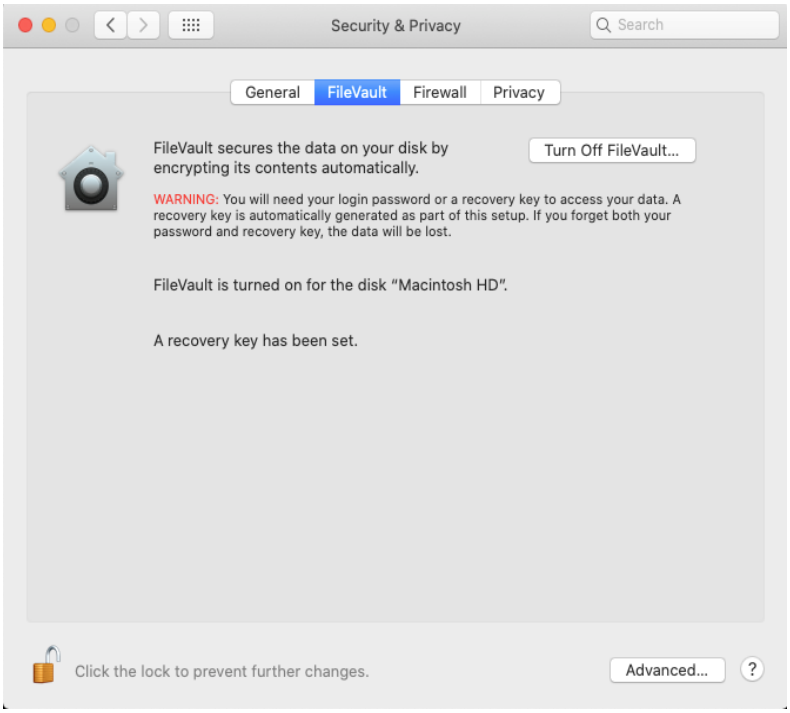



- A recovery key will be displayed on the screen. Click Continue.

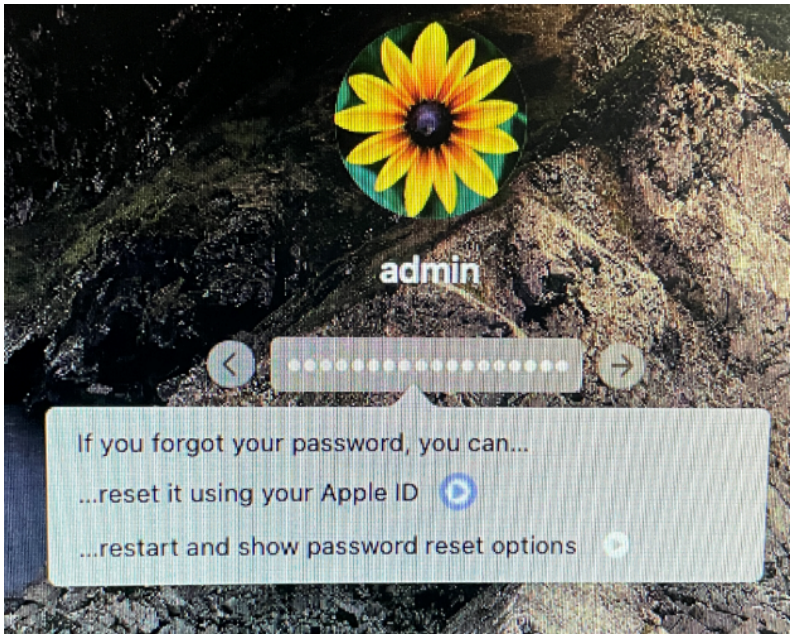
Note: It is recommended to manually make a note of the recovery key and store it in a safe place. Some characters of the recovery key are intentionally blurred below.



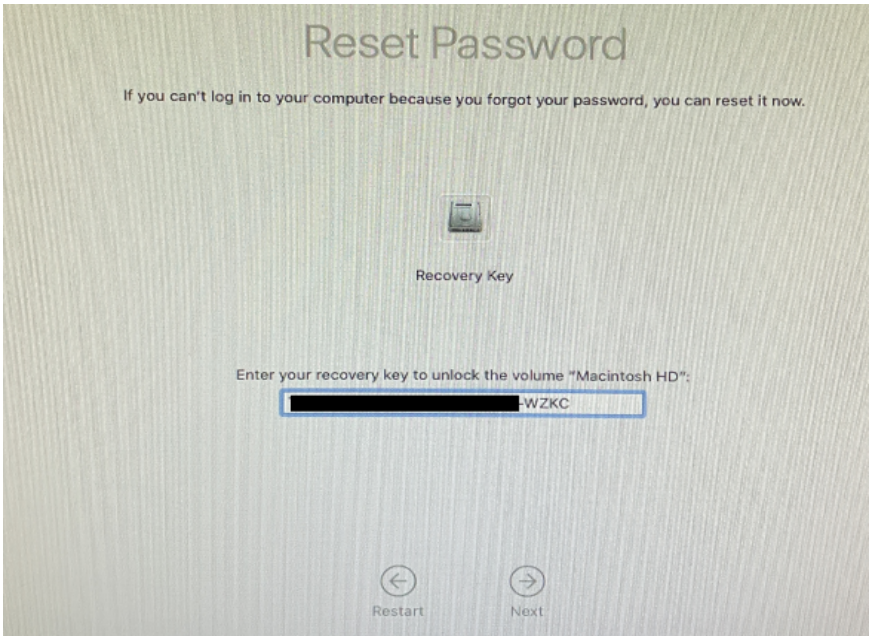
- Verify the recovery key is set



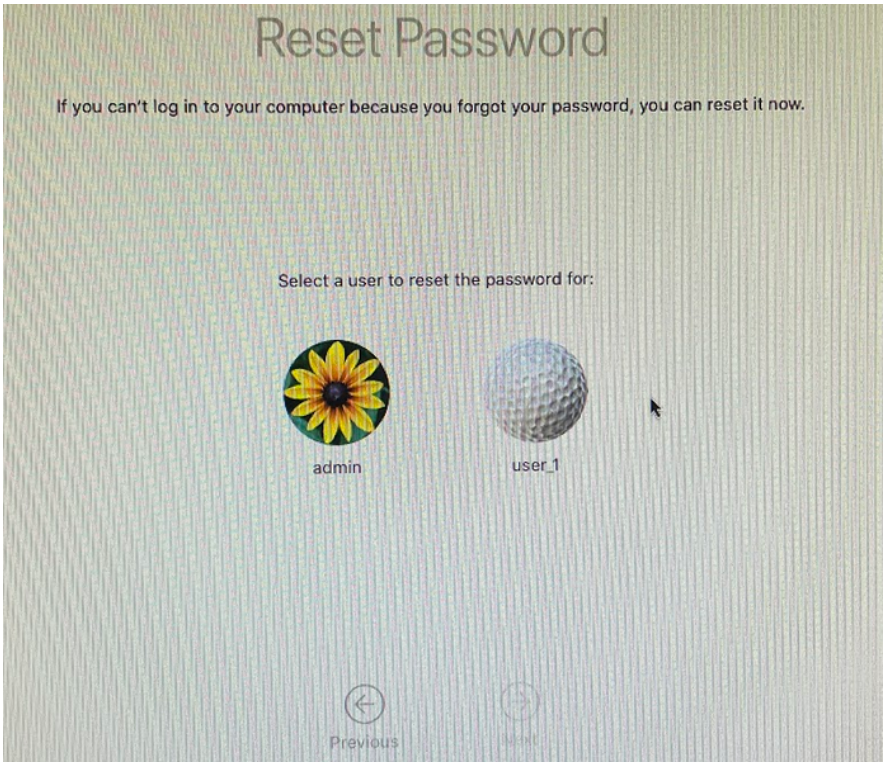

- Enter incorrect user password for multiple times. Then click on "....restart and show password reset options".



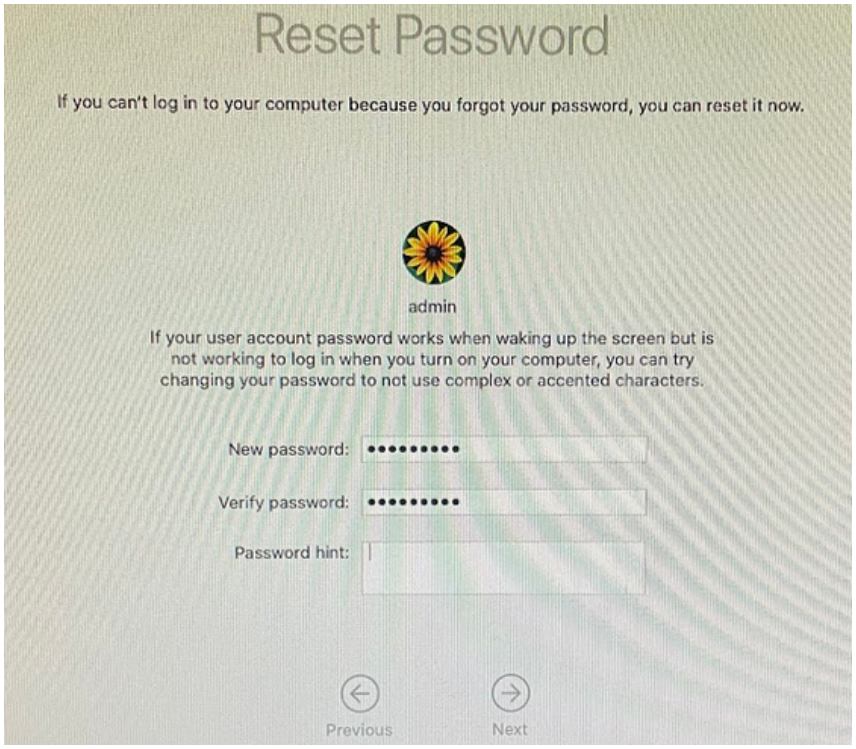
- To reset password, enter the recovery key. Then click Next



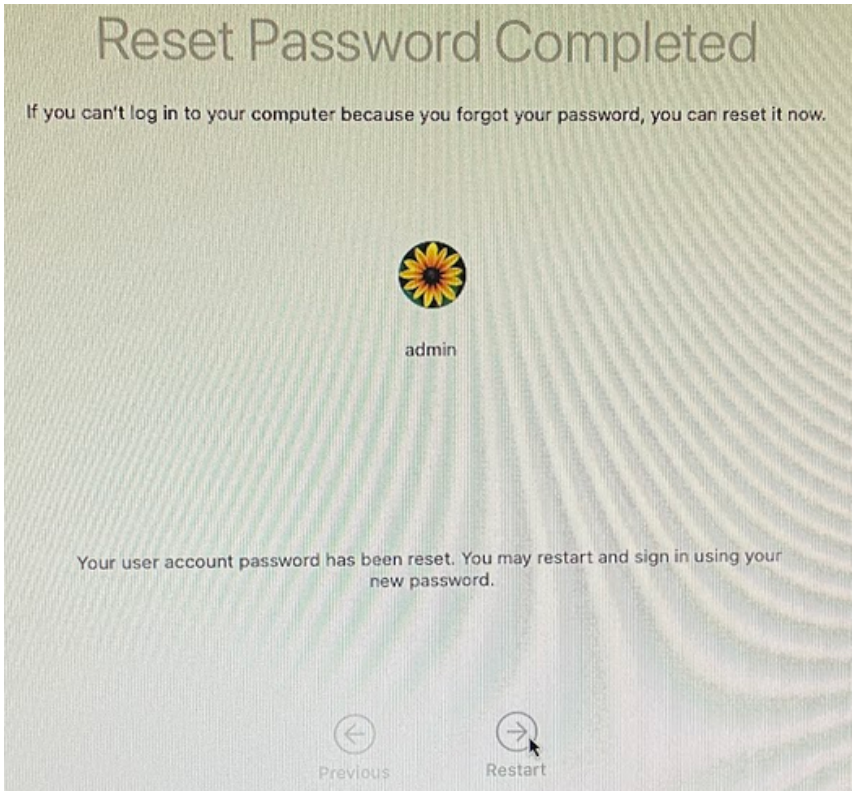

- Select user “admin” and click Next



- Enter new password and click Next




- Click restart



# 13 Bibliography

The table below provides a list of the website links that are included in this document:

| # | Title | Website Link |
|---|---|---|
| 1 | Apple Platform Security guide. | https://support.apple.com/en-ca/guide/security/sec59b0b31ff/web |
| 2 | macOS and Software Application updates. | https://support.apple.com/downloads/macos |
| 3 | Apple Platform Security: macOS Software/Firmware Integrity Tests. | https://support.apple.com/et-ee/guide/security/sec5d0fab7c6/1/web/1 |
| 4 | Disk Utility User Guide. | https://support.apple.com/guide/disk-utility/welcome/mac |
| 5 | macOS User Guide. | https://support.apple.com/guide/mac-help/reinstall-macos-mchlp1599/mac |
| 6 | macOS Startup Security Utility. | https://support.apple.com/lt-lt/guide/mac-help/mchlf5346320/10.15/mac/10.15 |
| 7 | Mac Startup Key Combinations. | Turn on your Mac: https://support.apple.com/kb/HT201150,<br>macOS Recovery: https://support.apple.com/kb/HT201314,<br>macOS Recovery installs different versions of macOS: https://support.apple.com/kb/HT204904,<br>Firmware Password: https://support.apple.com/kb/HT204455,<br>Startup Manager: https://support.apple.com/kb/HT202796,<br>Reset NVRAM: https://support.apple.com/HT204063,<br>Safe Mode: https://support.apple.com/HT201262,<br>Apple Diagnostics: https://support.apple.com/HT202731,<br>If your Mac supports network startup volumes: https://support.apple.com/kb/HT202770,<br>Target disk mode: https://support.apple.com/HT201462,<br>Verbose mode: https://support.apple.com/HT201573<br>Power Button: https://support.apple.com/kb/HT201150,<br>Startup Disk preferences: https://support.apple.com/kb/HT202796. |

| | | |
|---|---|---|
| 9 | NIAP CPP_FDE_AA_V2.0E | https://www.niap-ccevs.org/MMO/PP/CPP_FDE_AA_V2.0E.pdf |
| 10 | NIAP CPP_FDE_EE_V2.0E | https://www.niap-ccevs.org/MMO/PP/CPP_FDE_EE_V2.0E.pdf |

**END OF DOCUMENT**