

Apple Inc.



Apple macOS 13 Ventura: FileVault Common Criteria Configuration Guide

Version 1.1

November 28, 2023

NIAP VID 11348

Prepared by:

atsec information security corp

9130 Jollyville Road, Suite 260

Austin, TX 78759

www.atsec.com

Revision History

Version	Date	Changes
1.0	2023-11-03	First version
1.1	2023-11-28	Address 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.

Contents

List of Figures	3
1 Introduction	4
1.1 Target of Evaluation	4
1.2 Document Purpose and Scope	8
1.3 Excluded Functionality	8
1.4 Assumptions and Warnings	9
1.5 How to Invoke Common macOS Features	10
2 Installation, and Update, and Recovery	11
2.1 Installation	11
2.2 Update	12
2.2.1 Rapid Security Response (RSR)	13
2.3 Recovery	13
3 Configuration and Management	15
3.1 Enable Encryption	15
3.2 Sleep State	15
3.3 User Accounts	16
3.3.1 Add Users	16
3.3.2 Delete Users	16
3.3.3 Change Password	17
3.3.4 Changing/Erasing the Data Encryption Key	17
3.4 Firewall	17
4 Usage	19
5 Acronyms	20

List of Figures

Figure 1 – Apple silicon TOE Boundaries	4
Figure 2 – T2 TOE Boundaries	5
Figure 3 – macOS Version	11
Figure 4 – Software Updates	13
Figure 5 – FileVault	15
Figure 6 – Firewall	18

1 Introduction

This guide provides instructions to configure and operate Apple macOS 13 Ventura: FileVault in the Common Criteria evaluated configuration.

1.1 Target of Evaluation

The TOE is the Apple macOS 13 Ventura: FileVault full drive encryption solution. The TOE is both an authorization acquisition and encryption engine product. The TOE is the full drive encryption portion of the operating system which leverages specialized hardware in the Apple silicon and Apple T2 processors to perform the full drive encryption. The operating system core is a POSIX compliant operating system built on top of the XNU kernel with standard Unix facilities available from the command line interface.

Note: General Purpose Operating System functionality is not part of this evaluation.

Table 1 – TOE Identification

Category	Identifier
VID	11348
TOE Identifier	Apple macOS 13 Ventura: FileVault
TOE Version	13.2.1
TOE Developer	Apple Inc.
Keywords	Full Drive Encryption, Encryption Engine, Authorization Acquisition

The following diagrams depict the TOE boundaries on Apple silicon and Apple T2 based systems. The AA boundary is identified by a dashed blue line (-----), and the EE boundary is depicted by a dashed orange line (-----).

Figure 1 – Apple silicon TOE Boundaries

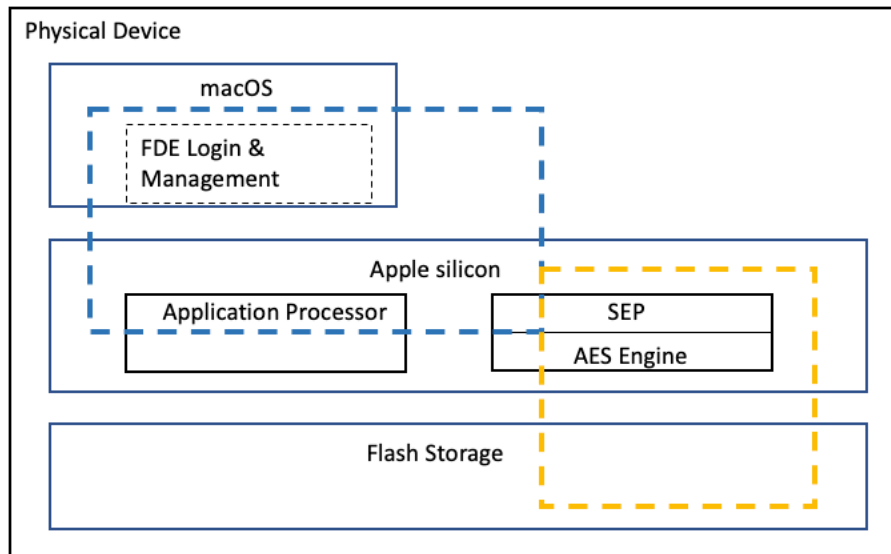
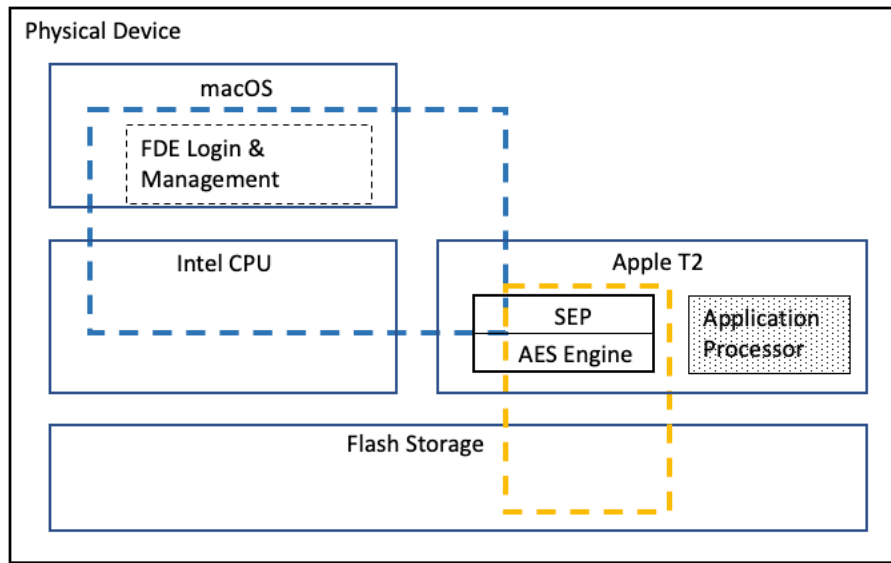


Figure 2 – T2 TOE Boundaries



The TOE is comprised of both software and hardware. The TOE hardware consists of the Apple silicon SoC or Apple T2 Security Chip which are custom silicon for Mac computers. It contains the SEP and AES Engine which provide the foundation for encrypted storage capabilities. The SEP provides hardware key management, and the AES Engine is a dedicated implementation for encrypting and decrypting data. macOS is software that contains the FileVault full disk encryption management program.

The TOE stores user data, OS data, and encrypted keys on the Flash Storage, but the Flash Storage does not implement any security functionality.

All processing for cryptography related to full drive encryption (FDE) functionality is performed using the SEP or AES Engine rather than the Apple silicon Application Processor or Intel CPU. Apple silicon-based systems use AES-XTS-256 for data encryption, and Apple T2-based systems use AES-XTS-128 for data encryption. No configuration of cryptographic engines, algorithms, or key sizes is necessary or available. The use of custom silicon ensures the key destruction requirements are always met and are not delayed by different hardware layers.

The TOE is integrated into Mac hardware, so the following devices constitute the physical boundary of the TOE.

Table 2 – Hardware Platforms

Marketing Name	Model #	Model Identifier	SoC/Processor	microArch	Security Chip
2023					
MacBook Pro (16-inch, 2023)	A2780	Mac14,6	M2 Max	ARMv8.6-A	SEP v2.0
		Mac14,10	M2 Pro	ARMv8.6-A	SEP v2.0

Marketing Name	Model #	Model Identifier	SoC/Processor	microArch	Security Chip
MacBook Pro (14-inch, 2023)	A2779	Mac14,5	M2 Max	ARMv8.6-A	SEP v2.0
		Mac14,9	M2 Pro	ARMv8.6-A	SEP v2.0
Mac mini (M2 Pro, 2023)	A2816	Mac14,12	M2 Pro	ARMv8.6-A	SEP v2.0
Mac mini (M2, 2023)	A2686	Mac14,3	M2	ARMv8.6-A	SEP v2.0
2022					
MacBook Pro (13-inch, M2, 2022)	A2338	Mac14,7	M2	ARMv8.6-A	SEP v2.0
MacBook Air (M2, 2022)	A2861	Mac14,2	M2	ARMv8.6-A	SEP v2.0
Mac Studio	A2615	Mac13,2	M1 Ultra	ARMv8.5-A	SEP v2.0
	A2615	Mac13,1	M1 Max	ARMv8.5-A	SEP v2.0
2021					
MacBook Pro (16-inch, 2021)	A2485	MacBookPro18,2	M1 Max	ARMv8.5-A	SEP v2.0
		MacBookPro18,1	M1 Pro	ARMv8.5-A	SEP v2.0
MacBook Pro (14-inch, 2021)	A2442	MacBookPro18,4	M1 Max	ARMv8.5-A	SEP v2.0
		MacBookPro18,3	M1 Pro	ARMv8.5-A	SEP v2.0
iMac (24-inch, M1, 2021)	A2438	iMac21,1	M1	ARMv8.5-A	SEP v2.0
	A2439	iMac21,2	M1	ARMv8.5-A	SEP v2.0
2020					
Mac mini (M1, 2020)	A2348	Macmini9,1	M1	ARMv8.5-A	SEP v2.0
MacBook Air (M1, 2020)	A2337	MacBookAir10,1	M1	ARMv8.5-A	SEP v2.0
MacBook Pro (13-inch, M1, 2020)	A2338	MacBookPro17,1	M1	ARMv8.5-A	SEP v2.0

Marketing Name	Model #	Model Identifier	SoC/Processor	microArch	Security Chip
MacBook Air (Retina, 13-inch, 2020)	A2179	MacBookAir9,1	Core i5-1030NG7 Core i7-1060NG7	Ice Lake	T2
MacBook Pro (13-inch, 2020, Four Thunderbolt 3 ports)	A2251	MacBookPro16,2	Core i5-1038NG7 Core i7-1068NG7	Ice Lake	T2
MacBook Pro (13-inch, 2020, Two Thunderbolt 3 ports)	A2289	MacBookPro16,3	Core i5-8257U Core i7-8557U	Coffee Lake	T2
iMac (Retina 5K, 27-inch, 2020)	A2115	iMac20,1 iMac20,2	Core i5-10500 Core i5-10600 Core i7-10700K Core i9-10910	Comet Lake	T2
2019					
MacBook Air (Retina, 13-inch, 2019)	A1932	MacBookAir8,2	Core i5-8210Y	Amber Lake	T2
MacBook Pro (13-inch, 2019, Four Thunderbolt 3 ports)	A1989	MacBookPro15,2	Core i5-8279U Core i7-8569U	Coffee Lake	T2
MacBook Pro (13-inch, 2019, Two Thunderbolt 3 ports)	A2159	MacBookPro15,4	Core i5-8257U Core i7-8557U	Coffee Lake	T2
MacBook Pro (15-inch, 2019)	A1990	MacBookPro15,1 MacBookPro15,3	Core i7-9750H Core i9-9880H Core i9-9980HK	Coffee Lake	T2
MacBook Pro (16-inch, 2019)	A2141	MacBookPro16,1 MacBookPro16,4	Core i7-9750H Core i9-9880H Core i9-9980HK	Coffee Lake	T2
Mac Pro (2019)	A1991	MacPro7,1	Xeon W-3223 Xeon W-3235 Xeon W-3245 Xeon W-3265M Xeon W-3275M	Cascade Lake	T2

Marketing Name	Model #	Model Identifier	SoC/Processor	microArch	Security Chip
Mac Pro (2019 Rack)	A2304	MacPro7,1	Xeon W-3223 Xeon W-3235 Xeon W-3245 Xeon W-3265M Xeon W-3275M	Cascade Lake	T2
2018					
MacBook Air (Retina, 13-inch, 2018)	A1932	MacBookAir8,1	Core i5-8210Y	Amber Lake	T2
Mac mini (2018)	A1993	Macmini8,1	Core i5-8500B Core i7-8700B	Coffee Lake	T2
MacBook Pro (15-inch, 2018)	A1990	MacBookPro15,1 MacBookPro15,3	Core i7-8750H Core i7-8850H Core i9-8950HK	Coffee Lake	T2
MacBook Pro (13-inch, 2018, Four Thunderbolt 3 ports)	A1989	MacBookPro15,2	Core i5-8259U Core i7-8559U	Coffee Lake	T2
2017					
iMac Pro (2017)	A1862	iMacPro1,1	Xeon W-2140B Xeon W-2150B Xeon W-2170B Xeon W-2190B	Skylake	T2

1.2 Document Purpose and Scope

This Common Criteria guidance document contains configuration information needed to configure and administer Apple macOS 13 Ventura: FileVault. Apple macOS 13 Ventura: FileVault conforms to the collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition (CPP_FDE_AA_V2.0E) and collaborative Protection Profile for Full Drive Encryption – Encryption Engine (CPP_FDE_EE_V2.0E). The information contained in this document is intended for Administrators who would be responsible for configuration and management.

This guide will show the administrator how to install and operate FileVault in a Common Criteria compliant manner.

1.3 Excluded Functionality

The following product functionality is not included in the CC evaluation:

- General Purpose Operating System functionality – The TOE is an integral part of macOS 13 Ventura; however, the evaluation is limited to the FDE functionality.
- Disk unlocking using an iCloud account.

1.4 Assumptions and Warnings

Users enable Full Drive Encryption on a newly provisioned or initialized storage device free of protected data in areas not targeted for encryption.

Upon the completion of proper provisioning, the drive is only assumed secure when in a powered-off state up until it is powered on and receives initial authorization.

Communication among and between product components (e.g., AA and EE) is sufficiently protected to prevent information disclosure.

Authorized users follow all provided user guidance, including keeping password/passphrases securely stored separately from the platform.

Users follow the provided guidance for securing the TOE and authorization factors.

The platform in which the storage device resides (or an external storage device is connected) is free of malware that could interfere with the correct operation of the product.

External tokens that contain authorization factors are used for no other purpose than to store the external token authorization factors.

The user does not leave the platform and/or storage device unattended until all volatile memory is cleared after a power-off, so memory remnant attacks are infeasible.

Authorized users do not leave the platform and/or storage device in a mode where sensitive information persists in non-volatile storage (e.g., lock screen or sleep state).

The user does not leave the platform and/or storage device unattended until the device has fully powered off.

Authorized administrators ensure password/passphrase authorization factors have sufficient strength and entropy to reflect the sensitivity of the data being protected.

The product does not interfere with or change the normal platform identification and authentication functionality such as the operating system login.

All cryptography implemented in the Operational Environment and used by the product meets the requirements listed in the cPP.

The platform is assumed to be physically protected in its Operational Environment and not subject to physical attacks that compromise the security and/or interfere with the platform's correct operation.

The platform is assumed to have a firewall enabled on the device.

1.5 How to Invoke Common macOS Features

If you are new to macOS 13 Ventura, there are a couple of interface terms that are important to know before using this document.

“**Apple** menu” refers to the pull-down menu in the top left corner of the menu bar.

“System Settings” is an app that provides access to and control of settings in macOS. It is a selection under the **Apple** menu and is also located in the Applications folder.

To help illustrate hierarchical menu structures, this document uses ‘>’ to indicate menu levels. For example, to invoke the System Settings app, this document will say:

 Navigating to **Apple** menu > System Settings

Thus, you would click on the **Apple** menu and select the System Settings menu item.

“Dock” refers to the bar, normally positioned at the bottom of the screen, that contains multiple icons. As you move your cursor across each icon in the Dock, the icon’s descriptive name will appear above the icon.

System Settings icon:



By default, the Dock contains the System Settings icon shown above. Clicking this icon provides an alternate method to launch the System Settings app.

Launchpad icon:



Another icon in the Dock is the Launchpad icon shown above. Launchpad provides the user with a screen containing one or more pages of icons, each representing an app or a folder. Clicking on an app will launch the app. One of the Launchpad pages will contain the “Other” folder. When you click on this folder, Launchpad will display additional apps contained within this folder.

Terminal icon:



One of the apps in the Other folder is the “Terminal” app. The Terminal app provides a command line shell program where the user can type in commands. When this document refers to command line commands like the chmod command, it implies that the user must execute the Terminal app and type the command into the window created by the app.

2 Installation, and Update, and Recovery

Apple macOS 13 Ventura: FileVault comes pre-installed on the hardware platforms listed in Table 2. macOS has a built-in update feature that the user can leverage to check for and install updates. Should the need arise, the administrator can manually download and re-install the same or newer version of the TOE on the supporting hardware.

To determine the running macOS version, click the  menu > About This Mac.

Figure 3 – macOS Version



2.1 Installation

If the hardware platform was purchased prior to the release of macOS 13 Ventura, macOS 13 Ventura can be installed:

1. Open the App Store

2. Search for “macOS Ventura”
3. Click Get
4. The installer for the currently available OS version will be downloaded to your Applications folder
5. Run the installer and follow the onscreen instructions

2.2 Update

The macOS operating system and software application updates can be downloaded manually through the following website: <https://support.apple.com/en-us/HT211683>.

An Apple server is leveraged for downloading firmware update code packages. The code packages containing the macOS, T2OS/firmware (on Intel with T2 Macs only), and sepOS/firmware are all bundled together as part of the download. The TOE stores the download in a temporary location on flash. Once the download is complete, the SEP verifies (authenticates) the digital signature on the bundle using the RTU public key and the algorithm stated in the Security Target. If the verification succeeds, the TOE installs the update and reboots the Mac. If the verification fails, the TOE terminates the update process with an error message.


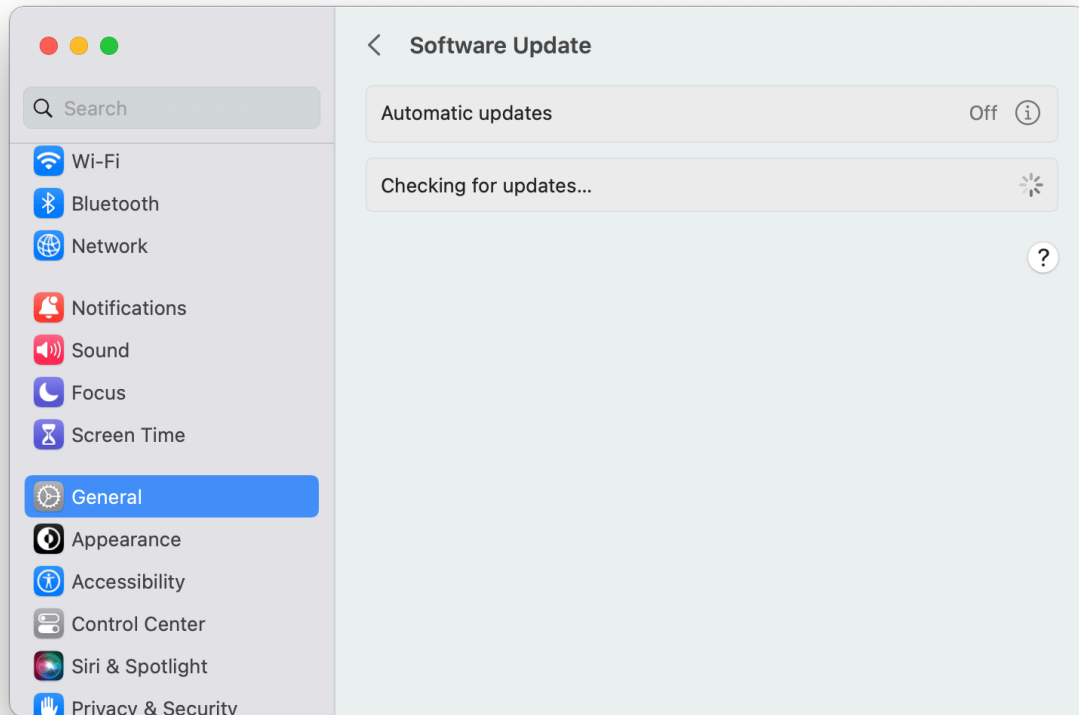
Updates to FileVault are bundled with macOS updates. Any user can check for updates to FileVault by navigating to  menu > About This Mac > Software Update... or opening the System Settings app and selecting Software Update. If updates are available, the user will be given the option of installing updates.

Figure 4 – Software Updates

Users can also check for updates from the command line by issuing the `softwareupdate -l` command. The user must be an authorized user (i.e., successfully logged in) to initiate an update.

2.2.1 Rapid Security Response (RSR)

Starting with macOS 13.2 Ventura, macOS supports Apple’s Rapid Security Response feature. This feature allows Apple to provide security fixes to users more frequently. RSR can be enabled/disabled in the Software Update dialog.

2.3 Recovery

If macOS encounters a problem (e.g., a system integrity error), it will boot into the paired macOS hidden Recovery partition installed and updated along with each and every macOS update. macOS Recovery will prompt the user for an administrator’s credentials and attempt to repair the problem. If macOS Recovery is able to repair the problem, macOS will boot normally.

If the repairs are unsuccessful, the administrator can reinstall macOS:

1. Boot into macOS Recovery
 - a. On a Mac with Apple silicon, press and hold the power button on your Mac until you see “Loading startup options.”
 - b. On an Intel-based Mac, press the power button. Press and hold *Command-R* until you see the startup screen

2. Make sure you're connected to the internet
3. Click Reinstall macOS Ventura, then click Continue
4. Follow the on-screen instructions

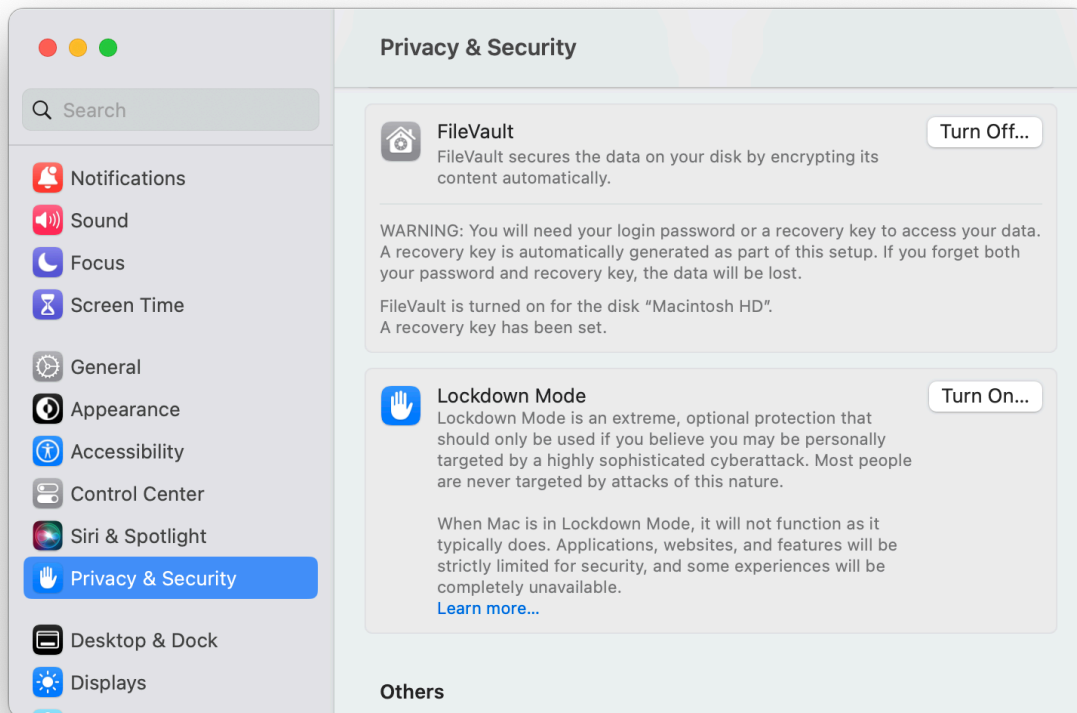
3 Configuration and Management

3.1 Enable Encryption

Once macOS is installed, FileVault is installed, it must be enabled by an administrator:

1. Open the System Settings app
2. Select Privacy & Security
3. Under FileVault, click "Turn On..."
4. Authenticate as an administrator when prompted

Figure 5 – FileVault



5. Do not select "Allow my iCloud account to unlock my disk." This functionality is unevaluated

Note: User data is always encrypted by the SEP. Enabling FileVault enables an additional password authentication factor.

3.2 Sleep State

macOS has a low power Sleep state; however, the drive is only assumed secure when in a powered-off state. In the evaluated configuration, the Sleep state must be disabled.

To disable Sleep, perform the following as an administrator:

1. Open Terminal
2. Run `sudo pmset -a disablesleep 1`

To re-enable Sleep, perform the following as an administrator:

3. Open Terminal
4. Run `sudo pmset -a disablesleep 0`

In the evaluated configuration, the TOE supports the G2(S5) (soft off) Compliant power-saving state. The TOE device can enter this Compliant power-saving mode when the user selecting the Shut down option on the TOE device or when power is lost. To resume from a Compliant power-saving state, the user must re-authenticate to the TOE with a correct username and password.

Please note that sleep state is not a Compliant power-saving state.

The TOE fully transitions into the Compliant power-saving state between approximately 2 seconds and 9 seconds, depending on the TOE model.

3.3 User Accounts

When user accounts are managed in macOS, they are automatically synchronized with FileVault.

3.3.1 Add Users

As an administrator:

1. Open the System Settings app
2. Select Users & Groups
3. Click "Add Account..."
4. Authenticate as an administrator when prompted
5. Enter the details for the new user:
 - a. New Account – This specifies the role for the user. The user can be assigned the Administrator role by selecting Administrator from the drop-down list
 - b. Full Name – This is a display
 - c. Account name – This will be used as the name in audit logs and for the user's home directory
 - d. Password – This is the user's initial password. Passwords may be up to 255 characters in length and composed of printable ASCII characters (i.e., character codes 0x20 to 0x7E inclusive)
6. Click Create User

3.3.2 Delete Users

As an administrator:

1. Open the System Settings app
2. Select Users & Groups
3. Click the information icon (the letter i in a circle) on the righthand side of the user to be deleted
4. Click "Delete Account..."
5. Authenticate as an administrator when prompted
6. On the "Are you sure ..." dialog:
 - a. Choose what to do with the user's home folder

- b. Click Delete Account

3.3.3 Change Password

As the user:

1. Open the System Settings app
2. Select Users & Groups
3. Click "Change Password..."
4. Enter the old password and the new password
5. Click Change Password

3.3.4 Changing/Erasing the Data Encryption Key

The data encryption key (DEK) can be changed or erased by performing the following as an administrator:

1. Follow the steps in Section 2.3 to boot into recoveryOS
2. Select Options
3. Authenticate as an administrator
4. Launch Disk Utility
5. Select Macintosh HD
6. Click Erase

Note 1: These operations do not directly erase the DEK, but rather erase the key used to wrap the DEK. By erasing this key, the plaintext value of the DEK becomes permanent irretrievable.

Note 2: Changing and erasing the DEK causes the same effect: the data cannot be recovered.

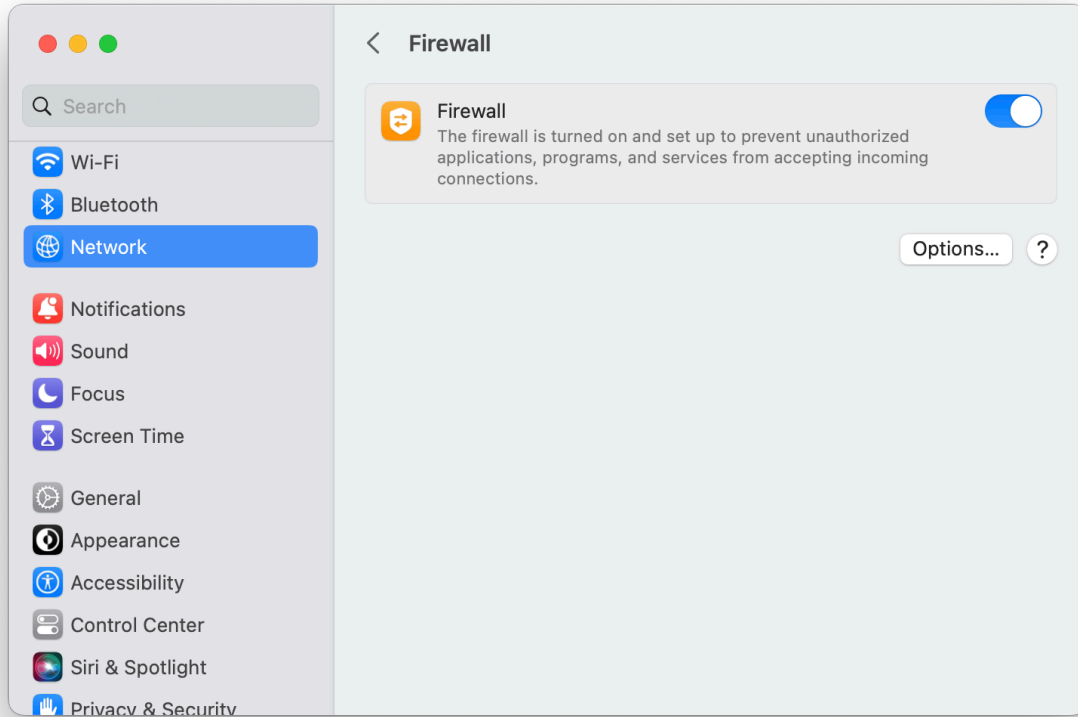
Note 3: The TOE does not depend on the operational environment for clearing memory.

3.4 Firewall

The host-based firewall can be managed by an administrator:

1. Open the System Settings app
2. Select Network
3. Select Firewall
4. Use the Firewall switch to enable and disable the firewall. Click "Options..." to configure specific application-based firewall rules
5. Authenticate as an administrator when prompted

Figure 6 – Firewall



4 Usage

When the system boots, the user will be prompted to select their account and enter their password authentication factor to unlock the disk.

After 10 consecutive failed attempts to unlock the disk, FileVault requires the system to be rebooted into recoveryOS. 10 additional authentication attempts are allowed in recoveryOS. FileVault blocks validation once these validation attempts have been exhausted.

All other operations are transparent to the user.

5 Acronyms

Table 3 – Acronyms

Acronym	Definition
AA	Authorization Acquisition
AES	Advanced Encryption Standard
BEV	Border Encryption Value
CC	Common Criteria
DEK	Data Encryption Key
DRAM	Dynamic Random Access Memory
EE	Encryption Engine
FDE	Full Drive Encryption
NIAP	Nation Information Assurance Partnership
PBKDF2	Password-Based Key Derivation Function 2
PP	Protection Profile
RSA	Rivest, Shamir, & Adleman
RSR	Rapid Security Response
RTU	Root of Trust for Update
SEP	Secure Enclave Processor
SFR	Security Functional Requirement
SoC	System on a Chip
SSD	Solid State Drive
SSV	Signed System Volume
ST	Security Target
TOE	Target of Evaluation
TSS	TOE Summary Specification
VID	Validation Identifier

End of Document