Apple Inc.

Apple macOS 26 Tahoe: FileVault Common Criteria Guide

Version 1.0

2026-06-29

NIAP VID 11696

Prepared for:

Apple
One Apple Park Way
Cupertino, CA 95014

Prepared by:

atsec information security
4516 Seton Center Parkway, Suite 250
Austin, TX 78759

Revision History

Version	Date	Changes
1.0	2026-06-29	First version

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.

Table of Contents

1 Introduction

This guide provides instructions to configure and operate Apple macOS 26 Tahoe: FileVault in the Common Criteria (CC) evaluated configuration.

1.1 Target of Evaluation

The Target of Evaluation (TOE) is Apple macOS 26 Tahoe: FileVault, which is a Full Drive Encryption (FDE) solution on Apple Mac computers with Apple silicon. The TOE is both an Authorization Acquisition (AA) and Encryption Engine (EE) product. The TOE is part of the Apple macOS 26 Tahoe operating system which leverages the Apple silicon Systems on Chip (SoCs). The TOE is comprised of both software and hardware.

The TOE hardware resides in the Apple silicon SoC used in Mac computers. The TOE hardware consists of the Secure Enclave and DMA Storage Controller which provide the foundation for encrypted storage capabilities. The Secure Enclave, which contains the Secure Enclave Processor (SEP), provides hardware key management. The DMA Storage Controller contains a dedicated AES crypto engine for encrypting and decrypting storage data.

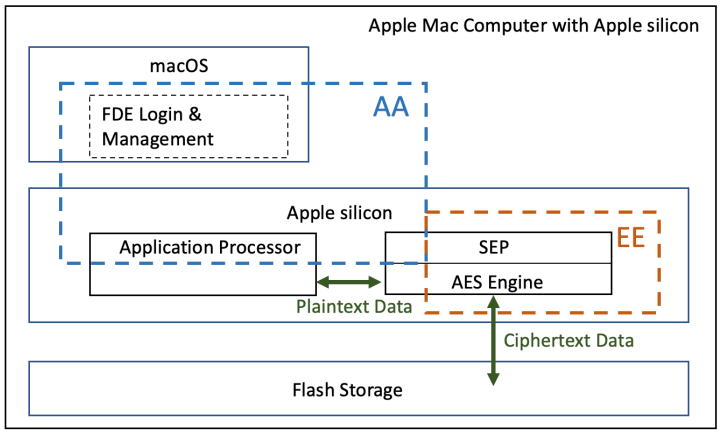
The TOE software/firmware is part of macOS and provides login and management functionalities. The macOS version used in evaluation testing is 26.3.

All processing for cryptography related to FDE functionality is performed using the SEP or AES Engine rather than the Apple silicon Application Processor. The DMA Storage Controller uses AES-XTS-256 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 devices covered by this evaluation are listed in the Security Target (ST).

The following diagram depicts the TOE boundaries on Mac computers with Apple silicon. The AA boundary is identified by a dashed blue line, and the EE boundary is depicted by a dashed orange line.

Figure 1 – TOE boundaries



1.2 Document Purpose and Scope

This document serves as the administrative guidance for the TOE, Apple macOS 26 Tahoe: FileVault. This document provides the preparative procedures and operational user guidance for the evaluated configuration. This document describes how to install, configure, and operate the TOE in the CC compliant manner.

The TOE conforms to the following Protection Profiles (PPs):

- [CFG_CPP_FDE_AA-CPP_FDE_EE_V1.0] PP-Configuration for Full Drive Encryption - Authorization Acquisition and Full Drive Encryption - Encryption Engine, Version 1.0, which consists of the following components:
    - [CPP_FDE_AA_V2.0E]: collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition, Version 2.0 + Errata 20190201.
    - [CPP_FDE_EE_V2.0E]: collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0 + Errata 20190201.

1.3 Evaluated Configuration

The following product functionalities are not included in the CC evaluation:

- General Purpose Operating System functionality. The TOE is partially implemented in the Apple macOS operation system; however, the evaluation is limited to the FDE functionality. General Purpose Operating System functionality is not part of this evaluation.
- Disk unlocking using an iCloud account.

1.4 Assumptions

The following assumptions apply when operating the TOE in the evaluated configuration:

- 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 the device has fully powered off. 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).
- 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.

1.5 Common User Interface Features

There are multiple user interface terms that are important to know while using this document:

- "Apple menu" refers to the pull-down menu located in the top-left corner of the screen.
- "System Settings" is an app that provides access to and control of settings in macOS. It is a selection under the Apple menu.
- To help illustrate hierarchical menu structures, this document uses '>' to indicate menu levels. For example, to instruct the reader to click on the Apple menu and select the System Settings menu item, this document will say:

  Choose Apple menu > System Settings
- "Dock" refers to the bar normally positioned at the bottom of the screen, that contains multiple application icons. As the cursor is moved across each icon in the Dock, the icon's descriptive name will appear above the icon. Below are some commonly used icons.

Table 1 - Icons

Icon	Usage
Launchpad 	By default, the Dock contains the Launchpad icon. Launchpad provides users 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 	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 and execute commands. When this document refers to command-line commands, it implies that the user must open the Terminal app and type the command into the window created by the app. Command-line commands are written on a new line and prefixed by % in this document.
System Settings 	Clicking this icon provides an alternate method to launch the System Settings app.

1.6 Obtaining TOE Devices

Customers can acquire the TOE devices (Mac computers) through various distribution channels:

- **Normal distribution channel**

  Individual customers can obtain Mac computers from the following sources:
  - The Apple Store (physical store or online at https://apple.com)
  - Apple retailers
  - Resellers
- **Business-specific distribution channel**

  Business customers can use the link https://www.apple.com/business/
- **Government-specific distribution channel**

  Government customers can use the link https://www.apple.com/government/
- **Apple Store Catalog for large customers**

Large customers can have their own Apple Store Catalog for their employees to purchase devices directly from Apple under their corporate employee purchase program.

2 Installation, Update, and Recovery

Apple macOS 26 Tahoe: FileVault may come pre-installed on the TOE hardware platforms. The TOE has a built-in update feature that the user can leverage to check for and install updates. Should the need arise, an administrator can download and re-install the same version of the TOE software/firmware on the supporting hardware.

The macOS operating system recognizes two kinds of user roles: Administrator and Standard. The first user account created is automatically assigned the administrator role.

To determine the running macOS version, a user can choose Apple menu > About This Mac.

2.1 Installation

If the TOE device was purchased prior to the release of Apple macOS 26 Tahoe, an administrator can install the TOE software/firmware on the TOE device as follows:

1. Open Software Update.
2. When Software Update opens, it automatically checks for new software. If new software is available for your Mac (i.e., macOS Tahoe 26.3), click the Update, Upgrade, or Restart Now button to install it.
3. Before installation begins, you're asked to enter your administrator password.
4. During installation, your Mac might restart and show a progress bar or blank screen several times.

Alternatively, an administrator can download and install macOS 26 Tahoe via the command-line interface:

1. Open the Terminal app.
2. Enter the following command to download the installer:

```
% softwareupdate --fetch-full-installer --full-installer-version 26.3
```

3. As macOS downloads to the Applications folder, Terminal shows the percentage installed (downloaded).
4. Open the Applications folder and double-click the macOS installer, named *Install macOS Tahoe.app*, then follow the onscreen installation instructions.

2.2 Update

The updates to the TOE software/firmware are all bundled together as part of macOS updates. An administrator can check for and install updates to the TOE as follows:

1. Choose Apple menu > System Settings, click General in the sidebar, then click Software Update.
2. The update information, if available, will be shown.
3. Follow the onscreen instructions for installation of the updates.

Signature verification of the update is performed by the TOE before the update is installed. If the signature verification fails, the update process is aborted.

2.2.1 Background Security Improvements

Starting with macOS 26.1, macOS supports Background Security Improvements feature. This feature allows for delivering important security improvements between software updates. It can be enabled/disabled under System Settings > Privacy & Security > Background Security Improvements.

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 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, an administrator can use macOS Recovery to reinstall macOS, which keeps files and settings intact when reinstalling.

1. Make sure the computer is connected to the Internet.
2. Choose Apple menu > Shut Down, press and hold the power button until the system volume and the Options button appear, select Options, click Continue.
3. In the Recovery app window, select "Reinstall macOS 26 Tahoe", then click Continue.
4. Follow the onscreen instructions.
5. When you're asked to select a disk, select your current macOS disk (in most cases, it's the only one available).

3 Configuration and Management

3.1 Enable Encryption

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

1. Choose Apple menu > System Settings, click Privacy & Security in the sidebar, then click FileVault.
2. Turn on FileVault.
3. Choose how to unlock your disk and reset your login password if you forget it:
   - Click "Create a recovery key and do not use my iCloud account". Write down the recovery key and keep it in a safe place.
4. Click Continue.

Note 1: Do not select "Allow my iCloud account to unlock my disk" in Step 3. This functionality is unevaluated.

Note 2: User data is always encrypted on the TOE device. Turning on FileVault provides an extra layer of security by keeping someone from decrypting the data without entering the correct password.

3.2 Power Saving State

In the evaluated configuration, the TOE supports only one Compliant power saving state:

- G2(S5) - soft off state: the system is powered down.

This feature is not configurable.

To activate the Compliant power saving state on the TOE device, the user needs to choose Apple menu > Shut Down, or press and hold the physical power button.

In the event of unexpected power loss, the Mac desktop enters the Compliant power saving state, whereas the Mac laptop switches to battery power. When the battery runs out of charge, the Mac laptop enters the Compliant power saving state.

To resume from a Compliant power saving state, the user must turn on the computer and re-authenticate to the TOE with the correct password.

The TOE fully transitions into the Compliant power saving state between approximately 9 seconds and 13 seconds, depending on the TOE device model.

Apple macOS 26 Tahoe 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. Execute the following command:

   ```
   % sudo pmset -a disablesleep 1
   ```

3. Authenticate as the administrator with the password when prompted.

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

1. Open Terminal.
2. Execute the following command:

   ```
   % sudo pmset -a disablesleep 0
   ```

3. Authenticate as the administrator with the password when prompted.

Note: The Sleep state is not a Compliant power saving state.

3.3 User Accounts

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

3.3.1 Add a User

As an administrator:

1. Choose Apple menu > System Settings, then click Users & Groups in the sidebar.
2. Click the Add User button below the list of users.
3. Click the pop-up menu next to New User, then choose a type of user.
   - Administrator: An administrator can add and manage other users, install apps, and change settings. The new user you create when you first set up your Mac is an administrator. Your Mac can have multiple administrators.
   - Standard: Standard users are set up by an administrator. Standard users can install apps and change their own settings, but can't add other users or change other users' settings.
   - Sharing Only: Sharing-only users can access shared files remotely, but can't log in to the computer or change settings. Note: This user type in not evaluated and should not be used in the evaluated configuration.
4. Enter a full name for the new user. An account name is generated automatically. To use a different account name, enter it now—you can't change it later.
5. Enter a password for the user, then enter it again to verify.
6. Click Create User.

3.3.2 Delete a User

As an administrator:

1. Choose Apple menu > System Settings, then click Users & Groups in the sidebar.
2. Click the information icon ⓘ (the letter i in a circle) next to the user to be deleted, then click Delete User.
3. Choose what to do with the user's home folder, then click Delete User.

Note: If a user is logged in to this Mac now, you can't select that user.

3.3.3 Change the Password

As a user (standard user or administrator):

1. Choose Apple menu > System Settings, then click Users & Groups in the sidebar.
2. Click the information icon ⓘ next to a user in the list, then do any of the following:
   - Click Change to change your login password.
   - Click Reset to change another user's login password as an administrator.

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. Choose Apple menu > Shut Down, press and hold the power button until the system volume and the Options button appear, select Options, click Continue.

2. Launch Disk Utility.
3. Select Macintosh HD.
4. 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 permanently 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.

4 Password Lockout

When the system boots, the user will be prompted to select the account and enter the correct password to unlock the data volume.

To help prevent brute-force attacks, when the TOE device starts up, no more than 10 password attempts are allowed at the Login Window, and escalating time delays are imposed after a certain number of incorrect attempts.

The table below shows escalating time delays after the entry of an invalid password.

Table 2 - Time delay escalation for authentication attempts

Incorrect attempts	Delay enforced (Login Window)	Delay enforced (recoveryOS)
1 - 3	None	None
4	1 minute	1 minute
5	5 minutes	5 minutes
6	15 minutes	15 minutes
7	1 hour	1 hour
8	3 hours	3 hours
9	8 hours	8 hours
10	8 hours	See below

If the 10 attempts are used up, 10 more attempts are available after rebooting into recoveryOS (also with escalating time delays). And if those are also exhausted, then 10 additional attempts are available using the FileVault (personal) recovery key[1]. After those additional attempts are exhausted, the Secure Enclave no longer processes any requests to decrypt the volume or verify the password and the data on the drive becomes unrecoverable.

[1] If enabled, 10 additional attempts are also available using iCloud recovery. As mentioned in Section 1.3 however, iCloud unlock is not evaluated.

5 Acronyms

AA
: Authorization Acquisition

AES
: Advanced Encryption Standard

CC
: Common Criteria

DEK
: Data Encryption Key

EE
: Encryption Engine

FDE
: Full Drive Encryption

NIAP
: National Information Assurance Partnership

PP
: Protection Profile

SEP
: Secure Enclave Processor

SoC
: System on Chip

ST
: Security Target

TOE
: Target of Evaluation

VID
: Validation Identifier