SecureDoc for Apple FileVault 2

Client Install/User Manual

V8.6SR1 HF4

WINMAGIC®
DATA SECURITY

Many products, software and technologies are subject to export control for both Canada and the United States of America. WinMagic advises all customers that they are responsible for familiarizing themselves with these regulations. Exports and re-exports of WinMagic Inc. products are subject to Canadian and US export controls administered by the Canadian Border Services Agency (CBSA) and the Commerce Department's Bureau of Industry and Security (BIS). For more information, visit WinMagic's web site or the web site of the appropriate agency.

Acknowledgements
This product includes cryptographic software written by Antoon Bosselaers, Hans Dobbertin, Bart Preneel, Eric Young (eay@mincom.oz.au) and Joan Daemen and Vincent Rijmen, creators of the Rijndael AES algorithm.
This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.OpenSSL.org/).
WinMagic would like to thank these developers for their software contributions.

Contacting WinMagic

WinMagic
501-5770 Hurontario St,
Mississauga, Ontario, L5R 3G5
Toll free: 1-888-879-5879
Phone: (905) 502-7000
Fax: (905) 502-7001

Sales: sales@winmagic.com Marketing: marketing@winmagic.com
Human Resources: hr@winmagic.com
Technical Support: support@winmagic.com
For information: info@winmagic.com
For billing inquiries: finance@winmagic.com

Who Should Read this Document?

This document explains how to use SecureDoc in an enterprise environment and is intended for either end users or administrators. It describes features available in all SecureDoc for macOS editions, with edition-specific features clearly labeled. Note that some features may not be available in some environments, or to some users.

This document assumes a basic working knowledge of Windows-based computer systems. It explains only SecureDoc-specific procedures.

Important Notes – Please read before installing/upgrading

IMPORTANT: On previous versions of macOS, SecureDoc for FileVault 2 could install Kernel Extension (KEXT) components. macOS 11 Big Sur does not permit third-party KEXTs, so installation of SecureDoc for FileVault 2 on Big Sur differs from previous versions.

When performing a fresh in stall of SecureDoc for FileVault 2 on macOS 11 Big Sur, there is no longer a requirement to authorize installation of SecureDoc Kernel Extensions, as these have been removed from this installer, in keeping with Big Sur's blocking the use of third-party Kernel Extensions (KEXTs).

V8.6 no longer supports SecureDoc's Full Media Encryption mode for removable media – it only supports Removable Media Container Encryption, which does not rely on use of our Kernel Extensions. SecureDoc V8.6 for FileVault 2 now offers a more feature-rich management tool for Removable Media called Removable Media Container Manager.

When installing SecureDoc for FileVault 2 on devices running macOS 11 Big Sur, the installation MUST be run by an Administrator. macOS Big Sur includes some additional stringency relating to credentials that did not exist in earlier macOS versions.

IMPORTANT: In Version 8.2SR1, SecureDoc's Pre-Boot for FileVault 2 (abbreviated as SDOTFV2) was removed from the product, and will no longer be available as an option for new devices.

NOTE: Existing macOS devices that are currently running SecureDoc's Pre-Boot for FileVault 2 (SDOTFV2) should be migrated as soon as possible to use SecureDoc's FileVault 2 (SDFV2) management in order to ensure that macOS can be upgraded going forward without risk of encountering issues following a macOS version upgrade.

Customers that still have devices running SecureDoc's Pre-Boot for FileVault 2 (SDOTFV2) are strongly urged to:

a) use the un-installation instructions in the section entitled "To uninstall SecureDoc from a Client Device", after which they should

b) install SecureDoc for FileVault 2 (SDFV2) using the installation instructions in this manual.

Note that such un-installation is not required for devices that are already running SecureDoc for FileVault 2 (SDFV2).

IMPORTANT: When installing SecureDoc for FileVault 2 on devices running macOS 10.15 Catalina (and subsequent versions), the installation MUST be run by an Administrator user. macOS Catalina (and recent Big Sur) includes some additional stringency relating to credentials that did not exist in earlier macOS versions.

On previous versions of macOS, SecureDoc for FileVault 2 supported having the Admin perform installation of SecureDoc for FileVault 2, stopping when SDForm is displayed, at which point the device could be brought to the device's end user (this end user could be a Standard user), and after that user provided his/her password FileVault 2 could be enabled successfully, completing the deployment of SecureDoc on that device.

However, on macOS Catalina and later, during enablement of FV2 there is now an additional prompt displayed. Even though a Standard user can click the OK button in this prompt to continue installation, it will actually fail to enable FileVault 2 because a required elevated credential is not met.

As a result, for macOS Catalina and later, WinMagic recommends that our customers always use an Admin user account to deploy SDFV2 package.

If using a Standard user, and failing to enable FV2, a message will appear, which can only be corrected by logging out, then logging back in with an Admin user account, then continuing the deployment under that account.

Contents

About SecureDoc for FileVault 2

About SecureDoc for FileVault 2

SecureDoc for FileVault 2 securely manages FileVault 2 for your Apple macOS computer (desktop or laptop).

In this document, **S**ecure**D**oc for **F**ile**V**ault **2** may be abbreviated to SDFV2.

SecureDoc for FileVault 2 can also be used to encrypt and decrypt USB flash media, protecting them with either a password or a key, and such encrypted media's contents can be read and updated *cross-platform* - on either macOS or Windows devices.

The purpose of SecureDoc working with FileVault 2 is to fulfill the security compliance needs that have been set. On its own FileVault 2 will encrypt a hard-disk, but this will not allow for administrator to achieve a major objective:

1) Allowing Administrators to recover credentials
    a. Administrators will need to be able to access the User Credentials in the case of a forgotten password or username
    b. Maintain a status on the device
        i. FileVault 2 will encrypt the partition, but there is still a chance for the files to be accessed (if the password was taken)
        ii. Administrators need to know if FileVault 2 is enabled or has been disabled, and SES' monitoring abilities will allow for this

SecureDoc includes a communication agent which allows it to communicate with the SES Server (through the SDConnex service).

Configuration of SecureDoc Device Profile settings and Installation Packages is covered in the main SES User Guide, so this guide has been reworked to focus primarily on how to install and use SecureDoc for Apple FileVault 2 on Apple macOS endpoint devices.

Note: SecureDoc's Pre-Boot for FileVault 2 (SDOTFV2) was removed in V8.2SR1 (whose documentation contained guidance on how to move to SecureDoc for FileVault 2). Nearly all references to SDOTFV2 have been removed from this manual, but guidance on how to move to SecureDoc for FileVault 2 has been retained for now, as a courtesy, for any customers who might still be using SDOTFV2. WinMagic urges any remaining customers who are still using SDOTFV2 to move to SDFV2 as soon as possible.

New in SecureDoc V8.6SR1 HF4

- SES Version 8.6SR1 HF4 provides support for macOS Monterey 12.0

Supported Environments and hardware

Supported Apple Operating System

- macOS Monterey 12.0
- macOS Big Sur 11.0
- macOS Catalina 10.15.x
- macOS Mojave 10.14.x

Supported Apple Devices

- MacBook Air 7.2
- Macbook 9.1
- Macbook Pro 11,5
- Mac mini 9,1 with M1 chip
- MacBook Air 10,1 with M1 chip
- MacBook Pro 18,3 with M1 Pro chip
- MacBook Pro 18,4 with M1 Max chip

How this Documentation has changed from V8.3 onward

This documentation has been updated since V8.2SR1 to identify how the user experience and required user inputs to the SecureDoc installation process will apply now that SecureDoc no longer offers support for SecureDoc "On Top" of FileVault 2 (SDOTFV2), removed in SES V8.2SR1.

In this version of the documentation, almost all references to SecureDoc "On Top" of FileVault 2 (SDOTFV2) have been removed, save (primarily) for the instructions relating to how to move off SDOTFV2 and onto SDFV2. These have been retained (for the moment) as a courtesy to customers to assist them in moving to SDFV2, but will be completely removed in a future version.

Why a new Installation Manual for a HotFix release?

Due to changes to process rights under macOS Monterey 12.1, the client installation process differs slightly from the process in previous versions. This documentation has been updated to indicate how installing on Monterey 12.1 diverges from previous OS version behavior.

Installing SecureDoc for FileVault 2 on Mac client devices

System Requirements

Apple macOS is supported for enterprise environments via FileVault 2 management support.

SecureDoc Enterprise Server is capable of managing FileVault 2 centrally, enforcing encryption policies and removable media encryption.

Make sure that the device is running a macOS version that is in the supported list above.

If upgrading:

Recommended Upgrade sequence: Upgrade SecureDoc to V8.6 before upgrading macOS to Big Sur

If SecureDoc is upgraded to V8.6 (e.g. on Catalina) before upgrading to macOS 11 Big Sur, the device will remain encrypted and all functionality will be smoothly transitioned, with no special considerations.

Special considerations if macOS is upgraded to macOS 11 Big Sur before upgrading SecureDoc to V8.6

If macOS 11 Big Sur is upgraded before upgrading SecureDoc, the device will remain encrypted but SecureDoc management for FileVault 2 will be silently disabled. The SecureDoc recovery account will still exist, so if the user has forgotten the password for this recovery account, this account can be used to log in after getting the password from the SES Console. Once logged in, another admin or user password can be reset for an account that exists on the device. NOTE: The recovery account password cannot be changed since, without the SecureDoc client being active, communication between the device and the SecureDoc Server is not working and the password update will not be passed back to SES for storage.

To reinstate SecureDoc Management for FileVault 2, simply install SecureDoc V8.6 for FileVault 2 on the device, which will reinstate all SecureDoc functionality.

Installation Process

Please read carefully:

There are certain limitations re: SecureDoc "taking over" management of an already-encrypted device currently managed by FileVault 2, as follows:

Through the use of SecureDoc for FileVault 2 (SDFV2), further users can be added to the unlock list through the SES console if desired. Under SDFV2, any new local user or AD user which already has SecureToken enabled and uses it to log in will be automatically added to the Unlock list. If RME/RMCE has been enabled in the profile setting, the user will be prompted to provide a password in order to get a Keyfile for creating/accessing RME/RMCE-protected media.

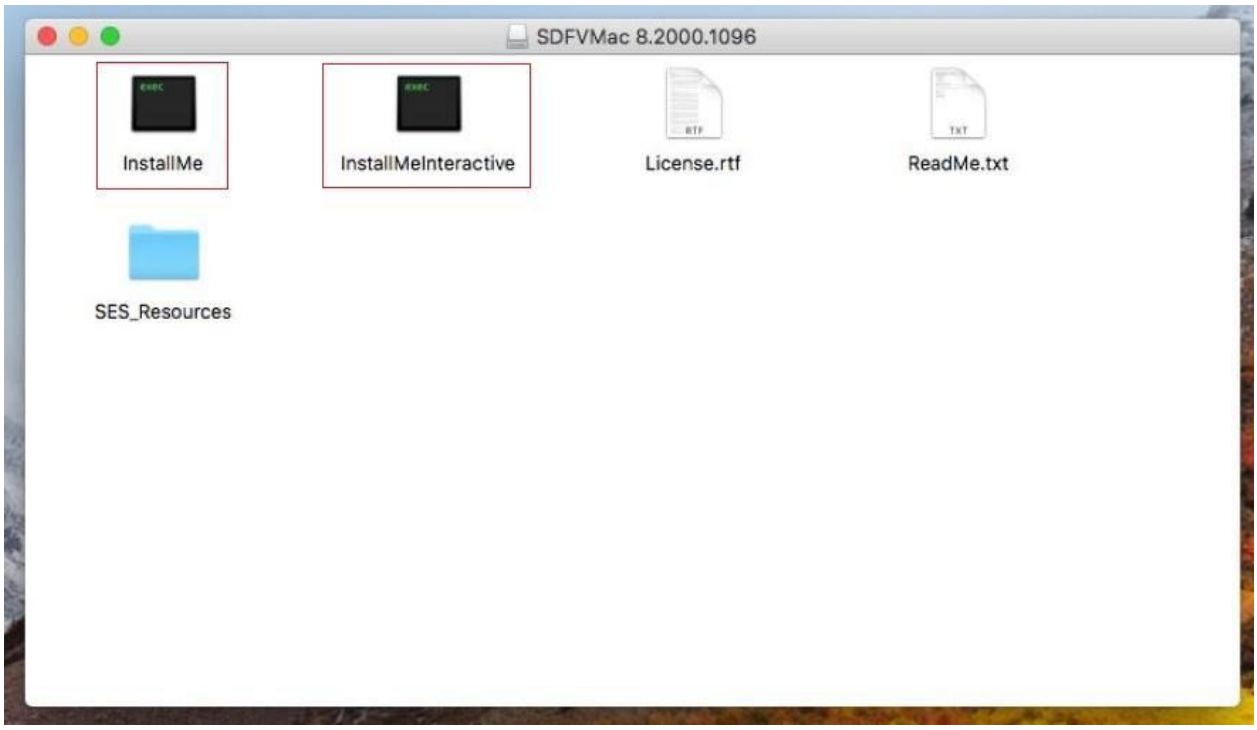
In Version 8.2 and onward, installing SecureDoc can successfully "take over" management of an already-encrypted FileVault 2-protected device.

Installing a SDFV2 device Profile will now differ depending on the type of installation being done. There are currently 4 separate profile installation modes which can be used:

- FileVault 2 with RMCE enabled
- FileVault 2 only
- RMCE Only
- Idle Mode SecureDoc, which will only provide communication.

1. Login to the Mac with an account that has administrator rights. An option has been added permitting the current user on the device to also perform the installation.

1. Copy the SDFVMac.dmg file onto the Mac device and mount it.
2. Open the mounted drive to display the installation scripts

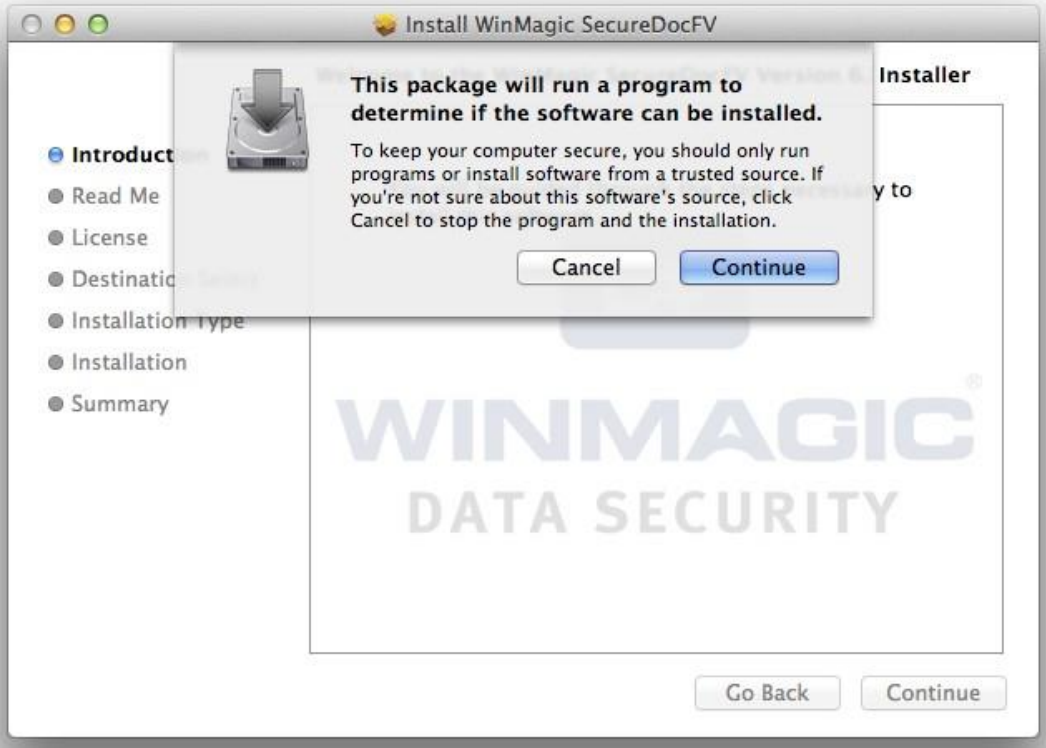


1. There are two means of installing SecureDoc on Apple Mac devices:

1) Double click on "**InstallMe**" (as in image above, left) to perform the silent installation method which briefly opens a terminal window and simply requires the user to enter their credentials before proceeding with the installation process. This is normally recommended to perform quick and easy deployments, or

2) Double click on the "**InstallMeInteractive**" script (as in image above, right) – This opens an Installation wizard and guides the user through the installation process step-by-step.

2. Authenticate
    a. Please enter the password of the installing user with Mac Admin rights to continue installation.
    b. If using "**InstallMeInteractive**", the following image will appear:



Click **Continue** and follow the instructions on the installer.

Click on **Agree** for the software license agreement to continue.

NOTE: If using the "**InstallMe**" installer on macOS versions prior to macOS 12.1 Monterey a terminal window will appear like in the following image that will show the logged commands being executed during this portion of the install process. No panel will appear if using the above "InstallMeInteractive" to install SecureDoc. The panel will show when to use "InstallMe" to run the application.

NOTE re: Monterey 12.1x: If using the "**InstallMe**" installer on macOS Monterey 12.1 and subsequent versions you will be prompted to provide elevated rights to a SecureDoc component called SecureDocD (instead of elevating terminal which might open certain security issues under Monterey 12.1). The installation steps below will indicate what new prompt panels will appear requesting the necessary steps be taken.

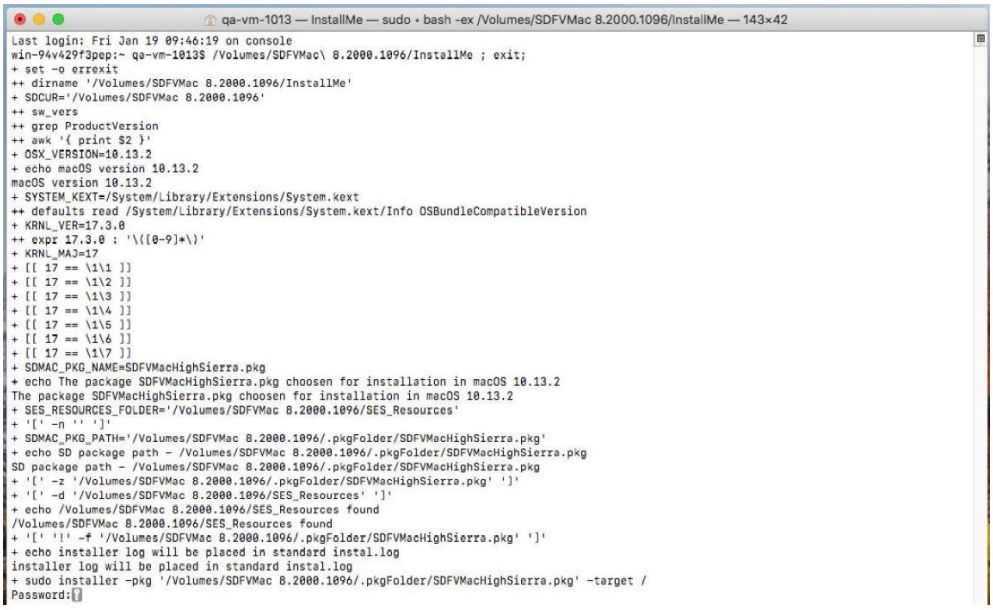
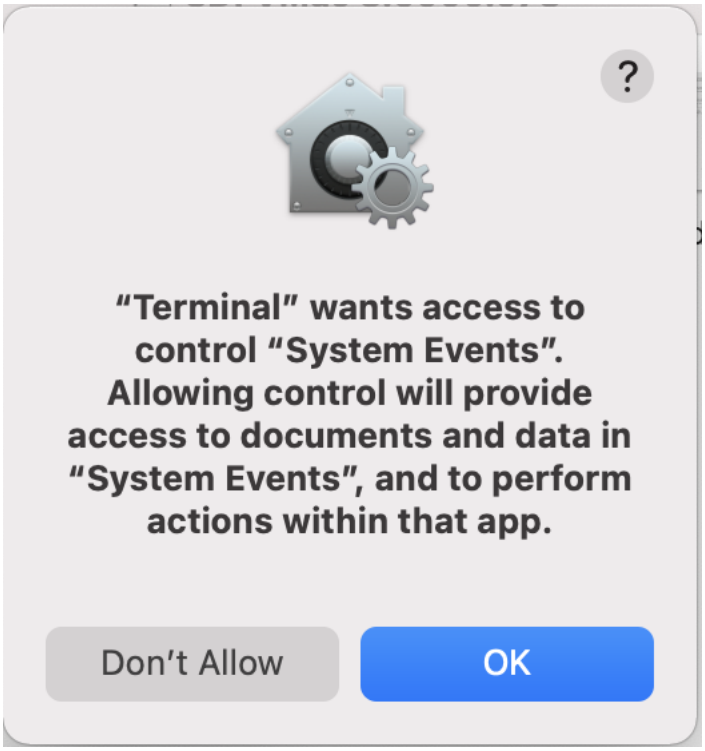


Figure 1 - Terminal window that appears for macOS prior to 12.1x Monterey

If installing on macOS Catalina or earlier, a message will appear indicating that macOS Security has blocked the addition of SecureDoc's extension (see image below). This Extension is still required on Catalina devices.

To allow the SecureDoc Extension on Catalina or earlier, follow one of the conditional instructions below, according to which version of macOS is on your computer.

NOTE: When installing on Big Sur and macOS Monterey versions up to 12.0x, there may be scenarios in which the following screen appears, indicating that the SecureDoc installer needs access to the Terminal, e.g. ` "**Terminal" wants access to control "System Events". Allowing control will provide access to documents and data in "System Events", and to perform actions within that app.** `
If the user had earlier permitted terminal access to System Events (e.g. during installation of another product), then this message will not appear.



Conditional Instructions – Mojave 10.14.x and beyond

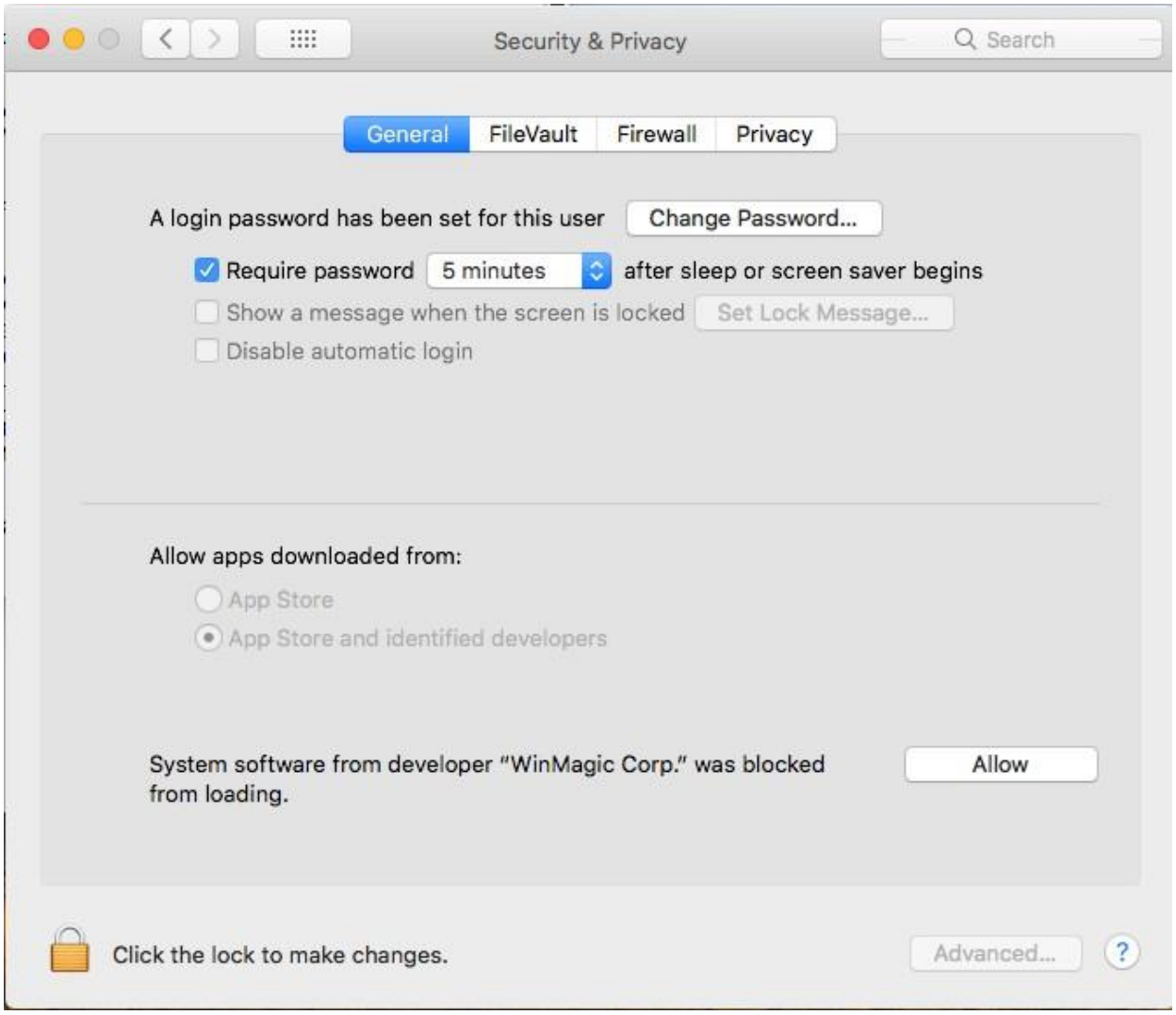
If installing on macOS Mojave 10.14.x or later, an option entitled "Open Security Preferences" will be displayed, and the user must click on that to access the Security Preferences screen (this new functionality effectively provides a one-button shortcut to that pane, as in the image above).

Use Security Preferences Panel to allow WinMagic System software to be loaded

Having accessed the Security Preferences panel, the user will see a notification near the bottom of that screen indicating "System software from developer "WinMagic, Corp" was blocked from loading.

Click the Lock icon near bottom left (near the phrase "Click the lock to make changes"), to enable the Allow button

Click the Allow button



3. A password will be required for FileVault 2, as in the image below.

The option the user clicks (and its behavior) is as follows:

- OK: This will resume the operation if the password is correct
- Cancel (by clicking on red button at top left): The application will stop and resume on the next reboot/login cycle.

NOTE: A similar dialogue prompting for a password may also appear whenever key information is required from SES or when a user is proposed to be added to the unlock list

macOS 12.1 Monterey (and beyond) Grant Full Disk Access to SecureDocD component

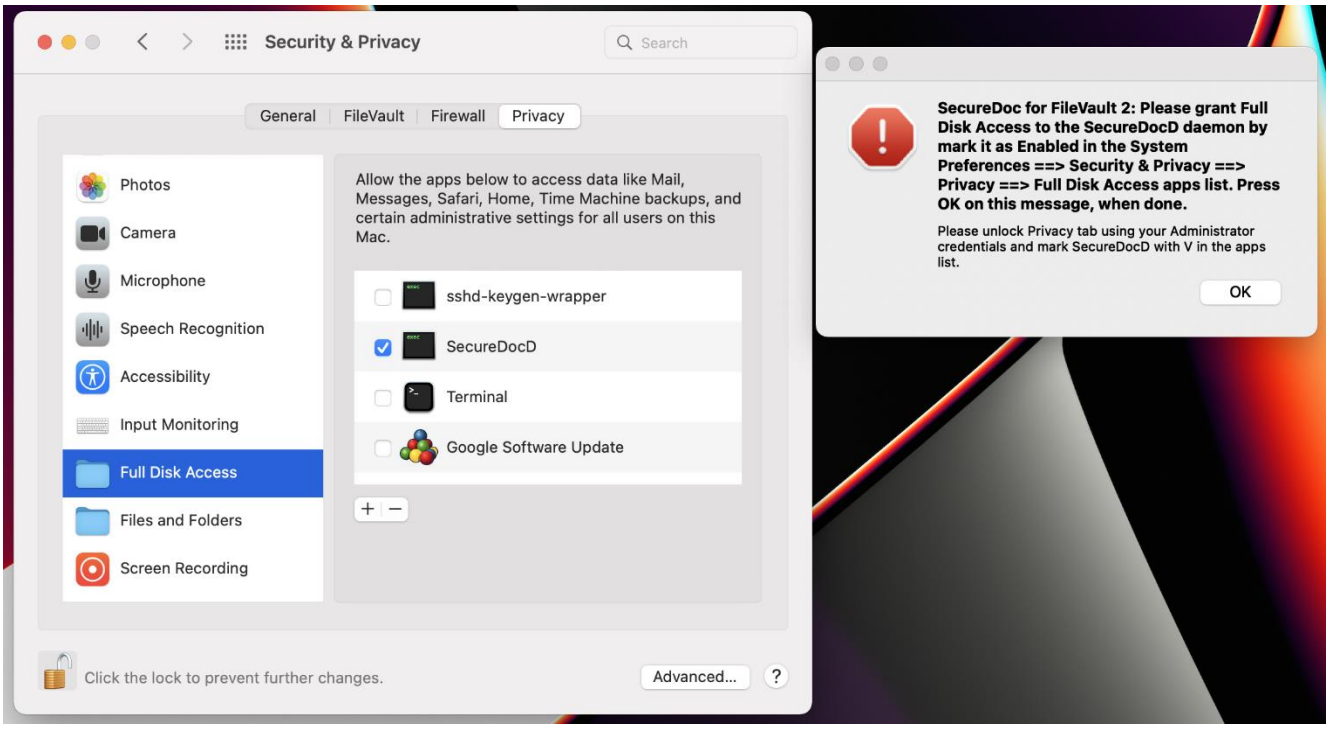
macOS 12.1 Monterey's security schema differs slightly from previous versions, and rather than providing broad rights to Terminal, WinMagic has developed a new component unique to the SecureDoc installation process that, when provided the necessary rights, handles the installation securely without broadening rights in Terminal.

During the process of installing SecureDoc, the user will be given 3 opportunities to set the necessary Full Disk Access rights to SecureDocD.

If customers don't provide the necessary access following the display of any of these messages, the deployment/upgrading process will continue and the process will finish without problem, but if customers log out or reboot the device (causing SecureDoc FV2 to re-start), the message will show up again until the necessary permission has been enabled.

NOTE: If installing SecureDoc 8.6SR1 HF4 or later using "InstallMeInteractive", the prompts shown below will appear after installation has completed, and the same granting of Full Disk Access rights to SecureDocD must still be performed.

12.1 Monterey process difference:
The image below shows the first of these messages near the top-right corner of the screen (adjacent to the Security and Privacy setting necessary to avoid display of subsequent messages).



1 – When this prompt appears, open the macOS **Security and Privacy** panel.

2 – Select the Privacy tab and click Full Disk Access in the left column.

3 – Click the lock icon. Enter your Password and select Unlock.

4 – Click on the checkbox to the left of SecureDocD to select that (a tick-mark will appear)

5 – Close the Security and Privacy panel.

6 – Now click OK on the "SecureDoc for FileVault 2: Please grant Full Disk Access…" message panel (e.g. at the top right of the image above) to permit the installation to proceed.

7 - The installation will proceed.

NOTE: if you click OK **without having granted SecureDocD the necessary Full Disk Access rights**, you will see the above message panel repeated.

If you click OK on the second appearance of the "SecureDoc for FileVault 2: Please grant Full Disk Access…" message panel at the top right without having provided the needed Full Disk Access rights in step 1 above:

- a variation of the message will appear (as in the image below), indicating that Full Disk Access has not been granted.

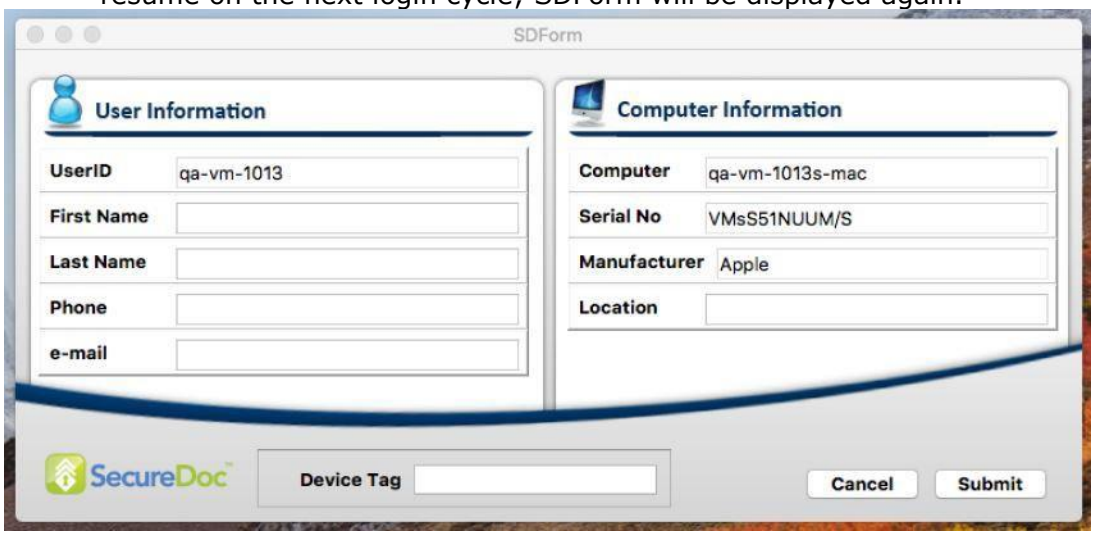
- If the installation is permitted to continue without granting the required Full Disk Access permission to SecureDocD it might affect SecureDoc functionality and, upon restarting the device, the user will again be prompted to apply the necessary permissions for SecureDocD.

4. (Optional) **SDForm** may be shown, as in the image below:

Note: SDForm appears only if the SES Administrator had selected the "Ask user to verify data before starting encryption" option during Profile configuration.

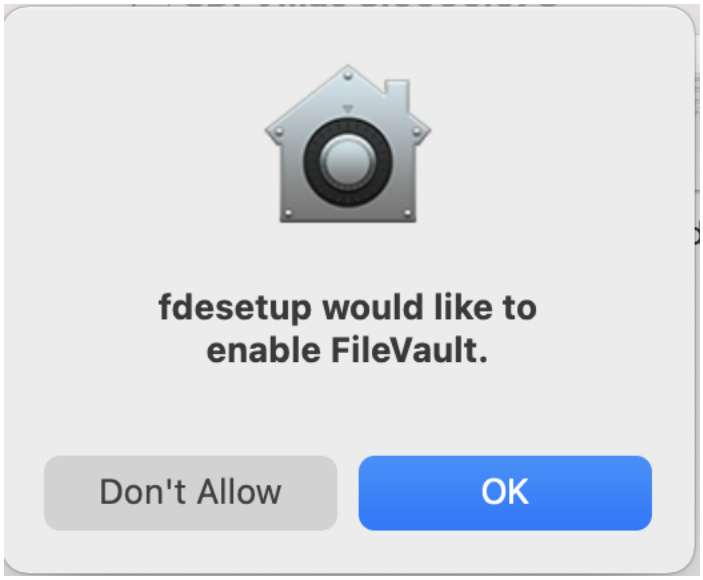
Options the user may use, and their behaviors, are as follows:

- Submit: Will submit the form and proceed with the next step.
- Cancel (by clicking on the red button at top left): Application will stop and resume on the next login cycle; SDForm will be displayed again.



If desired, the user may add or alter information in the SDForm panel (such as Location) but since device information will be derived from the device, and user information will be automatically derived from the logged in user at a later point, most users will simply click "Submit".

When installing on macOS Catalina onward, a message will appear, prompting you to enable FileVault (as in the image below). You must click OK on this message to enable FileVault.



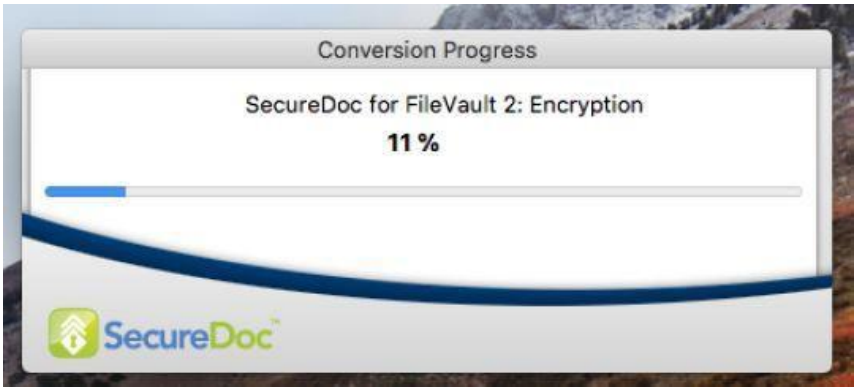
NOTE: If the prompt above is not responded to quickly enough, SecureDoc will automatically reboot the device, and then the user needs to type in password again to enable FileVault 2 (as in the "Current Account Password" image shown previously.

The SecureDoc icon will now appear in the system tray

Note: In the image above, the SecureDoc "Lock" icon appears in gray with a diagonal stroke through it, indicating this device is not yet fully encrypted.

NOTE: IF the device contains a disk drive that is NOT formatted as an APFS Container disk, macOS will require that the device be rebooted. A message will appear "FileVault 2 is already enabled. SecureDoc will start encryption after restarting your computer". This message will countdown and then automatically trigger the device reboot. See image below.

A progress bar may appear (if so configured) to indicate the progress of initial device encryption, as in the image below.



5. The device will now progress through initial encryption. Once encryption is finished, the SecureDoc icon in the system tray will be displayed in solid black, as in the image below.

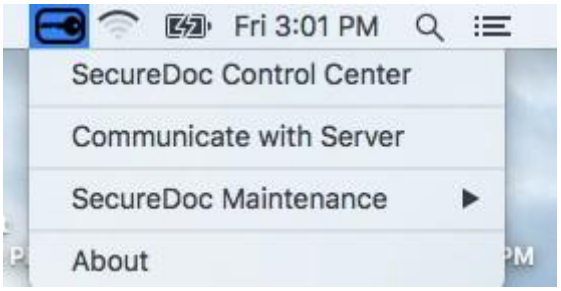
Note: In the image above, the SecureDoc "Lock" icon appears in solid black, without a diagonal stroke through it, indicating this device is fully encrypted – compare to the earlier image on a previous page.

SDFV2 Installation is now complete, and the device is fully protected.

This ends the section on installing SecureDoc for FileVault 2

Using the SecureDoc Control Center on macOS device

The SecureDoc Control Center is launched by clicking on the SecureDoc key-like icon in the macOS menu bar, and then selecting SecureDoc Control Center from the drop-down menu that will appear (as in the following image).



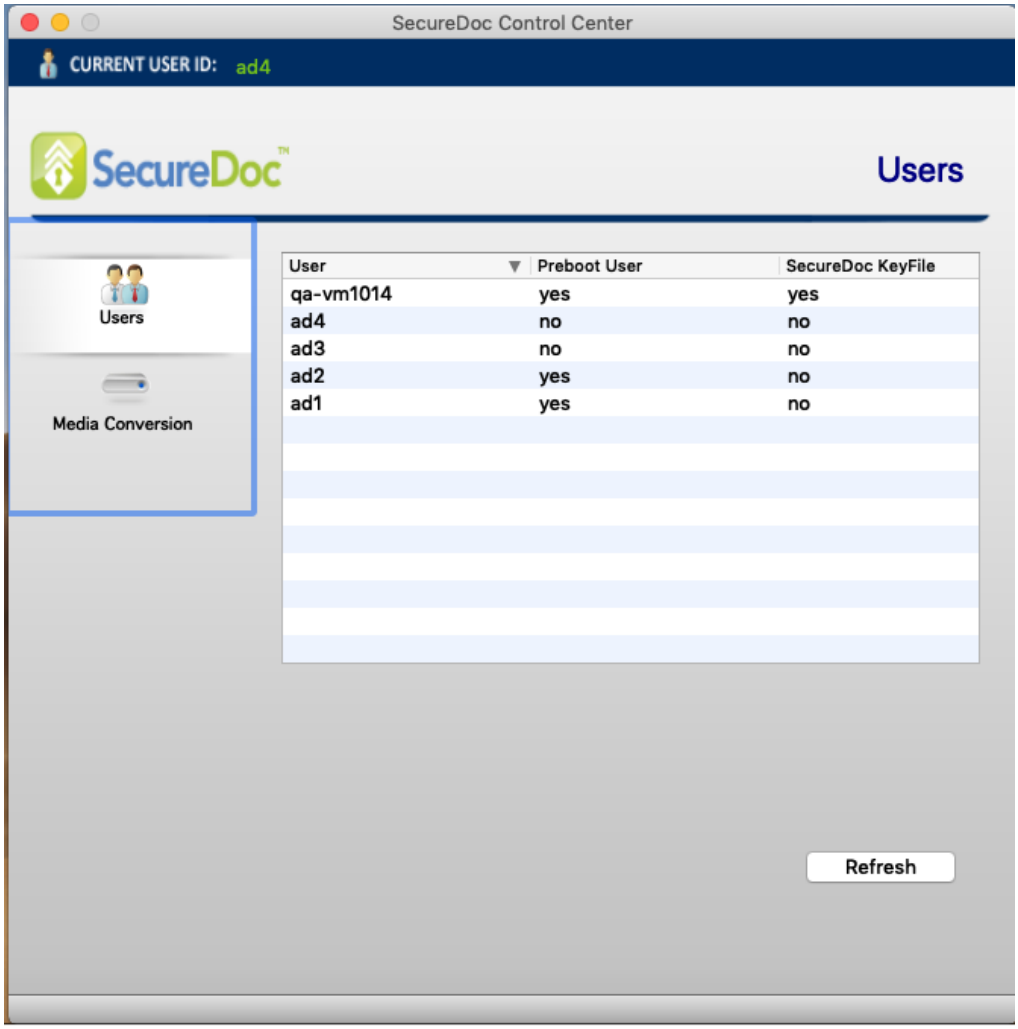
- There are 3 other options:
  - **Communicate with Server** option send and retrieve information from SES
  - **SecureDoc Maintenance**
    - To view logs
    - To collect SD Logs for troubleshooting and investigation.

  - **About**
    - View SecureDoc version information

The SecureDoc Control Center contains information in the "Users tab" and the "Media Conversion tab".

Users Tab

The Users tab lists the users who have accounts on the computer, and looks like the image below.



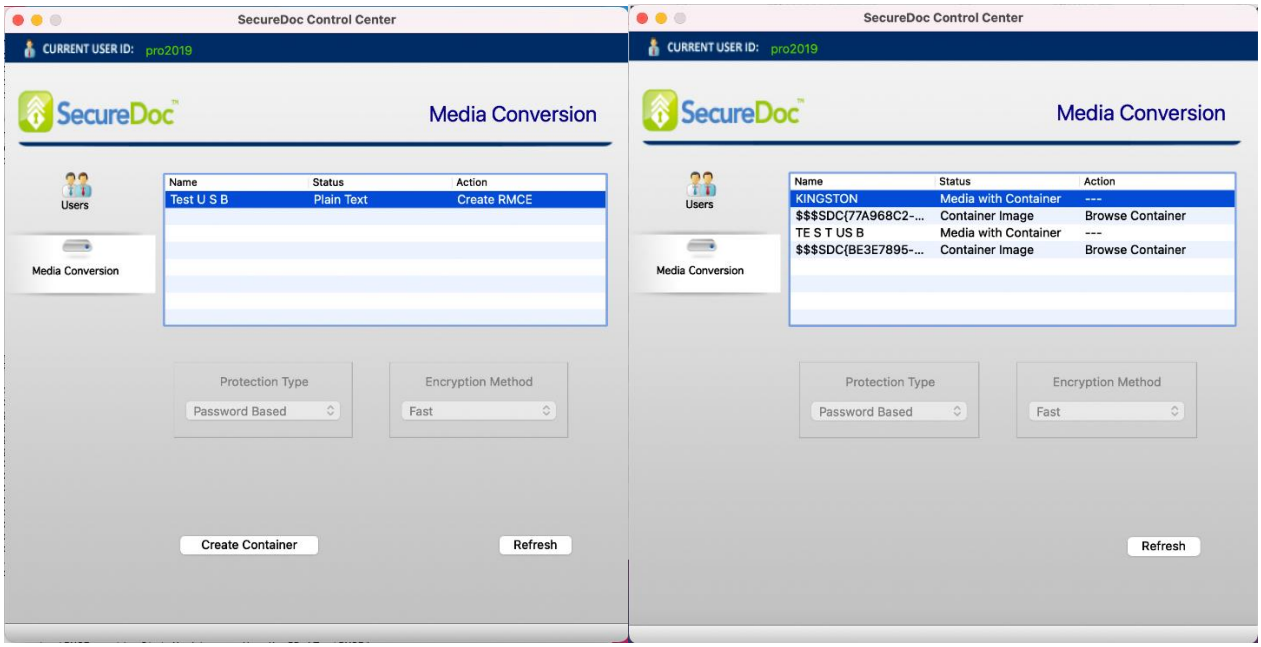
If the following conditions are not met, SecureDoc will need to communicate with SES to retrieve the appropriate information:

- User has not yet been added to device thru SES
- The user requires a keyfile from SES
- The user requires a password for the keyfile

Media Conversion Tab

Removable media is a general term for USB memory sticks, external disk. In previous versions these could be encrypted using RME (Full Media Encryption), but in this version and going forward, the only way to protect such media is through RMCE – Removable Media Container Encryption.

The tool (or app) now used to create RMCE-protected media is called RMCE_Manager



The Media Conversion tab lists the removable media currently attached to the machine. Each will have a status indicating whether:

Status	**Description**
Plain Text	The removable media is not encrypted.
Create RMCE	If the removable media status is “Plain Text”, SecureDoc will allow to perform create RMCE action on it.
Media with Container	The removable media contains a container, which allows a specific set in the removable media to be encrypted. This option is listed in conjunction with "Protected by Password".

Regarding the other two other controls on the screen:

- Protection Type is hard-configured to show Password (all RMCE Media is password-accessible)
- Encryption Method is hard-configured to be Fast.

To refresh the display (for example, when new media is inserted), click **Refresh**.

For information on media encryption, please refer to the SES main documentation.

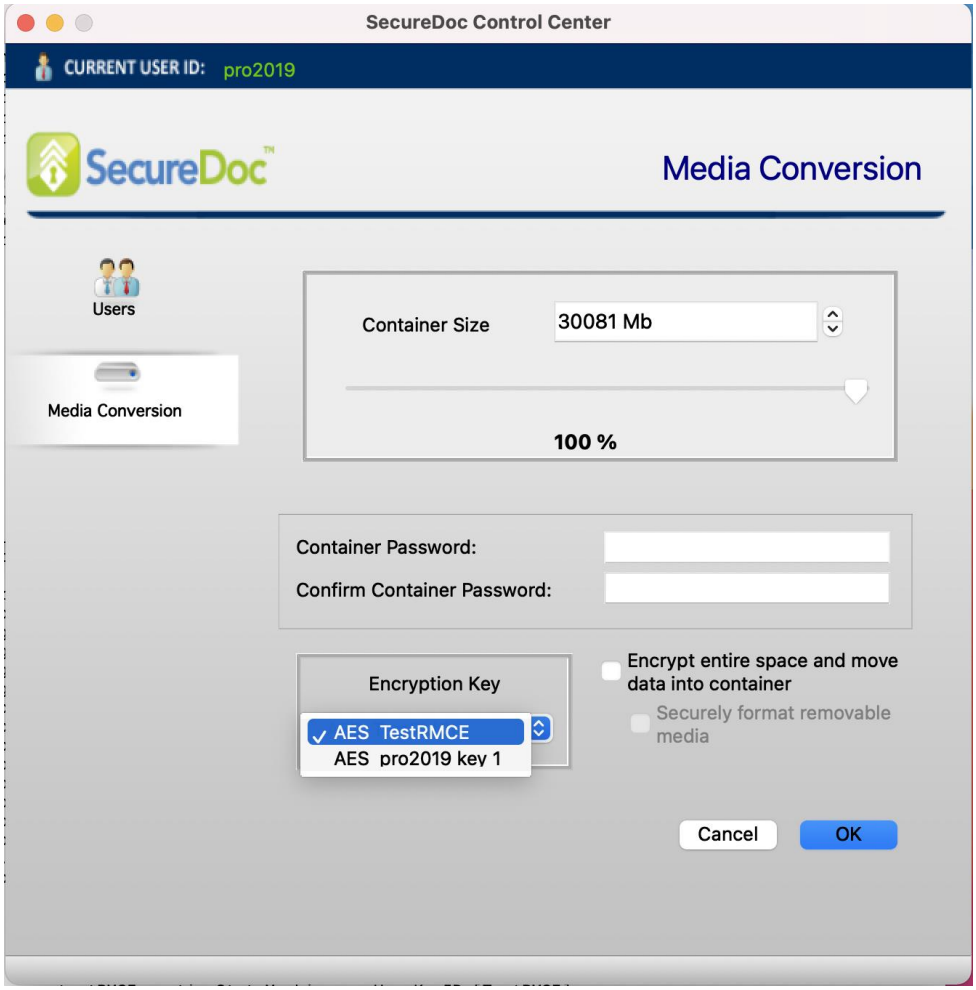
The following will show the available buttons for each status.

Plain Text

If the removable media has a Status of, "Plain Text", the following options are available (see image following text):

- Create Container - This will create a container within the removable media. Data can be placed within the container, and it will be encrypted. The defining feature of creating a container is that encrypted removable media can be used on machines that do not have SecureDoc installed. This is done through the RMCE Viewer which is packaged together with the Container in the Removable Media.

After clicking on the Create Container button, it will show the following dialog:



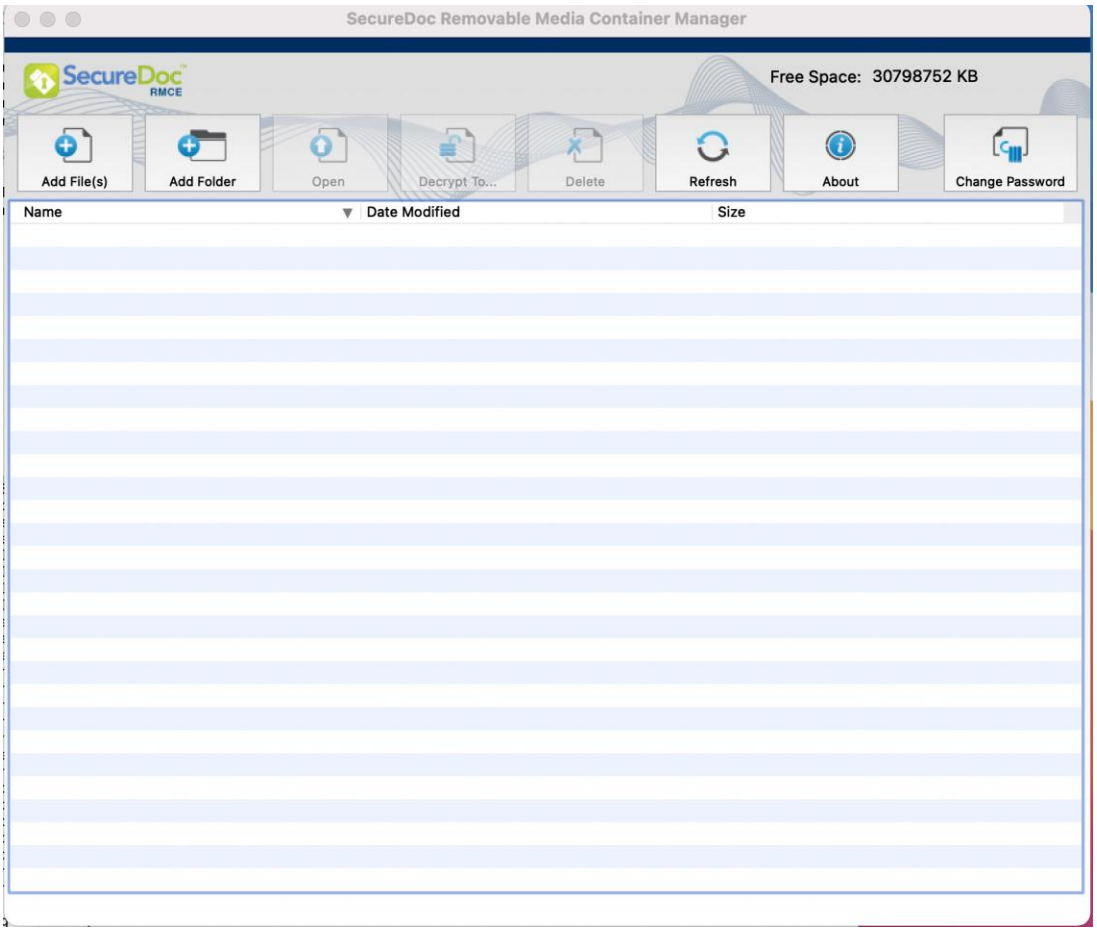
There are two modes that can be used with Removable Media Container Encryption

1. You can create an EMPTY container:

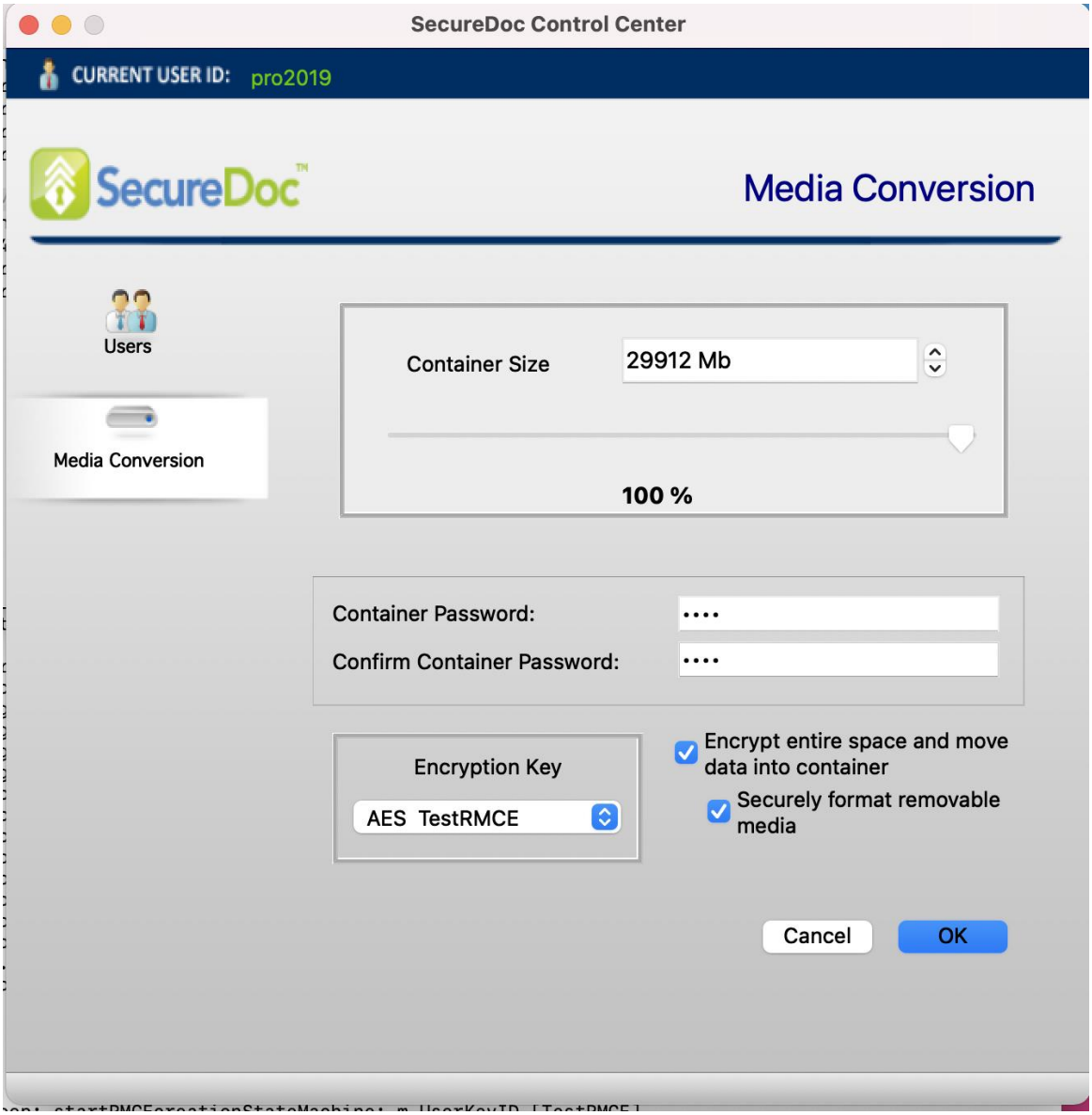
After providing values for "Container Password" and "Confirm Container Password", if no other options are defined the RMCE process will begin and it will create an EMPTY encrypted container.

This process will display the following progress bar:

After this process has completed, it will call the RMCE Manager application to open the empty container, permitting you to add files and/or folders to the container.



2. The other mode is to create a container using an item of Removable Media that already contains files and/or folders. This option will a) safely set aside the files/folders, and will then b) create the container and c) automatically move all the original content files/folders back inside the container:



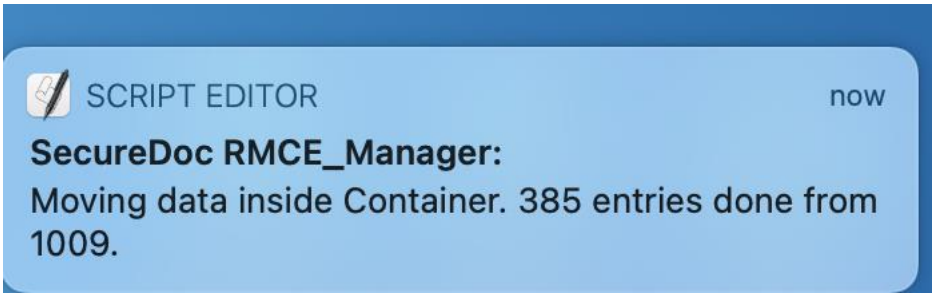
As in the first case, you must enter values for the "Container Password" and "Confirm Container Password" fields.

This time, however, select "Encrypt entire space and move data into container". In case the data you last stored on this item of media was of a particularly sensitive nature, you may wish to select "Securely format removable media".

Click OK.

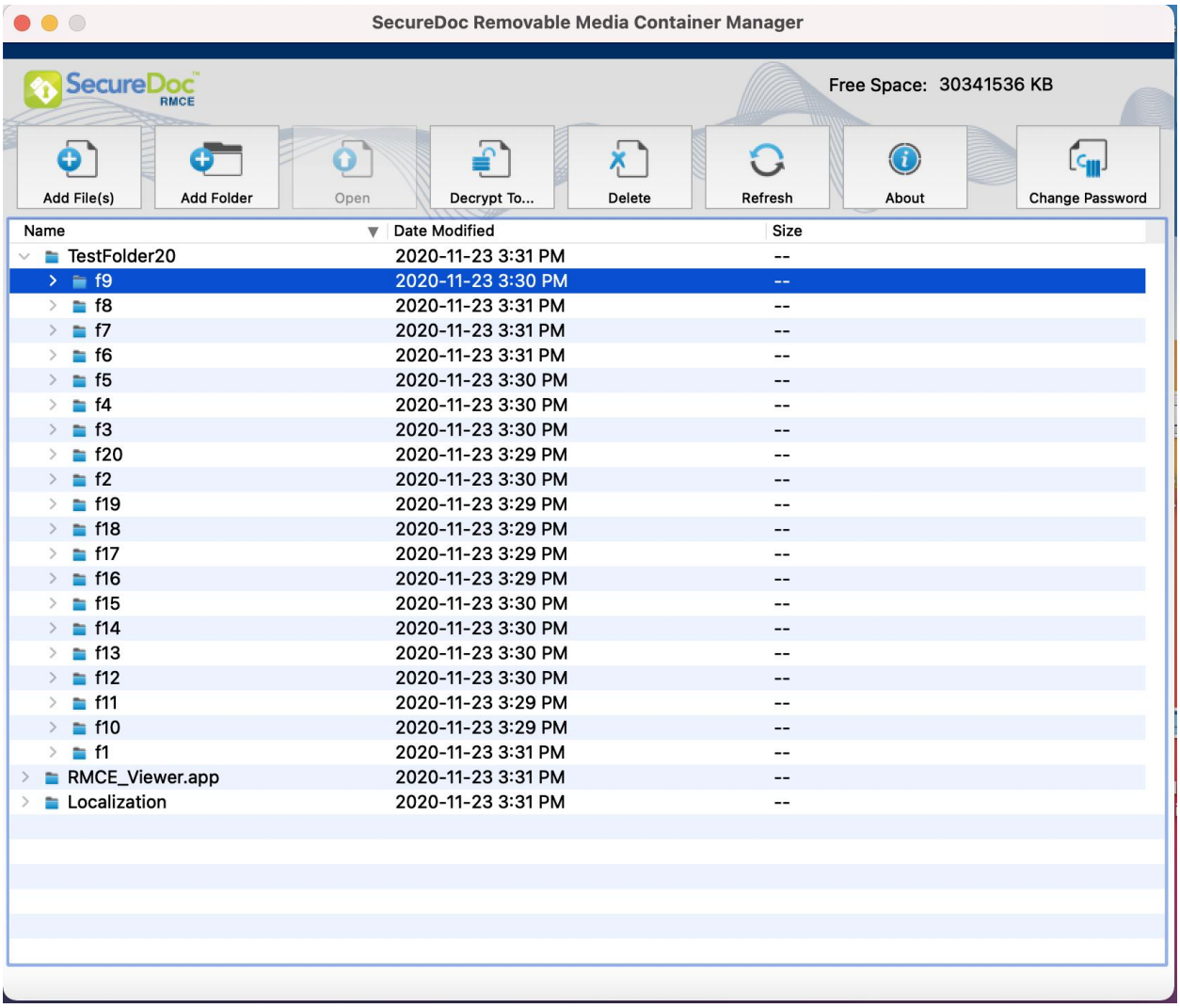
The process will begin, displaying the following progress bar:

After the above progress bar has completed, leave the media connected. The following "balloon" notification will appear:
Depending on the number of files or their size, this balloon message may take a full minute to appear as it calculates the work to be done in moving the files back into the Container.



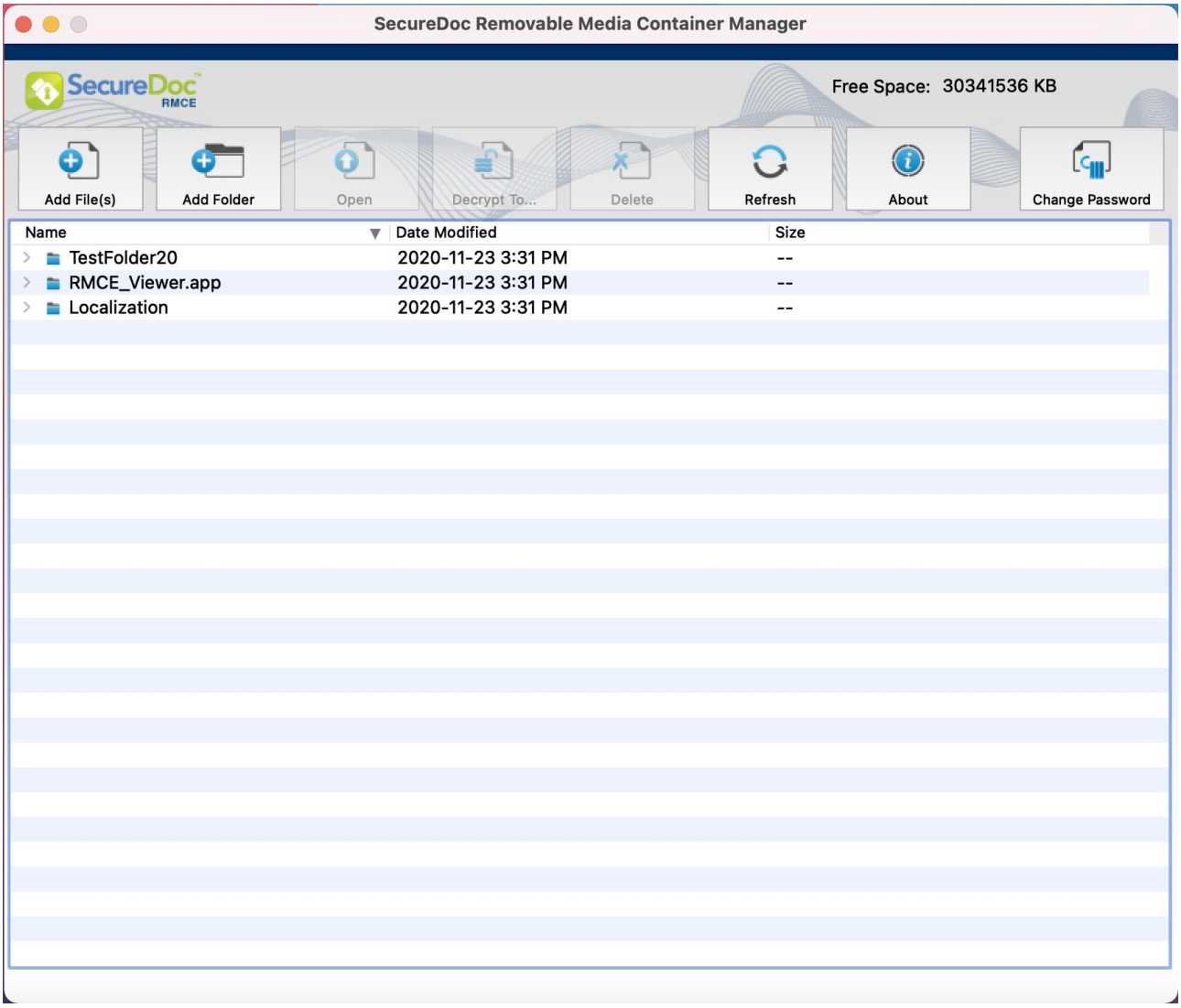
The above message will update to reflect the number of files moved.

After all data has been moved inside the container, the RMCE Manager application will open the container automatically, displaying the contents, as in the image below.

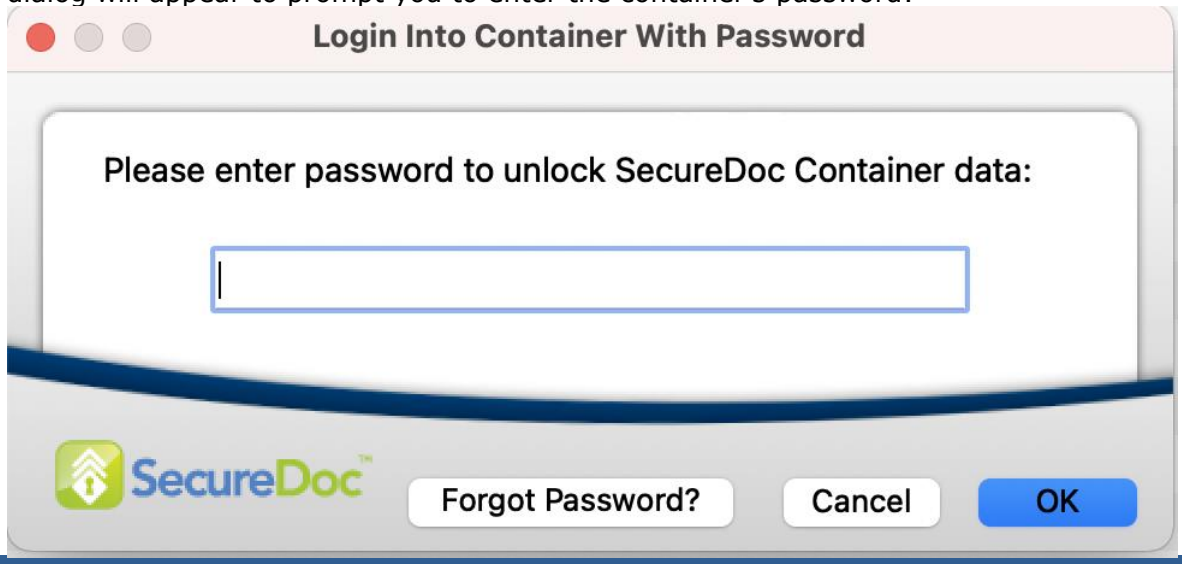


Ways to access container data:

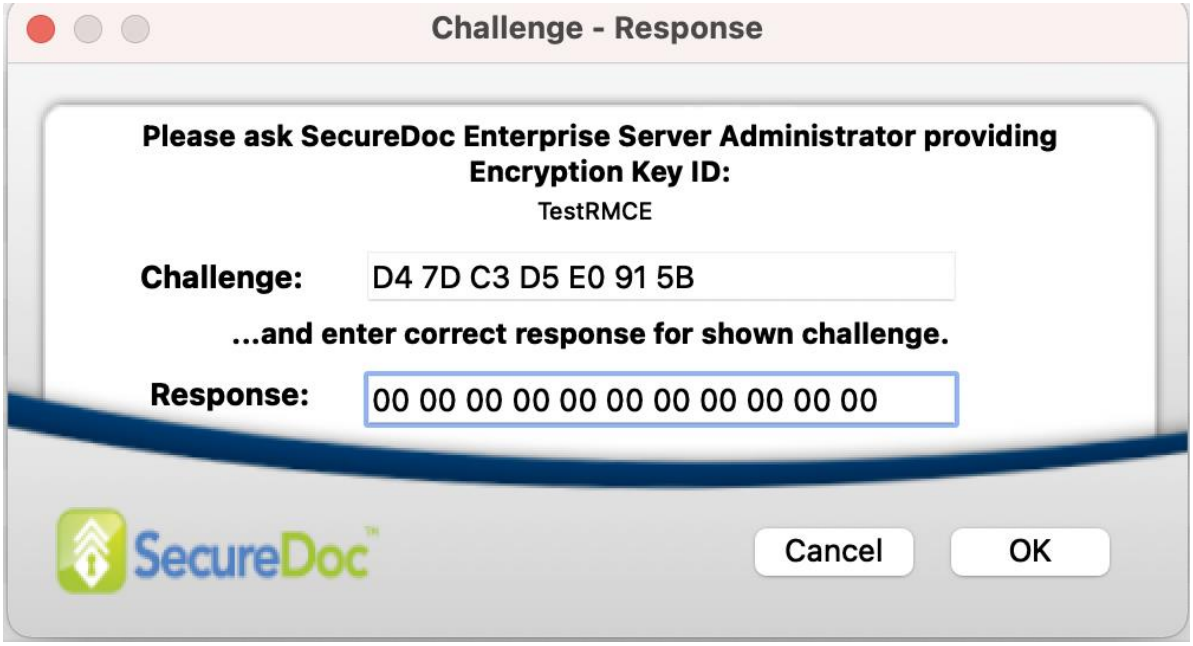
1. Insert an item of removable media into your device, if your logged in Key File contains the key which was used to create the container, RMCE_Manager will open the container automatically.



2. If your logged-in key file doesn't contain the Key used to protect the container the following dialog will appear to prompt you to enter the container's password:



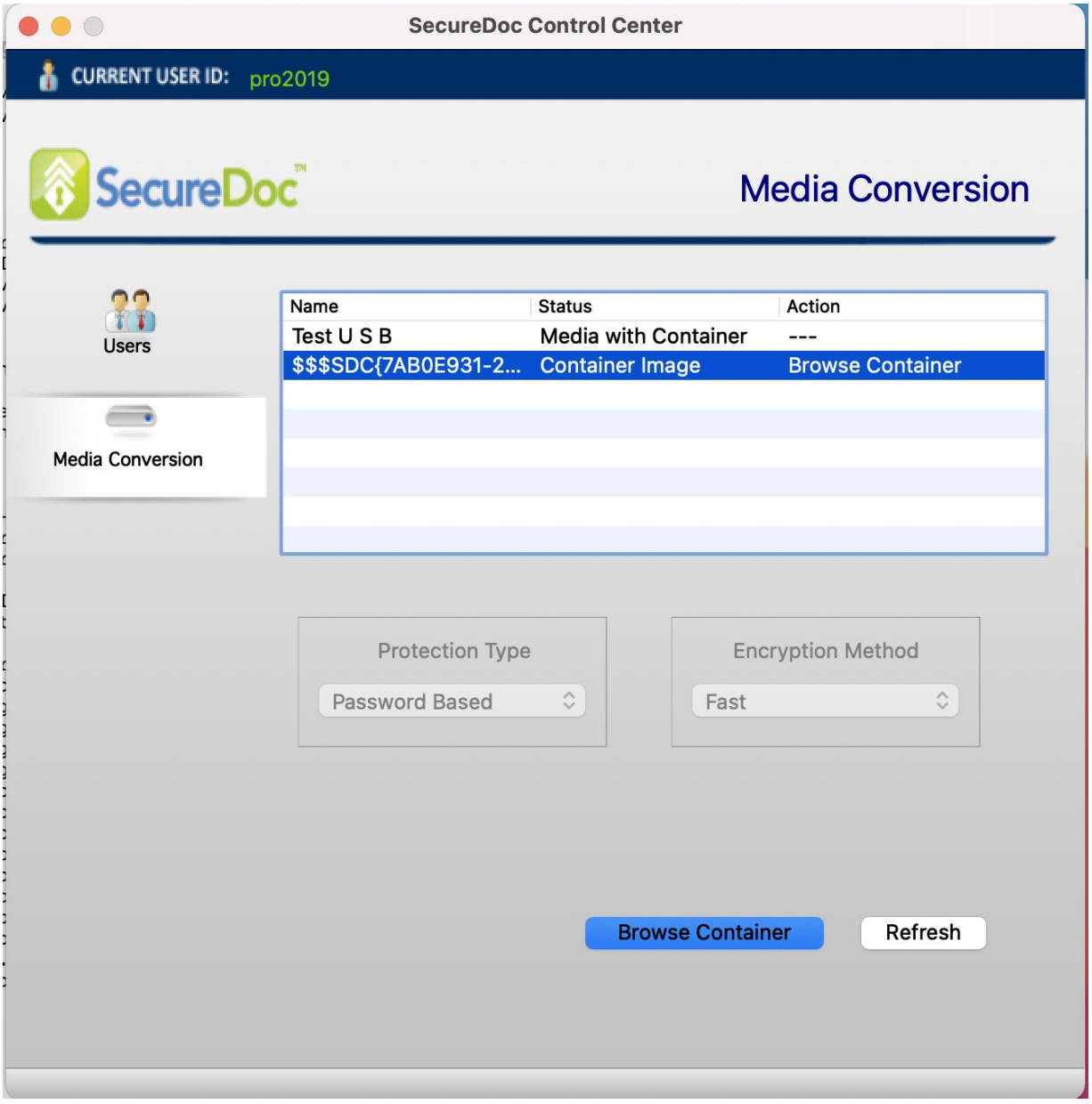
If you have forgotten the container password, you can perform Challenge/Response Recovery (with the assistance of an SES Administrator or HelpDesk user that has this functionality). To access Challenge/Response Recovery functionality, click on the Forgot Password button.



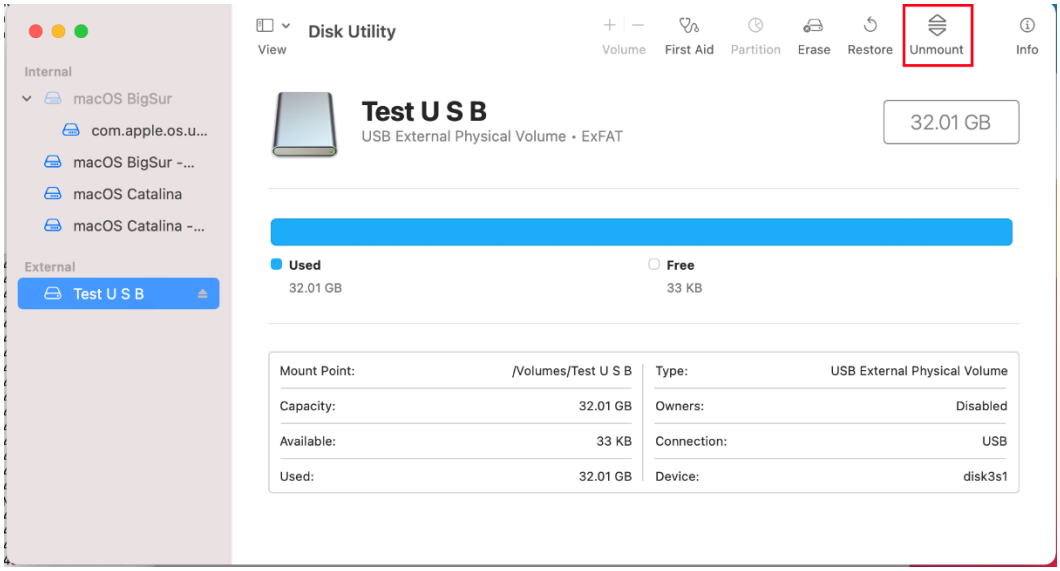
Contact your SES Administrator / HelpDesk, providing them with the Challenge String that appears. They will provide you with a Response String. After entering the correct Response string, RMCE_Manager will automatically open the container.

Two ways to re-open a container:

1. Keep removable media inserted into device, go to SecureDoc Control Center (SDCC) and click on the Browse button



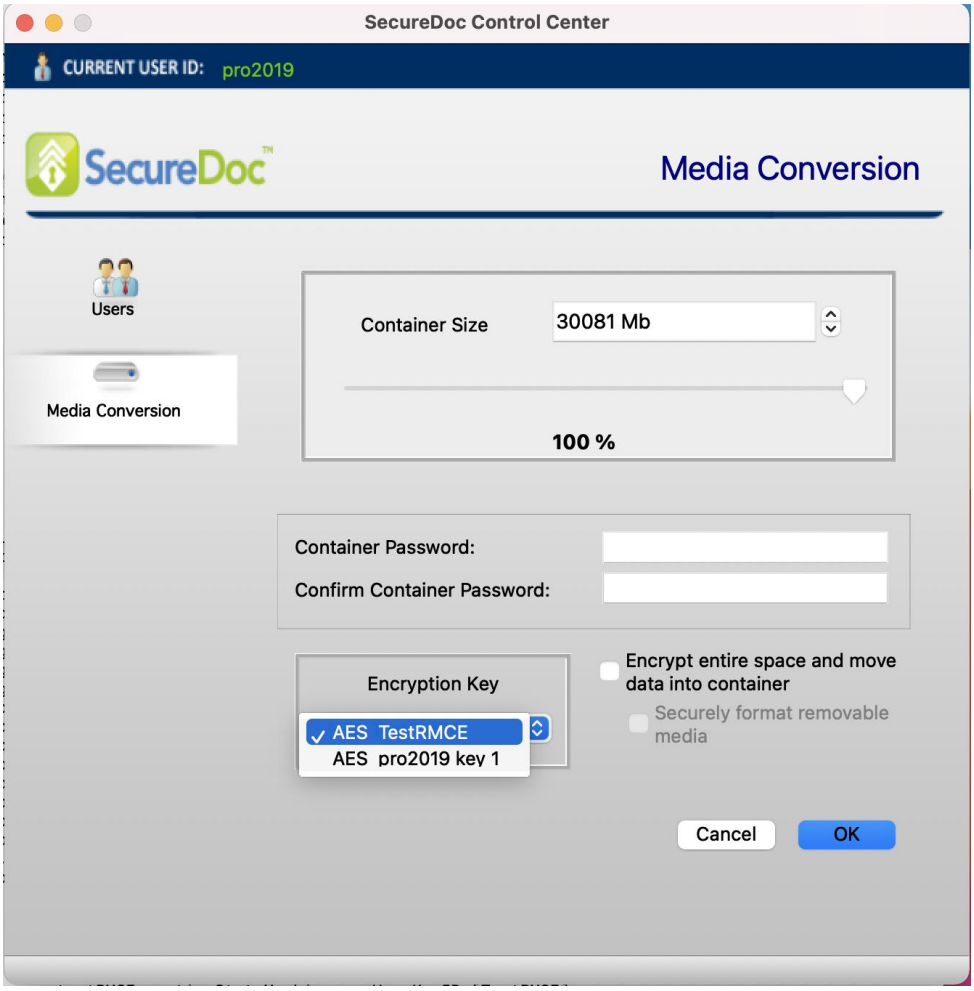
2. Use Disk Utility to Unmount and then mount the removable media again, or Eject the removable media and re-insert it. SecureDoc will automatically detect the reconnection of the removable media and will open the RMCE_Manager.app to open container



Altering Container Size in existing Removable Media

If you wish to alter the size of a container (or redefine the percentage of the media it occupies)

1. Re-mount the media
2. In the SecureDoc Control Center, change the media size values
3. Enter and confirm your password for this item of media
4. Click OK



The container will automatically be re-sized.

If you request a size that is smaller than the amount of data inside the container, a message will indicate you cannot re-size downward to the requested size.

Additional Security Considerations

Prevent additional users from being added to FV2 unlock list by System Preference

1) On the Mac device, open System Preferences -> Security & Privacy
2) Click on the **FileVault** tab
3) Click on the Lock icon on the bottom left corner and authenticate to make changes
4) Click on "**Enable Users…**"
5) Click on "Enable Users…" for the users you want to allow FV2 logon at FileVault's Native authentication.
    a. Enter their respective passwords
6) Click on **Done**
7) Restart the Mac Device; the added user may not appear in the File Vault2 preboot login page

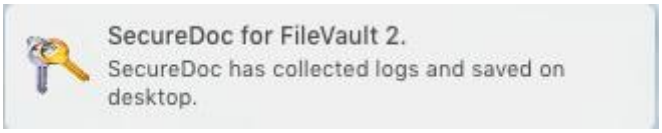
To report issues with SecureDoc on your Mac Device

When reporting client device problems, you may be asked to gather Log and other information from the device for analysis by WinMagic's Support team.

To report problems please do the following:

1) Collect logs
    a. Click on the SecureDoc icon in the system tray

    b. Click on **Collect SD Logs**
    c. The following prompt appears and logs will be saved on the desktop



    d. Please provide the foregoing file to your WinMagic Support member with the following information
        i. Subject : Your issue description and Case number
        ii. Your contact information (company name, user name, telephone#, etc)
        iii. Short description of the problem
        iv. How to reproduce it and/or under what circumstances the problem arose.
        v. Attach logs in step A above.

To Un-install SecureDoc from the SES Console

SecureDoc and FileVault 2 protection can be removed from a User Device through a Remote Command that can be triggered from the SES Console.

Included here for the SES Administrator's reference: This option is entitled "Uninstall SecureDoc". The option becomes available to the SES Administrator by right-clicking on a macOS device in the Devices tab, and selecting this option from the pop-up menu that will appear (the option appears near the bottom of the list of menu options, as in the image below). This option is covered in greater depth in the SES User Guide.

- Note: Use of this option is silent; The user on the client device does not need to do anything. Upon next connection with SES, the client will receive this command and will silently remove SecureDoc and disable FileVault 2, without requiring the user to confirm or otherwise interact with the un-installation functionality.

Enabling Users to uninstall SecureDoc from the Mac device

To permit a User to uninstall SecureDoc from the Client side, the Device Profile that is active on the device must contain a specific option that permits this.

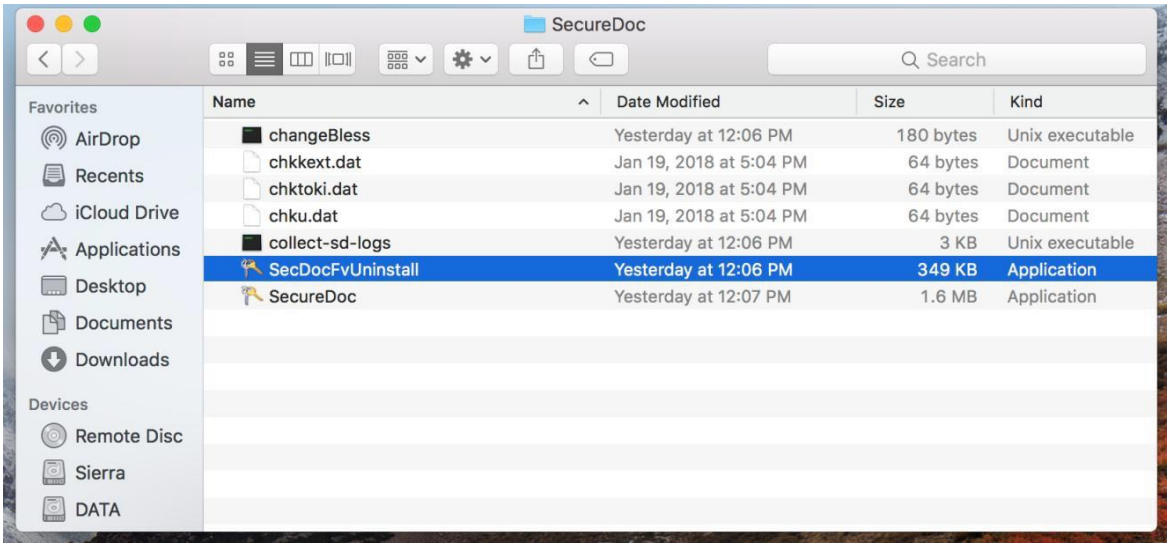
Included here for the SES Administrator's reference: The specific option (defined by the SES Administrator in the Device Profile) is entitled: "Allow SecureDoc uninstall by SecureDoc user with admin rights or local administrator".

This option is described more fully in the SES User Guide.

To Uninstall SecureDoc from a Client Device

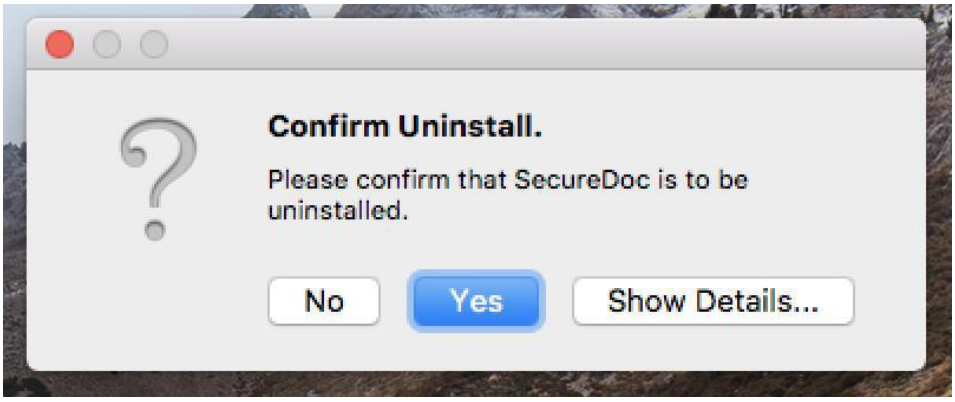
This section pertains to uninstalling SDFV2. If you have any devices still running SecureDoc V8.2 using SDOTFV2, please follow the instructions in the next section.

Step 1: Find the Uninstall application SecDocFvUninstall.app through Applications->WinMagic->SecureDoc



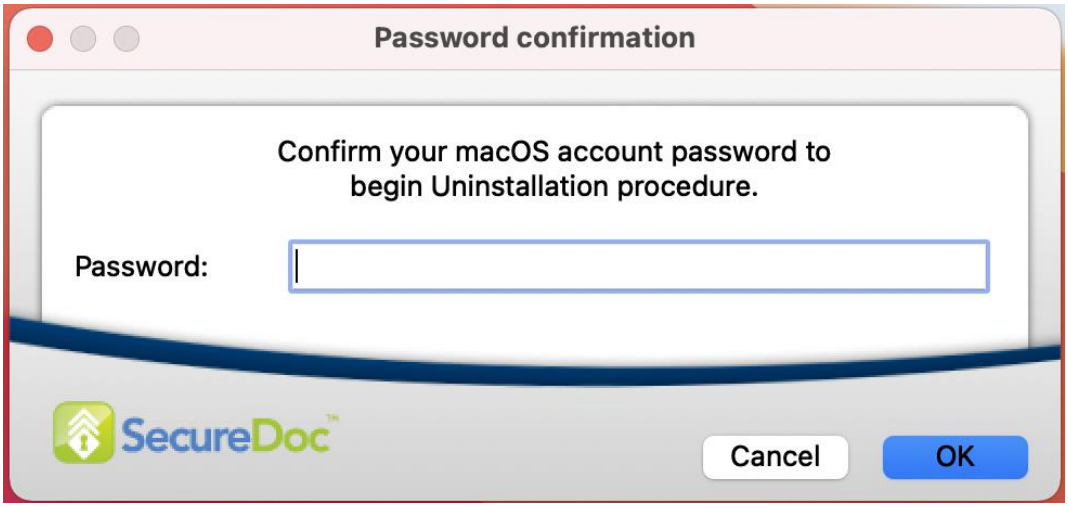
Step 2: Double-click on SecDocFvUninstall

A confirmation dialog box will appear, as in the image below:

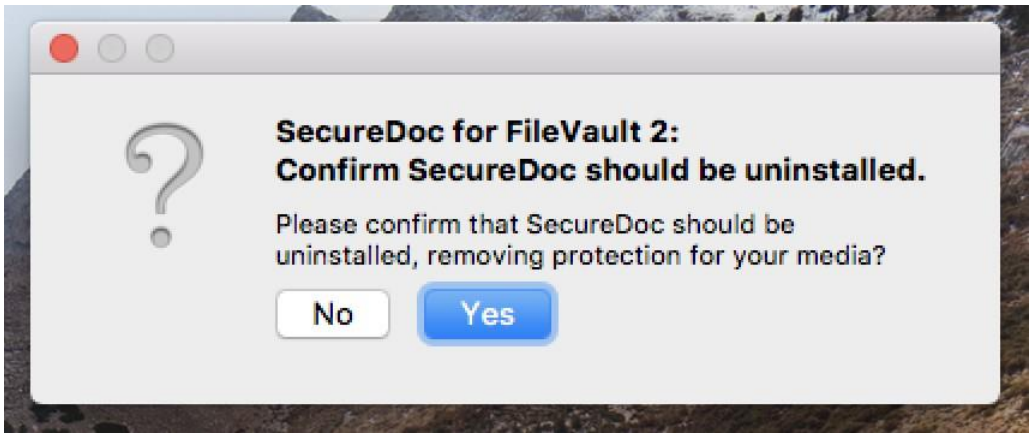


Step 3: Click on the Yes button, as in the image above.

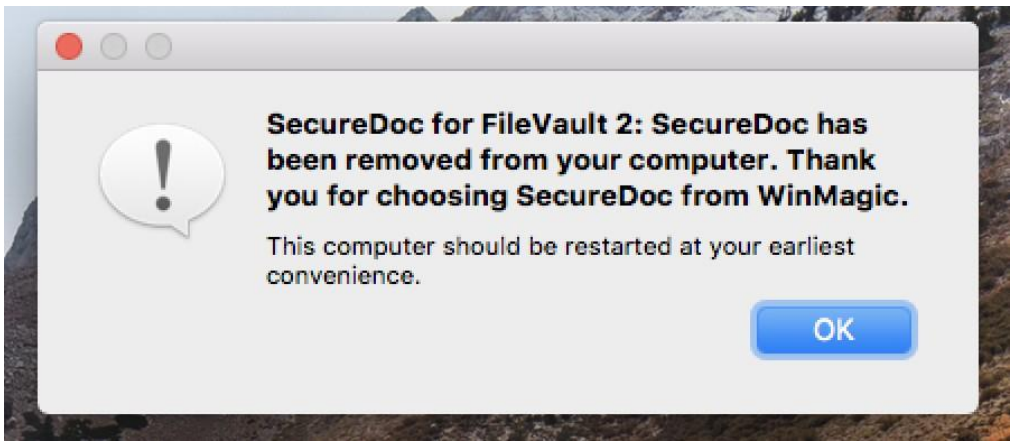
Step 4: A confirmation prompt message box will appear (as in the image below), asking you to provide password to uninstall SecureDoc.



Step 5: After providing password and click on OK. A confirmation prompt message box will appear (as in the image below). Click Yes to continue uninstallation.



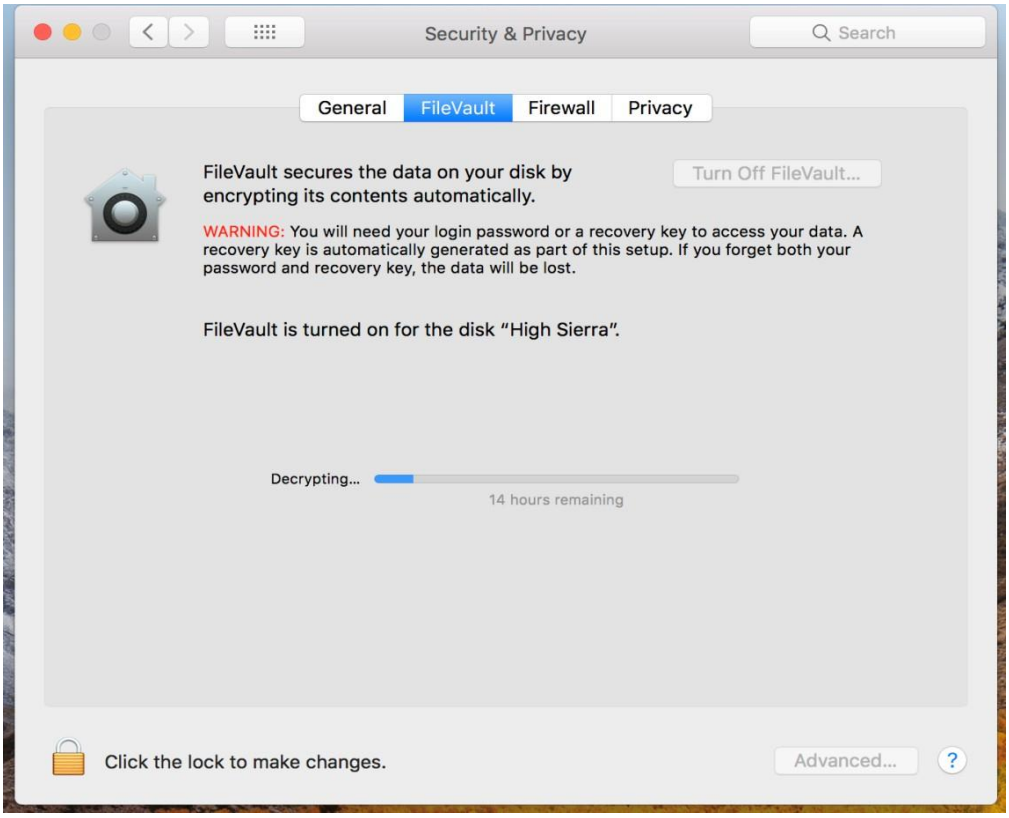
Step 6. Click OK to complete the un-installation of SDFV2



- All SecureDoc-related application components and folders will have been removed from

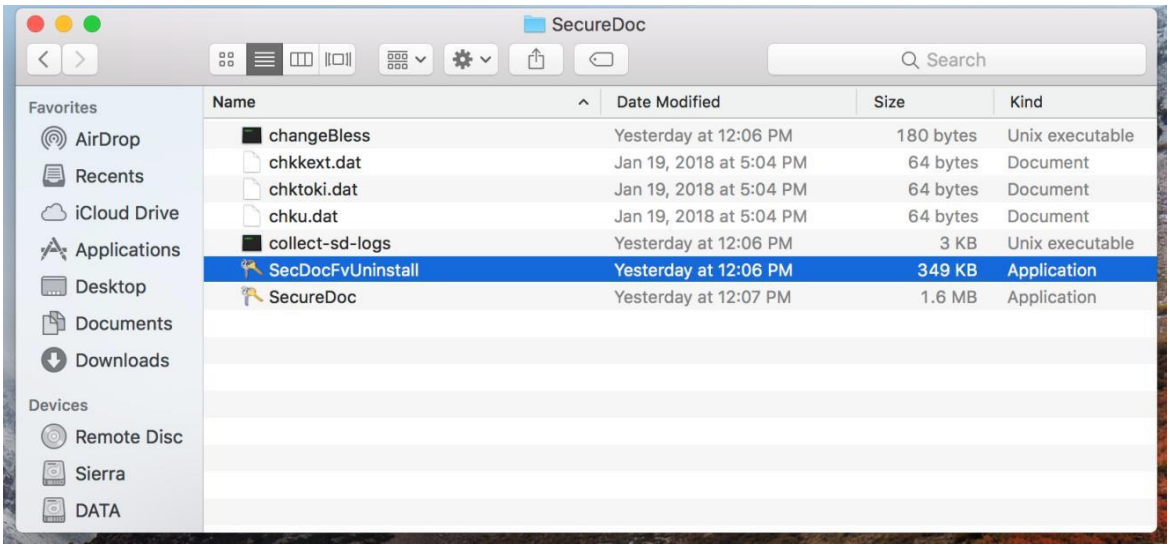
the device.

Users can see the progress of the decryption of the device drive from the Security and Privacy Panel, as in the following image. During the decryption process, this device will appear in “Decrypting” status on the SES Console and in the SESWeb console.



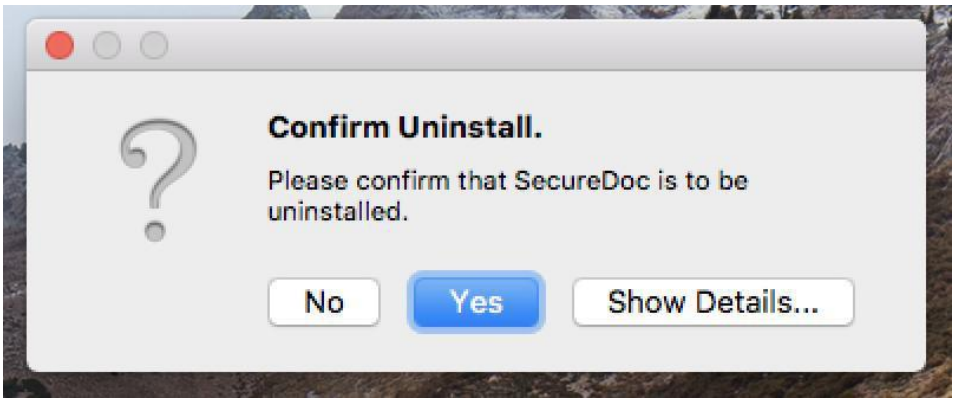
To Uninstall SecureDoc SDOTFV2 from a Client Device – applies to V8.2 or earlier

Step 1: Find the Uninstall application SecDocFvUninstall.app through Applications->WinMagic->SecureDoc



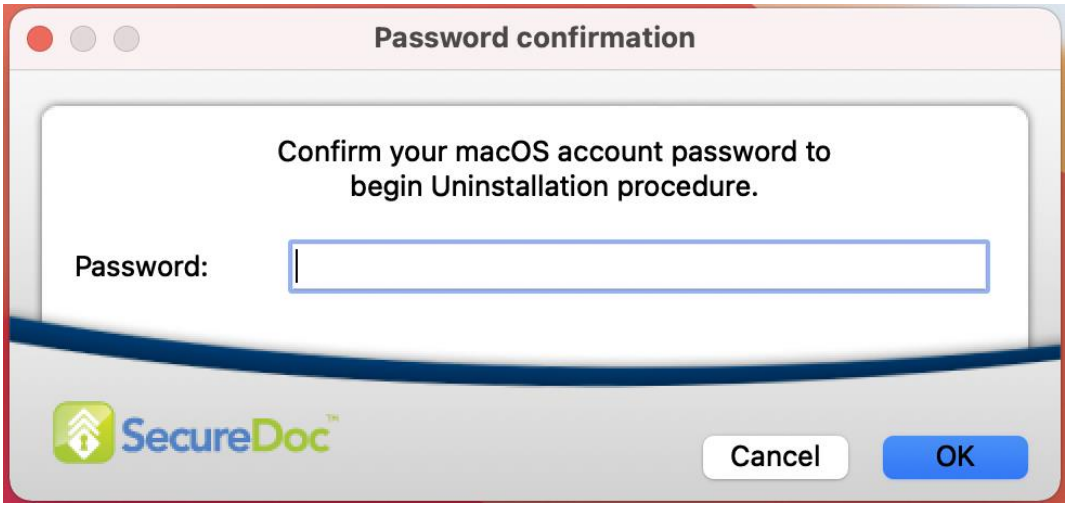
Step 2: Double-click on SecDocFvUninstall

A confirmation dialog box will appear, as in the image below:

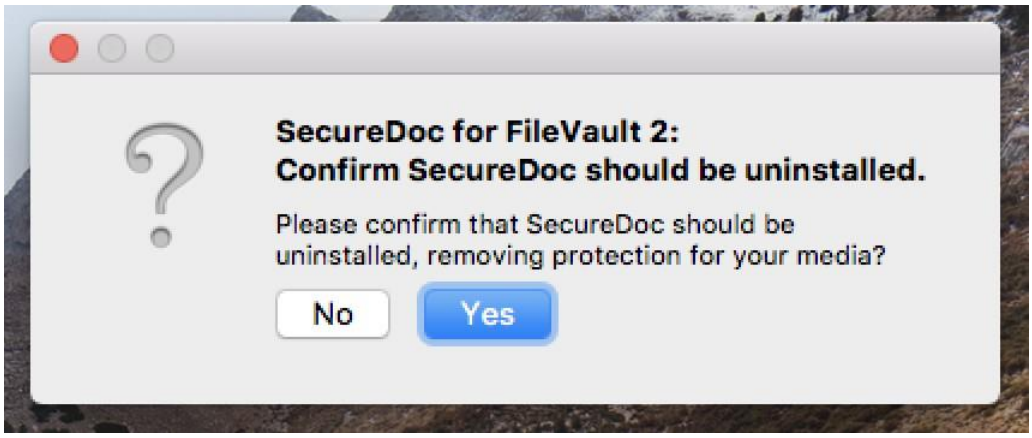


Step 3: Click on the Yes button, as in the image above.

Step 4: A confirmation prompt message box will appear (as in the image below), asking you to provide password to uninstall SecureDoc.



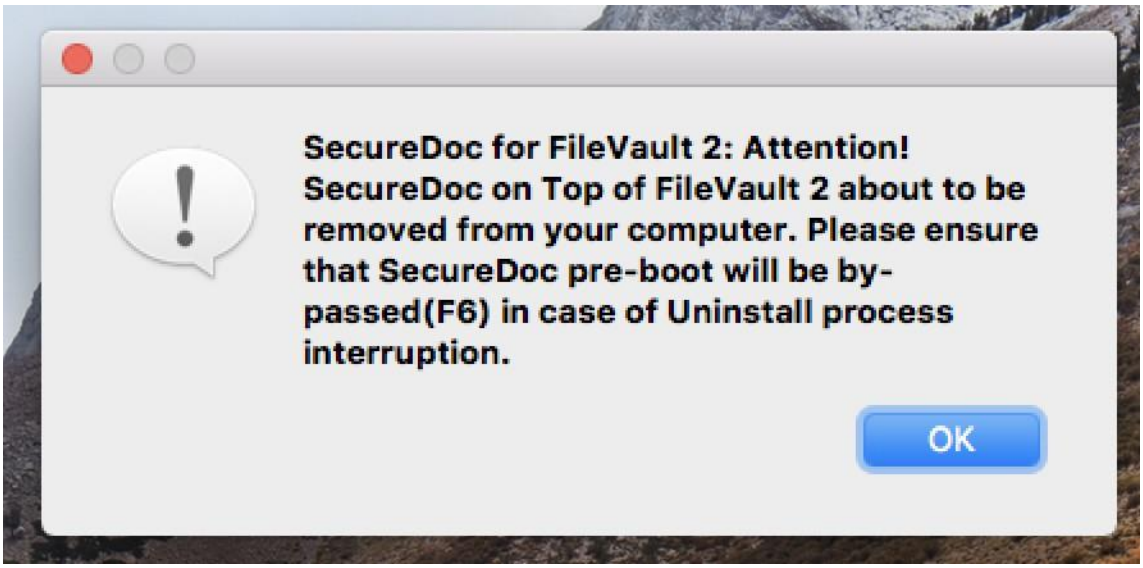
Step 5: After providing password and click on OK. A confirmation prompt message box will appear (as in the image below). Click Yes to continue uninstallation.



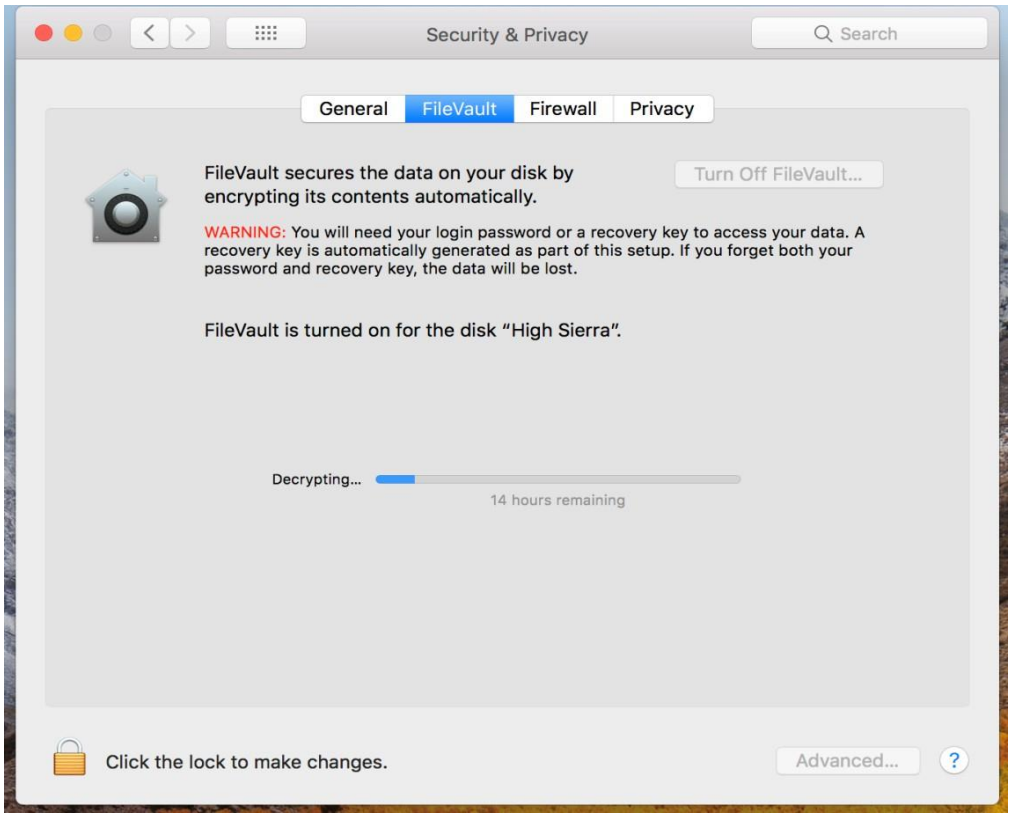
NOTE: Only if the device had been installed using SecureDoc's Pre-Boot for File Vault 2 devices (SDOTFV2) will an additional prompt panel appear, as in the following image.

Step 5B – Re-Enter your password, and click OK, as in the image above.

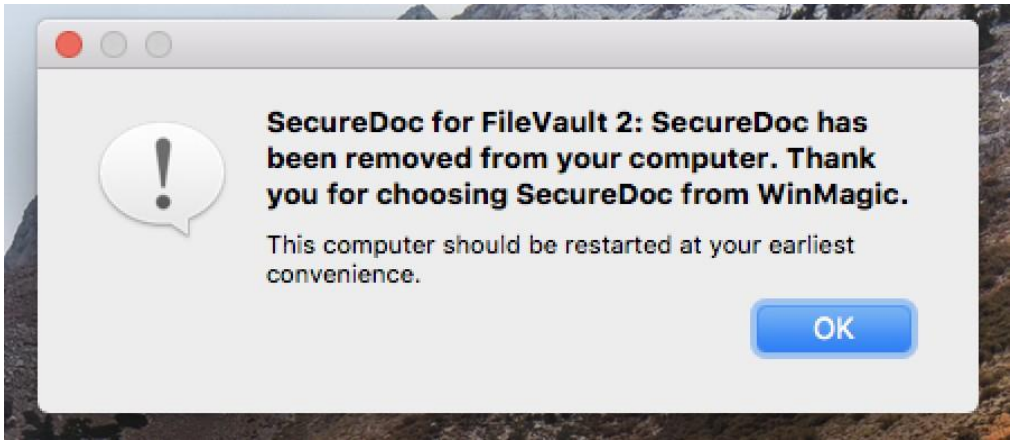
Step 5C – an additional message box will appear (as in the example below), clarifying that SecureDoc on Top of FileVault 2 is about to be removed. Click OK to continue. The lower part of this message box reminds you that you may need to use F6 to bypass the SecureDoc Pre-Boot if the un-installation process is interrupted or does not complete successfully.



Users can see the progress of the decryption of the device drive from the Security and Privacy Panel, as in the following image. During the decryption process, this device will appear in "Decrypting" status on the SES Console and in the SESWeb console.



Step 6. Click OK to complete the un-installation of SDOTFV2 for clients running V8.2 or earlier.



- All SecureDoc-related application components and folders will have been removed from the device.