SecureDoc for Apple FileVault2

Beta setup Manual
About SecureDoc for FileVault2

©Copyright 1997 - 2016 by WinMagic Inc. All rights reserved.
Printed in Canada

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
5600A Cancross Court
Mississauga, Ontario, L5R 3E9
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 Cloud Lite editions, with edition-specific features clearly labelled. 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.
Contents
About SecureDoc for FileVault2 ....................................................................................................................1
SecureDoc PreBoot for FileVault2 Introduction ..............................................................................................2
  SDOT FV2 Features .........................................................................................................................................2
  SDOT FV2 Limitations .......................................................................................................................................2
  Supported Environments and hardware .........................................................................................................3
Setting up the Environment ..................................................................................................................................4
  Installing SDOT FV2 on client devices ...........................................................................................................11
Using the SecureDoc Control Center on Mac device .......................................................................................15
  Users Tab .......................................................................................................................................................15
  Media Conversion Tab .....................................................................................................................................17
Managing SDOT FV2 devices from SES Console ...............................................................................................18
  Viewing SDOT FV2 information on SES Console ..........................................................................................18
Testing new functionality ....................................................................................................................................21
  Smartcard authentication at PreBoot .............................................................................................................21
  Network authentication at PreBoot ...............................................................................................................22
  Prevent additional users to be added to FV2 unlock list .............................................................................23
  Challenge and response password reset ....................................................................................................23
To provide feedback or to report issues with this Beta ......................................................................................24
About SecureDoc for FileVault2

SecureDoc for FileVault2 securely manages FileVault2 for your Mac computer (desktop or laptop). When the device is under management, SecureDoc's pre-boot authorization window (boot logon) appears each time you start the computer. At this window you must enter a SecureDoc credentials to complete the authentication and gain access to the encrypted data on your Mac. SecureDoc for FileVault2 can also be used to encrypt and decrypt USB flash drives, protecting them with either a password or a key.

The purpose of SecureDoc working with FileVault2 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 do two important things:

1) Allow them 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. FileVault2 will encrypt the hard-disk, but there is still a chance for the files to be accessed (if the password was taken)
      ii. Administrators need to know if FileVault2 is enabled or has been disabled, and SES monitor will allow for this

SecureDoc will have an agent which will allow it to talk with SES.
SecureDoc PreBoot for FileVault2 Introduction

This document explains the usage of SecureDoc PreBoot for FileVault2 (SDOT FV2) using the SES Management Console, as well as the local SecureDoc client application. SDOT FV2 is an advanced pre-boot authentication mechanism that provides strong authentication while enhancing ease of use.

SDOT FV2 Features

The following will explain the new features for SDOT FV2:

- **Two factor authentication with smartcards or tokens for FileVault2 enabled machines**
- **Authenticate with network accounts in SES and/or Active Directory at FV2 PreBoot**
- Prevents additional users being added to FV2 unlock list; only one account is used.
- Supports challenge and response at FV2 PreBoot for password recovery
- SecureDoc PreBoot will self-heal after major OSX upgrade (when the appropriate version is installed)
- Provides same PreBoot user experience across multiple platforms (Windows, Linux, Mac)
- Supports permanent autoboot
- SDOT FV2 requires a license. Currently, 10 licenses are automatically available for testing purposes in SES.
- Only single installation is required for all supported OSX.

SDOT FV2 Limitations

**NOTE:** Limitations will be resolved in future releases.

- Mac Mini is not supported at this time.
- On devices with multiple partitions, SDOT FV2 only supports installing and protecting on one of the (bootable) partitions.
- On OSX 10.11.x or newer, a manual step to disable SIP during installation and thereafter is required. We are working on resolving this limitation. For more information on SIP: [https://support.apple.com/en-ca/HT204899](https://support.apple.com/en-ca/HT204899)
- OSX 10.12 is NOT supported; currently under development.
- Only Thunderbolt to Gigabit Ethernet Adapters and WIRED Network adaptors that are built in to the device are supported for PreBoot Networking. Wireless and USB connected NICs are not yet supported.
SecureDoc PreBoot for FileVault2 Introduction

- The following 6 symbols in red are not supported for SecureDoc password '\', ',', '"', '\', '-', ':'. This will be fixed in the GA release. Installation will fail when these symbols are used.
- Local and remote Cryptoerase is not yet supported
- SDOT taking over FileVault2 management is not supported on OSX 10.9.5.
- With SDOT FV2 enabled, resetting NVRAM will cause SDOT to not function correctly. If this happens, SIP will need to be disabled so SecureDoc can Bless partition again.
- In rare cases, Finder might operate under incorrect permissions causing users unable to access their files. This can be resolved by restarting the Mac device, logout/login or restarting Finder. This issue is only reported on OSX 10.11.4 to 10.11.6.
- SecureDoc PreBoot for FV2 can only be enabled during installation time.
- NetBIOS name and FQDN are not supported as the SDConnex address used for PBN.

**Supported Environments and hardware**

**Supported Apple Operating System**

With SES 7.1SR4 HF3 and newer

- macOS Sierra 10.12

With SES 7.1SR4 and newer

- Mac OS x El Capitan 10.11 to 10.11.6
- Mac OS X Yosemite 10.10 to 10.10.5
- Mac OS X Mavericks 10.9.5

**Supported Apple Devices**

- MacBook 5.1 and newer
- MacBook Pro 5.5 and newer
- MacBook Air 6.1 and newer
- iMac 9.1 and newer

**Supported Smartcards for PreBoot Authentication**

- Gemalto CyberFlex Access 64k V2
- Gemalto 128k v2 (DOD CAC)
- Gemalto IDPrime.net
- Entrust PIV card
- Safenet Datakey 330 PDI Smartcard
- Oberthur ID-One PIV (Type A) Large D
- RSA SID 800
- HID Crescendo C1100
Setting up the Environment

1. Have SES environment setup already as per the quick deployment guide.
2. Login to SES Management Console
3. Click on Profile in the left pane. In the right pane, right click and select “Add Profile”
4. Add a “Mac FileVault2” profile
5. Enter a name for the profile. Eg. SDOT FV2.
6. Click on “General options”

7. Enter in the desired SDConnex server IP for communication. Netbios name and FQDN are not supported.
8. To test PreBoot Networking to support Network Login against SES or AD, please enable “Enable machine to communicate with SDConnex at PreBoot”
9. Click on “Advanced Options” in the left pane.
10. Enable "Enable FileVault2 as SES-Managed encryption mode for device"
11. Enable "Use SecureDoc PreBoot"
12. Click "OK"
13. Click "SAVE" to save this profile.
14. Click on "Installation Packages" on the left pane. Right click on the right pane and select "Add package". Select "Mac Filevault2" and click OK.
15. Give this package a name. eg. SDOT FV2
16. Click on “Browse” in the SecureDoc Profile Section and select the profile we create in step 13 above.

17. Click **OK** to save this installation package.
18. The installation package will now appear on the list. Right click on it and select “Browse package files”
19. A DMG file is created. This DMG will be used for installation on the client Mac device.
Installing SDOT FV2 on client devices

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

1. Copy the SDFVMac.dmg file onto the Mac device and mount it.
2. Open the mounted drive to display the installation scripts
3. Double click on “InstallMe” to start installation
   a. Please enter the password of the installing user with Mac Admin rights to continue installation.
Setting up the Environment

b. Enter in password of current Mac OSX user and click OK.

c. For OSX 10.11.x or newer, a manual step to disable the SIP might be required. User gets the message "Unable to Bless BOOT partition" and click "OK"
   i. Second message appears with instructions to disable nvram at recovery mode.
   ii. Click "OK" to automatically reboot the device
   iii. While rebooting press and hold command+R to enter recovery mode
   iv. On recovery mode Navigate to Utilities > Terminal
Setting up the Environment

v. run the following commands in terminal: csrutil enable --without nvram; reboot
vi. device reboots automatically
vii. Login to OSX

e. SecureDoc icon will now appear in the system tray

f. 

g. A countdown will appear once SecureDoc has communicated with the server to send back recovery information.

h. Click OK to restart computer immediately.
i. Upon restart, the SecureDoc PreBoot Authentication screen is displayed.
   i. Please enter in the User Name and Password (PIN if using smartcard authentication) then press RETURN.
j. Mac will now boot to the OSX user login screen.
k. Upon logon, SecureDoc Encryption Status bar is displayed.
Setting up the Environment

l. Once encryption is finished, the SecureDoc icon in the system tray will be displayed in solid black.

m. 

n. Installation is now complete. Device is fully protected.
Using the SecureDoc Control Center on Mac device

The SecureDoc Control Center is launched by clicking on the (SecureDoc icon) and selecting SecureDoc Control Center.

- 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, indicating which users have cached SD credentials to login at preboot, and whether or not they have a keyfile.

Under the PreBoot User column:
  - Yes
Using the SecureDoc Control Center on Mac device

- User has cached SD credentials to authenticate at SecureDoc PreBoot for Filevault2 and has a local Mac account.
- SDBoot-only
  - User has cached SD credentials to authenticate at SecureDoc PreBoot for Filevault2 only
- No
  - User only has a local Mac account and cannot login to SecureDoc PreBoot

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**

The Media Conversion tab lists the removable media currently attached to the machine, indicating whether the whole media is encrypted ("Media Encrypted"), a container on the media (two files will be listed "Media with Container" and "Protected by Password") or not encrypted ("Plain Text"). 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.
Managing SDOT FV2 devices from SES Console

Viewing SDOT FV2 information on SES Console

Changes on SES Console when a mac device is using SecureDoc PreBoot for authentication

1) Encryption Type will be **SDot FV2**

To view detailed device information, double click on the device. The device information window opens:
To view the recovery password for the device, click on "**View FileVault Properties**".

Password is displayed in a new window:

Viewing of this information is audited and a log is created in the Audit Log.
Managing SDOT FV2 devices from SES Console
Testing new functionality

Smartcard authentication at PreBoot

1) Open up SES console and add a new user
   a. Enter in User ID
   b. Select “**User key file(s) will be protected by token**”
   c. Select the appropriate “**User’s token type**” from dropdown.
   d. Go to the User X.509 certification section and click on “**Add**”
      i. Select the Public certificate for keyfile protection
   e. Click **Create**

2) Now assign this user to the Mac device
   a. Right click on the desired Mac machine under the Device pane
   b. Select **Add Users to device**
   c. Select the user created in Step 1 above. If ADSync is used and users with certificates are sync’ed into the SES database already, then select the appropriate user.
   d. Right click on the device, select “**Show Commands**”
   e. Once the status of the command changes to “Executed”, reboot the client device attempt authentication with the smartcard user.
Network authentication at PreBoot
To test network authentication at PreBoot, some server side settings are required.

Server side:

1) Setting Preboot Network settings
   a. Open up SES Console
   b. Click on Tools and PreBoot Network (PBConnex)
   c. Select PBConnex Global Options
   d. PBConnex Global Options Window displays
   e. Click on “Authenticate user against Active Directory” if AD is the desired authenticating server
   f. Click Save

2) Setting which users are authorized to login at PreBoot. (For ease of testing, we will allow all users to login to all devices. Groups can be used to restrict user/device combinations)
   a. Click on All Folders on the left pane
   b. Click on the Groups tab in the middle pane
   c. Double click “All User Group” to select it. (This group contains all users in SES)
   d. Click on “PBConnex Access Policies” on the left pane
   e. In the Get Key File via PBConnex section
      i. Select “Allow” and “Save Key File to client machine”
Testing new functionality

f. Click on “Member of groups” on the left pane
g. Click “Add …”
h. Select “All Device Group”
i. Click OK
j. Please ensure “Step 6 of “Setting up the environment” above
k. Please ensure “Enable machine to communicate with SDConnex at PreBoot” is enabled in the Device profile as per Step 8 of “Setting up the environment” section above.
l. Reboot the Mac device.
m. At SecureDoc PreBoot, please attempt to login with valid AD credentials. SecureDoc will communicate with SDConnex to validate the credentials entered at PreBoot. If it authenticates successfully, Mac device will boot up.

n. If users forget their AD password. Help desk can change their password at AD and the user can immediately use the NEW password at SecureDoc PreBoot to authenticate.

Prevent additional users to be added to FV2 unlock list

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.
   a. Enter their respective passwords
6) Click on Done
7) Restart the Mac Device
8) Hold the OPTION key and select to boot to the Mac Disk rather than SecureDocBoot.
9) Only the WinMagicProprietyUserForFV is allowed.
10) Restart the machine
11) SecureDoc PreBoot is displayed
12) Enter in valid SecureDoc credentials to unlock the system.

Challenge and response password reset

1) At SecureDoc PreBoot, enter in the User ID press Enter
2) Press F8
3) Challenge data is presented
4) In SES Console, find the corresponding User ID, right click and select Challenge Response
5) Enter in the Challenge in the text box under the “SecureDoc Challenge Response Recovery” section.
6) Click Get Response
7) On the Mac device, enter in the Response.
8) Press Enter.
9) If it’s correct, it will boot into the OSX login screen.
10) Once logged into OSX, SecureDoc will prompt the user to enter a new password for their SecureDoc account.
To provide feedback or to report issues with this Beta

To provide feedback or to report issues with this Beta

To report problems during the BETA period, please do the following:

1) Collect logs
   a. Click on the SecureDoc icon in the system tray
      ![SecureDoc Icon](image1)
   b. Click on **Collect SD Logs**
   c. The following prompt appears and logs will be saved on the desktop
      ![Log Collection Prompt](image2)
   d. Please send an email to [betafeedback@winmagic.com](mailto:betafeedback@winmagic.com) with the following information
      i. Subject: SDOT FV2 Beta Feedback
      ii. Your contact information
      iii. Short description of the problem
      iv. How to reproduce it
      v. Attach logs in step A above.

To provide feedback during the BETA period:

a. Please send an email to [betafeedback@winmagic.com](mailto:betafeedback@winmagic.com) with the following information
   vi. Subject: SDOT FV2 Beta Feedback
   vii. Your contact information
   viii. Detailed description of your comments. All comments or recommendations for improvements are appreciated.