Important Notes

Feature Deprecation

On July 6, 2018 WinMagic customers and partners were notified that the SecureDoc pre-boot authentication feature for macOS – known as SecureDoc On Top (SDOT) for FileVault 2 – would be deprecated in SecureDoc 8.2 SR1. As of this release, customers will no longer see this feature available for macOS configuration settings.

Please visit Knowledge Base Article 1760 for more information.

Before Upgrading

Prior to upgrading from v8.2 to v8.2SR1, please refer to KB article KB000001727 to follow the steps to ensure your client machine has Win7 with KB3033929. For more information on this limitation please see ticket SD-27495 Unable to load Windows after Win7 SDClient Upgrade from v8.2 to v8.2SR1 on client machine without KB3033929 in the Limitation section.
SecureDoc Support

WinMagic strongly recommends that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and new features.

Please visit Knowledge Base Article 1397 for more information on End of Life and End of Support timelines for SecureDoc software releases.

Customers running SecureDoc 6.5 and earlier should upgrade their server and clients to an actively supported software version. For more information on upgrading from SecureDoc 6.5 and earlier, please visit http://downloads.winmagic.info/SD8.2/HF2/SecureDoc_ReleaseNotes_SDV8.2HF2.pdf.

About This Release

This document contains important information about the current release. We strongly recommend that you read the entire document.

Purpose

The SecureDoc Enterprise Server (SES) 8.2 SR1 release resolves issues reported in previous versions, extends support to new platforms, and enhances the product with new features.

Rating

Recommended – WinMagic recommends this service release for all environments. Apply this update at your earliest convenience.

Previous Versions

<table>
<thead>
<tr>
<th>Version</th>
<th>Release Date</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2 DMG</td>
<td>February 5 2018</td>
<td>Support for macOS High Sierra 10.13.3 (macOS client)</td>
</tr>
<tr>
<td>8.2</td>
<td>April 19 2018</td>
<td>SecureDoc 8.2 General Availability (server/client)</td>
</tr>
<tr>
<td>8.2 HF1</td>
<td>June 8 2018</td>
<td>Support for Windows 10 RS4 (server/client)</td>
</tr>
<tr>
<td>8.2 HF2</td>
<td>June 20 2018</td>
<td>Support TLS 1.2 for PCI DSS compliance (server)</td>
</tr>
<tr>
<td>8.2 HF3</td>
<td>July 17 2018</td>
<td>Fix SDOT for BitLocker on HP devices (Windows client)</td>
</tr>
<tr>
<td>8.2 SR1</td>
<td>August 7 2018</td>
<td>New features, improvements and fixes (server/client)</td>
</tr>
</tbody>
</table>

Download the latest release notes for each version listed within Knowledge Base Article 1756.
System Requirements

For server and client system requirements: https://www.winmagic.com/support/technical-specifications

For supported devices, drives, smartcards and tokens: https://www.winmagic.com/device-compatibility

**Note:** It is strongly recommended to initially install Full-Text Indexing feature (Full-Text Search) into the Database Engine, before performing an SES installation.

More information is available here: http://msdn.microsoft.com/en-us/library/ms143786(v=sql.100).ASPX

During the installation of SES, if Full-Text Indexing has not been installed, a message will appear indicating the absence of the Full-Text Indexing. This message will not allow the user to stop the installation of SES which will require retrofitting Full-Text Indexing into an existing SQL Server.

**Note:** Use of the SES Console will require the user to have at least local admin rights on the server or client device (e.g. Admin desktop) on which it runs, in order for the console to function properly

Client OS Support

This section shows supported operating systems and upgrade paths for SecureDoc Endpoint Clients.

**Microsoft Windows**

<table>
<thead>
<tr>
<th>Version</th>
<th>Editions</th>
<th>Architecture</th>
<th>SR/Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 RS5 [1809]</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td>TBA</td>
</tr>
<tr>
<td>10 RS4 [1803]</td>
<td></td>
<td></td>
<td>SD 7.5 SR1 HF8 / SD 8.2 HF1+</td>
</tr>
<tr>
<td>10 RS3 [1709]</td>
<td></td>
<td></td>
<td>SD 7.5 SR1+</td>
</tr>
<tr>
<td>10 RS2 [1703]</td>
<td></td>
<td></td>
<td>SD 7.1 SR6+</td>
</tr>
<tr>
<td>10 RS1 [1607]</td>
<td></td>
<td></td>
<td>SD 7.1 SR4+</td>
</tr>
<tr>
<td>10 T2 [1511]</td>
<td></td>
<td></td>
<td>SD 7.1+</td>
</tr>
<tr>
<td>10 T1 [1507]</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| 8.1       | Enterprise Pro | 32/64-bit   | All versions                   |
| 7         | Enterprise Pro | 32/64-bit   | All versions                   |

**Apple macOS**

<table>
<thead>
<tr>
<th>Version</th>
<th>Editions</th>
<th>SR/Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Sierra</td>
<td>10.13.X</td>
<td>SD 8.2 DMG</td>
</tr>
<tr>
<td>Sierra</td>
<td>10.12.X</td>
<td>SD 7.1 SR6+</td>
</tr>
<tr>
<td>El Capitan</td>
<td>10.11.X</td>
<td>SD 7.1 SR2+</td>
</tr>
</tbody>
</table>
Device Types Not Supported in 8.2 SR1

At the time of the creation of this Service Release, the following device types are not supported in this version. WinMagic is string to provide support in a forthcoming release.

- HP ProDesk 600 G4
- HP EliteDesk 705 G4 DM

Device types that exhibit specific compatibility issues:

- HP ProDesk 480 G5 MT (Network Interface Card not supported at Pre-Boot) – See Limitations, SD-27453
- HP EliteOne 1000 (Network Interface Card not supported at 32bit Pre-Boot) – See Limitations, SD-27345

Network Interface Cards not supported for Pre-Boot Networking in this release:

- Intel AC 956
- Intel I219-LM

What’s New

New Features

SD-25580: SecureDoc now offers support for Red Hat Enterprise Linux versions 6.6, 6.7, 6.8, 6.9

SD-26659: A new user right and functional element has been added to SESWeb to permit access to an (optional) Simplified Password Recovery methodology.

A new user right has been added that can be the sole element in a new role type, or it can be added to existing roles, as the Administrator chooses. When used as initially intended - being the sole element in a new role type - users having that role will be limited to having access only to a new simplified Password Recovery panel. The benefit of this is that it neither requires nor offers access to any other information in the SES environment.

The objective of this improvement is so that large organizations that have a large number of help desk users can limit these help desk users to access only what they need to assist users in recovering access to locked device or where the user has forgotten his password. Compare this to "normal" SESWeb, where to perform password resets for Windows and Mac systems, the help desk user is able to navigate and see information they might not necessarily be entitled to.

How users will use this new feature is covered in greater detail in a new mini-manual that will be available from a link within WinMagic Knowledge Base article number: 000001758.

The documentation can also be accessed at: http://downloads.winmagic.info/manuals/Simplified_Password_Recovery_Manual_82SR1.pdf
Improvements

**SD-19279:** SecureDoc has been updated to support TLS 1.2 (Transport Layer Security version 1.2) for greater security, necessitating software changes to permit moving to .NET 4.5 which supports TLS 1.2.

This necessitated upgrading all SecureDoc components to use .NET Framework version 4.5 (from .NET 3.5 version used in SDConnex and the .NET 4.0 version used in SES Web). Those older versions required TLS 1.0 when using transport layer security but TLS 1.0 has known vulnerabilities.

So that organizations that are (or are becoming) PCI compliant can use TLS 1.2, WinMagic has undertaken this important security change.

---

**SD-25706:** WinMagic has added a scriptable means to disable/re-enable SecureDoc's BitLocker Tamper Protection functionality.

The objective is to provide a means to temporarily bypass SecureDoc's BitLocker Tamper Protection enforcement, permitting a script element to either disable or re-enable this protection to permit Windows and BIOS updates to run successfully. This script can be enforced via SCCM for both disabling Tamper protection and also for re-enabling it.

To use this new capability: There is a new stand-alone executable which will take the following parameters:

1. Path to a keyfile
2. Keyfile password
3. Enable/disable flag for tamper protection

This executable will (typically) be supplied to the client via SCCM. The package will also contain a full-admin keyfile (full rights). The SCCM script will run the executable to disable/enable the protection, as follows:

```
SDBLEnableProtection.exe admin.dbk passwordstring enable
SDBLEnableProtection.exe admin.dbk passwordstring disable
```

---

**SD-25796:** Improve pre-boot authentication error messages to be more general, so that a would-be attacker is not provided any guidance re: whether the User ID or the Password is invalid

Under certain circumstances, users would be provided information that defined that the User ID was not found, but then if the correct User ID was entered, the message would change to indicate that the password was not valid. This could have provided an attacker with information that he had landed on a valid User ID, and would so then only need to try to attack the password (up to the point that the maximum number of failed login attempts had been breached).

To improve security, these messages are now more generalized, notifying the person logging in of the problem in a more general sense - e.g. that the credentials are not valid, please re-enter and try again.
SD-25969: Activating autoboot locally or by remote command does not work on devices running Pre-Boot for Native UEFI devices (PBU) when using specific credentials

When sending an auto-boot command to a device, there is the option to specify the user credentials (keyfile name/password) for the user being used to activate autoboot. Using specific credentials are necessary when, for example, setting the device into a temporary auto-boot state after it has been auto-booted using PBConnex Auto-Boot. Since SecureDoc cannot activate temporary autoboot using the PBConnex auto-boot user information, it becomes necessary to specify credentials.

There was an issue with PBU (Pre-Boot UEFI) where although the command is sent and logs show it activated, PBU fails to auto-boot. This issue has been corrected in this version.

SD-25983: In Version 8.2SR1, SecureDoc changes the way that data is transferred from the Client device to the SES server for NEW installations.

For newly installed devices running 8.2SR1 or later, SecureDoc will no longer use the SDSend~.dat file. This means that customers that are accustomed to seeing this file or that are accustomed to deleting this file to fix client communication issues will no longer see this file in UserData folder. They should also experience substantially fewer issues relating to clients being unable to communicate to the server.

NOTE: All devices that are upgraded to 8.2 SR1 from a previous version will continue to use SDSend~.dat.

SD-26060: Improve data security for configuration elements residing in the /WinMagic directory tree in macOS devices

A risk was detected that indicated certain configuration elements that reside in the /WinMagic directory tree on macOS devices could be altered by users, potentially altering the behavior of SecureDoc on those devices.

This issue has been corrected, and protection of these files against tampering has been implemented.

SD-26231: WinMagic has implemented a general improvement to strengthen protection for internal elements used for Single Sign-on

An area was found that needed to be strengthened in order to ensure that specially-written third-party software cannot interrogate program primitives within the SecureDoc Client. WinMagic has instituted changes to protect the software from attempts to learn information that could be used in an attack.

SD-26284: A general re-architecting of aspects of the communication between client devices was undertaken to eliminate uncommon issues certain customers were encountering, such as devices attempting to add themselves to the SES database again, devices failing to add themselves (if missing) to the database, and devices that ceased attempting to communicate to SDConnex.

Among the issues addressed in this are: Attempts by client devices that are already in the database to add themselves to the database again (duplicate device IDs), scenarios where devices that may were missing from the
database (e.g. if database was restored from an old backup, or devices were deleted but existed in the real world) did not add themselves back into the database, as well as scenarios where client devices would cease attempting to communicate to SDConnex.

The scenarios under which these issues could occur have been identified and the software has been improved to ensure these scenarios and their impacts no longer occur.

SD-26413: Under SecureDoc for FileVault 2, an error message would mistakenly appear when users would perform Removable Media Container Encryption on USB media when the Profile option "Encrypt entire space and move files into container" was enabled.

This issue has been corrected, and use of RMCE on this platform works as documented/designated.

SD-26478: Add ability for AD/Mobile user to enable FileVault 2 under High Sierra versions 10.13, 10.13.1, 10.13.2 and 10.13.3.

Previous versions of SecureDoc did not allow for AD users to enable FileVault 2 under macOS High Sierra versions 10.13, 10.13.1, 10.13.2 and 10.13.3, which had been noted as a limitation in a previous version. Configuring a workstation to use a network or mobile account is beneficial in environments where administrators wish to manage authentication from a central server, utilize single-sign-on, or improve security by enforcing a password expiration policy.

Starting with macOS 10.13.4, Apple made some improvements that permitted SecureDoc to support using AD users for enabling FV2. This improvement only works on macOS 10.13.4 and later.

In order to make this work, certain preconditions must be met:

1. For a new AD user who logs in for the first time into a macOS 10.13.4 (or later) device, a dialog box will appear, prompting: "Enter a SecureToken administrator's name and password to allow this mobile account to log in at startup time".

   It requires the user to type in local admin username and password, then to press Continue.

2. After the user logs into the system, the user should open a Terminal session and type in command:
   ```
   sysadminctl -secureTokenStatus ADUserName
   ```
   and press Enter. It should return: “Secure token is ENABLED for user <ADUserName>”

3. (Optional) In order to use this optional step, the device user must know at least one local admin credential.
   If at previous step 1, instead of providing admin credential and pressing Continue the user pressed Bypass.
   After logging into system, the user can open a Terminal panel and type in the following command:
   ```
   sysadminctl -secureTokenStatus ADUserName
   ```
   and then press Enter; It returns: “Secure token is DISABLED for user <ADUserName>”
   The user can then try the following command to Enable secure token:
   ```
   sudo sysadminctl -adminUser AdminUserName -adminPassword AdminUserPassword -secureTokenOn ADUserName -password ADUserPassword
   ```
For Example: For the following criteria: AdminUserName: test, AdminUserPassword:1, ADUserName: ad, ADUserPassword:11

Then the command would look like this:

```bash
sudo sysadminctl -adminUser test -adminPassword 1 - -secureTokenON -Password 11
```

After executing the above command, the user can check secureTokenStatus, it should return: Secure token is ENABLED

4. For an existing AD user whose Secure token is DISABLED on previous High Sierra macOS versions 10.13.3 and earlier, after upgrading macOS to 10.13.4, the Secure token status still remains DISABLED and there is no system prompt after upgrading.

NOTE: In this scenario, AD users must perform Step 3 above to ENABLE the secure token.

Note: the above information is also available in the SecureDoc Knowledge Base, as article number: 000001766

---

**SD-26492: Improve how new AD Users are added to the FileVault 2 unlock list**

With this improvement, for each new AD user who (for the first time) logs into a device running macOS 10.13.4, the device will produce a dialog panel prompting the user to "Enter a SecureToken administrator's name and password to allow this mobile account to log in at startup time", This requires the user to type in a local admin username and password, and then to press Continue.

Note: the above information is also available in the SecureDoc Knowledge Base, as article number: 000001765

After logging into the system, the user must open a Terminal window and type in command:

```bash
sysadminctl -secureTokenStatus <ADUserName>
```

and then press Enter. The command should return:

“Secure token is ENABLED for user <ADUserName>”

Alternatively, in order to use the optional step below, the user must know at least one local admin credential.

Optionally, at the previous step instead of providing admin credential and pressing Continue, the user could press Bypass, which will leave the token in Disabled state.

**To Enable a Disabled Token**

Then, after logging into the system, the user must open a Terminal window and type in the command:

```bash
sysadminctl -secureTokenStatus <ADUserName>
```

(where <ADUserName> is the AD user’s name)

and press Enter. Upon successful completion, the command should return:

“Secure token is DISABLED for user <ADUserName>”

The user can also try the following command to Enable the secure token:

```bash
sudo sysadminctl -adminUser <AdminUserName> -adminPassword <AdminUserPassword> - -secureTokenOn <ADUserName> -password <ADUserPassword>
```

where <AdminUserName> is the name of the Administraotr, <AdminUserPassword> is that Admin's password,
<ADUserName> is the AD User Name and <ADUserPassword> is his/her password.

After that, the user should check secureTokenStatus as was performed in the beginning of this item. It should return:  
“Secure token is ENABLED”

For an existing AD user whose Secure token is DISABLED at previous High Sierra macOS 10.13.3 and earlier, after upgrading macOS to 10.13.4, the Secure token status still remains DISABLED and there is no system prompt after upgrading. 
Those kinds of AD user need to go through step shown under "To Enable a Disabled Token" in order to enable their secure token.

So, as long as AD users have their secure token enabled, those users can enable FileVault 2 under macOS High Sierra successfully. 
Otherwise, if the secure token remains Disabled, enabling FileVault 2 will not be successful, a message notifying the user of this will appear, and the user must go through the steps in the section above labeled "To Enable a Disabled Token"

Note: the above information is also available in the SecureDoc Knowledge Base, as article number: 000001765

SD-26590 and SD-26890: Updated version of 3rd-party tool integrated into SecureDoc to better support SecureDoc File Encryption

The most recent version of the external library that supports SecureDoc File Encryption has been implemented, correcting some issues customers had detected such as loss of Start Menu options when SFE was enabled under the previous version of this library.

SD-26773: Error 0x5401 or 0x9401 occurs during SecureDoc Installation of SDBM – SecureDoc BitLocker management: Error occurs when attempting to create SecureDoc partition

This issue can occur on Windows 7 or Legacy devices that already have the maximum permitted number of primary partitions; as a result, the SecureDoc installer is unable to create the SecureDoc partition.

A solution has been developed that permits the SecureDoc installer to locate/install the required SecureDoc elements elsewhere.

SD-26868: Device types NEC VG-U and VH-1 have been added to KnownConfig.xml

The above additional device types have been provided with device installation handling configuration information in the KnownConfig.xml file.
Resolved Issues

SD-23396: Error message "You login with the wrong key file.(0x0082)" appears when using Smart Card authentication.

Scenario:
This issue was only detected so far on Fujitsu Lifebook E746 devices with the Internal O2Micro OZ776 USB CCID smart card reader

Error message "You login with the wrong key file.(0x0082)" appears when the user is assigned only the FSIS_SD_User data object on their smart card and then presses 3.

If the user is assigned the FSIS_SD_User data object and the FSIS_SD_Admin on their smart card, and the user presses 3, the user can login.

When the user is assigned only FSIS_SD_Admin on their smart card, the user similarly will see Error Message: "You login with the wrong key file.(0x0082)"

When the user is assigned FSIS_SD_User and another random data object (NCR_Merivale), the user is able to login with the key file in slot 3.

This issue has been corrected in this version.

SD-25193: Certain devices are unable to boot when attached to a KVM (Keyboard-Video-Mouse) Switch when it was not the active device on the switch

Issue: In order for the Pre-Boot authentication screen to initialize, it must detect that there is an active video interface. However, when a device (typically set to UEFI bios mode) is not the active device on a KVM switch, and is powered on, the video card will not detect a monitor and will not initialize the graphics interface for use by the pre-boot operating system. This condition will also occur if no monitor is connected at all. In these scenarios, customers may want to still be able to boot into windows by enabling a permanent or network auto-boot mode.

Solution: The pre-boot logic has been improved to still attempt an auto-boot (if so configured) in the case there is no video interface available. Thus, “headless” systems should now be able to auto-boot.

NOTE: If the system is not configured to auto-boot, and a monitor is plugged in after powering on, the system may need to be rebooted in order for the bios to initialize the video adapter and display the pre-boot logon screen.

SD-25216: SecureDoc was exporting/saving Self Encrypting Drive (SED) hardware Encryption (HWE) data under a fixed-format file name, such as hwekeyfile.dbk and sdhwe.enc.

SecureDoc is supposed to export Hardware Encryption (HWE) information into file names that are derived from the SED’s (Self-Encrypting Drive’s) serial number.

This fix corrects the issue above, and HWE information will henceforth be saved in file names that are derived from the device's SED Serial number (e.g. "TSN12345QFTROETR6789.dbk").
SD-25770: SecureDoc File Encryption (SFE) was unable to encrypt files whose path length exceeded 170 characters.

Issue: SecureDoc File Encryption could not successfully encrypt files whose path length exceeded 170 characters.

This has been corrected in this version.

SD-25883: Message: "Encryption Engine Error" appears seemingly randomly on certain end user device running Windows.

Once this has occurred, the user is not able to log into SecureDoc Control Center.

This has been corrected in this version.

SD-26021: Issue detected in SecureDoc V7.5sr1 and V8.2 under Linux-based Pre-Boot - the Trackpad/Touchpad was not responsive on Dell E7380 devices.

This issue has been corrected in this version.

SD-26070: Certain Dell devices (e.g. 7480) running SecureDoc's 64-bit Linux-based Pre-Boot - when docked in a TB16 Thunderbolt Docking Station - lose network connectivity at Pre-Boot, thus preventing PBConnex network authentication when docked.

Such devices would work fine when un-docked, but when docked would not be able to complete a connection to SDConnex, and therefore could not use PBConnex network-brokered authentication. This issue applied only to devices running the 64-bit PBLU Linux-based Pre-Boot.

This has been corrected in this version.

SD-26212: Windows 10RS4 – The Start Menu options of Windows are disabled when SecureDoc File Encryption (SFE) was enabled

Issue: When the SecureDoc client software was deployed with SecureDoc File Encryption enabled, the start menu options are disabled and the user is not able to enter text in the search text box.

This issue is now resolved.

SD-26430: After upgrading from V7.5 to V8.2, it was noticed that after resizing or re-ordering columns in the SES console, the console would revert back to the pre-change column sizes and order.

This has been corrected, and column resizing and re-ordering will be retained.
SD-26450: The Windows Automatic Repair screen would be displayed after updating Windows 10RS2 to Windows 10RS4 using Windows Update with Secure Boot enabled

This issue did not occur if deploying a SecureDoc package on a fresh Windows 10 RS4 client with secure boot enabled. This issue also did not occur if upgrading windows using the “Reflectdrivers” method.

This issue has been corrected.

SD-26465: Correct problem where PBLU Linux-based Pre-Boot for UEFI devices does not offer touch-screen support on HP Pro x2 612 G2 Tablet devices

This issue was first reported as affecting devices running SD 7.5SR1 and then also again in 8.2. Customers needed this support for PBLU access with touch-screen support for PBConnex authentication. It was noticed that when such devices were installed with a PBU (Pre-Boot for Native UEFI) profile the touch screen/virtual keyboard would work fine on the tablet.

This issue has been corrected, and a new set of override settings for this device type has been added to KnownConfig.xml. Customers installing SES V8.2SR1 will receive the updated KnownConfig.xml file.

SD-26470: SecureDoc File Encryption (SFE) feature: – Unable to encrypt a file with a long file name (up to 255 characters) using SecureDoc File Encryption.

Issue: User is unable to complete individual file encryption due to file name being too long.

This issue is now resolved.

SD-26473: Password sync would not work following the upgrade of a SecureDoc Client from Windows 10RS2 to Windows 10 RS4

This has been corrected.

SD-26479 The Crypto-erase Key Sequence functionality was not being removed from the SecureDoc Client Boot Configuration after being removed from the Device Profile

Issue: Despite having been removed/disabled in a Device profile, and that device profile having been communicated to the Client device, the user of the device still retained the ability to execute the Crypto-erase key strokes and to crypto-erase the device.

This has been corrected - sending down a revised Profile to the device that disables the Crypto-erase functionality will bar the user from being able to Crypto-erase the device locally.
SD-26487: When installing Linux on SDCloud client devices or physical Linux servers, some devices were taking an inordinately long time to register to the SES server - in excess of 2 minutes in some cases

This has been corrected, and such devices will typically register to the SES Server in no more than 25 seconds.

SD-26490: Certain SDPin.exe messages do not appear correctly for Client devices installed in German-language Windows.

Issue: For deployments of the SecureDoc client software to client devices running German-language Windows, the SDPin.exe element of SecureDoc does not show the expected "hover" message when the mouse hovers over the tray icon after encryption is finished. This problem did not occur in English nor in any other language, only in German.

This issue has been corrected in this version.

SD-26493: Client devices installed with SecureDoc V7.5SR1 HF5B could encounter a Blue Screen halt code (BSOD) referencing SDTToki.

This issue is now resolved.

SD-26508: Error "0x7017 Buffer Error" may appear when displaying SDForm during a new device installation

Issue: It was found that with very large profile sizes, a buffer error could appear. The cause was determined to be that related to enabling the Port Control feature, but not actually defined any device settings within Port Control. The problem arose because, when Port Control is defined, even with no device settings, it would normally still create a large block of information. With no Port Control device settings this block would contain all zeros, so it actually adds no valuable settings to the profile, but it does occupy a lot of space in the profile information.

This issue has been solved. When Port Control detects that there are no device details actually defined to be managed by Port Control, it will suppress the creation of the large block of zeros, so ensuring that the Profile information stays within a reasonable size and the buffer issue should no longer occur.

SD-26604: Touching/moving an external USB mouse attached to a NEC VH-1 device running SecureDoc's Pre-Boot for UEFI devices would cause the device to hang. This issue appeared to have been unique to this specific device type and has not been found to be a problem except on NEC VH-1 devices.

This issue has been corrected.

SD-26789: An issue with the displayed Field Width of certain Input Boxes in SES Console limits the number of characters that can be entered for SQL Server Name and Database name. This prevented initial database creation where the name values exceeded this limit.

When trying to use Azure hosted servers to install SES and SQL, the SQL server name could be longer than the "width" of the input box available for defining these values, and it would not allow entry of the additional
characters that were required. This typically occurred due to the server FQDN requiring subdomains and domains when configuring SES on these Servers.

This issue has been corrected, and now longer names can be entered for the SQL server and Database.

---

SD-26804: Corrected an issue that was preventing devices that were missing from the database from re-registering themselves into the SES Server/database at the next communication with SES.

Where a given device might have inadvertently or intentionally been deleted from the SES Database but it does exist as a SecureDoc-protected device in the real world, this correction reinstates original functionality to ensure that such devices will re-establish their device record and other information into the SES Database at the next available communication with the SES Server.
**Known Limitations**

**SD-25048: HP ProOne 600 G3 WiFi does not work in the SecureDoc pre-boot environment**

At present, there exists no workable Linux driver for the Realtek RTL8723DE 802.11b/g/n WiFi adapter type installed in the HP ProOne 600. WinMagic is monitoring for the development of such a driver and will incorporate it into a future version once one becomes available.

---

**SD-26150: Single Sign-on (SSO) does NOT work (on devices having Self-Encrypting Drives, e.g. Opal) after the device OS has been upgraded from Windows 10 RS3 to Windows 10 RS4**

Work-Around:

a) Create a copy of the existing device profiles in use on such devices (only those that enable Single Sign-on) e.g. if profile is called ABC, copy could be called ABC_NoSSO

b) Disable the Single Sign-on feature in these new _NoSSO copies of the existing profiles

c) Send the new _NoSSO profiles to all devices that have an existing profile that enables SSO

d) Upgrade the devices to Windows 10RS4 while SSO has been thus disabled

e) Reinstate SSO by sending down to the devices the original device Profiles

f) Once there are no devices still running the _NoSSO versions of the Device Profiles (indicating that all have been returned to their original versions of the Device Profiles that enable Single Sign-on), then the _NoSSO versions of the device profiles can be Deleted from the Console and the SES environment.

---

**SD-26170: The Windows 10 upgrade from RS3 to RS4 will fail if SecureDoc File Encryption is enabled on the client device at the time of the upgrade.**

WinMagic has determined that if an existing SecureDoc-protected Client device that has SecureDoc File Encryption ENABLED is permitted to be upgraded from Windows 10 RS3 to Windows 10 RS4, that Windows upgrade will fail.

Work-Around:

For Devices that have SecureDoc File Encryption ENABLED, customers should:

a) Create a copy of the existing device profiles in use on such devices (only those that enable the SecureDoc File Encryption feature) e.g. if profile is called ABC, copy could be called ABC_NoSFE

b) Disable the SecureDoc File Encryption feature in these new _NoSFE copies of the existing profiles

c) Send the new _NoSFE profiles to all devices that have an existing profile that enables SFE

d) Upgrade the devices to Windows 10RS4 while SFE has been thus disabled

e) Reinstate SFE by sending down to the devices the original device Profiles

f) Once there are no devices still running the _NoSFE versions of the Device Profiles (indicating that all have been returned to their original versions of the Device Profiles that enable SFE), then the _NoSFE versions of the device profiles can be Deleted from the Console and the SES environment.

g) Deploy the new Profile copies to affected devices

NOTE: The above considerations do not apply for fresh installations of the SecureDoc client on a Windows 10 RS4 device (with or without SecureDoc File Encryption enabled). Such installations will work fine, with no issues.
**SD-26207: Dell Precision 7520 Touch-pad does not work at SecureDoc Pre-Boot on Windows 7 machines**

This device type’s touch-pad does work fine on devices running Windows 10, and USB mice are not negatively impacted.

Work-around: On Dell Precision 7520 devices, please connect a USB Mouse at Pre-Boot until a solution has been found.

**SD-26415: Duplicate entries for Self-Encrypting Drives (SEDs) in devices upgraded from 7.5 SR1 to 8.2**

The logic to detect the Serial Number of Self Encrypting Drives installed in endpoint devices is different in 7.5 versus in 8.2, thus different device serial numbers are being reported into SES, which is treating them as new or different drives, creating a second disk record attached to the device.

Note;
The Serial numbers of NVME disks are presented differently by different Windows 10 Redstone versions.

Work-Around: Until WinMagic is able to define a solution to this issue, customers should use the lowest record number of the same disk type in the event that it is necessary to perform a recovery action.

**SD-26504 SecureDoc File Encryption appears to not complete the encryption of any files that are already encrypted using EFS (Encrypting File System) built into Windows**

A limitation of the 3rd-party Library that SecureDoc uses for SecureDoc File Encryption is that if there is any attempt to SFE-encrypt a file that has already been encrypted using the EFS tool built into Windows, that attempt will fail.

Customers should determine that if they wish to proceed with SecureDoc, they should stop the use of EFS and permit only one product to handle encryption on the devices, not a hybrid/blended solution.

Work-Around: If there is any use of EFS within the target device, those files or partitions should be decrypted using EFS before attempting to install SecureDoc.

Note that compression is still silently ignored by SecureDoc and compressed files are decompressed on the fly as they are opened.

**SD-26586: Dell E7270 devices with Self-Encrypting Drives (SEDs) fail to boot into Windows after login using 64-bit Linux-based Pre-Boot (PBLx64)**

Work-Around: Until WinMagic can determine a solution, please use a Profile and Installation package for these specific devices that specifies the use of 32-bit Pre-Boot (PBLx32).

**SD-26595: The red "lock" icon does not appear on SFE-encrypted files that have file names 255 characters in length when viewed through Windows 7 or Windows 8 devices that do not have the Encryption Key used to protect the files.**

This issue applies to [SFE] Missing red lock icon on encrypted file with long name 255 characters on SDClient without required key (Windows 7 & 8). This issue does not occur on Windows 10 devices.
SD-26775: Upon installing SecureDoc on Linux platform within VMware ESXi 6.5, the device is automatically rebooted after Cryptsetup and libpwquality-tools packages have been installed. Further, the wmsd folder is corrupted. Note that this issue does not affect Clients running RHEL 7.x

Issue details:
- Client has no free space and subscription
- Client is a fresh install (the cryptsetup and libpwquality-tools packages had not previously been installed)

The default package can be successfully created on SES Web successful
The package can be deployed and installed on a Linux client (using './install-s' command)
The expectation is that Cryptsetup and libpwquality-tools packages will be automatically installed on Linux, then the drive kernel would be downloaded and registered to SES successful

Actually what occurs is:
- The device is automatically rebooted after Cryptsetup and libpwquality-tools packages are installed and wmsd folder is corrupted.
- It is not possible to access the log file on the client device
- This issue does not occur on clients running RHEL 7.x

Work-around:
This is a known issue known to affect VMware ESXi 6.5.

This issue is resolved in VMware ESXi 6.5 Update 1, available at VMware Downloads.

To work around this issue if you do not want to upgrade, use any one of these options.
Option 1
Add the vmxnet3.rev.30 = FALSE parameter in the vmx file of virtual machine:
Power off the virtual machine.

Edit the vmx file and add the below parameter:
vmxnet3.rev.30 = FALSE

Power on the virtual machine.

Option 2
If you do not want to power off the virtual machine, disable the receive data ring for each vmxnet3 vNIC (virtualized network interface card) on the VM by running this command:

`ethtool -G ethX rx-mini 0`

Note: Replace ethX with virtual machine interface name.

SD-26884: All SecureDoc "On Top" of FileVault 2 (SDOTFV2) functionality has been removed from SecureDoc Enterprise Server, and all client devices will be migrated to SDFV2 (SecureDoc’s native management of FileVault 2, without the SecureDoc pre-boot).

WinMagic has decided to depreciate SDOTFV2 after V8.2, so V8.2SR1 and onward will no longer have the ability to
define SDOTFV2 settings through the SES User Interface.

This change will also change any existing profiles to define the use of SDFV2 instead of SDOTFV2

For new client installations; the devices will be configured only to use SD FV2.

Existing client devices that may have been defined with an SDOTFV2 profile will continue to work, but customers are strongly recommended to migrate these devices to the new SDFV2 profiles as soon as possible.

**SD-26967: No support for pre-boot on Gen-2 Windows Server Virtual Machines with SecureBoot on Hyper-V**

SecureDoc pre-boot (with Microsoft-signed drivers) is not currently supported on Gen-2 Hyper-V Virtual Machines when SecureBoot is enabled.

Work-Around: Disable SecureBoot on Gen-2 Hyper-V Virtual Machines until a solution has been found.

**SD-26989: Linux Virtual machines running in MS Azure or under Hyper-V that have disks of type .vhdx do not encrypt using the Fast conversion option. They perform thorough/All Sectors conversion, even though the profile may be set to Fast Conversion.**

WinMagic is working on a correction to this issue.

**SD-27050: New Simplified Recovery option allows assisting recovery of users/devices outside of the user's Folder limitations**

When a Support technician using the new Simplified Recovery option in SESWeb assists users of Apple Mac devices, he/she can provide assistance even to users/devices that are outside of the Support technician’s permitted-access folders.

WinMagic is working to find a solution to this limitation.

**SD-27093: When SecureDoc is upgraded from SES V8.2 to 8.2SR1 on client devices running Yosemite or El Capitan versions of macOS, and the user logs in with the WinMagic recovery account, then a series of System message will appear. The texts of these messages include: "macOS needs to repair your library to run applications." "A keychain cannot be found to store." "iCloud drive may not work properly." and there may be others.**

Issue: When SecureDoc is installed on client machine with SES V8.2, and is then upgraded to 8.2SR1, the device will communicate to the SES Server. The user will then reboot the device and login to the Recovery account. At this point a series of redundant/irrelevant dialog boxes will be displayed, including "macOS needs to repair your library to run applications." "A keychain cannot be found to store." "iCloud drive may not work properly."

Work-around:

a) The user should ignore those system messages and wait for the "Account Password Reset" dialog to appear.

b) The user should choose the desired Account Short Name from the list displayed. This list contains all users in the FileVault 2 Unlock list.

c) Type in new password in the dialog and click OK
d) Log out will be performed automatically
Now the user can use the Mac account chosen in step (b) and the new password set in step (c) to login to macOS.

Note:
The redundant dialogs discussed above are not displayed when logging in with the recovery account on a fresh device installation - only on an upgraded device.

SD-27189: When SecureDoc is upgraded from SES v7.5, v7.5SR1 or v8.2 to 8.2SR1 on client devices running Sierra or High Sierra versions of macOS, and the user logs in with the WinMagic recovery account, then a series of System message will appear. The texts of these messages include: "macOS needs to repair your library to run applications." "A keychain cannot be found to store." "iCloud drive may not work properly." and there may be others.

Issue: When SecureDoc upgraded from any of SES v7.5, v7.5SR1 or v8.2 to 8.2SR1, the device will communicate to the SES Server. The user will then reboot the device and login to the Recovery account. At this point a series of redundant/irrelevant dialog boxes will be displayed, including "macOS needs to repair your library to run applications." "A keychain cannot be found to store." "iCloud drive may not work properly."

Work-around:
a) The user should ignore those system messages and wait for the "Account Password Reset" dialog to appear.
b) The user should choose the desired Account Short Name from the list displayed. On Sierra, the list contains all users in the macOS device (not only those in the FileVault 2 unlock list).
c) Type in the new password in the dialog and click OK
d) The device will automatically log out after 2-3 minutes.
Now the user can use the Mac account chosen in step (b) and the new password set in step (c) to login to macOS.

Note:
The redundant dialogs discussed above are not displayed when logging in with the recovery account on a fresh device installation - only on an upgraded device.

SD-27257: Unable to deploy SDLinux on clients without an existing boot partition due to (Legacy) Grub 1 limitation

Linux devices that still utilize the (Legacy) Grub boot loader (versions of Grub prior to 2.0) will be unable to deploy SDLinux on such client devices, due to a limitation in Grub 1.
To clarify:
• If a Linux environment has an existing boot partition already configured and has a Legacy grub version, they will still be able to deploy SDLinux on this. In most cases the default installation for RedHat and Ubuntu always includes a boot partition
• However, If a Linux environment does NOT have an existing boot partition already configured and also has a Legacy grub version, then they will NOT be able to deploy SDLinux.

Normally for Linux environments without a boot partition already configured, if they have the Grub 2.x version, when SDLinux is deployed SecureDoc will automatically the necessary partition (boot partition) and will create SDSpace successfully on the device. WinMagic found that for versions of Grub prior to 2.0 the SecureDoc installer was unable to do this successfully.
Work-Around:
The first recommendation would be to have the boot partition configured beforehand, prior to deploying SDLinux. Note: During SecureDoc testing, deployment was performed on an environment on which the boot partition was configured as part of a fresh OS installation (i.e. on a clean, new system installation). WinMagic has not yet tested manually creating the necessary boot partition post-OS-installation and then subsequently deploying SDLinux.

SD-27345 Intel Wired network adapter in HP EliteOne 1000 is not supported in Linux-based Pre-Boot (PBL)

This Network Interface Card is not supported in either the 32-bit or 64-bit versions of the Linux-based SecureDoc Pre-Boot, so such devices cannot be used for PBConnex network-brokered authentication.

WinMagic is working on a solution to support these devices in a future release.

SD-27356 Maximum Failed login attempts provision not locking users out of devices after upgrading PBU (native Pre-Boot for UEFI) device to 8.2 HF1

This issue prevents the “maximum failed login attempts” policy from working after the client is upgraded to 8.2. Users are NOT locked out of their devices.

This issue only impacts systems that are running PBU; it does not impact systems using either SecureDoc's Linux-based Pre-Boot for non-UEFI devices, not the Linux-based Pre-Boot for UEFI devices.

This issue only impacts systems that are upgrading to 8.2 (and newer versions).

Work-Around: Update the user’s key files from an SES v8.2 console.

If the user’s device is configured to use password sync, they can either change the SecureDoc Pre-Boot Password, or change the Windows password. In either of these cases, SES will generate a new key file and send it down to the client machine.

SD-27399 and SD-27405: Linux-based Pre-Boot “loops”, rebooting specific HP device types

Issue: The following HP device types will loop back to reboot after authentication, instead of loading Windows. The affected device types are:

- HP ProDesk 600 G4
- HP EliteDesk 705 G4 DM

WinMagic has identified the resolution for this, but the solution was found after Service Release V8.2SR1 was sent to production. WinMagic anticipates having support for these device types in a forthcoming hot fix update.

SD-27445 Error message “Please contact Winmagic Technical Support (0x6210)” is displayed randomly on Azure devices at Preboot when cloning an encrypted Windows VM

For virtualized devices running in Azure datacenter environments, after successfully installing SecureDoc on the devices, upon rebooting the device an error message may randomly appear on the device. The message text is: "Please contact Winmagic Technical Support (0x6210)".

WinMagic is working to resolve this issue.
Work-Around: If this message appears:

a) If the option exists to reboot the device, do so and allow the Pre-Boot Auto-Boot sequence to be re-tried.
b) If there is no option available to reboot the device, then either:
   a. Redeploy or re-clone the VM that failed to autoboot at preboot during the "Creating" stage in Azure, or
   b. Delete the VM that failed during provisioning and create a new clone

SD-27453 Realtek PCIe GBE Family Controller Wired network adapter in HP ProDesk 480 G5 MT is not supported at in Linux-based Pre-Boot (PBL)

This Network Interface Card is not supported in either the 32-bit or 64-bit versions of the Linux-based SecureDoc Pre-Boot, so such devices cannot be used for PBConnex network-brokered authentication.

WinMagic is working on a solution to support these devices in a future release.

SD-27495 Unable to load Windows after Win7 SDClient Upgrade from v8.2 to v8.2SR1 on client machine without KB3033929

If your machine isn’t updated with KB3033929, the upgrade from v8.3 to v8.2SR1 will be unsuccessful. Please refer to KB article KB000001727 to follow the steps before upgrading.
How to Install/Upgrade

Customers with an active support plan should contact support@winmagic.com to receive the latest download link for their SecureDoc upgrade.

Contact 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

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.

©Copyright 1997 - 2018 by WinMagic Inc. All rights reserved.