

SecureDoc Enterprise Server

Release Notes

Product Version: 8.3

Published February 4th 2019

Contents

Important Notes	1
Feature Deprecation	1
Before Upgrading.....	2
SecureDoc Support	2
About This Release	2
System Requirements.....	3
Client OS Support.....	3
What's New	4
Improvements/New Features.....	4
Resolved Issues.....	10
Limitations	13
How to Install/Upgrade	15
Contact WinMagic	15
Acknowledgements	15

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.

Lenovo deprecated a software technology named Hardware Password Manager on August 28, 2016. For more information on the depreciation of this technology, please see:

<https://support.lenovo.com/us/en/solutions/ht082564>

SecureDoc support for this Lenovo technology has been removed from SecureDoc Enterprise Server and the SecureDoc Client in version 8.3.

Support for definition of GINA settings has been removed from this version (affecting only Windows XP, support for which was deprecated in a previous version).

Support for specific Hewlett Packard license types has been removed, and WinMagic will no longer offer specific pricing for customers migrating from old devices running HP ProtectTools encryption to SecureDoc encryption.

Before Upgrading

Prior to upgrading from v8.2SR1 to v8.2SR2, 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 previous release note v8.2SR1 http://downloads.winmagic.info/manuals/Release_Notes_8.2SR1.pdf

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/SD8.2SR1/HF2/Release_Notes_8.2SR1HF2.pdf.

About This Release

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

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

Previous Versions

Version	Release Date	Details
8.2 DMG	February 5 2018	Support for macOS High Sierra 10.13.3 (macOS client)
8.2	April 19 2018	SecureDoc 8.2 General Availability (server/client)
8.2 HF1	June 8 2018	Support for Windows 10 RS4 (server/client)
8.2 HF2	June 20 2018	Support TLS 1.2 for PCI DSS compliance (server)
8.2 HF3	July 17 2018	Fix SDOT for BitLocker on HP devices (Windows client)
8.2 SR1	August 7 2018	New features, improvements and fixes (server/client)
8.2 SR1 HF1	August 22 2018	Improvements and fixes (server/client)

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](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

Version	Editions	Architecture	SR/Update
10 RS5 [1809] 10 RS4 [1803] 10 RS3 [1709] 10 RS2 [1703] 10 RS1 [1607] 10 T2 [1511] 10 T1 [1507]	Enterprise Pro	32/64-bit	8.1 SR1 HF2+ SD 7.5 SR1 HF8 / SD 8.2 HF1+ SD 7.5 SR1+ SD 7.1 SR6+ SD 7.1 SR4+ SD 7.1+
8.1	Enterprise Pro	32/64-bit	All versions
7	Enterprise Pro	32/64-bit	All versions

Apple macOS

Version	Editions	SR/Update
Mojave	10.14.X	MAC 8.3+
High Sierra	10.13.X	SD 8.2 DMG
Sierra	10.12.X	SD 7.1 SR6+
El Capitan	10.11.X	SD 7.1 SR2+

What's New

Improvements/New Features

SD-12126 – Client data transfer preparation improved for increased efficiency and reliability

Improvement on how client communication data is prepared. The key changes are:

- No SES transfer data is stored in a file
- Data transfer beyond 60k data file size will be successful
- RME logs will have less priority and will not block other SES data from being sent with lower priority
- Client password change updates will have highest priority

SD-19723 – Lenovo Hardware Password Manager Functionality has been removed

Lenovo deprecated a software technology named Hardware Password Manager on August 28, 2016. SecureDoc support for this Lenovo technology has been removed from SecureDoc Enterprise Server and the SecureDoc Client in version 8.3. For more information on the depreciation of this technology, please see:

<https://support.lenovo.com/us/en/solutions/ht082564>

SD-21911 – Improve Folder Management for Mac Clients

Mac clients are able to use the same three options as Windows SES clients when configuring the Mac installation package. This allows the installation to create the device record in the SES database in a specific folder location. (Owner Folder, Registration Folder, or Specific folder)

SD-26341 – General Improvements to SDLinux Deployment

General Improvements were made to make the SDLinux installation/deployment more robust and user-friendly.

SD-26429 – With V8.3, WinMagic now offers a separate Pre-Boot Compatibility Testing tool that can be used by customers to verify whether the devices they intend to encrypt with SecureDoc will be successful, (compatible) or may run into technical issues that may require deeper investigation (potentially incompatible)

The pre-boot compatibility tool installs a special version of the SecureDoc Pre-Boot environment, reboots the device to perform testing, and following the reboot will produce a device-level report of what it was able to find out about the device behavior. Each report will include a summation of whether the device is found to be compatible, or if not, will provide information about the compatibility issues discovered.

Customers finding incompatible device types are encouraged to send those reports to WinMagic for further investigation, and so that WinMagic can determine how to incorporate functionality into SecureDoc that can enhance its abilities to handle such devices.

SD-26583 – General improvements to V4 Legacy Pre-boot Updates

Improvements were made to support and use smaller V4 SDSpace when performing Boot Logon updates.

SD-26724 – SecureDoc FileVault2 RMCE Improvements

The SecureDoc for Mac SDFV2 client has been improved to show similar progress messages as seen on windows clients during creation/encryption of Removable Media Container-Encrypted Media (RMCE). This was done to more closely align the user experience customers encounter when RMCE-protecting media on Windows devices.

SD-26728 – Improve capability to customize Pre-Boot text

An improvement was made to allow more customization of the pre-boot text, to allow for an SES administrator to modify according to company requirements.

SD-26731 – Improve SFE uninstallation

An improvement was made to seamlessly remove SFE encryption from existing SecureDoc client machines.

SD-26871 – Improvement for SecureDoc File Encryption (SFE) support on servers to permit running encryption or decryption tasks inside a service session (no user login required)

Prior to this improvement, all SFE operations required a user to login into a desktop session. Now, it is possible to enable a service session to perform this encryption, without requiring a user to logon. This new feature is disabled by default to save system resources.

SD-26881 – A new registry setting permits initial encryption of endpoint devices to be delayed until triggered later

This new feature is primarily oriented toward the encryption of Cloud-hosted Servers and Virtual Desktop Infrastructure (VDI) devices.

A custom Registry setting has been added, whose non-zero value will prevent SDForm from appearing/acting when the device loads into windows. This will prevent registration of the device to the SES server and will pause the rest of the installation process. This functionality is described below:

If the following registry entry is set to a non-zero value (e.g. through scripting or a command process), SDForm will not appear and the device will not register or request a unique random encryption key.

```
HKEY_LOCAL_MACHINE\SOFTWARE\WinMagic  
[DWORD] DormantSetupMode=1
```

The ability to register the device will be restored once this setting is removed or set to 0, which can similarly be triggered through scripting or a command process. Once so set, SDForm will appear, (or if configured for invisible registration, will be processed automatically) and the device will register and request a unique random encryption key, then proceed through initial encryption.

SD-27074 – Block SID detection for OPAL drives

SecureDoc now successfully halts installation with a notification message when it detects an Opal Self-Encrypting Drive protected with BlockSID.

Background Context:

BlockSID is a feature that can prevent an OPAL SED from becoming managed. It is implemented through the combination of the BlockSID capability of an OPAL SED, and a manufacturer BIOS that can activate this capability.

Earlier versions of SecureDoc were able to detect whether the BlockSID feature was enabled, so that when OPAL management failed (or was likely to fail) due to BlockSID, an appropriate error popup appears. However, the installation is left in a partial state.

Improvement:

In this version, the method for installing against a BlockSID-protected SED has been improved so that SecureDoc is not left in an incomplete state if BlockSID is enabled at the time of install, as well as adding logging information to SDConnex that identifies if BlockSID is the cause of an incomplete SecureDoc deployment due to OPAL management being blocked. Once having logged the issues, the installer will gracefully close.

SD-27368 – Support for new MacOS Versions

SDFV2 clients now support macOS Mojave (10.14.X)

SD-27558 – Improvements to SFE in order to support folder redirection for environments with variables

Where customers have folder redirection enabled in their client devices, in previous versions SecureDoc File Encryption would not be able to follow the redirection to encrypt the contents of the redirected folder.

This has been corrected in this version. Now when users access their SFE-encrypted folders on their C drive, both Windows and SFE will redirect the user to the actual folder residing elsewhere, the contents of which will now be successfully encrypted using SecureDoc File Encryption.

SD-27306 – The SecureDoc OSA Installation process has been substantially improved

Issues:

1 – In previous versions, OSA installation was done via USB or PXE boot, neither of which could be automated or run completed silently. The Administrator or delegate needed to physically access the device before installing/encrypting it. Of these methods, USB was the easiest method, as PXE boot was complex to setup and WinMagic's documentation needed to be revamped on this topic.

2 – Pre-boot compatibility: OSA included its own static pre-boot that did not utilize the currently-installed Linux version. This could cause OSA to not work with certain devices, and frequently required WinMagic to rebuild OSA if customers were running on newer systems. This issue became more critical relating to support for networks (e.g. wired, wireless, 802.x etc), as in order for OSA to run it needs to communicate with SES as a first step, and some customers found issues in deployment where OSA did not support their network cards.

3 – Capture of User/device information: Administrators are often required to fill user/device information when SDForm appears, in order to continue the deployment. This requires manual action & often became an onerous task, adding complexity if customers were planning to deploy a large number of devices.

4 – Staging users for offline usage: Previous versions did not implement Key File deployment for users to be staged during & right after installation. OSA would often require user to login to pre-boot in order for them to have staged a user Key File to the device, or the administrator would need to assign the user to the device using the SES Console.

Solution:

The InstallApp has been extended to support command line invocation.

The OSA package contains two archives:

wmsd_osa_x64.tar.gz

wmsd_osa.tar.gz

Copy one of the above PLUS the "boot" directory (only initrd.gz is required) PLUS the PackageSettings.ini, SDProfile.spf, and SDConnex.cer files to the target Linux system.

Untar the archive in some directory (e.g. osa) :

```
cd osa
```

```
tar -xvf wmsd_osa_x64.tar.gz
```

The CLI usage:

```
InstallApp [<command>] [<variables>][<options>]
```

If no valid command specified, InstallApp operates in a GUI mode

Supported CLI commands are:

Install	Used to install OSA client, the following variables are supported:
userid=<userid>	Specify userid, if not specified Linux userid is used
email=<email>	Specify email address for registration
firstname=<firstname>	Specify User's First Name
lastname=<lastname>	Specify User's Last Name
phone=<phone>	Specify User's phone
dir=<dir>	Specify working directory, if not specified, used "temp"
logfile=<logfile>	Specify debug log file name

Example of invocation:

```
sudo env LD_LIBRARY_PATH=. ./InstallApp install userid=joe phone="+1 977 102 833"
```

uninstall	Used to uninstall OSA client, the following variables are supported
password=<password>	Specify password for the SED pin key files obtained from SES. Currently all the files are expected to have same password

InstallApp command line interface (CLI) uses the working directory as a place to store temporary files. During installation InstallApp creates a pair of files <SED SERIAL>.dbk and <SED SERIAL>.enc. These files can be used to revert a SED to its default (not enrolled) state in case, for some reason, the InstallApp had terminated abnormally.

Example of invocation to use local pin files, located in the working directory

```
sudo env LD_LIBRARY_PATH=. ./InstallApp uninstall
```

Example of invocation to use pin files exported from SES

```
sudo env LD_LIBRARY_PATH=. ./InstallApp uninstall password=MyPassword  
status
```

Used to display current status of hard drives

Example of invocation

```
sudo env LD_LIBRARY_PATH=. ./InstallApp status
```

SD-27559 – SES Admin able to push certificates from SES to SecureDoc clients using Profiles for supporting shared certificates with 802.1x authentication at pre-boot

New options have been added to the Global settings and to the Windows Enterprise client and OSA device profiles to permit customers that require definition of Device Authentication Certificates to be used on certificate-authenticated 802.1X networks.

In the Global Settings, a new Device Authentication Certs panel permits the import of up to two Certificates (an original certificate, then prior to its expiration a second replacement certificate can be added).

In the Device Profile settings, a new option permits the Administrator to choose which of the above Certificates is to be sent to Client devices through the Profile. Once a new or replacement certificate has been connected to the Device Profile, all clients using that profile will become "out of date" and will download and apply the revised Profile at their next communication with SDConnex. Use of this new functionality for customers that use 802.1X Certificate-authorized Networks is covered the SES Administrator/User Guide for this version.

SD-27597 – During SES installation and/or upgrade all client installers are now available

In certain earlier versions of SES, the size of the SES installer had exceeded 2GB, a limitation of InstallShield. This had required that certain elements be removed (like the .msi client installers) from the SES installer to bring the installer executable below the 2GB threshold.

This issue has been fixed, and now all SES elements are installed from within a single executable.

SD-27867 – The SDProfile General section now has an option to control the Win10 upgrade message notification

Win10 upgrades can remove Password sync settings from the Windows Registry. SecureDoc offers automatic recovery against this removal and typically asks user to reboot once the recovery is done. With the new manual setting in SD profile this behavior can be controlled by customers.

SuppressWin10UpgradeMsg=

0 (display the message, default setting)

1 (automatically reboot right after Windows starts up)

2 (do nothing, a reboot is required in order to restore PwSync functionality)

SD-28195 / SD-28476 / SD-28477 / SD-28478 / SD-28479 – Update SFE Libraries

This version of SES and SecureDoc integrates the latest-available version of the file encryption libraries that underpin the SecureDoc File Encryption (SFE) functionality, necessary to support Windows 10 RS5.

SD-28202 – File date/time stamps are not changed after encryption process is completed

SecureDoc File Encryption has been improved to now ensure that SFE-encrypted files retain their original date/timestamp information after file encryption has completed, rather than be re-date-stamped to the date/time they were encrypted.

This was required because certain organizations perform audits at the file level to monitor for file updates or tampering, and under the previous method, SFE-encrypting a file (which did not alter the contents of the file) would result in numerous "false positive" file change results during such audits.

SD-27868 / SD-28244 – Hidden profile option to disable network detection for PBU only

An issue was raised by certain customers whose wired network is secured using 802.1x, to which the simple network handling built into UEFI is not capable of authenticating. In this scenario, any devices that use PBU-based Pre-Boot (SecureDoc's pre-boot for Native UEFI) would encounter lengthy delays at pre-boot while those devices would try each SDConnex server but fail to communicate due to the failure to authenticate via 802.1X.

This issue would not occur if users were using either Pre-Boot Linux (PBL) or the Linux-based Pre-Boot for UEFI (PBLU), which do support 802.1X-protected networks.

A solution to this has been implemented in this version which permits PBU to act like SecureDoc's V4 preboot in legacy mode, permitting deployment of a single profile, which retains PBLU networking, but disables PBU networking, thus ensuring there is no lengthy pause while PBU tries each of a lengthy list of SDConnex servers.

Result: For those customers that require this functionality, by adding PbulgnoreNetworkStack=1 into the SDSpace section of the SecureDoc Profile, any devices that were configured to use PBU will no longer attempt to connect to SDConnex at pre-boot, permitting the user to authenticate to a local key file without the lengthy delay mentioned above. This will not affect the use of the PBLU pre-boot, which has supplicant capability to connect to 802.1x.

Example of how to add this option:

```
----- beginning of SDProfile.spf file -----  
...  
[SDSpace]  
...  
PbulgnoreNetworkStack=1  
...  
----- end of SDProfile.spf file -----
```

SD-28316 – SES 8.3 introduces new Linux client device type Profile and Installation Package

With the advent of SES Version 8.3, WinMagic now offers the ability to manage endpoint encryption on Linux devices, such as Linux on Laptops, Desktops and virtual devices. Note that this is separate from its ability to manage Cloud-IaaS Servers running Linux inside Amazon AWS or Microsoft Azure

Initially, the license tracking for these new client types will be merged with the OSA/Linux licenses, so where customers wish to protect Linux devices they will need to have available the required number of OSA/Linux licenses. In a future version, WinMagic's intention is to track these Linux device licenses separately.

SD-28453 – Enable file security on local WM Directory folder has been removed

The Mac FileVault 2 Installation Package setting entitled "Enable file security on the local VM Directory Folder" has been removed from the SES User Interface.

The option to change this has been removed, and in the SES console logic, SecureDoc will enable file security on the local VM Directory Folder as a standard practice from this version onward.

Resolved Issues

SD-17511 – Preferred RMCE Key configurations were not correctly updating to macOS for auto RMCE creation

This issue is now resolved.

SD-26392 – Install fails to notify user or log errors if Profile is not found in the database

If, during the installation of the SecureDoc Windows Client, SES is unable to locate the Device Profile the client installer is configured to use, the installation continues instead of stopping and producing an error message.

Issue: When installing the Windows Client, if the profile is not found in the database, the client installation would continue without loading any profile. No warning or Log entry would be generated to notify the installer or deploying user that the profile was not found. The device would register successfully, but fail to ever communicate to SDConnex, nor provide an option to communicate. Manually importing the profile caused the system to regenerate a new device UniqueID and register as a new device.

This issue could occur if a customer has not updated their install packages after the profile index has changed. While this is an unusual issue, WinMagic determined it is necessary to produce an error message and abort the install if the profile is not found, in order to avoid this scenario.

This has been corrected in this version. Failure to find the SecureDoc Profile in SES will cause the SecureDoc Client Software installation to stop with an error message.

SD-26503 – SES 8.2 detected some Windows license as Hewlett-Packard license

This issue is now resolved.

SD-26530 – SDSERVICE was using 50% of CPU on Windows 7 (32 and 64-bit) system after the combination of: a) SecureDoc was upgraded from 7.1 SR5 to 8.2 and b) a new SecureDoc Profile was created and used on the device

This issue has been corrected, and SDSERVICE will not consume excessive amounts of the processor's bandwidth.

SD-26627 – SDSERVICE takes a long time to start and initialize during Windows Start-up

An issue was encountered by some customers that SecureDoc's SDSERVICE service would take a long time to start and SDPin would consider it to be "down" or inaccessible.

This has been corrected and SDPin will now wait longer before considering SDSERVICE to be "down" or inaccessible.

SD-27121 – Installing SecureDoc over existing Bitlocker-protected device would prompt user to enter Bitlocker Recovery Key

This issue has been corrected, and end users will no longer be prompted to enter the Bitlocker Recovery Key when SecureDoc assumes control/management of a device already protected with Bitlocker.

SD-26932 – Certain customers had found that, upon installing the SecureDoc client, they were no longer able to print via IPharm Print Software

Issue: It was determined that the version of the third-party library used to implement SecureDoc File Encryption was causing this blocking behavior.

Solution: This version implements an updated version of this third-party library and the iPharm Print Software incompatibility issue has been resolved.

SD-26933 – Failed to login at PBU with key file protected by IDPrime MD830B

Issue: Customers had been unable to authenticate under certain device/configuration combinations using Gemalto IDPrime Smart Cards.

This version corrects this issue and these Smart Cards can be used in all configurations.

SD-26988 – WMSD partition is shown after upgrading from 7.5.106.385 to 8.2.1.1253

Issue: Certain customers, having upgraded client devices from V7.5 build 106.385" to V8.2 SR1 build 1253" on Windows 10 (1703) found that the WMSD partition had become visible and accessible on the devices.

This has been corrected in this version.

SD-27466 – Exempted Devices list was showing as empty, even if there were devices that had been marked to appear in that list

Issue: Per our documentation, a device that does not fall under any of the policies applied to a folder is moved automatically to the Exempted Devices folder. This would provide customers with the mistaken impression that these devices had disappeared.

This has been corrected in this version, and the contents of the Exempted devices list will be visible in the SESWeb console.

SD-27524 – Error 0x7885 occurs during client install - Message "Cannot create a personal key when the same personal key name exists in SES" appears

Issue: When the global setting is enabled that defines that a personal key is to be created for each user, SES was failing to create a new key when the existing user's Key already exists in the database.

Earlier functionality had been disabled inadvertently which handles this scenario by incrementing the key number by 1 and trying to save the key under a numerically different name, which it would do up to 999 times in order to ensure it can create a new unique key name.

This functionality has been reinstated in this version.

SD-27799 – In some instances, the Drive list for a given device would not be fully populated with the device's disk drives during installation of the SecureDoc client software

This issue has been resolved in this version, and the drive list will be correctly populated with all the drives connected to the device.

SD-27749 – Message appears in SecureDoc Log after initial installation and then during initial encryption, SecureDoc fails with this message in Log file: "There are complications with sector size. Contact your Administrator. (0x8884)" in log file

This issue has been proved using VMWare client devices, and also on certain hardware having an Intel S2600GZ motherboard.

This issue seemed to appear starting with V8.2 SR1, when the combinations of the following were encountered: a) "Standard" mode conversion (Data Only), and b) WMSD (the SecureDoc partition) exists. The workaround was to configure the profile to encrypt every sector.

This issue has been corrected in this version.

SD-27818 – Rapidly repeated error logging occurred when attempting to use SecureDoc File Encryption to encrypt files whose full path + file name exceeded 260 characters, eventually consuming available disk space

Issue: Windows has a limit of 256 character path length. Windows explorer can access the actual folder path but if the folder path + File name resolved to be in excess of 260 characters in length, SecureDoc File Encryption (SFE) fails and keeps logging SFE-related errors

Note: The same issue occurred when folder path is 144 bytes in length or greater, and any folder after that fails to encrypt files.

In both cases the file having the long path would fail to encrypt, and SecureDoc would retry and keep logging this error in Windows until system has no disk space.

This has been corrected in this version.

SD-27881 – A problem has been corrected, under which, using the combination of Permanent Autoboot + No provisioning mode, the SecureDoc client was unable to be deployed using the currently logged-in user's AD user credentials and Error 0x7036 would appear

Context: Due to the above issue, SDConnex was mistakenly being sent an empty string instead of the user's password.

This issue has been corrected in this version.

SD-28120 – Apple Mac Clients generating numerous 0x971c errors in SDConnex logs under certain circumstances

This issue has been corrected, and communication from such client devices will no longer cause extraneous 0x971c errors in SDConnex logs.

SD-26923 – Removed SDOT attributes and PBA data from SES profile and SES GUI

Since SecureDoc no longer supports its own pre-boot authentication (PBA) layer for Apple macOS devices, the Device Profile main navigation landing page no longer offers a button link to the Boot Text and Color panel, which in previous versions had permitted definition of the attributes of the (now removed) SecureDoc Pre-Boot for FileVault 2 (previously referred to as SecureDoc On Top of FileVault 2, abbreviated as SDOTFV2).

SD-28645 – Malicious Code Injection risk found due to unquoted service definitions in registry.

Issue: A review determined there was some risk of malicious code injection attacks due to unquoted Service Paths, as detailed in CVE-2018-20341.

Solution: This has been corrected, and SES and SecureDoc will now encapsulate the paths to its services/components using quoted strings.

Limitations

SD-19208 – SecureDoc treats User IDs that use or do not use UPN format as separate user IDs, and will create separate Key Files and user-to-device relationships for these users.

If a user logs in to take ownership of a device after SecureDoc has completed initial encryption as (say) user123, and then later logs in using the UPN form of his/her user ID (say) user123@company.com, SES will send a second Key File to the device for this second user ID and will treat them as discrete users, even where those user accounts may involve single-sign-on to the same Windows account.

Work-around: Ideally, Customers should consider how they will be logging on to SecureDoc-protected devices and determine the format of their User IDs early in their implementation decisions. WinMagic recognizes that with the success of products like Office365 which encourages UPN sign-on, legacy customers may encounter issues with redundant key files.

WinMagic is investigating how best to mitigate this issue.

SD-23790 – If installing SES 8.1 or later on Windows 2008 Server SP1 or SP2, and attempting SecureDoc Services registration, an error message will appear relating to the WinMagic.SecureDoc.Management.ServiceSnapin.dll.

NOTE: This issue does not occur on Windows Server 2012 R2 or later.

Solution: Customers are requested to move SecureDoc Enterprise Server off Windows 2008 SP1 and SP2 and onto Windows 2012/2016-platform servers. SES no longer supports Windows Server 2008 SP1/SP2-platform servers, due to their lack of support for the .NET 4.7 Framework and Visual C++ 2017 which are required by SES 8.2+.

SD-24867 – UEFI: Failed to boot into Client's clone

SecureDoc does not currently support cloning of SecureDoc-protected vSphere instances through exporting the client to an OVA File.

WinMagic is working on determining how to surmount this limitation.

SD-26595 – Missing the red lock icon on the encrypted file with names longer than 255 characters on SDClient without required key

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-28979 – The SESWeb Browser-based Console does not render correctly in Internet Explorer.

Customers are recommended to use Chrome, FireFox or Microsoft Edge browsers. Internet Explorer is no longer officially supported.

SD-27811 – Dell Wyse 5070 unable to resume offline encryption after forced shutdown

If using SecureDoc Linux client installation on Dell Wyse 5070 Thin Client device with:

a) A Device Profile configuration that calls for the combination of Permanent Auto-boot and Offline-Standard encryption and b) power is interrupted during initial full disk encryption, then it is not possible to continue encryption following resumption of mains power.

Work-Around: Ensure any such devices are attached to an uninterruptible power supply (UPS) before starting initial encryption.

SD-28716 – Unable to deploy Cloud package to Windows server 2016

WinMagic has determined that installation of the SecureDoc Client on an Amazon AWS T1 Micro type Virtual Machine is not successful due to the lack of necessary memory. Installation on AWS requires 2GB of memory, minimum, which exceeds the typical memory size of the T1 Micro VM type.

SD-29033 – SecureDoc cannot support XenDesktop VDI where the virtualized device uses the combination of Windows 10 with EFI BIOS and is hosted on vSphere

Background:

- Citrix XenDesktop VDI can provision VM's hosted on either Xen Server or vSphere Private cloud platforms, and users are able to configure VM's with either EFI or Legacy BIOS.
- Xen Server platform currently only supports Legacy BIOS
- vSphere platform supports both EFI and Legacy BIOS
- SecureDoc is able to support all Legacy BIOS across both of these platforms - meaning when SD is installed on the master image the machine catalog creation process is able to create VDI VM's successfully.

However, for XenDesktop VDI (specifically), SecureDoc cannot support Windows 10 with EFI BIOS hosted on vSphere. The effect of attempting to install SecureDoc in this environment is that when SD is installed on the master image, the machine catalog process will fail. During the creation process the temp VM displays a BSOD error which causes the whole machine catalog creation process to fail.

Note that this issue does not affect the Horizon VDI, which does support Windows 10 EFI deployed with SecureDoc on vSphere.

How to Install/Upgrade

Customers with an active support plan should contact support@winmagic.com to receive the latest download links 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 (ey@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 - 2019 by WinMagic Corp. 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.

WinMagic, SecureDoc, SecureDoc Enterprise Server, Compartmental SecureDoc, SecureDoc PDA, SecureDoc Personal Edition, SecureDoc RME, SecureDoc Removable Media Encryption, SecureDoc Media Viewer, SecureDoc Express, SecureDoc for Mac, MySecureDoc, MySecureDoc Personal Edition Plus, MySecureDoc Media, PBConnex, SecureDoc Central Database, and SecureDoc Cloud Lite are trademarks and registered trademarks of WinMagic Inc., registered in the US and other countries. All other registered and unregistered trademarks herein are the sole property of their respective owners. © 2019 WinMagic Corp. All rights reserved.

© Copyright 2019 WinMagic Corp. All rights reserved. This document is for informational purpose only. WinMagic Inc. makes NO WARRANTIES, expressed or implied, in this document. All specification stated herein are subject to change without notice.