SecureDoc Enterprise Server

Release Notes

Product Version: 9.0 SR2

Published December 9, 2022

SecureDoc by WinMagic

Contents

SecureDoc Support 2
About This Release 3
System Requirements 3
Client OS Support 4
The KnownConfigs.XML File 4
Version 9.0SR2 5
How to Install/Upgrade 6
New Features 7
Authentication 7
macOS 8
Linux 8
SaaS – Software as a Service 8
Improvements 8
SecureDoc Console or SESWeb Console 8
SecureDoc Client - Linux 12
SecureDoc Client - Windows 12
SecureDoc Client - macOS 12
Authentication 13
Authentication - Recovery 15
Encryption 16
Encryption - Linux 16
Resolved Issues 17
SecureDoc Console or SESWeb Console 17
Authentication 17
Authentication - Tokens 18
Linux 19
Encryption 19
SecureDoc Client - Windows 19
Limitations 20
SES Console or SESWeb Console 20
MacOS Devices 20
Authentication 21
Authentication – Remote Desktop 26

Contact WinMagic 27
Acknowledgements 27

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.

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.

Version	Release/EOL Dates	Details / Build Information
9.0 SR2 (Current)	December 9, 2022 EOL: Dec 8, 2025	New Features, Improvements, and fixes (server/client) Build# 9.0.200.207 (Server, all other clients), Build# 9.0002.198 (macOS)
9.0 HF1	September 7, 2022 EOL: Mar 30, 2025	Hotfix containing improvements (see release notes) Build#9.0.001.1053 (Windows client installer only)
9.0 SR1	July 21st, 2022 EOL: Jul 21, 2025	New Features, Improvements, and fixes (server/client) Build# 9.0.100.149 (Server, all other clients), Build# 9.0001.73 (macOS)
9.0	March 31st, 2022 EOL: Mar 30, 2025	New Features, Improvements, and fixes (server/client) Build# 9.0.000.1047 (Server, all other clients), Build# 9.000.1030 (macOS)
8.6 SR1	September 8th, 2021 EOL: Sep 7, 2024	New Features, Improvements, and fixes (server/client) Build# 8.6.100.148 (Server, all other clients), Build# 8.6001.85 (macOS)
8.6	December 8th, 2020 EOL: Dec 7, 2023	New Features, Improvements, and fixes (server/client) Build# 8.6.100.148 (Server, all other clients), Build# 8.6000.594 (macOS)
8.5 SR2	June 11th, 2020 EOL: Jun 10, 2023	New features, improvements, and fixes (server/client) Build# 8.5.200.688 (Server, all other clients), Build# 8.5001.632 (macOS)
8.5 SR1	April 8th, 2020 EOL: Apr 7, 2023	New features, improvements, and fixes (server/client) Build# 8.5.100.638 (Server, all other clients), Build# 8.5001.632 (macOS)
8.5	December 5th, 2019 EOL: Dec 4, 2022	New Features, Improvements, and fixes (server/client) Build# 8.5.000.480 (Server, all other clients), Build# 8.5001.448 (macOS)

NOTE: End of Life date for Hotfixes is the same as the Version or Service Release upon which they are based.

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

System Requirements

If using features that use the TPM (e.g., MagicEndpoint, or other TPM-based authentication such as TPM protection for Key Files), devices must have TPM 2.0 – TPM 1.2 or earlier are not supported.

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 for the console to function properly.

Client OS Support

Devices utilizing MagicEndpoint authentication must have Windows 10 or 11 – Windows 7 is not supported.

For a detailed view of which specific versions of SecureDoc are supported under various versions of Windows, macOS or Linux: See: https://www.winmagic.com/support/technical-specifications

Mobile Token-based authentication using Bluetooth is not supported on any pre-Windows 10 Operating Systems

The KnownConfigs.XML File

Customers are strongly advised to download the most current KnownConfigs.XML file, then replace the current version (if older) in the SES Application folders and

Installation Packages.

WinMagic strongly recommends that you seek out the most up-to-date version of the KnownConfigs.XML file and incorporate it into your SES implementation on a regular basis (e.g., monthly). This will help ensure your SES Version will take advantage of new client installation override settings that have been added since the version of the KnownConfigs.XML file that came with your version of SES. This will improve installation success on any new device makes/models you might purchase since installing SES, utilizing the new special settings available in newer versions of this file.

Customers are advised to look to the SecureDoc Knowledge Base for a link to the available KnownConfigs.XML files, then check that document (e.g., on a monthly basis) for updates to this file, then use the new version to replace all versions of the KnownConfigs.XML file in their SES Implementation folder structure. For example:

1. Position Windows Explorer to: c:\Program Files(x8)\WinMagic\SDDB-NT, then

2. Search for files like *.xml.

3. Sort the resulting search list by name

4. In each directory where a KnownConfigs.XML file is found, replace it with the new one that you have downloaded from the WinMagic Knowledge Base article.

Additional information can be found here: Installing or updating the KnownConfigs.xml file (Applies to SES from Version 7.5 onward).

The latest versions of the KnownConfigs.XML files can be found at the following links:

- SecureDoc Device KnownConfigs.XML File for SES V8.2 And Later- Download the

latest version of this here: https://na80.salesforce.com/articles/Service/SecureDoc-Device-KnownConfigs-XML-File-for-SES-V8-2-Download-the-latest-version-of-this-here

- SecureDoc Device KnownConfigs.XML File for SES V7.5 - Download the latest

version of this here: https://na80.salesforce.com/articles/Service/SecureDoc-Device-KnownConfigs-XML-File-for-SES-V7-5-Download-the-latest-version-of-this-here

The contents of the KnownConfigs.XML file are reserved to be developed and advanced by WinMagic solely. While customers might consider enhancing it, WinMagic cannot be held responsible for issues that might arise from such modifications and may (at its sole discretion) levy an additional support charge to any customers that encounter support issues that can be traced back non-sanctioned customer-initiated changes to KnownConfigs.XML.

WinMagic welcomes customer ideas and suggestions on how KnownConfigs.XML can be extended and improved, but WinMagic reserves the sole right to test, approve and to publish any changes to KnownConfigs.XML that it deems to be in the broader customer interest, and makes no commitment to act upon or publish all, or indeed any customer-recommended changes.

Version 9.0SR2

Which customers should upgrade to 9.0SR2?

Version 9.0SR2 is a Service Release upgrade to the SecureDoc Enterprise Client and Server.

All customers are recommended can safely upgrade to 9.0SR2.

NOTE: Any customers wishing to use Microsoft Azure AD (as opposed an on-premises Active Directory) must upgrade to V9.0 (or higher). Azure AD is not supported on earlier versions of SecureDoc Enterprise Server.

Any Azure AD-joined Devices must be either initially installed using V9.0, or any existing devices that will be joined to an Azure AD must be upgraded to the V9.0 (or later) client software before being joined to the Azure Active Directory.

NOTE: SecureDoc installer now **no longer supports installation on macOS Mojave**. Version 9.0SR2 ends support for macOS Mojave, and as a result the macOS Mojave target has been removed from the SecureDoc executables framework, installation, and run-time scripts.

IMPORTANT: For customers wishing to utilize **SecureDoc's Bluetooth Low Energy mobile device-based authentication at Pre-Boot:**

1 - At this stage, Bluetooth Low Energy-based authentication is not supported on Hardware encrypted devices/Self-Encrypting Drives, so the disk must be software-encrypted

2 - The device Profile must specify the Linux-based Pre-Boot (whether for legacy BIOS or for UEFI devices) – termed as either PBL or PBLU in this documentation.

3 – Bluetooth must be enabled in the endpoint computer's hardware configuration (BIOS or UEFI settings)

Where the use of Bluetooth Low Energy mobile device-based authentication is a compelling security feature., customers wishing to use it on devices equipped with Self-Encrypting Drives (SEDs) must convert such devices to software-encrypted. Such devices can be rapidly decrypted, then a new profile should be applied to them that has the profile option "Use hardware encryption if available" un-selected/un-checked. Once applied, this new profile will re-encrypt the drive using software-based encryption. Following completion of such software encryption, Bluetooth Low Energy mobile device-based authentication becomes possible (if so configured) on such devices.

NOTE: These release notes are presented in a new format compared to prior releases. A) Rather than leading with the ticket number(s), these will include the ticket(s) at the end of each release note; b) Issues and improvements will be grouped into meaningful groups that discuss specific aspects of the product (e.g., Authentication, Server, client, and other groupings).

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.

New Features

Authentication

SecureDoc's Authentication now supports Token-based Authentication using Phone as authenticator (via Bluetooth) for Windows and pre-boot authentication.

Issue: WinMagic is constantly striving to make Windows Login and SecureDoc Pre-Boot Authentication to be the Gold Standard for advanced authentication into Encrypted Endpoint devices.

Solution: In this version, WinMagic adds support in SecureDoc for Windows Login and Pre-Boot Authentication for Token-based Authentication where the Phone is the authenticator (via Bluetooth). Note that this applies only to the Linux-based Pre-Boot (PBL and PBLU) environments - it does not apply to native UEFI environment due to limited capabilities inherent in the UEFI environment. A new pre-boot icon indicates Bluetooth roaming/link status.

Affected tickets: SD-36728, SD-38599, SD-38614, SD-38615, SD-38616, SD-38750, SD-40407

Major new features in support of Mobile Device-based Authentication

Issue: WinMagic is rapidly improving and positioning MagicEndpoint and Mobile Device-based MFA

Solution: New features and functionality include: Bluetooth Low Energy (BLE)-based Phone enrollment; Creation of SecureDoc boot key files for Windows users now supports their conversion to phone-based protection when new users log into Windows; New central management for phone-based Key File policy; Challenge/Response recovery has been added to the Windows Login and to SecureDoc Control Center when user has a BLE-protected Key File to ensure users can still access endpoints if the user's Phone is unavailable; New ability to secure the Endpoint and Phone using pairing; New ability to renew user's certificates on phone and to store renewed certificates in SES; Storing the token-converted Key File public key to the SES database.

Affected tickets: SD-42477, SD-42504, SD-42505, SD-42506, SD-42507, SD-42508, SD-42509, SD-42138

Challenge/Response recovery is now possible for both SecureDoc Credential Provider and the SecureDoc Client Control Center application, to ensure that users who rely upon Multi-Factor authentication (e.g. using their Phone's WinMagic Authenticator app) can still access these if the phone is lost, battery dead, etc

Issue: It is necessary to support a workaround means of authentication to bypass Multi-Factor Authentication at Windows login or at SecureDoc Control Center login if the user's normal factor of authentication (e.g. phone) is not available.

Solution: Users can log in using Challenge-Response at the SecureDoc Credential Provider, or at SecureDoc Control Center login - much as they can do at Pre-Boot.

NOTE: The SecureDoc User Account must exist on the device (usually Password Sync is enabled), otherwise the Challenge/Response option will not be available.

Affected tickets: SD-42506, SD-42508, SD-42800

---

macOS

Support has been added for macOS Ventura

Linux

SecureDoc supports deployment on RHEL 8.x hardened systems (NIST)

SaaS – Software as a Service

SaaS – Installation/management for MSPs (Managed Service Providers) is supported for deployment in a SaaS environment by an authorized MSP.

Improvements

SecureDoc Console or SESWeb Console

New settings permit allowing/blocking Administrators from logging in to several concurrent SESWeb console sessions.
Issue: It is common that an SESWeb Administrator may need to log in to the console more than once and maintain several open sessions. This has been the default behavior in previous versions. However, it should also be possible to block this behavior, ensuring a given Administrator can only be logged on to one SESWeb Console session at a time.

Solution: A new "EnableSimultaneousLogin" field settings in the SES Web Web.config file. The default value of this field is FALSE, which means SES-WEB allows Simultaneous login as it has done historically. If the value is set to TRUE, once an Administrator logs in for the second time, upon electing to access a panel within the SESWeb interface, the user's earlier session will be logged out. NOTE: This feature will not work if SESWeb access is accessed through a network load balancer.

Affected tickets: SD-29967

SESWeb console now shows the last time the user logged into the console.

Issue: Administrators find it beneficial to know when the Administrator console was last logged into, allowing the Administrator to spot potential compromise situations where another person has logged into their credentials.

Solution; This information has been added to the SESWeb so that Administrators can readily see when their login credentials were last used. The last logged in information appears on the system page of SESWeb.

Affected tickets: SD-41800

The Self-Help Recovery Question selection function has been moved from the Installation Package to the Device Profile on SESWeb (to conform to how it is in the SES Console)

Issue: There have been concerns that the Self-Help Question/Answer combinations set by users are retained (effectively) indefinitely and form a sort of secondary password which is not subject to any form of regular rotation. For the sake of greater security, it would be ideal if users could be forced to answer a different set of questions on an Admin-defined basis.

Solution: In a redesign of some of the product functionality, the process of selecting which of the Globally-defined Self-Help Recovery questions to send to endpoint users during installation has been moved to from the Installation Package to the Device Profile. This permits Administrators to either a) Deploy new questions to users by altering the existing questions in the Profile (which will then update devices that have that profile) or b) Creating an equivalent profile (or profiles) encompassing different questions, then sending that/those profile(s) to endpoints. These options will ensure users will be obliged to answer said different questions or update their answers on existing questions.

NOTE: Self-Help Question selection and deployment has been moved into the Device profile from the Installation Package.

Both the SES Console and the SESWeb console have UI elements in the Profile (and these have been removed from the Installation package definitions). Devices running older versions of the SecureDoc Client can be upgraded to this new one without being forced to make any question/answer changes – their existing questions and answers will be retained. However, if later updated to a Profile that contains questions/answers, they will be prompted to answer the new questions present in the Profile.

Affected tickets: SD-42525

In SESWeb the profile now includes an option to permit enforcing Multi-Factor Authentication for the native Windows login.

Issue: SES Console has this option from a previous version, but SESWeb had no analogous option.

Solution: In SESWeb, on the Authentication and Recovery panel's Multi-Factor Authentication section, this option has been added for consistency with the SES Console.

Affected tickets: SD-42635

A Dashboard showing Pie-Charts, and reports have been added to SESWeb to provide heuristics and context to the deployment of MagicEndpoint within the enterprise.

Issue: As MagicEndpoint progresses as an Enterprise-level authentication solution, strong visibility features are required to aid Administrators in understanding the status of deployment and other information across the Enterprise.

Solution: A Dashboard showing Pie-Charts, and reports have been added to SESWeb to provide heuristics and context to the deployment of MagicEndpoint within the enterprise. Pie-Chart "Slices" can be clicked on to drill down into the detailed information underpinning them.

Documentation needs to be updated to include screenshots of the Dashboard, and reference information on the types of reports available - affects SESWeb documentation. See Description field for info on how to present that.

Affected tickets: SD-42672

In SESWeb there is now a color-based visual cue in the "No Communication" column, to highlight devices that have an alert status due to lack of communication within a set period to the SES server.

Issue: The lack of an easy way to spot devices that had failed to communicate to SES within the period of time set by an alert rule was identified in V8.6SR1.

Solution: This issue is fixed on SES 9.0 SR2. Devices that have breached the no communication rule will appear with text in black on a red background in the No Communication column, which shows how long since the last communication from the device.

Affected tickets: SD-42860

Authentication settings for SESWeb now permit removing the option of logging into SES Web using a username/password once use of Identity Provider-based authentication has been set

Issue: MagicEndpoint now offers the Administrator the option to log in using the strength of Identity Provider-based authentication, rather than sending a password across the network. However, SESWeb should offer the option to log in either using Identity-Provider authentication, or (optionally) be able to log in using the Administrator's local credentials (local being as they're known to the server).

Solution: With this change, once the use of Identity Provider-based authentication has been defined, it should be possible to use IdP-based authentication. However - the Administrator can also define whether local credentials can continue to be used, or not.

Affected tickets: SD-43145

Enhanced Security Measures for SES Web Login

Issue: In previous versions, SES Web relied on the encryption provided by the TLS session to secure user authentication parameters. This method, while effective, left room for potential vulnerabilities in the transmission of user credentials during the login process.

Solution: New security measures have been implemented to enhance the protection of user credentials when logging into SES Web. Now, SES Web generates a new RSA key pair on startup. The public key is embedded into the HTML template, which is then used to encrypt the password field before establishing the TLS session with the server. The server uses the corresponding private key to decrypt the authentication parameters, ensuring that the credentials are securely transmitted and protected from potential interception.

Affected tickets: SD-43536

SecureDoc Client - Linux

SecureDoc now supports SDLinux deployment on RHEL 8.x FIPS enabled systems

Issue: Previous versions of SecureDoc supported deployment on RHEL 7.x systems with FIPS enabled, but in those versions RHEL 8.x was not FIPS-certified yet. During attempts to install earlier versions on RHEL 8 FIPS version, the installation would proceed successfully but upon automatic reboot, at start-up the system could no longer boot back to the OS.

Affected tickets: SD-38249

SecureDoc Client - Windows

SecureDoc Windows client now supports Thales IDPrime 930 smart card for Pre-Boot Authentication

Issue: In previous versions there was no support for the Thales IDPrime 930 smart card.

Solution: The SecureDoc client now supports Thales IDPrime 930 smart card for Pre-Boot Authentication. It must be configured using the "Certificate on Token" mode.

Affected tickets: SD-39955

SecureDoc Client - macOS

To support macOS Ventura, an additional step is required to add SecureDocD to System Settings -> Privacy & Security -> Full Disk Access.

Issue: As was encountered in earlier versions to support macOS Monterey, the SecureDocD program file must be added to System Settings -> Privacy & Security -> Full Disk Access.

Solution: During SecureDoc installation, a Finder window will be opened to the location where the SecureDocD file is located. The user must then drag and drop SecureDocD into the System Settings -> Privacy & Security -> Full Disk Access panel, which will automatically enable SecureDocD once dragged-and-dropped.

Affected tickets: SD-42603

Authentication

SecureDoc Pre-Boot networking has been improved to permit retention of a number of Wi-Fi SSN/Authentication combinations for Wi-Fi access at multiple locations (e.g. work, home, etc.).

Issue: In previous versions, only one Wi-Fi SSN could be stored at a time, so where end users need to move from work to home and back again, they would face having to re-enter the Wi-Fi credentials for each of those networks, since logging on to one network would wipe out the credential settings of the previous one.

Solution: This is corrected in V9.0SR2. With this solution, a list of available networks is shown, allowing the user to select any available entry and try to connect to the corresponding network using either the "Connect" button or by double clicking on the selected table entry.

An attempt to connect to an un-saved network will be preceded with a Wireless Security Settings dialog where user should choose the appropriate connection type, enter user ID (if required) and password and continue connection with "Connect" button or just pressing "Enter" key right after entering password.
Each such new manual connection will save the connection parameters into user defined wireless connection list, and the new connection (new SSID) will be put on top of the list. The oldest connections will drop off the list once the number of entries exceeds the maximum allowed (currently 5).

Affected tickets: SD-40974

The updated NIST library supporting the PIV standard has been integrated into SecureDoc/SES, offering support for new smart cards.

Issue: Without integrating this library into SES, certain PIV cards will not work correctly at SecureDoc's Pre-Boot.

Solution: SecureDoc now has implemented support of new PIV cards, version 2, including new/optional features that were introduced in SP 800-73-4. This version contains the library necessary to provide this integration, and to support these new PIV cards.

Affected tickets: SD-41449

RDP Login has been restructured to permit No User Action authentication via integration between SecureDoc Credential Provider and MagicEndpoint, MagicEndpoint IdP

Issue: The use of MagicEndpoint's new authentication strengths could provide major ease-of-use coupled with authentication strengthening for users who use Remote Desktop.

Solution: Improvements to the Through the use of MagicEndpoint, MagicEndpoint IdP, coupled with SecureDoc Credential Provider on the remoted-to desktop, the result is a No User Action authentication experience for the RDP login.

Affected tickets: SD-42375, SD-43499

An option has been added to configure the authentication of users against Azure AD through SDConnex

Issue: Where customers have their Local AD synchronized to Azure AD, it should be possible to authenticate users against Azure AD.

Solution: This shortcoming has been corrected in this version and is beneficial for SaaS users where the SaaS-hosted SES cannot communicate with an on-premises Active Directory.

Affected tickets: SD-42733

In SESWeb, the Installation Package option specifying that the Key File is to be converted from Password to Token-protection has been moved into the Device Profile.

Issue: Particularly with the advent of MagicEndpoint and MagicEndpoint IdP-based authentication, greater flexibility is required in managing which devices will use Token-based Key Files.

Solution: The Installation Package option specifying that Key File is to be converted from Password to Token-protection has been moved into the Device Profile. This option was chosen since the Installation package's "sphere of influence" expires at the end of installation, and even during a client upgrade its ability to effect changes on the client are much less flexible than using a Device Profile, which can be deployed to a device ad-hoc by the Administrator.

NOTE: Existing customers who have updated to this version will need to transcribe their historical Token settings from existing Installation Packages to the Profiles they will be using to install SecureDoc on new devices since NEW devices that will be installed using this (or later) versions of SES will only receive their Token settings from the Profile used.
Old settings will remain in the Packages, so previously-deployed devices will continue to use the Installation Package .ini file settings, as they have in the past. Such devices will be unaffected by Token Settings sent via Profile changes.

Affected tickets: SD-42735

The SecureDoc Credential Provider user interface has been changed to conform more closely with the Windows Login.

Issue: Many users have different accounts that are used depending on their rights (e.g., a given user may act as a Manager/Administrator, as well as a User), so a means must exist to permit the user to choose the right account to log in to Windows with. To this point, the SecureDoc Credential Provider login user interface has been distinct from what is used at Windows.

Solution: In this improvement over V9.0 and V9.0SR1, the user selection will be done using native Windows tools rather than a SecureDoc-specific prompt. This also eliminates the need for an additional click to continue that had existed in those prior versions.

Affected tickets: SD-43172

Global Settings can now define that SDConnex can perform user authentication against Active Directory plus Azure AD and OKTA. If using Azure AD, a new field permits definition of the Azure AD AppID.

Issue: Many customers include Azure AD or OKTA Universal Directory into their Directory Services, and SDConnex/PBConnex must be able to be configured to authenticate against these alternatives to Active Directory.

Solution: A new portion of the Global settings Other panel now includes areas in which an Azure AD AppID can be defined, plus the Administrator can enable use of Azure AD (which requires that the Azure AD AppID has already been entered), and/or OKTA Universal Directory, and/or traditional Active Directory services.

Affected tickets: SD-43320

Authentication - Recovery

Where customer is using SecureDoc Credential Provider with 2-factor authentication for Windows Login, users have access to full Challenge/Response functionality, including numerals-only recovery string

Issue: Where the SecureDoc Client has been deployed successfully with the settings in the profile to permit a numeric-only Challenge/Response option, the Challenge/Response panel shown at Credential Provider login should show the numeric options, similar to what is shown at Pre-Boot.

Solution: In this version, the Challenge/Response panel shown at Credential Provider login now shows the numeric Challenge and Recovery options, like what is shown at Pre-Boot, as well as displaying the same guidance information (e.g. who to call for Challenge/Response assistance) that appears at Pre-Boot.

Affected tickets: SD-43328, SD-43350

Following Challenge/Response recovery to successfully unlock the device at SecureDoc Credential Provider, the user now gets directly into the Windows Desktop.

Issue: Having deployed a package that specified Linux-based Pre-boot, software encryption of the disk and use of SecureDoc's Credential Provider to handle Windows Logon, there had been a problem with users being prompted again to perform multi-factor authentication (e.g. using their phone) before they could get to the Windows Desktop AFTER they had successfully performed Challenge/Response recovery to unlock the Key File at the SecureDoc Credential Provider.

Solution: This issue has been corrected, and upon completing Challenge/Response Recovery at the SecureDoc Credential Provider login panel into Windows, the device will correctly take the user to the Windows Desktop.

Affected tickets: SD-42550

Encryption

NIST updates to the FIPS implementation guidelines have mandated these be implemented into newest macOS SecureDoc Client installers, to ensure that the active-list modulus "sunset date" is extended to ensure applicability.

Issue: After 2021, applicability of our FIPS certificate became limited (moved to historical list), so compliance requirements mandated changes to ensure compliance with the validation standards.

Solution: The macOS installer in SES V9.0SR2 has been updated to include the current FIPS validated model.

Affected tickets: SD-41713

The latest drivers underpinning SecureDoc File Encryption have been integrated into the core of the SES client installers

Issue: As Windows evolves, the drivers that underpin the SecureDoc File Encryption feature must be updated to ensure compliance with Windows internals.

Solution: The latest release of the drivers that underpin SecureDoc File Encryption have been integrated.

Affected tickets: SD-43501

Encryption - Linux

SecureDoc for Linux now supports deployment on Ubuntu FIPS-mode systems.

Issue: Earlier versions of SES were unable to create a SecureDoc installer that could maintain end-to-end FIPS-validation on some versions of Ubuntu when in FIPS-mode.

Solution: This issue has been corrected, and SES can now create FIPS compliant installations of the SecureDoc for Linux client on FIPS-mode versions of Ubuntu, supporting 18.04 and 20.04.

Affected tickets: SD-43446

Resolved Issues

SecureDoc Console or SESWeb Console

SESWeb data exports of Device List report contents to a CSV or XLSX file would be corrupted or would contain only a single row of data

Issue: SESWeb data exports of Device List report contents to a CSV or XLSX file would be corrupted or would contain only a single row of data.

Solution: This issue has been corrected in this version.

Affected tickets: SD-42390

Authentication

Error "No private Key in Token(0x7730)" encountered upon logging into SecureDoc pre-boot on RHEL7 when using smart card: ID-One PIV 2.4 From IDEMIA.

Issue: An error message "No private Key in Token(0x7730)" can be encountered upon logging into pre-boot using PIV smart card: ID-One PIV 2.4 From IDEMIA. This was found on an endpoint running RedHat RHEL-7, and no similar errors were encountered with older PIV cards.

Solution: This issue has been resolved in SES V9.0SR2

Affected tickets: SD-41112

Some users found they had no user rights in SecureDoc Control Center on fresh installs of SecureDoc 9.0

Issue: Customer upgraded to SES V9.0 from SES V8.5, then created a NEW installation package using the SES V9.0 console.

When a user (known to have full admin rights) logs into the SecureDoc Control Center on a device NEWLY installed using this installation package, they have no rights.

The issue does not occur if the Installation Package is used to upgrade a device that already has the previous version (8.5) of SecureDoc on it.

Solution: This issue has been corrected in this version, and users will have the expected rights.

Affected tickets: SD-42443

An issue encountered in which PBConnex network-brokered autoboot was not working on SD V8.6 SR1, or V9.0 on Dell 5420/5520 devices.

Issue: WinMagic determined that the issue was caused by incompatibilities with the Network Interface Cards (NICs) installed in these models.

Solution: To correct for this issue, V9.0SR2 can adapt to these NIC models when the Device Profile is manually changed as follows:
A parameter must be added to the "Boot parameters" field (separated by a space if the field is not empty) in the SecureDoc Control Center application on the affected endpoint devices: Once in SecureDoc Control Center, go to Boot Control | Advanced Options | select tab: Advanced Options".

Add the following:

e1000e.CheckNVMCrc=0

Save the changes, restart the device and PBConnex Autoboot will work.

Affected tickets: SD-42467

In V9.0SR1, WinMagic added the "owl" image to the SecureDoc Credential Provider. Certain customers found it flashed on-screen briefly, others found it remained too long - for several seconds.

Issue: Previous version of 8.5, 8.6 and 8.6 SR1 had no WinMagic login screen nor the owl logo/page. With 9.0 SR1, the owl picture flashes just after the user logs into Windows and is intended to remain on-screen for approximately 3-5 secs before it disappears. Some customers who noticed it flashed very briefly and disappeared found it disturbing as it was so brief, they were unsure what it was.

Solution: The image now shows for the same duration under all circumstances.

Affected tickets: SD-42761

Authentication - Tokens

Random failures to authenticate were encountered when using Yubikey tokens, receiving error code 0x7721 (card reader error).

Issue: Certain customers using Yubikey tokens at Pre-boot for key protection were encountering issues where authentication would randomly fail - approximately once in 10 attempts to authenticate at Pre-Boot. This issue was detected on Dell Latitude 5521, though other device types might have been affected. A customer claimed this issue began a few weeks ago on devices that had been deployed some months earlier.

Solution: This issue has been resolved in this version.

Affected tickets: SD-42297

Linux

An issue was encountered with SecureDoc for Linux build 8.6.100.148 (8.6SR1). Following what appeared to be a successful installation the device would not boot to the Linux OS.

Issue: A customer deploying SDLinux version 8.6.100.148 (in this case on DELL Latitude 5310 and Precision 7530 devices running RHEL OS 8.4 (kernel 4.18.0-305)). Drivers were checked successfully, and the devices registered to the SES system, but when the devices rebooted, they did not boot up to the Linux OS.
Note that this issue did not occur on the same Dell Latitude 5310 machine with Ubuntu 20.04.3 installed.

Solution: This issue has been corrected in V9.0SR2

Affected tickets: SD-42769

Encryption

Dell 5531 machines were encountering issues during installation. They were not launching initial encryption.

Issue: In a previous version of SecureDoc, Dell 5531 machines were encountering issues during installation - they were not launching initial encryption.

Solution: In this version, this issue has been corrected and Dell 5531 models will encrypt successfully.

Affected tickets: SD-42844

SecureDoc Client - Windows

Missing balloon message for failed login attempts at Boot Logon in Windows screen on Windows 11 22-H2

Issue: In version 8.6SR1, when using Fast Startup with a Self-Encrypting Drive, SDService will not synchronize pre-boot data from OPAL::DS to the mirror-SDS. As a result, SDPin won't detect any failed logins which were recorded in the OPAL::DS. From the SDService log, it seems the client does not log the POWER TRANSACTION notification event when the device powers on with Fast Start-up enabled.

Solution: This has been solved in this version, and failed login attempts when using Fast Startup with SED disks be correctly reported once the user has logged in at Windows.

Affected tickets: SD-43284

Limitations

IMPORTANT: Mobile Token-based authentication using Bluetooth is not supported on any pre-Windows 10 Operating Systems.

SES Console or SESWeb Console

Where setting up groups to be notified via Email of alarm events in SES, there is no support for sub-groups at present

Issue: SES allows for the configuration of groups (typically of administrators or security monitoring professionals) who will be sent an email when alarm-specific events occur. However, where a group contains a subgroup, and that subgroup references users, those subgroup users will not be sent a notification.

Solution: WinMagic is looking to find a solution for this issue, but for this version, where group members to be sent emails please ensure that those users are added directly to the specific group associated with alarm emails - and not to a sub-group of that group.

Affected tickets: SD-42910

MacOS Devices

SecureDoc installer now no longer supports installation on macOS Mojave.

Issue: macOS Mojave is old enough that WinMagic no longer supports it.

Solution: Version 9.0SR2 ends support for macOS Mojave. The macOS Mojave target has been removed from the SecureDoc executables framework, installation and run-time scripts.

Affected tickets: SD-42090, SD-43242

Authentication

Bluetooth-based Authentication will not work with devices using SecureDoc Pre-Boot for Native UEFI (PBU) or older versions of SecureDoc

Issue: SecureDoc authentication using Bluetooth does not work where the device has SecureDoc's Pre-Boot for Native UEFI devices (PBU) implemented, and any devices using Bluetooth authentication must have SecureDoc 9.0SR2 installed.

Affected tickets: SD-42658

Where customers utilize WinMagic Mobile Token (Phone)-protected Key Files, the global setting for Password Expiry should be set to not permit Passwords to Expire

Issue: Where the Global Setting for Password Expiration is set to a non-zero value (e.g. 120 days), this setting can adversely affect user Key Files that are protected by a WinMagic Mobile Token (phone-based via Bluetooth).

Work-Around: Until WinMagic has a solution that will permit such Mobile Token-protected Key Files to ignore Password Expiration rules (which are set at the Global level), customers are requested to not set a Password longevity value (a zero indicates that passwords never expire) in the Global settings.

Since many customers synchronize to Active Directory and to the Windows password, in practical terms the password updates will tend to occur anyway based on the settings defined in Active Directory or Windows for password retention.

Affected tickets: SD-43302

Lenovo ThinkPad L14 Gen 3 AMD devices unable to perform Bluetooth phone-based login at Pre-boot – displaying error "BT device not found" appears

Issue: The wireless Network Interface Card (NIC) ID installed in these Lenovo devices is 14c3 ("MEDIATEK Corp."), device: 0616 ("MT7922 802.11ax PCI Express Wireless Network Adapter") also incorporates the Bluetooth functionality.
The SecureDoc Pre-Boot Kernel does not support this hardware in the Linux versions used in V9.0SR2 and prior.

WinMagic will strive to incorporate this into the Kernel in a build after 9.0SR2 as it encompasses a complex and substantial Pre-Boot Linux kernel change.

Work-Around: If possible, customers who wish to use PBConnex with Bluetooth-enabled mobile device-based authentication should consider purchasing a compatible USB-pluggable Bluetooth adapter capable of Bluetooth Low Energy communication, and disabling the internal Bluetooth adapter in the device BIOS. WinMagic recognizes that some devices have unsupported Bluetooth hardware and is beginning validation of USB-connected Bluetooth adapters.
One such adapter is: ORICO-BTA-608 Bluetooth 5.0 (Realtek driver - RTL8761B), which has passed our QA testing. More information available at: https://www.orico.cc/usmobile/product/detail/id/7382Affected

Affected tickets: SD-43363

Use of the option "Lock computer when token is removed" is incompatible with use of Bluetooth Low Energy-based authentication.

Issue: If SecureDoc is deployed to an endpoint device with these options enabled:
- Credential Provider-based Single Sign-on
- Lock computer when token is removed.
- Bluetooth Low Energy mobile token-based authentication
and the MagicEndpoint client is installed.

Sequence: Following installation of SecureDoc Pre-boot, initial encryption, then the Client device is converted to Bluetooth Mobile Token-based authentication successfully

Following a reboot, instead of the user being able to log in at Pre-Boot using the Mobile Token and then Single Sign-on into Windows via the SecureDoc Credential Provider, the device instead prompts the user to authenticate at SecureDoc Credential Provider.

Further, if using Self-Help or Challenge/Response recovery at Pre-Boot (which are successful), instead of the device correctly performing Single Sign-on into Windows via SecureDoc Credential Provider, again the device prompts the user to authenticate at Credential Provider. In this case, the user is able to login using the Mobile token but is then prompted to change his password or PIN.

Solution: If intending to use Bluetooth Mobile Token-based authentication. do not configure use of the Profile option "Lock computer when token is removed".

Affected tickets: SD-43667

For Azure AD-joined users, Password Synchronization does NOT work after the user has changed his password using SecureDoc Control Center

Issue: Currently, SDCC is not able to change Azure AD passwords. Where a user in Azure AD logs in to a SecureDoc-protected endpoint, if the user changes his password using SecureDoc Control Center - where password synchronization using an on-Premises AD User account would normally change the user's Windows (and therefore on-premises AD) passwords - this is not happening for Azure AD-joined users.

A message: "Windows password was synchronized with SecureDoc password" is shown, but in fact the user will be unable to log in subsequently and the message "The password is incorrect. Try again" is shown.

Work-Around: Until a solution is found, either a) Change the password using Windows methods (e.g. Ctrl+Alt+Del, then change the Windows password manually) then reboot and log in again so the new password can be propagated into SecureDoc Control Center, or b) Only if the password has already been changed in SecureDoc Control Center, then the user should exit SecureDoc Control Center, then change the password using the Windows change password methods, then reboot and log in again to ensure the new password has been propagated into SecureDoc Control Center.

Affected tickets: SD-43450

User unable to login at pre-boot with Password after disabling phone token in Device Profile and performing Password Recovery

Issue: In this scenario, a user's Key file had been converted to Mobile Device- based protection and was working successfully. The user wanted to switch back to password-protected authentication.

Solution: To achieve this change, a new Key File must be sent to the endpoint device for the user AFTER a set of steps have been performed; These are:
The Administrator must apply a profile to the endpoint device that disables mobile device-based protection.
Since the user's Key File already has mobile device- based protection, the Administrator must disable that option in SES, and send down a new Key File for the User on that Device.
Once the new Key File (with the Mobile Protection option disabled) has been received on the endpoint device, the User will be switched to being able to log in using a Password.

Affected tickets: SD-43464

Where using Mobile Device (Phone)-based authentication to access SecureDoc Control Center (SDCC), one user must completely close the SDCC application before another can log in.

Issue: Assume a given device has two or more Key Files, each protected by a different Phone-protected Key File. If one user logs in successfully to SecureDoc Control Center, then logs out to the SecureDoc Control Center login screen, another user cannot log in successfully. This does not occur if the second user starts the SecureDoc Control Center application executable

Work-Around: Until WinMagic has a solution for this issue, each user on a shared device should completely close the SecureDoc Control Center application after using it.
Alternatively, any user of a shared device that finds that SDCC is already running should first close the SecureDoc Control Center application before attempting to log in, on the assumption that the previous user had not closed the application.

Affected tickets: SD-43535

Error "An unidentified error has occurred. Error code: 0x9B0424" can display when Phone is paired to a device using Bluetooth and the Windows feature Dynamic Lock is enabled.

Issue: This issue was encountered on a device on which SecureDoc PBLU was deployed. The device was encrypted, and the option was enabled to Convert to Token protection with the phone token protecting the user's Key File.
Upon logging in the user encountered the dialog that prompts to convert to token-protected key file. The user entered his password and clicked Login.

Instead of being prompted to "Authorize" conversion to phone-based Key File protection to complete the conversion, the user encountered error message "An unidentified error has occurred. Error code: 0x9B0424".

Solution: This issue does NOT occur where the Phone has been Bluetooth-paired and the Dynamic lock feature is disabled, so until a solution is found to this limitation, customers are requested to disable the Dynamic Lock feature in Windows.
If the problem persists after disabling Dynamic Lock, search for “iPhone” as a hidden device in Device Manager under "Portable Devices" and uninstall it. You may also need to check if FidoEazy (under Bluetooth) and Apple iPhone (under Portable device) are listed - and remove them.
Then in Device Manager - disable and then re-enable Bluetooth device
Reboot the computer.
The user should now be able to login at SecureDoc Pre-boot, SecureDoc Credential Provider and into SecureDoc Control Center using Bluetooth.
For a complete view of this solution, with screenshots of the settings panels affected, please see Knowledge Base article number 1956,

Affected tickets: SD-43542

A client device deployed with TPM-PIN + Mobile Token Bluetooth-based authentication - with alternate password option enabled – will fail to prompt the user to convert key file to Mobile Token-protected after use of Challenge/Response or Self-Help Recovery.

Issue; WinMagic has encountered this issue in the following scenario:
1 - Following initial encryption (or installation of SecureDoc Pre-Boot if disk is not encrypted)
2. The device is rebooted.
3. At SecureDoc's pre-boot, the user performs Self-Help Recovery or Challenge-Response recovery.
4. The client device will boot into the Windows desktop following such recovery.
5. A dialog box prompting the user to "Change password/PIN" will appear
6. The user enters a new password or PIN, and confirms that entry, then clicks OK.
At this point, contrary to expectations, SecureDoc does NOT prompt the user to convert key file protection mode to Mobile Token-protected.

This process will continue to fail to prompt the user to convert to Mobile Token-based Authentication, even if steps 2 through 6 are repeated any number of times.

Solution: This issue is caused by configuring protection for the SecureDoc Key File using both TPM+PIN AND with Mobile Token-based protection.
At this point, one can use either TPM+PIN-based or Mobile Token-based authentication, but they cannot be combined.

Work-Around: Ensure that any Device Profiles define EITHER "TPM+PIN with Alternate Password protection" OR "Mobile Token (via Bluetooth)-based Authentication" but NOT BOTH.

Affected tickets: SD-43719

Authentication – Remote Desktop

Remote Desktop (RDP) access will not work from a device registered to a local/On-Premises AD to another device that is registered only on an Azure AD domain.

Issue: Where attempting to perform Remote Desktop (RDP) access from a device registered to a local/On-Premises AD to another device that is registered only on an Azure AD domain, such RDP access will not work.

This behavior is consistent with Microsoft's design.

Some details of why this behaves as it does can be found in the article in the following link:
https://learn.microsoft.com/en-us/windows/client-management/connect-to-remote-aadj-pc

Work-Around/Mitigation:
Both PCs (local and remote) must be running Windows 10, version 1607 or later. Remote connections to an Azure AD-joined PC running earlier versions of Windows 10 are not supported.
The PC from which you are attempting remote access (the Local PC) must be either Azure AD-joined or Hybrid Azure AD-joined if using Windows 10, version 1607 and above, or Azure AD-registered if using Windows 10, version 2004 and above. Remote connections to an Azure AD-joined PC from an un-joined device or a non-Windows 10 device are not supported.

Both the local PC and remote PC must be in the same Azure AD tenant. Azure AD B2B guests aren't supported for Remote desktop.

Affected tickets: SD-42925

Contact WinMagic

WinMagic		Sales:	sales@winmagic.com
5770 Hurontario Street, Suite 501		Marketing:	marketing@winmagic.com
Mississauga, Ontario, L5R 3G5		Human Resources:	hr@winmagic.com
Toll free: 1-888-879-5879		Technical Support:	support@winmagic.com
Phone: (905) 502-7000		For information:	info@winmagic.com
Fax: (905) 502-7001		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 – 2024 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. © 2022 WinMagic Corp. All rights reserved.

© Copyright 2024 WinMagic Corp. All rights reserved. This document is for informational purpose only. WinMagic Corp. makes NO WARRANTIES, expressed or implied, in this document. All specification stated herein are subject to change without notice.