SecureDoc Enterprise Server

Release Notes

Product Version: 9.1

Published November 11, 2023

SecureDoc™ by WinMagic

Contents

SecureDoc Support 2
About This Release 2
System Requirements 3
Client OS Support 3
The KnownConfigs.XML File 3
Version 9.1 4
How to Install/Upgrade 6
New Features 7
SecureDoc for Windows 7
SecureDoc Console or SESWeb Console 7
macOS 8
Linux 9
Improvements 10
SecureDoc Console or SESWeb Console 10
SecureDoc Client - macOS 10
Resolved Issues 12
Authentication & Recovery 12
Limitations 13
Contact WinMagic 14
Acknowledgements 14

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
9.1 (Current)	November 11, 2023 EOL: November 11, 2026	New Features, Improvements, and fixes (server/client) Build# 9.1.000.1349 (Server, all other clients), Build# 9.1.000.1349 (macOS)
9.0 SR4 HF1	June 27, 2023 EOL: May 7, 2026	New Features, Improvements, and fixes (server/client) Build# 9.0.401.80 (Server, all other clients), Build# 9.0.401.80 (macOS)
9.0 SR4	May 9, 2023 EOL: May 7, 2026	New Features, Improvements, and fixes (server/client) Build# 9.0.400.60 (Server, all other clients), Build# 9.0.400.60 (macOS)
9.0 SR3	March 2, 2023 EOL: Mar 1, 2026	New Features, Improvements, and fixes (server/client) Build# 9.0.300.118 (Server, all other clients), Build# 9.0003.103 (macOS)
9.0 SR2	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 HF7	February 23rd, 2023 EOL: Sep 7, 2024	Fix for 8.6SR1 HF6 (client) Build# 8.6.107.180 (Clients)
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)

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 9.1

IMPORTANT

For customers deploying 9.1 to devices containing Self Encrypting Drives (SEDs), if you encounter any unexpected messages indicating that SecureDoc Installation is not proceeding on such a device, please contact WinMagic Support for assistance.

Note: Starting with version 9.1, support for 32-bit operating systems is discontinued. This decision is aligned with industry trends and allows us to focus on optimizing and enhancing the performance, security, and features of our software for modern, 64-bit operating environments. Users are encouraged to transition to 64-bit operating systems to ensure compatibility with the latest developments and to benefit from the full range of capabilities provided by our software.

Which customers should upgrade to 9.1?

Version 9.1 is a release upgrade to the SecureDoc Enterprise Client and Server.

All customers are recommended can safely upgrade to 9.1

Why upgrade? **https://winmagic.com/blog/5-reasons-to-update-your-winmagic-securedoc-investment/**

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 9.1 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.

End of Life Notice:

As of the current date, macOS Catalina has officially reached its End of Life (EOL) status. Users are strongly advised to upgrade to a newer macOS version to ensure the security and functionality of their systems. We are no longer supporting macOS Catalina.

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

1 - The device Profile must specify the Linux-based Pre-Boot for UEFI devices – termed as PBLU in this documentation. Phone-based authentication (whether using Bluetooth Low Energy communication or network-based communication) does not work with

2 – Bluetooth must be enabled in the endpoint computer's hardware configuration (BIOS or UEFI settings), as use of Bluetooth Low Energy mobile device-based authentication is a compelling security feature.,

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

SecureDoc for Windows

A new feature permits users the ability to recover access and log into Windows using a One Time Password (OTP) provided on the user's Mobile Device.

Description: To assist users in authenticating to a SecureDoc-protected Endpoint, a means must be found to provide users the ability to recover and log into Windows using a One-Time Password (OTP) that is provided on their phone.

Example use cases that support this need are Bluetooth Low Energy communication is not available/not enabled on the user's Mobile Device; User is offline; The Mobile Device's TPM isn't available.

Solution: This new feature permits users the ability to recover access and log into Windows using a One Time Password (OTP) provided on the user's Mobile Device. Once the user has keyed in this One Time Password at Pre-Boot, the user's SecureDoc-protected endpoint will boot into Windows.

Affected tickets: SD-43976

SecureDoc Console or SESWeb Console

Revised Licensing Approach for Full Disk Encryption (FDE) and ME Remote Authentication.

Description: A revised licensing model has been introduced to accommodate the integration of encryption and authentication within the new MagicEndpoint product. The updated approach involves the implementation of Product Tiers, defining the entitlement of customers to specific features. The provided licensing model spreadsheet outlines the various Product Tiers, their respective features, and pricing.

The licensing user interface in the SES Console/SESWeb has been streamlined. Desktop client types have been consolidated into a single line for Enterprise Clients, while Servers have been merged into a singular category, emphasizing core client features.

Solution: Upon upgrading to the latest version, licenses have undergone a comprehensive reorganization:

- Former endpoint encryption categories are consolidated as "FDE Enterprise Client."
- Server-related categories now fall under "FDE Enterprise Server."
- The "SecureDoc File Encryption" feature is now categorized as "Add-on: SFE." New licenses introduced include "Add-on: Phone Token (Bluetooth)" and "MagicEndpoint Authentication" for Access Management and FIDO Eazy Enterprise.
-

Affected tickets: SD-40686, SD-44557, SD-43992

SESWeb now supports Admin authentication using FIDO2.

Description: As WinMagic advances its support for robust authentication through MagicEndpoint, administrators should have the capability to enhance the security of their authentication to SESWeb by employing FIDO2 methods.

Solution: SESWeb now supports Admin authentication using FIDO2.

Affected tickets: SD-44454

---

macOS

Our system to now include support for macOS 14 and 14.1 Sonoma.

Description: We have implemented support for macOS 14 and 14.1 Sonoma in our system.

Solution: At present, SecureDoc has been updated to offer compatibility with the latest macOS version, macOS 14, also known as Sonoma.

Affected tickets: SD-45360

Upgrade to TLS 1.3 for Enhanced Security for Windows, Mac and Linux

Description: We have implemented support for Transport Layer Security (TLS) 1.3, enhancing the encryption of communication between web applications and servers. This is particularly crucial when web browsers are loading websites, ensuring a secure and encrypted data exchange.

Solution: We have introduced a Configuration UI in SDConnex and Profile settings, offering various TLS options. In SDConnex, three modes are available: Disable TLS, Use HTTPS or TLS 1.3 if supported, and Force the use of TLS 1.3. SES Console, within Windows, Linux, or Mac profiles, presents two modes: Disable TLS or Force the use of TLS 1.3. Additionally, the OSA installer has been upgraded to dynamic OpenSSL 3.0.8 to address outdated OpenSSL versions that do not support FIPS 140-2. Furthermore, all Windows projects have been upgraded to OpenSSL 1.1.1m to overcome the limitations of the older OpenSSL version, ensuring compatibility with TLS 1.3. Finally, TLS 1.3 options have been added for both Mac and Linux platforms.

Affected tickets: SD-41244, SD-41290, SD-41256, SD-41257, SD-44458, SD-41241

Linux

Now providing support for the new SDLinux RHEL9 package and its deployment.

Description: Enhanced support for SDLinux installer scripts to accommodate the new RH9 distro.

Solution: We changed how SecureDoc for Linux is installed so that it can now work on the newer RedHat Enterprise Linux 9 (RHEL9). We also made sure it supports a specific kernel version, 5.14.0-162.23.

Affected tickets: SD-44304

[SDLinux] The implementation now includes the addition of an exclude user feature for SDLinux.

Description: Implement the capability to exclude users, a functionality already present in Windows, to SDLinux profiles and clients.

Solution: A new feature has been incorporated into the Linux system, presenting an 'Exclude Accounts' interface that parallels the setup found in Windows profiles. When a user attempts to log in during provisioning and is enlisted in the excluded users list, they will not encounter the SecureDoc Primary Owner screen. In contrast to Windows, excluded users logging in won't receive any prompts or messages. To maintain consistency with the Windows setup, users listed as excluded should be separated by commas.

Affected tickets: SD39375

Improvements

SecureDoc Console or SESWeb Console

Implement measures to ensure that Active Directory (AD) credentials are not stored in the database following a login via SES Web.

Description: To address the issue of Active Directory (AD) credentials being stored in the database (DB) after logging into SES Web, the request is to prevent the storage of AD passwords in SES Web. Currently, if a user resets their password in the AD server, both the old and new passwords can still be used for SES Web login. The emphasis is on maintaining Active Directory as the sole source of truth for authentication.

Solution: A new tool, "SDTool.exe," has been added to clear and update passwords in the SES Database. Users can run the tool and input essential information like the Server name, Database name, SQL username ("sa"), and its password. The tool removes old passwords and ensures a refreshed password state in the SES Database.

Affect tickets: SD-44439

SecureDoc Client - macOS

The option to convert from Password- to Token-protection has been moved into the Device Profile for SES clients, and therefore this becomes a manageable option for the SecureDoc Control Center application.

Description: 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: SecureDoc Control Center will now offer options specifying that the user's Key File is to be converted from Password to Token-protection.

Affected tickets: SD-42729

SES now supports user account names that contain single quote characters.

Description: In previous versions, SES did not support user accounts that contain the single quote character. Customers have requested this support since AD supports usernames that contain single quotes.

Solution: SES now supports user account names that contain single quote characters to conform to all user ID characters that can be used in Active Directory.

Affected tickets: SD-44007

Implement Windows Password Provisioning and Auto-Update on Windows Client.

Description: Windows password rotation in SecureDoc, in conjunction with Password Sync (PwSync), smoothly operates until the Windows password changes during rotation, pausing PwSync and assuming only the SD password is known.

This feature offers provisioning of Windows passwords to applications through hotkey/clipboard functions, enabling automatic password pasting and submission for third-party applications/websites. Automatic password change after submitting the hotkey allows end-users to decide on the password change. SecureDoc initiates an automatic attempt to change the Windows password within 15 seconds, considering Windows AD password policies that may limit changes to once every 24 hours, adapting changes upon the next suitable opportunity.

Solution: Implemented changes to enable automatic Windows password provision and management via a specific set of features. A dedicated "Password Manager Options" segment accessible in SES Server, SD Control Center, and SES WEB within the Profile settings, specifically located in General Options/Credential Provider.
Issue.

Affected tickets: SD-44782, SD-45342

Resolved Issues

Authentication & Recovery

Real-time Updating of Password Criteria from SES

Description: Enabling the continuous and automatic updating of global password criteria and expiration details within each package whenever there is a change in password option(s).

SES facilitates this process: Any alterations made by the administrator to the Password Rules (reflected in the Global setting) will be disseminated to ALL profiles after the 'OK' button is clicked in the user interface.

Additionally, there exists a global option governing the update of modified profiles to clients within SES, termed 'Automatically update device's profile settings when profiles are modified.'

Solution: This setting determines whether the updated profiles are sent to the devices immediately or require manual intervention.

Affected tickets: SD-37781

Problem with vulnerability scan for JQuery 1.12.1 with SD 8.6 SR1HF2 SESWeb

Description: The application using a vulnerable version of JQuery UI v1.12.1 affecting SESWeb.

Solution: We recommend upgrading JQuery UI to version 1.13.2 to resolve this issue.

Affected tickets: SD-44881

Enable the inclusion of single quotes in user email addresses.

Description: SES currently does not accommodate user email addresses containing single quotes. This limitation has been identified, as Outlook allows for email addresses with single quotes. To ensure compatibility and enable the inclusion of such emails in our database, it is imperative that SES is enhanced to support email addresses with single quotes.

Solution: This issue is now resolved.

Affected tickets: SD-46544

Limitations

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

In upcoming updates, the Catalina target will be excluded from build, installation, and run-time scripts, as well as from business logic in the context of Sonoma.

Description: Due to the absence of updates and security fixes from Apple for Catalina, and with HTTPS support beginning from macOS Big Sur, SD 9.1 will exclude macOS 13 - Catalina as a target from build, installation, and run-time scripts. This affects all associated scripts and components.

Limitation: We won't be supporting Catalina moving forward.

Affected tickets: SD-46089

After BL Installation and Reboot, Legacy System Displays Black Screen

Description: Upon deploying the package to the client, following the installation of BootLog and system reboot, the Windows startup process halts at a black screen, preventing the normal loading of Windows.

Limitation - Windows 7, 8.1, and 10 Legacy BIOS will not be supported in version 9.1.

Affected tickets: SD-45891

Windows WMI API failure occurs when attempting to log in with a UPN/AAD user.

Description: When trying to log in with a UPN/AAD user, a failure in the Windows WMI API is encountered.

Limitation: Due to the way Windows manages these names, it appears to be an issue in obtaining the email while using the UPN address as it is displayed.

Affected tickets: SD-45096

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 – 2023 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, SecureDoc Cloud Lite, MagicEndpoint and MagicEndpoint FIDO Eazy 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. © 2023 WinMagic Corp. All rights reserved.

© Copyright 2023 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.