There is a vulnerability in the SecureDoc Windows

SecureDoc Enterprise Server

Release Notes

Product Version: 9.1 HF3

Published Februrary 16th 2024

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 HF3 4
How to Install/Upgrade 6
Android OTP 7
New Features and Enhancement 7
IDP 7
New Features and Enhancement 7
SecureDoc Console or SES Web 9
Resolved Issues 9
Limitation 10
SecureDoc for Windows (Boot Code) 11
Resolved Issues 11
Contact WinMagic 12
Acknowledgements 12

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 HF3 (Current)	February 16, 2024 EOL: November 11, 2026	New Features, Improvements, and fixes (server/client) Build# 9.1.003.1365 (Server, all other clients), Build# 9.1.003.1365 (macOS)
9.1 HF2	December 14, 2023 EOL: November 11, 2026	New Features, Improvements, and fixes (server/client) Build# 9.1.002.1354 (Server, all other clients), Build# 9.1.002.1354 (macOS)
9.1 HF1	November 23, 2023 EOL: November 11, 2026	New Features, Improvements, and fixes (server/client) Build# 9.1.000.1352 (Server, all other clients), Build# 9.1.000.1352 (macOS)
9.1	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)
09.0 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)

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 HF3

IMPORTANT

For customers deploying 9.1 HF3 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 HF3?

Version 9.1 HF3 is a release upgrade to the SecureDoc Enterprise Client and Server.

All customers are recommended can safely upgrade to 9.1 HF3

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 HF3 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.

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.

Android OTP

New Features and Enhancement

SD-47111 Enhancing Android Mobile App: OTP Support and Number Matching Integration

Description: Enhance the functionality of the mobile application on Android by incorporating support for OTP (One-Time Password) and implementing number matching capabilities. This improvement aims to provide users with enhanced security features and a more versatile user experience, allowing for a seamless integration of OTP verification and the verification of numerical input for various purposes within the application.

Solution: To address the requirements, the solution involves implementing key enhancements to the Android mobile app. These improvements aim to elevate the app's functionality, ensuring a more secure and versatile user experience.

IDP

New Features and Enhancement

SD-47032 Enhancements for User Control and Security: Mobile Lockout, Turnstile Integration, and Number Matching Push

Description: The problem at hand is about making security and policy enhancements for IDP. To address this, a set of improvements has been proposed.

These include displaying which service provider is requesting authentication, setting limits on push notifications to emails after rejections, allowing phone registration/re-registration only when users log in using MagicEndpoint on the IDP dashboard, implementing a number matching system on push notifications to prevent accidental acceptance, and exploring the use of Federated logout upon termination of a persistent connection (pending further research).

Solution: The system now includes a new "Enable mobile lockout" feature, allowing administrators to set the maximum number of mobile rejections before triggering a lockout and specifying the lockout duration.

An easy-to-use interface for unblocking users has also been added. Another addition is the "Enable Turnstile" toggle, which involves copying keys from Cloudflare to the IDP portal. Additionally, a configuration for number matching push has been introduced in the Global settings. Enabling it prompts the mobile phone to display a number for verification, while disabling it retains the current accept/reject functionality.

These updates enhance control and security for a smoother user experience.

SD-47039 Enhanced Security Configuration in IDP: Mobile Lockout and User Unblock Features

Description: The issue is with the IDP system, which needs to limit push notifications when a user rejects them consecutively. This is crucial to prevent potential social engineering attacks where an attacker bombards a user's phone with notifications, hoping the user will accept them.

Solution: A new configuration has been introduced on the IDP page under Configuration/Global settings. This includes the addition of a toggle named "Enable mobile lockout," allowing administrators to specify the maximum number of mobile rejections before triggering a lockout and setting the lockout duration in minutes. Additionally, a user-friendly interface has been incorporated to facilitate the unblocking of users.

SD- 47041 Securing Mobile Registration: Enhancing Authentication and Access Control

Description: To enhance security, a solution is proposed, requiring users to accept a push notification on their currently registered phone before proceeding with re-registering a new phone. For users without a phone, an alternative option involves receiving a code by email for new phone registration. This process still requires login from an endpoint client and entering the code for added security without the need for the old phone.

Solution: The user must confirm their identity on their registered phone once before initiating the registration of a new phone. In the absence of the registered phone, a verification code is sent to their email, and they need to authenticate using this code before proceeding with the registration of a new phone.

SD-47040 Enhancing Security with Cloudflare's Turnstile CAPTCHA Integration in IDP Server

Description: IDP needs to prompt users to solve a captcha input when accessing applications through Mobile Push.
To enhance security, it is proposed to mandate captcha input during application logins via mobile push. This measure safeguards against bot attacks or login flooding on unauthorized devices. The configuration of this option will be under the control of the administrator, allowing them to enable or disable this feature as needed.

Solution: The integration of Cloudflare's smart CAPTCHA service, "Turnstile," into the IDP server is facilitated through the Configuration/Global settings. By adding a toggle option to enable Turnstile and copying the associated site and secret keys from Cloudflare to the IDP portal, this integration enhances security. It's important to be aware that enabling Turnstile prevents users from logging in using Mobile Push on the Internet Explorer browser.

SecureDoc Console or SES Web

Resolved Issues

SD-46654 Troubleshooting IDP Launch Error in SES Console

Description: The problem is that attempting to launch the IDP page results in an HTTP Error 500, specifically when trying to log into the portal.

Solution: To address this issue, it is suggested to install IDP on the same server as SES Console. A resolution for this problem is expected in version 9.1.

SD-46956 Restoring Crypto Erase Functionality for BitLocker Devices in SES Console and SES Web

Description: The issue identified pertains to the absence of the "Crypto-erase a device" option for BitLocker devices in SES. This functionality, previously available in SES 8.6, is no longer present in the current version.

Solution: The task at hand involves re-enabling the crypto erase feature for BitLocker-managed devices through both the SES console and SES Web interfaces.

SD-47056 Analysis and Mitigation of Identified Server Vulnerabilities

Description: Potential issues with the 128006-HDE server. A scan of the SecureDoc Webapp. The report pointed out a few things, like an average level concern called Open Redirect, and some lower-level issues in Cookie Security (Missing SameSite Attribute and Overly Permissive SameSite Attribute), Flash Misconfiguration (Vulnerable Flash Engine), and HTML5 misconfigurations (Misconfigured Content Security Policy, Privacy Violation through Autocomplete, and System Information Leak related to Internal IP).

The main reasons for these concerns are Open Redirect, Cookie Security problems, and Flash Misconfiguration.

Solution: The identified issues, including a medium-level Open Redirect and low-level concerns related to Cookie Security and Flash Misconfiguration, have been successfully resolved.

SD-47278 Extended pre-boot delays observed after successful authentication, causing a prolonged hang

Description: The system encounters a problem when the BLE thread repeatedly checks for advertisements during prescan, especially in environments with numerous BLE signals. This continuous loop hinders the system thread from completing its tasks effectively.

Solution: By adding and checking the "thread_stop" flag in the loop handling BLE advertisements, we provide a way to control the loop's behavior. This helps prevent prolonged delays in the system thread caused by continuous looping, especially in environments with many BLE signals.

Limitation

SD-47158 Enhancing IdP Installer for Seamless Installation on Servers with dotnet

Description: Installation of IDP on a server with dotnet installed fails initially, automatically stopping during the first attempt. However, success is achieved upon reinstalling.

Limitation: Adjust the IdP installer to enable installation on servers with dotnet already installed.

SD-46800"Upgrade Process: SES and SDClient 9.1 SR1 - Addressing Error 1921

Description: An error occurs when upgrading SES and SDClient from the existing 9.1 release with AzureAD synchronization.

Limitation: Before upgrading the server software, make sure that none of the SES services are running. Manually stop them if needed.

SecureDoc for Windows (Boot Code)

Resolved Issues

SD-46756 Preventing Stack Smashing in PBL (E3.bin): Buffer Size Adjustment for Password Handling

Description: The problem is with the PBA system, showing the error "PBA returned 134" after the user enters the "Challenge Response" string correctly. The root cause is related to the SES Global Option, specifically the Password Limit Length set to 32 bytes instead of the default 10.

This issue is caused by a "smashing stack" problem, which involves using a local buffer with an insufficient hardcoded size.

Solution: To address the issue, it is recommended to allocate a sufficient size for the buffer and ensure that the password size does not exceed the buffer length. This preventive measure aims to avoid stack smashing in PBL (E3.bin).

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, 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. © 2024 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.