SecureDoc Enterprise Server

Release Notes

Product Version: 9.2 SR1

Published January 28th, 2026

SecureDoc by WinMagic

Contents

SecureDoc Support 2
About This Release 2
How to Install/Upgrade 2
New Features 3
Improvement 7
SecureDoc Console or SESWeb Console 7
Linux 8
Fixed Bugs 9
SecureDoc Console or SESWeb Console 9
SD Client 10
Limitation 11
Contact WinMagic 13
Acknowledgements 13

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

SecureDoc 9.2 SR1 is a maintenance update focused on resolving known issues and improving product stability. No new features or functional changes are introduced in this Hotfix. Customers running SecureDoc 9.2 or 9.2 SR1 are encouraged to upgrade to this version to benefit from the latest fixes and enhancements.

Recommended – WinMagic recommends applying this release to maintain optimal stability and compatibility with SecureDoc 9.2 environments. This update addresses specific issues identified since the general availability of SecureDoc 9.2 and ensures continued reliability for enterprise deployments.

Version	Release/EOL Dates	Details / Build Information
9.2 SR1 (Current)	Jan 28, 2026 EOL: May 7, 2028	New Features, Improvements, and fixes (server/client) Build#9.2.100.428 (Server, all other clients), Build#9.2.100.403 (macOS)
9.2 HF3	May 21, 2025 EOL: May 7, 2028	New Features, Improvements, and fixes (server/client) Build#9.2.003.301 (Server, all other clients), Build#9.2.003.301 (macOS)
9.2 HF2	September 4, 2025 EOL: May 7, 2028	New Features, Improvements, and fixes (server/client) Build#9.2.002.293 (Server, all other clients), Build#9.2.0.291 (macOS)
9.2 HF1	June 25, 2025 EOL: May 7, 2028	New Features, Improvements, and fixes (server/client) Build#9.2.001.292 (Server, all other clients), Build#9.2.0.291 (macOS)
9.2	May 8, 2025 EOL: May 7, 2028	New Features, Improvements, and fixes (server/client) Build#9.2.0.291 (Server, all other clients), Build#9.2.0.291 (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.

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

Operating System Support

- Added support for Red Hat Enterprise Linux (RHEL) 9.6.
- Added support for Red Hat Enterprise Linux (RHEL) 9.7.
- Added support for Ubuntu 24.04 LTS in FIPS-compliant deployments.

Linux Deployment and Profile Enhancements

- Added support for defining an administrator user list during deployment.
- Added support for pushing client profiles from SecureDoc Enterprise Server (SES) to Linux clients.
- Added new client profile options to enable or disable permanent autoboot.

Identity and Preboot Features

- Added support for setting and updating the device owner from SES.
- Added Single Sign-On (SSO) support for RHEL 8 and RHEL 9 operating systems.
- Added support for Manager Approvals at preboot.

IdP – SAML Assertion Encryption Support

Description: SecureDoc now supports optional encryption of SAML assertions to enhance protection of user identity information during federated authentication. This helps organizations meet higher federation assurance requirements when using SAML-based Single Sign-On (SSO).

Availability: SAML assertions generated by an identity provider can now be encrypted using a service provider (SP) encryption certificate.

Note: Some identity providers, such as Microsoft Entra ID, may require inbound SAML assertions to be signed but may not support encrypted assertions.

Affected tickets: SD-52452

[SFE] Persistent Encryption Options Remain Available

Description: Persistent Encryption options remain available in SES Profiles and SecureDoc Control Center (SDCC) in SecureDoc 9.2 SR1. Although earlier documentation suggested this feature was being phased out, it continues to be supported in this release.

Guidance: Customers can continue configuring Persistent Encryption through the SES Console and SDCC. Release documentation will be updated to reflect its current availability.

Affected Ticket: SD-51673

[SDCP] Support for Phone-Based Certificate Login (CBA)

Description: SecureDoc now supports logging in through SDCP using phone-based Certificate-Based Authentication (CBA). This provides a seamless, passwordless Windows sign-in experience by allowing users to authenticate with a certificate stored on their mobile device, with no additional steps required at the Windows logon screen.

Availability: Phone-based CBA login is supported starting in SES 9.2 SR1.

Affected Ticket: SD-51508

MFA Configuration Options for ME and SDCC Login

Description: SecureDoc now provides additional configuration options to support multi-factor authentication (MFA) for MagicEndpoint (ME) and SecureDoc Control Center (SDCC) logins. This enhancement helps organizations strengthen authentication workflows and improve access security.

Availability: MFA configuration options are available through the SES Console, SDCC, and SES Web starting in SecureDoc 9.2 SR1.

Affected Ticket: SD-51349

MFA Support for Windows Login

Description: SecureDoc now supports multi-factor authentication (MFA) at Windows login, enabling organizations to require an additional verification step after the primary keyfile login. This helps strengthen endpoint access security and supports modern authentication workflows, including biometrics as a second factor.

Availability: MFA options for Windows and SDCP login are available starting in SecureDoc 9.2 SR1 through SES Console and SDCC configuration settings.

Note: MFA is applied after password- or PIN-based login methods and is not triggered when logging in through BLE or Network Phone authentication.

Affected Ticket: SD-51132

Extended Manager Approval Support Across All Keyfile Types

Description: SecureDoc now extends Manager Approval login support across all keyfile types, allowing users to regain access even when their mobile device is unavailable. This provides greater flexibility at both Windows and preboot login through a push-based approval workflow with an assigned manager or administrator.

Availability: Manager Approval is supported for Password, Token, BLE, and TPM-PIN keyfiles starting in SecureDoc 9.2 SR1, with configuration available through SES and profile settings.

Affected Ticket: SD-51075

SES Web Supports SAML 2.0 Single Sign-On (SSO)

Description: SES Web now supports SAML 2.0 authentication for Single Sign-On (SSO), enabling users to log in through external identity providers such as Microsoft Entra ID or Okta. This enhancement simplifies access for organizations using federated identity systems while ensuring reliable login behavior across supported SAML configurations.

Availability: SAML 2.0 SSO login is supported starting in SES 9.2 SR1, including improved compatibility with Entra ID and Okta identity provider setups.

Affected Ticket: SD-50912

SSO Support for SDLinux on RHEL 8 and RHEL 9

Description: SecureDoc now supports Single Sign-On (SSO) for SDLinux on Red Hat Enterprise Linux (RHEL) 8 and RHEL 9. This enables the preboot-authenticated user to complete the first desktop login more seamlessly, reducing the need to re-enter credentials after unlocking the system.

Availability: SSO for SDLinux is supported starting in SecureDoc 9.2 SR1 for RHEL 8 and RHEL 9 environments.

Affected tickets: 50286

[SESWeb] Support for mTLS Certificate-Based User Authentication

Description: SES Web now supports mutual TLS (mTLS) certificate-based authentication, allowing users to be securely authenticated using a valid client certificate. This can streamline access by validating trusted certificates and reducing reliance on traditional login prompts.

Availability: mTLS authentication for SES Web is supported starting in SecureDoc 9.2 SR1. Organizations can configure SES Web on IIS to require client certificates for enhanced authentication and access control.

Affected Ticket: SD-49622

[PBU] Proxy Support for SDConnex During Preboot

Description: Pre-Boot Authentication (PBA) now supports proxy configurations, allowing SDConnex to connect successfully in environments where network access is routed through a proxy. This improves reliability for managed and restricted networks and helps ensure seamless connectivity during preboot operations.

Availability: Proxy settings can be applied during preboot starting in SecureDoc 9.2 SR1 when configured in the client profile.

Affected Ticket: SD-49562

[ME_TLS] Mutual TLS (mTLS) Authentication for SES Web

Description: SecureDoc now supports mutual TLS (mTLS) authentication for SES Web, enabling strong certificate-based verification of both users and devices during login. This strengthens access security by ensuring only trusted endpoints with valid client certificates can connect.

Availability: mTLS authentication is supported starting in SecureDoc 9.2 SR1 through MagicEndpoint integration, providing certificate-based user and device authentication for SES Web access.

Affected Ticket: SD-49534

[ME_TLS] Registration of ME TLS and SSH Keys in SES

Description: MagicEndpoint now supports automatic generation and registration of user and device TLS and SSH keys with SecureDoc Enterprise Server (SES). This enables centralized key management and supports secure services such as mTLS authentication and protected communications.

Availability: SecureDoc 9.2 SR1 adds support for registering and activating ME TLS and SSH keys through SES, with SDConnex used as the communication channel.

Affected Ticket: SD-49449

Improvement

SecureDoc Console or SESWeb Console

Enhanced Protection Against Suspicious Login Activity

Description: SecureDoc now includes improved controls to help organizations detect and respond to suspicious login behavior. New policy options allow administrators to limit repeated failed login attempts and enforce configurable lockout durations to reduce the risk of unauthorized access.

Solution: SecureDoc 9.2 SR1 introduces group policy settings for maximum failed login attempts and lockout duration. Geolocation-based access controls are also available to restrict logins to approved countries, with email notifications supported when login activity occurs outside permitted locations.

Affected Ticket: SD-50670

SES Web Support for All User Group and All Device Group

Description: SES Web now provides visibility of the built-in All User Group and All Device Group, aligning functionality with the SES Console. This enhancement supports administrative workflows where global user and device groups are required for assignments and policy management.

Solution: In SecureDoc 9.2 SR1, All User Group and All Device Group are available in SES Web under the Users and Devices pages. These built-in groups are protected and cannot be deleted or directly modified.

Affected Ticket: SD-42403

SES Web Support for All User Group and All Device Group

Description: SES Web now includes visibility of the built-in All User Group and All Device Group, aligning the web experience with the SES Console. This improvement supports administrative workflows where global user and device groups are needed for policy and folder assignments.

Solution: In SecureDoc 9.2 SR1, All User Group and All Device Group are now available in SES Web under the Users and Devices pages. These built-in groups are protected and cannot be deleted or directly modified.

Affected Ticket: SD-9767

Linux

Support for Manager Approval at Preboot

Description: SecureDoc now supports Manager Approval at preboot for Linux endpoints. This extends the existing Manager-approved recovery and login experience to SDLinux, enabling organizations to apply consistent approval-based access controls across both Windows and Linux clients.

Solution: Manager Approval at Linux preboot is now supported in SES 9.2 SR1, with configuration available through SES Console and SES Web.

Affected tickets: SD-52125

Fixed Bugs

SecureDoc Console or SESWeb Console

External Monitor Display Support for HP Docked Preboot Authentication

Description: In some HP laptop and docking station configurations, external monitors may not display the SecureDoc preboot authentication screen when the system is docked with the lid closed. This can impact users in multi-monitor workstation and enterprise docking setups.

Solution: This issue has been addressed in SecureDoc 9.2 SR1 through updated preboot display and hardware support. Customers using HP ZBook systems with USB-C or Thunderbolt docking stations are encouraged to upgrade to this release for improved external monitor compatibility.

Affected tickets: SD-52186

Third-Party Library Version Transparency (SES Web)

Description: SES Web includes several third-party web components that may appear with older version labels during customer security scans or library inventory reviews, such as jsTree or jquery-confirm. WinMagic continues to monitor third-party dependencies to ensure they align with enterprise security expectations and deployment best practices.

Solution: Customers who require additional validation for internal security or compliance reviews are encouraged to contact WinMagic Support for the latest mitigation guidance and recommended upgrade or remediation options.

Affected Ticket: SD-51905

[SFE] Blue Screen Issue on Windows 10 After Upgrading to SecureDoc 9.2

Description: In some cases, Windows 10 systems may experience a Blue Screen error after upgrading from SecureDoc 9.0 to SecureDoc 9.2.

Solution: This issue has been resolved in SecureDoc 9.2 HF3. Customers experiencing this problem are encouraged to upgrade to the latest hotfix release.

Affected Ticket: SD-51226

Login Issue After Upgrading SecureDoc and MagicEndpoint

Description: In some upgrade scenarios, users may experience login difficulties when accessing the MagicEndpoint identity provider (IdP) or integrated service providers immediately after upgrading SecureDoc and MagicEndpoint. This behavior may be related to cached browser data retained from earlier client versions.

Solution: This issue is resolved in SecureDoc 9.2 SR1.

Workaround: If users experience login issues after upgrading MagicEndpoint, clearing browser cache and reinstalling MagicEndpoint may help restore normal authentication behavior. Customers requiring additional assistance are encouraged to contact WinMagic Support.

Affected Ticket: SD-44104

SD Client

Upgrade Deployment Guidance for Error 1921 (SecureDoc Client)

Description: When upgrading SecureDoc clients from earlier releases (such as 8.6 SR1 or 9.0 SR2) to SecureDoc 9.2, some automated deployment environments (for example, MECM/SCCM or Intune) may encounter installer Error 1921 during the upgrade process.

Solution: This upgrade can be completed successfully by deploying the MSI with the following recommended silent installation parameters:

"/qn /norestart ALLUSERS=2 SDEBUG=1 SDREBOOT=NO SDPROMPTRESTART=NO REBOOT=ReallySuppress INSTALLLEVEL=3"

If additional assistance is required, please contact WinMagic Support for upgrade guidance.

Affected ticket: 51723

Limitation

Standalone – Updated Windows Server Support for SecureDoc Control Center (SDCC)

Description: Standalone SecureDoc installations are supported on newer Windows Server versions. Windows Server 2012 R2 is not supported for launching SecureDoc Control Center (SDCC) in this release.

Workaround: For the best experience, deploy Standalone SecureDoc on Windows Server 2016, 2019, 2022, or later.

Affected tickets: SD-52704

IdP Registration May Remain Pending After Installation with Elevated Credentials

If MagicEndpoint (ME) is installed while a user is already signed into Windows with an Active Directory (AD) standard account, but the installation is performed using an administrator account for elevation, IdP key registration may not complete for the signed-in user. In this case, the ME icon may remain yellow with the status: "IDP: Online – Pending user registration."

Workaround: Sign out of Windows and sign back in using the affected standard user account to allow IdP registration to complete successfully.

Affected Ticket: SD-52518

Exit Confirmation Alert May Flash Briefly During Logout on macOS Tahoe

On macOS 26.x Tahoe (26.1), the MagicEndpoint (ME) exit confirmation message ("Alert: Are you sure you want to exit the app after logging out?") may appear briefly and then disappear during system logout or shutdown.

Resolution: This issue is fixed in SES 9.2 SR1.

Affected Ticket: SD-52276

SecureDocD Daemon May Require Manual Full Disk Access Setup on macOS Tahoe

Description: On macOS 26.x Tahoe, after installing SecureDoc FileVault 2 (SDFV2), the SecureDocD daemon may not automatically appear in (System Settings > Privacy & Security > Full Disk Access). As a result, the permission may need to be granted manually to ensure SecureDoc operates as expected.

Workaround: Open the Full Disk Access list in System Settings, locate SecureDocD under `/usr/local/lib/WinMagic/`, and drag it into the list to provide the required access.

Affected Ticket: SD-52239

Manager Approval Support Scope for TPM-PIN and Token-Protected Keyfiles

Description: Manager-approved recovery login is available for password-based keyfiles, providing a streamlined approval workflow for supported login scenarios. At this time, clients using TPM-PIN or hardware token–protected keyfiles continue to use their existing authentication and recovery methods.

Solution: In SecureDoc 9.2 SR1, Manager Approval is supported for password-protected keyfiles, while TPM-PIN and token-protected configurations rely on alternative supported login and recovery options. Customers with specific deployment requirements are encouraged to contact WinMagic Support for guidance.

Affected Ticket: SD-52036

Limitation: Password Synchronization May Not Complete After Signing In with Another Windows User

Description: In some AD or Azure AD (AAD) environments, Password Sync may not function as expected after signing in with a different Windows user. In this case, Key File Protection may remain empty when the SecureDoc package is deployed, particularly if the Windows policy “Configure the transmission of the user’s password in the content of MPR notifications sent by winlogon” is not enabled.

Workaround: To ensure Password Sync works correctly, set the policy “Configure the transmission of the user’s password in the content of MPR notifications sent by winlogon” to Enabled in Group Policy under Computer Configuration > Administrative Templates > Windows Components > Windows Logon Options.

Affected Ticket: SD-51928

Preboot Authentication May Be Skipped After Hibernation on Linux Boot-Only Encryption

Description: On SDLinux systems deployed with the “Boot disk only” encryption option, resuming from hibernation may bypass the preboot authentication screen. After the system enters hibernation (for example, using the systemctl hibernate command), the device may resume directly to the OS login screen instead of prompting for preboot authentication again.

Workaround: Hibernation and resume are not supported on RHEL systems configured with boot-only encryption. To ensure preboot authentication is always enforced, avoid using hibernation or consider a deployment option that includes additional disk encryption coverage.

Affected Ticket: SD-51194

SD-51137 – Token PIN authentication is not available after password recovery when password expiration is enabled.

In environments where token-based key file protection is enabled, token PIN authentication may not be available after a user completes a password recovery and is required to change their Windows password due to password expiration policies.

After recovery, the system may require password-based authentication at pre-boot and in the SecureDoc Control Center, and reverting back to token PIN authentication may not succeed.

Workaround: For token-protected users, do not enable password expiration enforcement policies.

Affected Ticket: SD-51137

Contact WinMagic

WinMagic		Sales:	sales@winmagic.com
11-80 Galaxy Blvd.		Marketing:	marketing@winmagic.com
Toronto, ON M9W 4Y8, Canada		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 – 2026 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 Corp., registered in the US and other countries. All other registered and unregistered trademarks herein are the sole property of their respective owners. © 2026 WinMagic Corp. All rights reserved.

© Copyright 2026 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.