

| SecureDoc Enterprise Server

リリースノート

製品バージョン: 9.2

(Rev 1.0)

更新履歴

日 付	バージョン	更新内容
2025 年 7 月	初版	

。

目次

更新履歴	1
本リリースバージョンについて	3
システム要件	4
注意事項	4
KnownConfigs.XML ファイルについて	5
プログラム(プロダクト)名、用語について	6
新機能および機能強化	7
SES または SES Web コンソール	7
SecureDoc Enterprise for Windows	8
SDLinux	9
MagicEndpoint IdP	9
改善された問題	10
SES または SESWeb コンソール	10
SecureDoc Enterprise for Windows	11
SDLinux	12
改善した問題(特定のデバイスに関連)	14
制限事項	15
SecureDoc Enterprise for Windows	15
SDLinux	15
MagicEndpoint – スマートフォン	15
サポートが必要なお客様	16
連絡先	16

本リリースバージョンについて

このドキュメントには、本バージョンに関する重要な情報が含まれており、全体を確認されることを強くお勧めします。最新バージョンでは、過去の不具合の修正及び新機能の追加など、製品が強化されています。改善された機能、安定性のための修正プログラム、セキュリティ強化のために、最新バージョンをインストールして利用されることを強くお勧めします。

バージョン	リリース日	EOL (End of Life)	ビルド情報
9.2	2025 年 5 月 8 日	2028 年 5 月 7 日	Build# 9.2.0.291

旧バージョンについて

バージョン	リリース日	EOL (End of Life)	ビルド情報
9.1 SR1	2024 年 7 月 26 日	2027 年 7 月 25 日	Build# 9.1.100.267
9.1 HF3	2024 年 2 月 16 日	2026 年 11 月 10 日	Build# 9.1.003.1365
9.1 HF2	2023 年 12 月 14 日	2026 年 11 月 10 日	Build# 9.1.002.1354
9.1 HF1	2023 年 11 月 23 日	2026 年 11 月 10 日	Build# 9.1.000.1352
9.1	2023 年 11 月 11 日	2026 年 11 月 10 日	Build# 9.1.000.1349
9.0 SR4 HF1	2023 年 6 月 27 日	2026 年 5 月 7 日	Build# 9.0.401.80
9.0 SR4	2023 年 5 月 9 日	2026 年 5 月 7 日	Build# 9.0.400.60 Build# 9.0003.103 (macOS)
9.0 SR3	2023 年 3 月 2 日	2026 年 3 月 1 日	Build# 9.0.300.118 Build# 9.0003.103 (macOS)
9.0 SR2	2022 年 12 月 9 日	2025 年 12 月 8 日	Build# 9.0.200.207 Build# 9.0002.198 (macOS)
9.0 SR1	2022 年 7 月 21 日	2025 年 7 月 20 日	Build# 9.0.100.149 Build# 9.0001.73 (macOS)

注 Hotfix の EOL は、そのベースとなるバージョンまたはサービスリリースと同じです。

注 EOL を迎えたバージョンはテクニカルサポート終了となります。

※ 旧バージョンのリリースノートは、以下のサイトでご確認ください。

<https://www.winmagic.com/jp/support/jp-release-notes>

システム要件

SecureDoc Enterprise Server 及び SecureDoc クライアントのシステム要件:

<https://winmagic.com/ja/data-security-support-jp/system-requirements/>

デバイスの互換性:

<https://winmagic.com/en/data-security-support/device-compatibility/>

注意事項

SecureDoc Enterprise Server

- SES の DB 作成に必要な SQL のインストールでは、「機能の選択」で、「検索のためのフルテキスト抽出とセマンティック抽出」をインストールしておく必要があります。
フルテキスト検索については、マイクロソフトのサイトで、ご確認ください。
- SES コンソールの機能を適切に使用するためには、SES コンソールが稼働しているサーバーや管理用デスクトップマシンなどにおいて、少なくともローカルの管理者権限を持っている必要があります。
Active Directory の OU をインポートする場合、ドメインにログインするアカウントは管理者権限が必要です。
- Azure Active Directory (Azure AD) の使用を希望するお客様は、v9.0 以降の SES が必要です。
旧バージョンの SES では Azure AD はサポートされません。
旧バージョンの SecureDoc クライアントのデバイスを使用されている場合、Azure AD に参加させる前に、v9.0 以降のクライアントにアップグレードする必要があります。

SecureDoc Enterprise for Windows

- v9.1以降、**32bit OS** はサポートされません。**Legacy BIOS**モードはサポートされません。
- MagicEndpoint を利用する場合、MagicEndpoint をインストールする前に、SecureDoc クライアントソフトウェアをインストールし、デバイスを SecureDoc Enterprise Server (SES) に登録する必要があります。
- MagicEndpoint を利用する場合、**v1.5** が必要です。
それ以前のバージョンの MagicEndpoint は SecureDoc v9.2 ではサポートされません。
また、MagicEndpoint v1.5 は SecureDoc 9.2 より前のバージョンとは互換性がありません。
- MagicEndpoint を利用するデバイスでは **TPM 2.0** が必要です。
- キーファイルを TPM 保護する場合、**TPM 2.0** が必要です。TPM 1.2 及びそれ以前のバージョンはサポートされません。

Bluetooth (Bluetooth Low Energy) 接続のスマートフォン (モバイルトークンベース) をプリブート認証で利用したいお客様へ

- Windows 10 または Windows11 のみのサポートです。
- プリブート認証プログラムは **PBLU** を選択してください。PBU では利用できません。
- コンピュータのハードウェア構成 (UEFI 設定) で Bluetooth を有効にしてください。

KnownConfigs.XML ファイルについて

Windows デバイスへのSecureDoc のインストールで、個別の設定が必要なデバイスについて情報が得られると、ウィンマジックは、そのデバイスに必要な設定内容をKnownConfigs.XML ファイルに追記します。

通常、SES で作成したWindows デバイス向けSecureDoc クライアントのインストールパッケージには、KnownConfigs.XML が含まれています。クライアントへのインストール時にインストーラーがデバイスを検知し、KnownConfigs.XML 内にそのデバイスを見つけた場合、記述されている設定内容に従ったインストールを自動でおこないます。

KnownConfigs.XML によって、特定のデバイスにおける既知情報の知識を必要とせず、インストール時における問題を回避することができます。

※ 最新のKnownConfigs.XML ファイルについては、製品をご購入いただきました販売代理店へお問合せください。

KnownConfigs.XML ファイルの変更方法：

1. Windows Explorer から c:\Program Files(x86)\WinMagic\SDDDB-NT に移動します。
2. 次に、*.xml のように XML ファイルを検索します。
3. 検索結果リストを名前別にソートします。
4. KnownConfigs.XML ファイルが見つかった各ディレクトリで、最新の KnownConfigs.XML と置き換えます。

注 KnownConfigs.XML ファイルは、ウィンマジックのみがその開発および機能強化する権利を保持しています。お客様による KnownConfigs.XML ファイルの変更に起因するサポートを要求される場合、ウィンマジック独自の裁量で追加のサポート費用を請求することがあります。ウィンマジックは、KnownConfigs.XML を拡張および向上する方法についてのお客様からのアイデアや提案を歓迎していますが、ウィンマジックは、多くのお客様にとって利益になると考えられる KnownConfigs.XML に対する変更、テスト、承認、および公表する唯一の権利を保持します。

プログラム(プロダクト)名、用語について

プログラム名

- SES** ... SecureDoc Enterprise Server の略称、SecureDoc クライアントを管理します。
SES Web ... SecureDoc Enterprise Server Web コンソール (SDWeb と記載している場合があります)
SDConnex ... クライアントとの通信をおこなう通信プログラム

機能名

- PBA** (Pre-boot Authentication) ... プリブート認証 (OS 起動前の認証)
RME (Removable Media Encryption) ... リムーバブルメディア暗号
RMCE (Removable Media Container Encryption) ... リムーバブルメディア コンテナ暗号
SFE (SecureDoc File Encryption) ... SecureDoc ファイル暗号
FFE (File Folder Encryption) ... ファイル フォルダー暗号
DAC (Disk Access Control) ... ディスクアクセス コントロール
Port Control ... ポート コントロール

Windows デバイスのプリブート認証(PBA)プログラムについて

- PBL** (Pre-boot for Legacy) ... Legacy デバイス向け、PBA プログラム
PBU (Pre-boot for UEFI) ... UEFI デバイス向け、デフォルトの PBA プログラム
PBLU (Pre-boot for Linux UEFI) ... UEFI デバイス向け、Linux ベースの PBA プログラム

Windows サインインの認証方法について

- SDCP** (SecureDoc Credential Provider) ... サインインに SecureDoc Credential Provider を使用

プリブートネットワーク認証について

- PBN** (Pre Boot Network) ... プリブート認証で、ネットワークを利用すること
PBNA (Pre Boot Network Authentication) ... プリブート時に、SDConnex と接続しネットワーク認証する
PBConnex ... SDConnex を使用して、ネットワーク認証をおこなう機能

BitLocker 管理について

- SDBM** (SecureDoc for Bitlocker Managment) ... BitLocker の暗号化・管理を SES でサポートするプログラム
SDBL (SecureDoc for BitLocker) ... BitLocker 標準機能のプリブートを使用し、SES で管理する
SDOT BL (SecureDoc on top for BitLocker) ... BitLocker 向け SecureDoc のプリブート認証プログラム

File Vault2 管理について

- SDFV2** (SecureDoc for FileVault2) ... FileVault2 の暗号化・管理を SES でサポートするプログラム

Linux 管理について

- SDLinux** (SecureDoc for Linux) ... Linux の暗号化・管理を SES でサポートするプログラム

その他

- SDOSA** (SecureDoc for OSA) ... OSA (Operating System Agnostic)
 TCG Opal ディスク用のプリブートプログラム
 オペレーティングシステムを選びません。
MagicEndpoint ... FIDO2 に対応した認証アプリケーション

※以降、SecureDoc を【SD】、MagicEndpoint を【ME】と表記している場合があります。

新機能および機能強化

SES または SES Web コンソール

リファレンス	説 明
SD-47442	【SES Web】クライアントから暗号化進捗状況を伝送する機能が追加されました SecureDoc クライアントでの暗号化進捗状況(%)を SES Web のレポート機能で確認できるようになりました。 ディスク全体(パーティションベースではない)の暗号化状況を追跡し、進捗の 10% 毎にレポートを更新し、処理が 100% に達するまで「10%」、「20%」のように表示されます。 注 本機能を有効にする方法 プロファイルの [General] セクションにパラメータ「UpdateProgressToServer=1」を手動で追加してください。 注 この機能は、以下のシナリオではサポートされません。 1. SD コントロールセンターから開始された復号化 2. SD コントロールセンター経由の再変換(再暗号化) 注 これは SD ソフトウェア暗号化のみの機能です。 BitLocker やハードウェア暗号化 (SED) デバイスには適用されません。
SD-49184	スマートカードから BLE への変換のサポート強化 Windows のサインインにスマートカードのみを使用しパスワードを使用していない環境の場合(証明書などを使用)、SecureDoc の導入にあたり、BLE への変換時にパスワードが必要なため、これまでのバージョンでは処理が中断されます。 本バージョンでは、ユーザーがパスワードを使用していない環境でも、BLE への変換をサポートできるようになりました。
SD-49797	SES コンソールに PWM 設定 UI が追加されました SecureDoc Password Manager (PWM) は、パスワードレス認証をサポートしていないアプリケーションにおける、手動のユーザー名/パスワードログインを支援または代替するために設計されたコンポーネントです。互換性のないアプリケーションの認証情報入力を管理することで、ME による認証を補完します。PWM にはクライアントコンポーネントと SES コンポーネントの両方が含まれており、旧バージョンでは手動で設定する必要がありました。 新しい UI は、プロファイルセクションの「SecureDoc Password Manager」から利用できます。

SecureDoc Enterprise for Windows

リファレンス	説 明
SD-48888	スマートフォンによる認証へ変更するための新しいユーザインタフェース Bluetooth Low Energy (BLE) 端末の登録とパスワードベースのキーファイル(KF)からの変換をサポートする新しい UI とワークフローが導入されました。 これには以下が含まれます。 ・ パスワード保護のキーファイルから BLE 接続のスマートフォンによる認証への切り替えを可能にするローカル変換プロセス ・ リカバリ完了後の BLE 接続スマートフォン再登録(オンラインのみ) ・ BLE 接続スマートフォンの保護デバイスで、キーファイルリカバリログイン時に、ユーザーはパスワード保護のキーファイルにリセットするか、QR コードをスキャンしてスマートフォンによる保護に変換するかを選択できます。 ユーザーの柔軟性とセキュリティを改善する一環として導入されたこの新機能は、スマートフォンに MagicEndpoint v2 が必要です。
SD-49529	Windows 11 24H2 における WMIC の非推奨に対応 Windows 11 24H2 との互換性を維持するため、SecureDoc は、従来の WMIC ユーティリティがデフォルトで利用できなくなったシステムでもシームレスに動作するように改善しました。 この更新により、KnownConfigs.xml に関連付けられたハードウェア検出タスクが、インストール時およびシステム構成時に引き続き期待どおりに機能するようになります。 WMIC 機能が不足している場合はパッチを適用し、タスク完了後に削除する動的なフォールバックメカニズムを実装し、ハードウェア検出とセットアップが中断されることはありません。 この変更により、ユーザーによる手動操作は不要になり、新しい Windows ビルドでの一貫した展開動作が保証されます。
SD-49561	【PBA】プロキシ設定のサポート プリブート認証(PBA)がプロキシ設定をサポートするようになりました。 プロキシの詳細(アドレスとポート)をシステム設定から読み取り、プリブート時に適用できます。 これにより、インターネットアクセスがプロキシ経由でルーティングされる環境でも、SDConnex と正常に接続できるようになります。
SD-50185	BLE 接続スマートフォン認証ユーザーに、新しいスマートフォン登録のサポート。 Bluetooth Low Energy (BLE) 端末による認証を使用しているユーザーが、何らかの理由でスマートフォンを利用できず、代替パスワードでログインすることになった場合、ログイン後、新しいスマートフォンの登録ができるようになりました。 これは、ユーザーが元のスマートフォンを紛失した場合や故障、スマートフォンアプリにアクセスできない場合などで役立ちます。この機能強化により、認証に使用する新しいスマートフォンをシームレスに再設定できます。 さらに、この機能は、チャレンジ・レスポンス、セルフヘルプ、またはワンタイムパスワード(OTP)方式による復旧ログイン時に、ローカルキーファイル(KF)の変換をサポートします。
SD-50197	【PBA】ビープ音によるアクセシビリティ サポート スピーカーを搭載していないノート PC で、プリブート認証時のアクセシビリティ サポートを強化するために、サウンドデバイスによる「ビープ音」を利用できるようになりました。 必要に応じて、ビープ音の動作を微調整できます。

SDLinux

リファレンス	説 明
SD-49991	RHEL 9.5 をサポート 本バージョンでは、カーネルバージョン 5.14.0-503.23 を含む Red Hat Enterprise Linux (RHEL) 9.5 をサポートします。

MagicEndpoint IdP

リファレンス	説 明
SD-49487	SAML 2.0 のサポート MagicEndpoint IdP は SAML 2.0 をサポートします。
SD-49815	スマートフォンによる認証ユーザーへの機能強化 ネットワークを介したスマートフォンによる認証を設定しているユーザーがスマートフォンを自宅に置き忘れた場合など、スマートフォンを利用できない場合、デバイスからロックアウトされます。 本バージョンでは、従来のチャレンジ・レスポンス方式に加え、新しいログイン方法「マネージャーの承認によるログイン」という機能を実装しました。 ユーザーは割り当てられたマネージャーにログイン承認をリクエストできるようになりました。 マネージャーは、自身のスマートフォンにプッシュ通知を受け取ります。 管理者は、IDP または SES Web インターフェースを介して特定のユーザーグループにマネージャーを割り当てることで、ユーザーがデバイスが利用できない場合でも承認ルーティングによって、エンドユーザーをサポートできます。

改善された問題

SES または SESWeb コンソール

リファレンス	説 明
SD-47948	BitLocker デバイスへの「Crypto Erase」コマンド 旧バージョンでは、BitLocker 管理デバイスでの Crypto Erase 機能を利用可能でしたが、SES v9.0 SR1 / 9.1 では、BitLocker で暗号化されたデバイスへ Crypto Erase コマンドを実行使用できないように仕様変更していました。 これは、SecureDoc の機能で暗号化した場合と異なり、Crypto Erase コマンドで鍵を消去した BitLocker は回復できないためです。 しかし、旧バージョンを使用していたお客様の声により、本機能を有効にするように変更しました。SES コンソールおよび SES Web コンソールから BitLocker 管理デバイス (SDOT/SDBM) へ Crypto Erase を実行できます。 注 BitLocker暗号化デバイスも、Crypto Erase コマンドを実行した場合、回復することはできません。システム回復不能になりますので、ご注意ください。
SD-48723	【ADSync】同期において SID が NULL の場合の警告メッセージが削除されました グループの SID (セキュリティ識別子) が欠落している場合、完全同期中に ADSync ログに警告メッセージが表示されていました。 これは機能には影響しませんが、不要な懸念や混乱を招く可能性がありました。 SID が NULL の場合でもシステム処理がより適切になり、警告を表示しないように改善しました。これにより、同期がよりスムーズになります。
SD-49053	【SES Web】レポート機能の改善 ユーザー、デバイス、グループ、鍵のレポート操作時に、より正確で直感的な結果を提供できるようになりました。 Yes / No フィールドのフィルターがチェックボックスオプションを使用するように更新され、不要またはサポートされていないフィルターが削除されたため、使いやすさが向上しました。 名、姓、メールアドレス、電話番号などのフィールドでは、null 値または空値を正しく処理できるようになり、日付フィルターは、時刻値に関係なく、選択した日付と正確に一致するよう修正しました。さらに、SaaS 環境のグループ別鍵のレポートに影響を与えていた内部サーバーエラーを修正。
SD-49080	【SES Web】ログイン時に、エラー500が発生する 旧バージョンから SES 9.1 SR1 へのアップグレード後、以前の有効な認証情報を使用しているも、SES Web にログインする際に HTTP エラー500 または「ユーザーが登録されていません」というメッセージが表示される場合があります。 この問題は、本バージョンで修正されています。 ログイン時のユーザーアカウントデータの処理を改善し、有効なユーザーによる予期しないエラーを防止するように修正しました。
SD-49188	【SES Web】レポート機能の改善 - 権限によって正しくフィルタリングされない 旧バージョンでは、一部のレポートで、ルートフォルダやごみ箱など、ユーザーがアクセス権限を持たないフォルダの情報が表示されていました。 この問題は、本バージョンで修正されています。 フォルダベースの権限がレポート全体で正しく適用されるようになり、ユーザーは、アクセス権限が

リファレンス	説 明
	付与されたフォルダのレポートデータのみを表示できます。 この修正は、以下のレポートに適用されます。 - MagicEndpoint ユーザー登録 - ドメイン別ユーザー - デバイス別キー - グループ別キー - ユーザー別キー さらに、特定のレポートメニューとダッシュボードへのアクセスには、割り当てられたロール権限が必要になりました。たとえば、デバイスレポートメニューまたはダッシュボードを表示するには、ロールにデバイスデータの読み取り権限が含まれている必要があります。
SD-50398	【SES Web】大文字と小文字を区別しないユーザー名による同時ログイン問題 旧バージョンでは、同時ログインが無効になっている場合でも、大文字と小文字が異なるユーザー名（例：“TERMINAL”、“terminal”、“TerMinAl”）を入力すると、同じユーザーID で複数のログインセッションを開始することができました。 この問題により、意図せず複数のセッションが作成されてしまう可能性がありました。システムは「最終ユーザーログイン」のタイムスタンプを正しく追跡していましたが、大文字と小文字が異なる場合、セッション制限が適用されていませんでした。 この問題は、本バージョンで修正されています。 ユーザー名の大文字と小文字の区別に関わらず、同時ログイン制限が一貫して適用され、セッションポリシーが確実に適用されます。

SecureDoc Enterprise for Windows

リファレンス	説 明
SD-49990	9.1 SR1 へアップグレード後、プリブート時に SAM ID を使用してサインインできない 8.6 / 9.0 SR3 から 9.1 SR1 へのアップグレードで、従来の Domain\UserID から UPN 形式（例：user@domain.com）に切り替わっていました。 これは、ドメインエイリアスが使用されている場合に、システムがアカウント照合を優先する方法が原因でした。 この問題は、本バージョンで修正されています。 本バージョンでは、ドメインエイリアスとキャッシュされた認証情報を使用している環境でも、SAM ID を正しく認識するように修正しました。

SDLinux

リファレンス	説 明
SD-43713	Ubuntu 22.04 の FIPS 対応システムへの展開をサポート 旧バージョンの SES では、一部の Ubuntu FIPS モード環境でエンドツーエンドの FIPS 検証を維持するインストーラーを生成できませんでした。 この問題は、本バージョンで修正されています。 Ubuntu 22.04 用の FIPS 準拠の SecureDoc インストーラーを作成できるようになり、セキュリティ強化された環境へのスムーズな導入を実現します。
SD- 49508	RHEL 9.4 におけるドライブ暗号化のパフォーマンス強化 RHEL 9.4 システムにおけるドライブ暗号化が想定よりも大幅に遅いという問題が確認されました。パフォーマンス低下の原因は、ドライバーが暗号化時のデータ変換を管理する方法の変更に関連していました。 この問題は、本バージョンで修正されています。 ドライバーによるデータ変換の処理方法を最適化することでパフォーマンスが向上し、暗号化時間が想定レベルに戻り、RHEL 9.4 システムへの導入が迅速におこなえるようになりました。
SD-49858	暗号化されたシステムに接続された暗号化 LVM ディスクのリカバリサポートを強化 暗号化された LVM ディスクをロック解除し、別の暗号化されたシステムに接続すると、実際にはロック解除されておらず、マウントできずに追加の暗号化ボリュームにアクセスできないという問題がありました。 この問題は、本バージョンで修正されています。
SD-49992	io_load=256 設定を必要とするシステムを自動検出します 旧バージョンでは、io_load=256 設定を必要とするシステムで、その設定がされていない場合、インストールに失敗するため、手動で /etc/secdoc/io_load ファイルを作成し、io_load を 256 に設定する必要がありました。 本バージョンでは、io_load=256 設定が必要な場合、自動的に検出し、インストール時に適用するように改善しました。これにより、手動設定は不要になります。 下記のカーネル バージョンでは、これが必要となることが分かっており、RHEL 8.10 および 9.5 システムにおいて、よりスムーズなセットアップが可能になります。 RHEL 8.10 カーネル 4.18.0-553.x RHEL 9.5 カーネル 5.14.0-503.x
SD-50023	インストール時に USB メモリが接続されていた場合、正常に起動しない インストーラーが USB デバイスに SD スペースを割り当ててしまう可能性があり、結果としてブート環境が誤って構成されたり、機能しなくなったりする可能性があります。 この問題は、本バージョンで修正されています。 インストール中にリムーバブルディスクを検出してスキップする修正が実装され、SD スペースが USB デバイスに割り当てられるのを防ぎました。 注 予期しない動作を回避するため、インストール中は USB メモリ等がシステムに接続されていないことを確認してください。

リファレンス	説 明
SD-50149	16 ボリュームを超えるシステムのサポート 旧バージョンでの暗号化は 16 ボリューム以下のシステムに限定されていました。 システムに 16 を超えるボリュームがある場合、暗号化は失敗するか、追加のボリュームで暗号化を開始できませんでした。 v9.2 では、この制限がなくなり、ユーザーは 16 ボリュームを超えるシステムの暗号化を正常に実行できるようになりました。

改善した問題(特定のデバイスに関連)

リファレンス	説 明
SD-47414	【HP ZBook Power G10】 - 起動時に画面が真っ黒になる 起動後、画面が真っ黒なまま。ログイン画面が正しく表示されません。正しい資格情報を入力することで、認証に成功し起動することができますが、内蔵、外付けディスプレイのいずれも正しく表示されません。 プロファイルの詳細設定に、「nomodeset」を追加することで、画面表示の問題が解決し、ログイン画面が期待どおりに表示されるようになります。
SD-49138	【HP ZBook Firefly G11】 - MediaTek Wi-Fi 6E アダプター 休止状態から再開した後に MediaTek Wi-Fi 6e MT7922 (RZ616) 160MHz PCIe アダプターが検出されません。接続を復元するために完全な再起動が必要でした。 この問題は、本バージョンで、解決しています。
SD-49296	【Dell Precision 3591】 - Intel Wi-Fi 6E AX211 のサポート 旧バージョンでは、Intel Wi-Fi 6E AX211 アダプターを搭載した Dell Precision 3591 デバイスにおいて、ブートログインプログラムがサポートしておらず、プリブート認証時に NIC が検出されません。 この問題は、本バージョンで更新した PBL カーネル(6.11)により、解決しています。
SD-50236	【Lenovo T16 Gen 3】 有線 LAN で、PBU Auto Boot が動作しない。 旧バージョン(9.1 SR1)で、有線 LAN に接続し、プリブートネットワーク認証で、Auto Boot が動作しません。Ctrl + Alt + Del キーを押すと処理は続行されますが、ユーザーエクスペリエンスの観点からは理想的ではありませんでした。 これは PBU を選択した場合の問題で、PBLU では問題は発生しません。 この問題は、本バージョンで修正されています。
SD-50481	【HP ZBook Firefly G11】 - Intel Wi-Fi 6E AX211 のサポート 旧バージョンでは、ブートログインプログラムがサポートしておらず、プリブート認証時に NIC が検出されません。 この問題は、本バージョンと、システムドライバーと BIOS を更新することで、解決されます

制限事項

SecureDoc Enterprise for Windows

リファレンス	説 明
SD-50537	アップグレード時の表示問題 - 対象: BLE ユーザー BLE および MagicEndpoint を有効にしたクライアントパッケージを展開し、アップグレード後、SDCP 画面にユーザーID のみが表示され、ログイン方法が表示されない場合があります。続行しようとする、「指定されたユーザー名が無効です」というメッセージが表示される場合があります。 これは、アップグレード後の最初の起動時のみ発生します。システムを再起動すると、SDCP 画面に正しいログインオプション(「MagicEndpoint 電話アプリでログイン」と「代替パスワードでログイン」)が表示され、ユーザーは正常にログインできます。

SDLinux

SD-50700 SD-50747	暗号化のボリューム数制限 インストール済の SecureDoc クライアントで、20 を超えるボリューム構成で暗号化を実施することはできません。20 を超えるボリューム構成で暗号化を有効には、SecureDoc クライアントを完全にアンインストールした後、新規インストールする必要があります。 既に 31 の暗号化ボリュームを持つシステムでは、secdoc.py add などのコマンドを使用してさらにボリュームを追加して暗号化しようするとエラーが発生する場合があります。これは、最大ボリュームしきい値に達しているため、それ以上の暗号化ができなくなるためです。 注 大規模ボリューム構成を計画している管理者は、導入時にこれらの制約を考慮する必要があります。
----------------------	--

MagicEndpoint – スマートフォン

リファレンス	説 明
SD-50721	位置情報の制限は、MFA、IdP ポータル、RADIUS および LDAP ログイン等の方法には適用されません。 位置情報ポリシーは、ユーザーと関連付けられたサービスプロバイダーの両方を評価するように設計されています。 両方が、許可された場所が定義された同じグループ内に設定されている場合、位置情報制限が完全に適用されます。この動作は、承認された場所からのアクセスのみが許可される、帯域外(OOB)認証を使用したサービスプロバイダー(SP)ログインでサポートされます。 OOB 経由の SP ログインでは、設定に従って位置情報制限が適用されます。 その他の認証方法はどこからでもアクセス可能なため、該当する場合は一貫したユーザーアクセスが確保されます。

サポートが必要なお客様

弊社製品をご購入いただきました販売代理店によって、問い合わせ窓口が異なります。
サポートが必要なお客様は、製品をご購入いただきました販売代理店にて承ります。
既に SecureDoc をご利用いただいております、アップグレードに関するサポートが必要なお客様も、製品をご購入いただきました販売代理店にて承ります。

連絡先

ウィンマジック・ジャパン株式会社

〒105-0022

東京都港区海岸 1-2-3

汐留芝離宮ビルディング 21 階

電話番号: 03-5403-6950

<https://www.winmagic.co.jp/>

<https://winmagic.com/ja/home-jp/> (グローバルサイト)

営業担当者へのお問い合わせ:

sales.jp@winmagic.com

テクニカルサポート:

support.jp@winmagic.com

謝辞

本製品では、Antoon Bosselaers、Hans Dobbertin、Bart Preneel、Eric Young (eay@mincom.oz.au)、そして Rijndael AES アルゴリズムの開発者である Joan Daemen および Vincent Rijmen によって開発された暗号化ソフトウェアが使用されています。

「本製品では、OpenSSL Toolkit での使用を目的として、OpenSSL Project (<http://www.OpenSSL.org/>) によって開発されたソフトウェアが使用されています。」

ウィンマジックは、このプロジェクトの開発者によるソフトウェアの提供に対して、ここに感謝の意を表します。

©Copyright 1997 - 2025 by WinMagic Corp. All rights reserved.

Printed in Canada

カナダおよび米国では、多くの製品、ソフトウェアおよびテクノロジーが輸出規制の対象となっています。

ウィンマジックの製品の場合、お客様ご自身でこれらの規制の詳細を理解して戴く必要があります。

ウィンマジック製品の輸出と再輸出は、カナダ国境サービス庁 (CBSA) と、アメリカ合衆国商務省産業安全保障局 (BIS) のそれぞれが管理する、カナダおよびアメリカ合衆国の法律の規制を受ける場合があります。

より詳しい情報は、ウィンマジックの Web サイトまたは関係省庁の Web サイトで、ご確認ください。

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 および SecureDoc Cloud Lite は、米国およびその他の国における WinMagic Corp. の商標です。

本文中のその他の社名、製品名等は、各社の商標、または登録商標です。

© 2025 WinMagic Corp. All rights reserved.

このドキュメントは、情報提供のみを目的としています。

ウィンマジックは、明示的にも暗黙的にも、このドキュメントについて保証を一切しません。

ここに記載されているすべての仕様は、予告なしに変更されることがあります。