SecureDoc Enterprise Server

Version 9.2

リファレンス マニュアル

WinMagic SecureDoc

2025 年 8 月

はじめに

SecureDoc は、ディスク暗号化ソフトウェアの名称です。
SecureDoc Enterprise Server（以下、「SES」という。）は、Windows や mac デバイスへ SecureDoc をインストールするためのインストレーションパッケージの作成や、暗号化状態の監視、セキュリティポリシーの一元管理、パスワード失念時の救済などの機能を有しています。
暗号化には、ウィンマジックの暗号化エンジンだけでなく OS が実装している暗号化機能（BitLocker 及び FileVault2）を使うことも可能で、BitLocker 及び FileVault2 に SecureDoc が提供する多くの機能を追加できます。
現在、多くの企業では、様々なデバイスが存在します。既に Microsoft BitLocker で暗号化済のデバイスや自己暗号化ドライブ（TCG Opal）を搭載した Windows デバイスなど、暗号化の導入にはそれらを一元管理できるソリューションが必要です。SES は、ウィンマジックの暗号化エンジンで暗号化した SecureDoc クライアントだけでなく、既に BitLocker で暗号化済のデバイスや自己暗号化ドライブ（TCG Opal）搭載 PC や mac を包括的に管理できます。

本ガイドの目的

システム管理者が SES を使って、Windows デバイスへ SecueDoc をインストールし運用する上で、必要な情報を提供することを目的とします。使用頻度の低い機能については割愛しておりますので、予めご了承ください、

・SES で設定可能な各機能について一覧で説明します。
・SecureDoc の特長の１つであるプリブートネットワーク認証の設定方法について説明します。
・よく利用される設定方法や、ユーザーサポートに必要とされる機能について説明します。
・旧バージョンからのアップグレード手順について説明します。

SES のインストール及び基本的な設定と、Windows PC を暗号化するためのインストレーションパッケージの作成方法については、「SecureDoc Enterprise Server Version 9.2 クイックインストールガイド」をご参照ください。

SecureDoc Enterprise Server Version 9.2 リファレンスマニュアル

連絡先

WinMagic Inc. （カナダ本社）
200 Matheson Blvd West, Suite 201
Mississauga, Ontario, L5R 3L7
フリーダイヤル： 1-888-879-5879　電話：(905) 502-7000　Fax：(905) 502-7001
テクニカルサポート：support@winmagic.com

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：03-5403-6950　Fax：03-5403-6953
営業：sales.jp@winmagic.com　テクニカルサポート：support.jp@winmagic.com
URL：https://www.winmagic.co.jp/
https://winmagic.com/ja/home-jp/ （グローバル）

更新履歴

日　付	バージョン	更新内容
2025 年 7 月	初版	
2025 年 8 月	第 2 版	・ スマートフォンによる認証の説明を MagicEndpoint から MagicEndpoin2 に変更 ・ USB トークン保護への変更に関する説明補足

※　設定画面の説明で、旧バージョンの GUI が使われている場合があります。

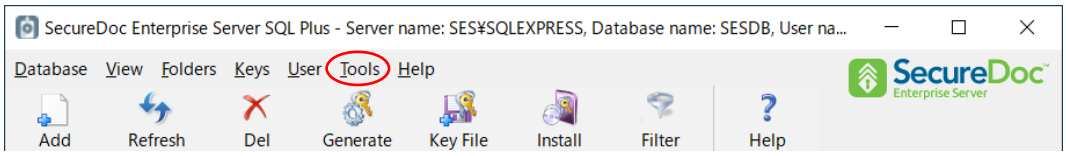
ご注意

最新の情報については、WinMagic にお問い合わせいただくか、WinMagic のホームページをご覧ください。
また、本ガイドでは、SES 環境として Microsoft Windows Server 2022 および Microsoft SQL Server 2022 Express を使用しておりますが、お客様が使用する製品バージョンと異なる場合、画面イメージや操作手順が異なる場合がありますので、予めご了承ください。

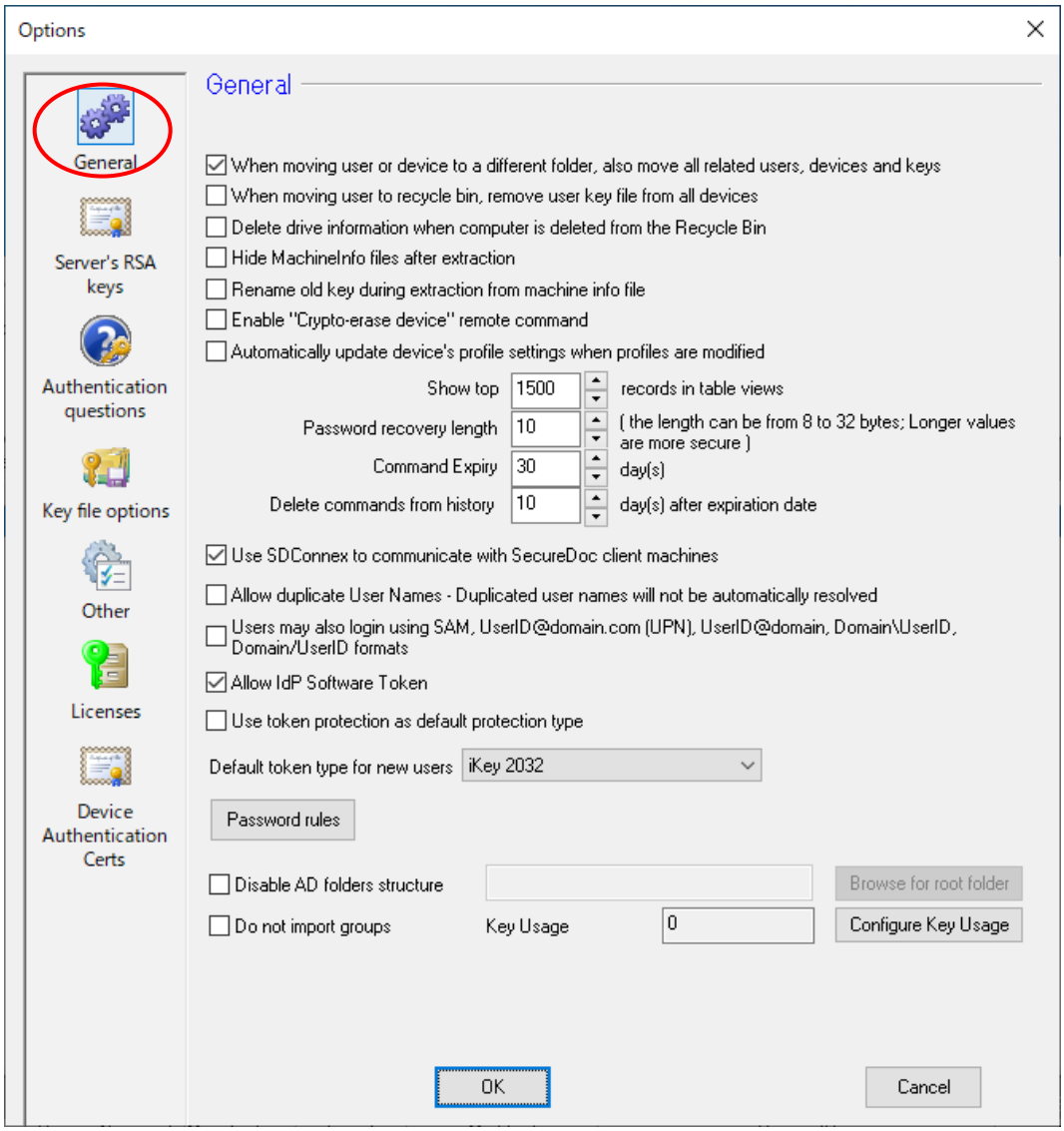
目 次

1. グローバルオプション設定

グローバルオプションの設定は、ライセンスの違いに関係なく SES 及び全てのクライアントデバイスに関与します。SES のメニューバーから、[Tools] -> [Options] をクリックします。



[General]

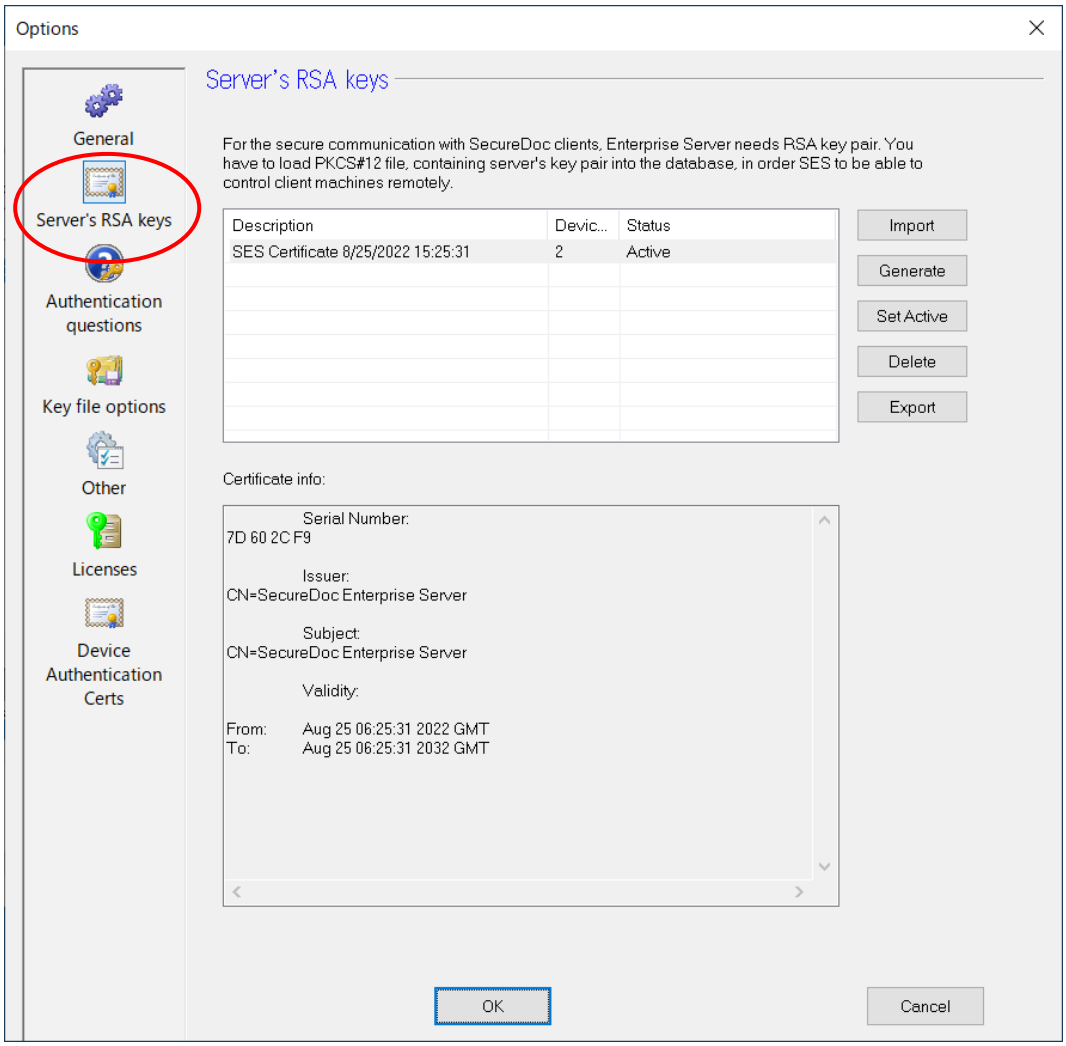


設　定	説　明
☐ When moving user or device to a different folder, also move all related users, devices, and keys	ユーザーまたはデバイスを別のフォルダに移動すると、関連するすべてのユーザー、デバイス、および鍵も移動します。
☐ When moving user to recycle bin, remove user key file from all devices	ユーザーを [Recycle Bin]（ごみ箱）に移動するときは、すべてのデバイスからユーザーのキーファイルを削除します。
☐ Delete drive information when computer is deleted from the Recycle Bin	コンピュータが [Recycle Bin]（ごみ箱）から削除されたときにドライブ情報を削除します。
☐ Hide Machine info files after extraction	MachineInfo ファイルには、クライアントデバイスとユーザーに関する情報が含まれています。 SDConnex と通信せずにオフラインでインストールした場合、そのデバイスを SES で管理するためには SES コンソールの左ペインの [MachineInfo Files] でインポートする必要があります。 SES DB に登録が済んだら、SES 管理コンソールにこれらのファイルを表示しないようにするには、このオプションをオンにします。
☐ Rename old key during extraction from machine info file	通常は使用しません。 以前に暗号化されたことのあるデバイスが再イメージ化され、再インストールを実行した時にそのクライアントデバイスからのネットワーク応答がないという特殊な状況を処理するために使用します。 MachineInfo File ファイルには、デバイスに最初に割り当てられた鍵が含まれます。このオプションをオンにすると、SES は古い鍵の名前を変更し、このクライアントデバイスの暗号化のために新しい鍵を生成します。
☐ Enable “Crypto-erase device” remote command	SES からリモートコマンドで Crypto Erase を実行できるようにします。 Crypto Erase はデバイスから鍵を削除するので、復号化することはできず、データは破壊されたのと同様になります。 Crypto Erase を受信したクライアントデバイスは、ブートログオンプログラムも正しく動作しなくなります。 誤った操作を防ぐ為に、デフォルト設定はでは無効です。
☐ Automatically update device’s profile settings when profile are modified	既存のプロファイルを変更した際、変更前のプロファイルが適用されているデバイスへ自動で変更したプロファイルを SDConnex 経由で配信し適用します。 このオプションの使用には、十分注意する必要があります。
Show top XXXX records in table views	SES コンソールで、上位の XXXX レコード（行）を表示します。 主に関係するのは、SES コンソールの左ペインにある「Logs」で表示される行です。 デフォルト設定は 1500 です。
Password recovery length XX (the length can be 8 to 32 bytes; longer values are more secure)	ユーザーのパスワード忘れ時に利用するチャレンジ&レスポンスで、レスポンス値の長さを指定します。 長いほど、安全性は高まりますが、長すぎると利便性を犠牲にします。 デフォルト設定値は「10」であり、セキュリティと実用性のバランスが取れていると見なされます。
Command Expire XX Day(s)	クライアント デバイスへのコマンド (Crypto-Erase コマンドを除く) を保持する時間を指定します。指定した日数を経過すると、コマンドの有効期限が切れます。 デフォルト値は「30」日です。 注　Crypto-Erase コマンドの有効期限は「10,000」日に設定されます。 SES 管理者は Crypto-Erase コマンドの有効期限を設定できないため、必要がなくなった場合、キャンセルする必要があります。

設　定	説　明
Delete commands from history XX day(s) after expiration date	有効期限の XX 日後に履歴からコマンドを削除します。 クライアントデバイスへのコマンドを破棄するまでの保持期間を指定します。 ここで設定した日数以内にデバイスがサーバーと通信しない場合、たとえば、このデバイスのプロファイルを更新するリモート コントロール コマンドは期限切れになります
☐ Use SDConnex to communication with SeueDoc client machines	SeueDoc クライアントデバイスは、SDConnex を使用して通信します。
☐ Allow duplicate User Names - Duplicated user names will not be automatically resolved	重複ユーザー名を許可します。
☐ Users may also login using SAM, User ID@domain.com(UPN), UserID@domain, Domain¥UserID, Dmian/UserID formats	ユーザーは、SAM、User ID@domain.com(UPN)など 各フォーマットでログインすることも可能です。
☐ Allow IdP Software Token	ユーザーは認証時に IdP ソフトウェアトークンを使用できます。バージョン 9.0SR3 では、SES と MagicEndpoint IdP が連携して、ユーザーのソフトウェアトークンを SES データベースに保存します。
☐ Use token protection as default protection type	クライアントデバイスでトークンプロテクションをデフォルトで使用する場合にチェックします
Default token type for new users	SES で作成するキーファイルに使用するデフォルトのトークンタイプを選択します。
<Password rules>	パスワードルールを設定します。 「SecureDoc Enterprise Server version 9.x クイックインストールガイド」をご参照ください。
☐ Disable AD folders structure	Active Directory からインポートしたすべてのユーザーとグループが同じフォルダに配置されるようにします。 Active Directory のフォルダ構造を使用しません。
☐ Do not import group	Active Directory グループをインポートしません。
Key Usage	Active Directory から証明書をインポートする際に考慮すべき鍵の使用法 (証明書の目的) を選択できます。 すべてのタイプの証明書をインポートするには、digitalSignature のデフォルト値 (0) のままにします。 特定の証明書のみをインポートするには、他の値を選択します。たとえば、UserSMIMECertificate 値を持つ証明書のみをインポートします。

[Server's RSA keys]

ここにリストされている鍵は、SES データベースの作成中に作成されたものです。単一の証明書が作成され、「アクティブな」証明書として設定されています。ほとんどの場合、SES インストールによって作成された鍵で十分です。独自の CA から作成された証明書を使用する必要がある場合、<Import> をクリックしてインポート後、<Set Active> をクリックして、それを有効にします。

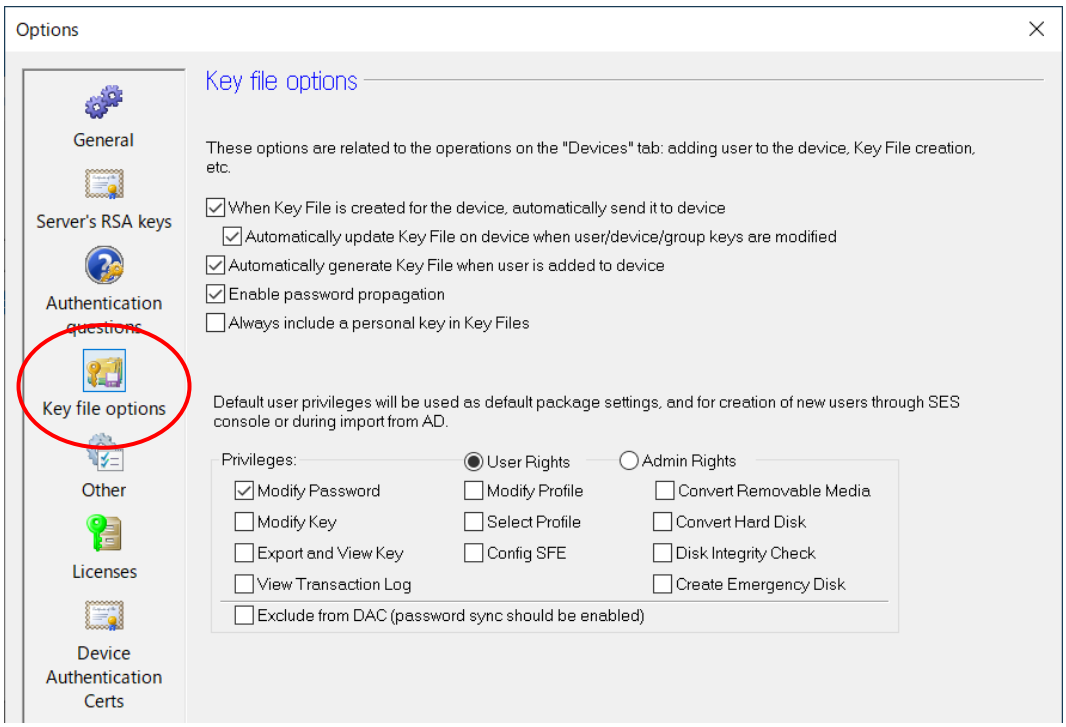


[Authentication questions]

日本語環境ではご利用いただけません。

[Key file options]

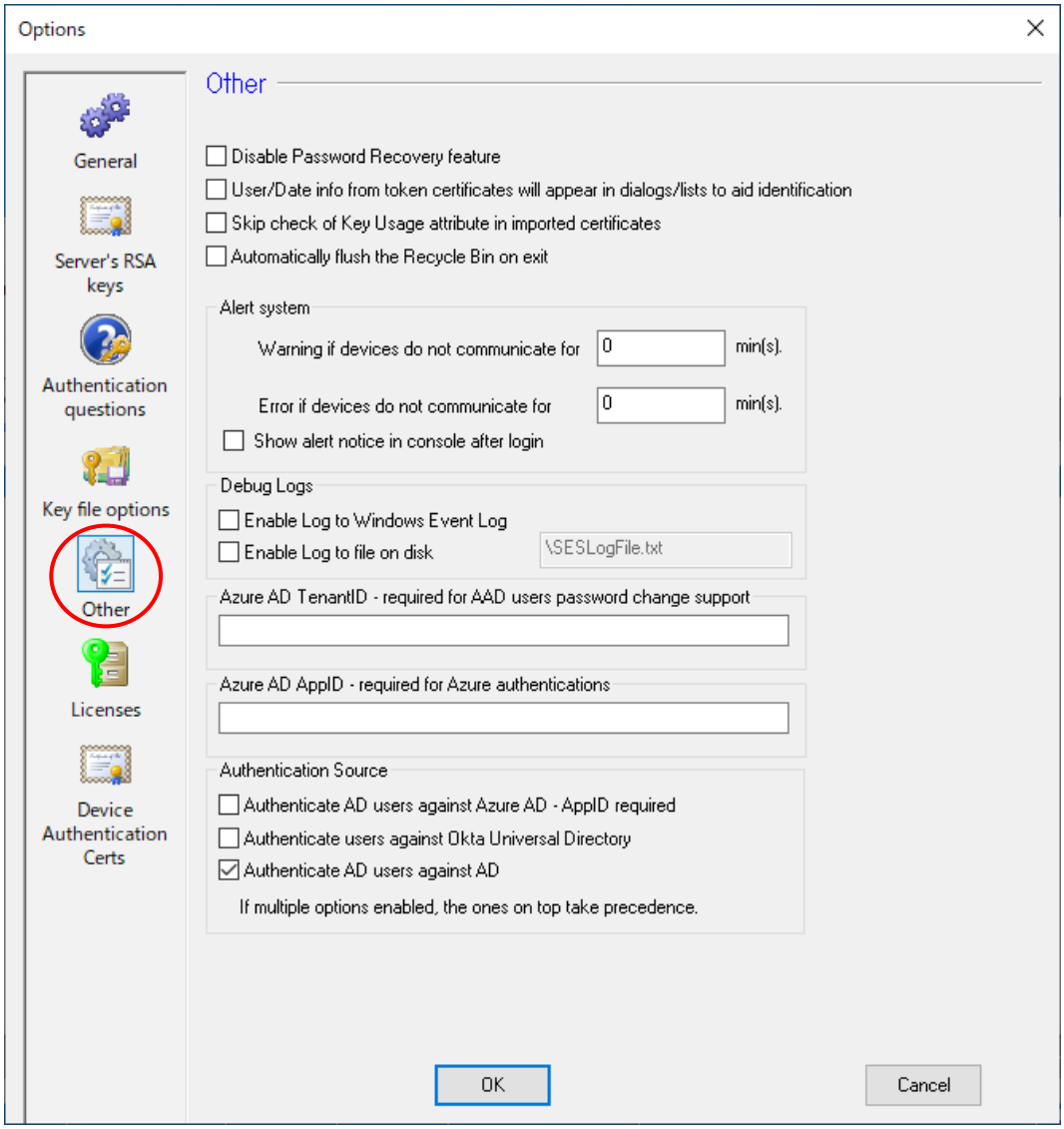
権限設定など、ここで設定した内容がインストレーションパッケージ作成時にデフォルト設定として読み込まれます。



設　定	説　明
☐ When Key File is created for the device, automatically send it to device	デバイス用にキーファイルが作成されると、それを自動的にデバイスに送信します。
☐ Automatically update Key File on device when user/device/group keys are modified	ユーザー/デバイス/グループのキーが変更された場合、デバイス上のキーファイルを自動的に更新します。
☐ Automatically generated Key File when user is added to device	ユーザーをデバイスに追加した際、キーファイルを自動で作成します。
☐ Enable password propagation	パスワードの伝搬を有効にします。 複数のデバイスに同じユーザーが登録されている場合、ユーザーがパスワードを変更した際、SDConnex を介して他のデバイスに変更したパスワードを送ります。 注　同一ユーザーが登録されているデバイスが SDConnex と通信していない場合（電源が入っていない等）、そのデバイスは新しいパスワード情報を受け取れないので、電源投入後のプリブート認証では変更前のパスワード入力が必要です。OS 起動後、SDConnex と通信すると変更されたパスワード情報を受け取り、次回の認証時からは新しく設定されたパスワードが必要になります。
☐ Always include a personal key in Key Files	キーファイルには、必ずパーソナルキーを入れるようにします。

設　定	説　明
Privileges:	
◎ User Rights	デフォルト設定は、「☑ Modify Password」のみです。 権限一覧から、必要な権限を付与できます。
◎ Admin Rights	チェックすると、全ての権限が付与されます。
☐ Modify Password	ユーザーは、パスワードを変更できます。
☐ Modify Profile	ユーザーは、プロファイルを変更できます。
☐ Convert Removable Media	ユーザーは、リムーバブルメディアを暗号化できます。
☐ Modify Key	ユーザーは、鍵を生成、削除、およびインポートできます。
☐ Select Profile	ユーザーは、プロファイルを選択できます。
☐ Convert Hard Disk	ユーザーは、ディスクの暗号化/復号化をおこなえます。
☐ Export and View Key	ユーザーは、鍵を操作できます。たとえば、キーファイルをエクスポートすることや、鍵を他のキーファイルにエクスポートしたりできます。
☐ Config SFE	ユーザーは、クライアント側で、SecureDoc ファイル暗号化を定義することができます。
☐ Disk integrity Check	ディスクの整合性チェックが失敗した場合でも、ユーザーは作業を続行できます。デバイスを検査し、ディスクの整合性のために新しい署名を再作成します。
☐ View Transaction Log	ユーザーは、Audit Log を見ることができます。
☐ Create Emergency Disk	ユーザーは、エマージェンシーディスクを作成できます。
☐ Exclude from DAC (password sync should be enabled)	DAC を無効にします。（通常は選択しません） インストレーションパッケージのプロファイルの設定にて、ディスクアクセスコントロール（DAC）が有効に設定され、外部メディアへの接続が制限されている場合、外部メディアへのアクセスが行えず、ディスクをアンロックしても、外部メディアなどへデータの移動が行えません。

[Other]



設　定	説　明
☐ Disable Password Recovery feature	オンにすると、すべてのユーザーのパスワード回復が無効になります。特別な理由が無い限り、有効にしないでください。
☐ User/Date info from token certificates will appear in dialogs/lists to aid identification	トークン証明書のユーザー/日付情報がダイアログ/リストに表示され、本人確認を容易にします。
☐ Skip check of Key Usage attribute in imported certificates	証明書がユーザー レコードの一部としてインポートされると、SES はその証明書が暗号化に使用されるかどうかを確認し、そうでない場合は使用しません。 証明書を使用するには、このオプションをオンにします
☐ Automatically flush the Recycle Bin on exit	SES コンソールの終了時に [Recycle Bin] の内容を自動で削除します。

設　定	説　明
Alert System	
Warning if devices do not communicate for X min(s).	エンドポイントデバイスが SDConnex との通信がない場合、SES 管理者に警告するのに十分な懸念があると見なされる時間（分）を指定します。 注　このオプションは、ATM などで使われるデバイスを想定しています。
Error if devices do not communicate for X min(s)	デバイスが X 分間通信しない場合は、エラーとします。
☐ Show alert notice in console after login	管理者が SES コンソールにログインすると、「ポップアップ」メッセージによるアラート（警告もしくはエラー）が表示されます。
Debug Logs	
☐ Enable Log to Windows Event Log	SES Audit Log 以外に、Windows イベントログにログを保存します。
☐ Enable Log to file on disk	SES Audit Log 以外に、指定した場所にログを保存します。
Authentication Source	
☐ Authenticate AD users against Azure AD – AppID requied	Azure AD に対してユーザーを認証するには、このチェックボックスをオンにします。
☐ Atuthenticate users against Okta Universal Directory	Okta Universal Directory に対してユーザーを認証するには、このチェックボックスをオンにします。
☐ Authenticate AD users against AD If multiple options enabled, the ones on top take precedence	このチェックボックスをオンにすると、ユーザーを（通常はオンプレミスの）Active Directory に対して認証します。 複数のチェックボックスを選択した場合、ユーザーは表示されている順序でこれらのディレクトリサービスに対して検証されます。

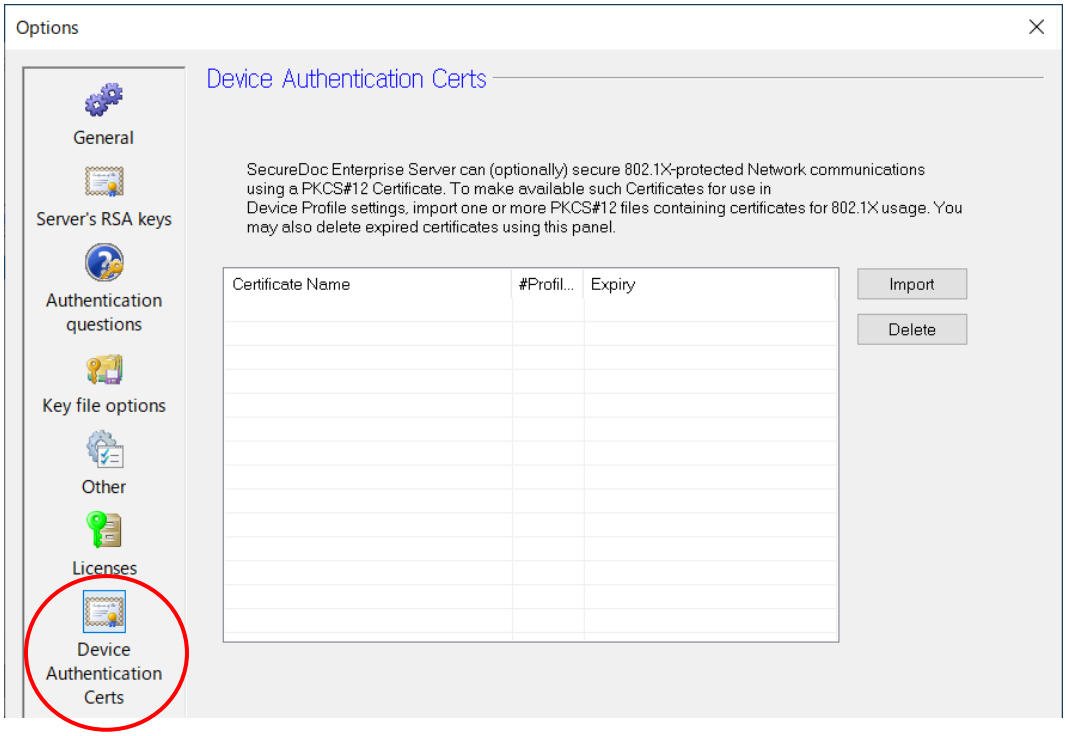
[Licenses]

「SecureDoc Enterprise Server version 9.2 クイックインストールガイド」をご参照ください。

有効ライセンス数を超えて、クライアントデバイスに SecureDoc をインストールすることはできません。

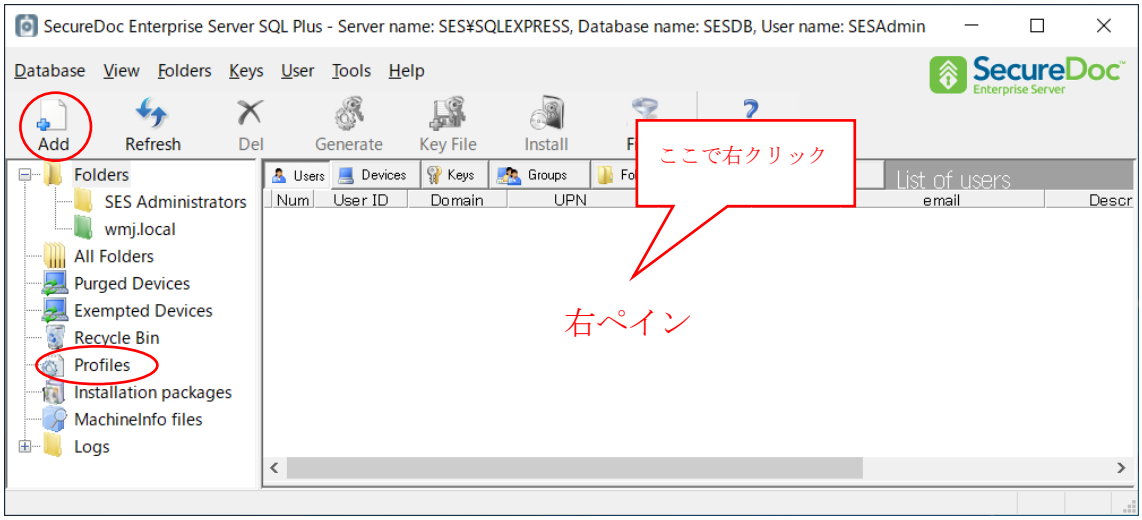
[Device Authentication certs]

802.1X を使用するネットワーク環境で、グローバル証明書ベースのデバイス認証を必要とする場合、このパネルを使用して証明書をインポートする必要があります。

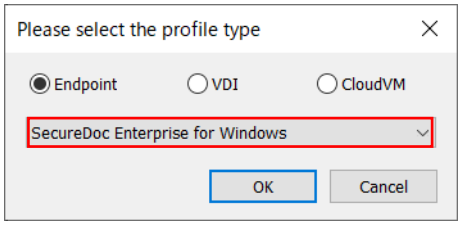


2. SecureDoc Enterprise for Windows プロファイル

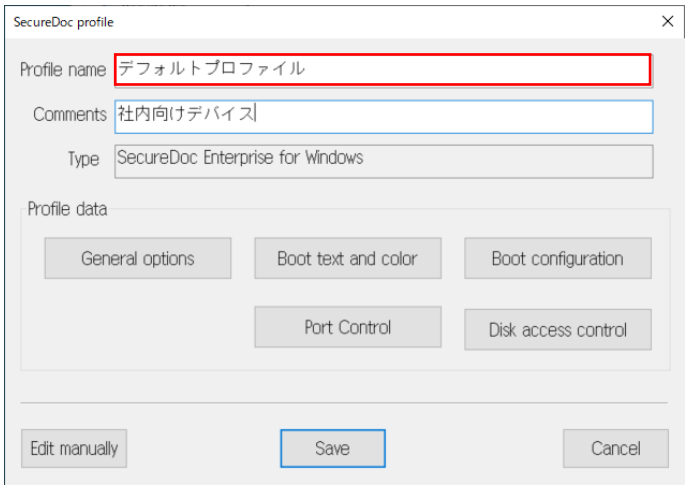
① 左ペインの [Profiles] アイコンを選択し、<Add> をクリックするか、右ペインの上で右クリックし、コンテキストメニューから [Add profile] をクリックします。



② [Please select the profile type] ウィンドウが表示されますので、[◎ Endpoint] のプルダウンメニューより「SecureDoc Enterprise for Windows」を選択し、<OK> をクリックします。

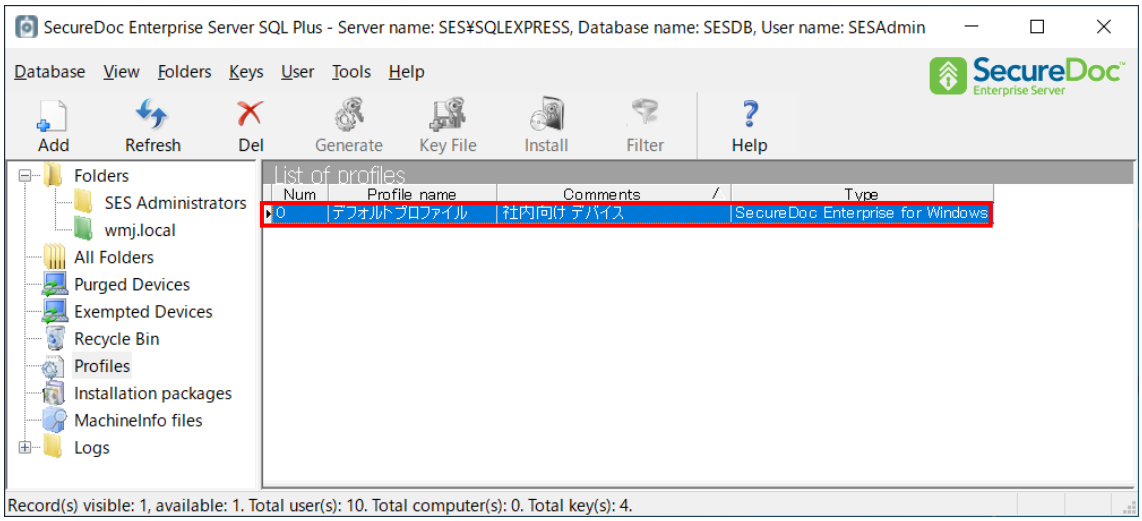


③ [Profile name] 欄にプロファイル名を、必要に応じて [Comments] 欄にコメントを入力します。



④ 個々の設定が完了したら、最後に<Save> をクリックして保存します。

SES 上にプロファイルが作成されたことを確認します。

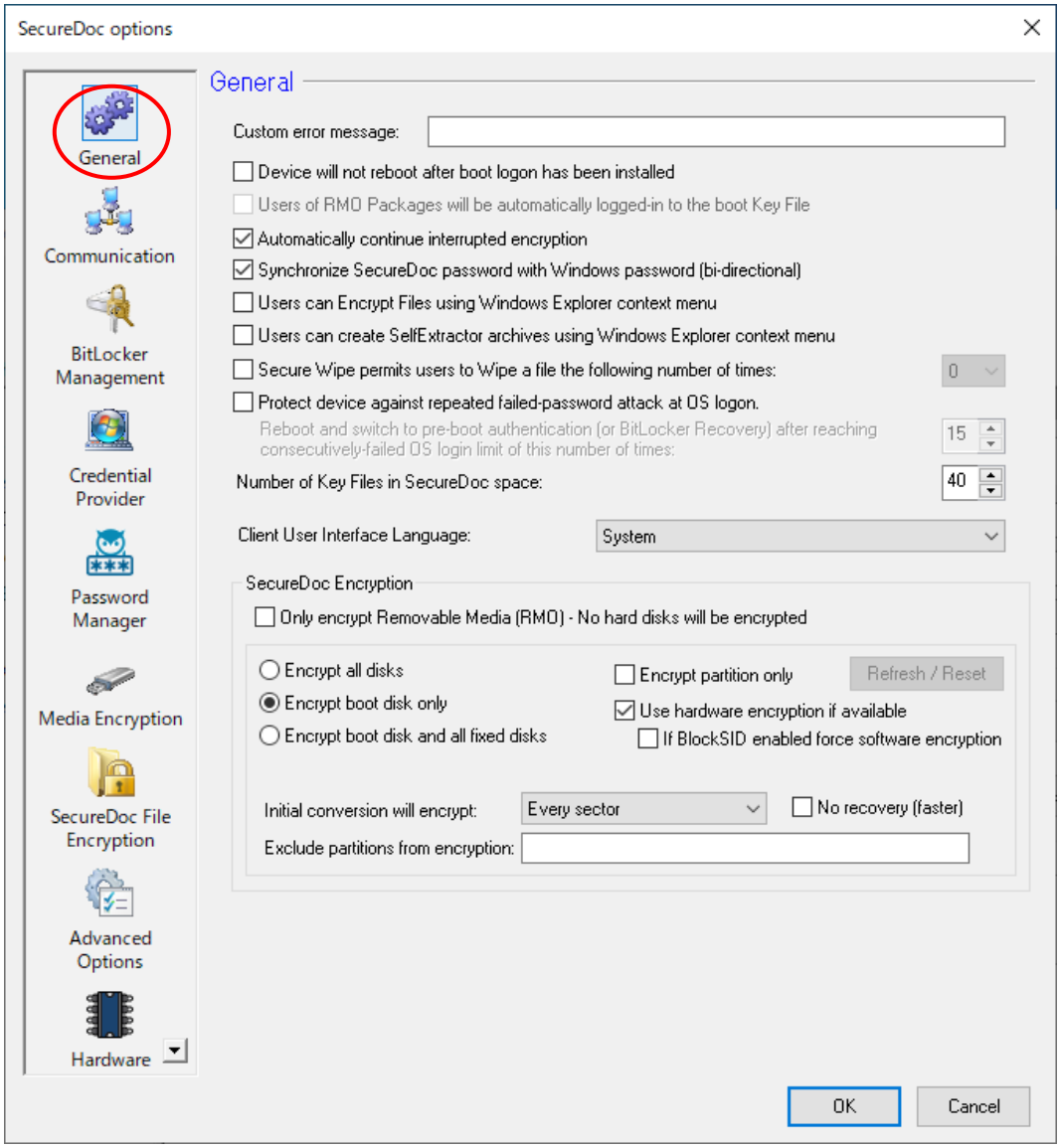


※　複数のプロファイルを作成する場合、作成済のプロファイルを編集することで簡単に作成できます。
作成済のプロファイルを右クリックして、コンテキストメニューから [Copy Profile] を実行します。
[Profile name] に新しいプロファイル名を入力し、必要な項目を編集して保存してください。

2.1. General options

[General]

暗号化をおこなう対象のディスク指定など、デバイス共通の設定箇所です。



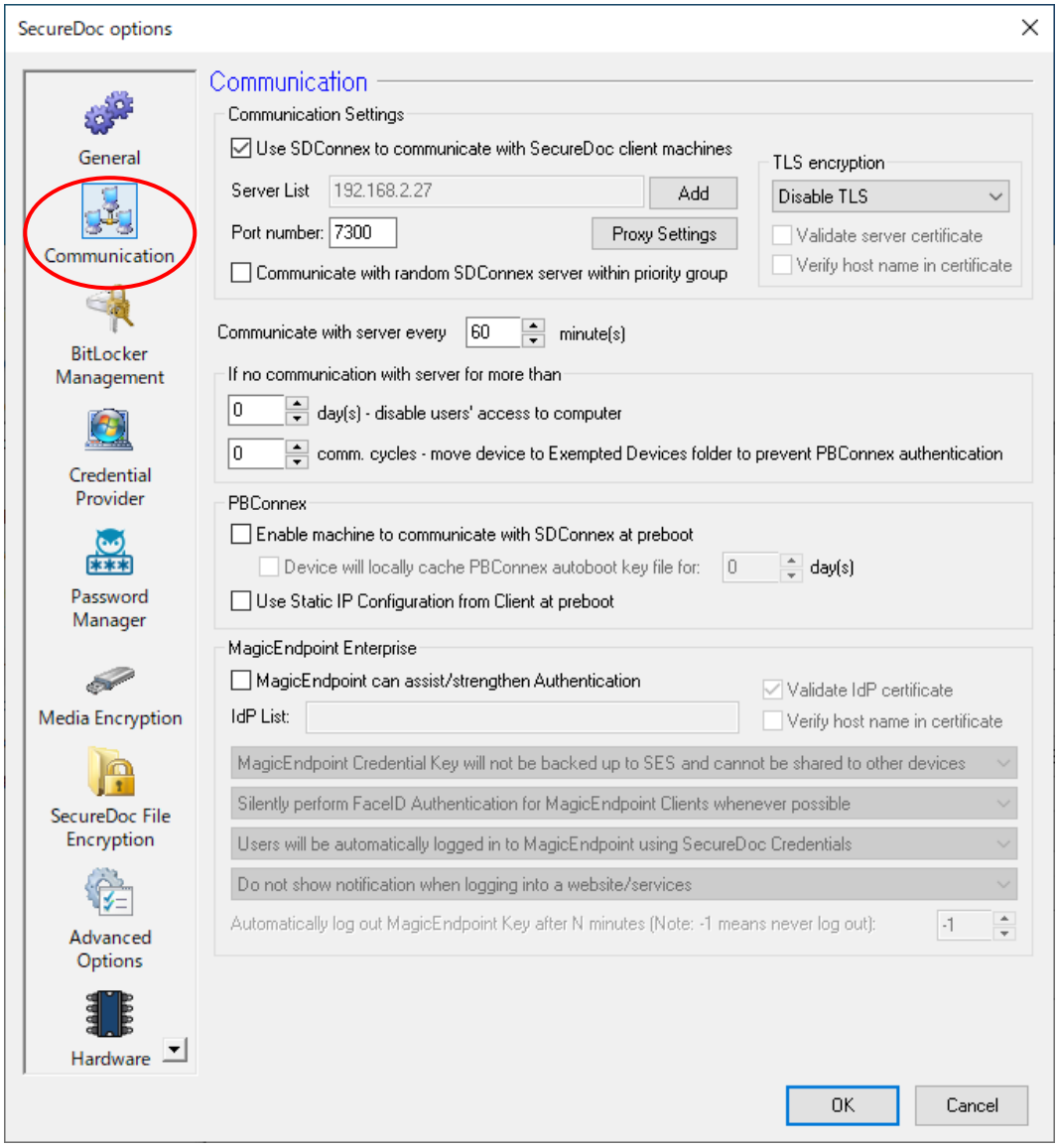
設　定	説　明
Custom error message:	SecureDoc で使用されているデフォルトのエラーメッセージをカスタマイズできます。 例）ヘルプデスク（内線番号 1234）までお問い合わせください。
☐ Device will not reboot after boot logon has been installed	SecureDoc のブートログオンインストール後、OS の再起動をおこなわないようにします。
☐ Users of RMO Package will be automatically logged-in to the boot Key Files	リムーバブルメディア暗号のみを使用する RMO パッケージのユーザーは、ブートキーファイルに自動的にログインします。暗号化の設定で、[Only encrypt Removable Media (RME)] を選択した場合に、プリブート認証を必要としない設定です。 「Boot Configuration」設定で、 [Force permanent Auto-Boot] オプションが有効になっている必要があります。

設　定	説　明
☐ Automatically continue interrupted encryption	何らかの理由で暗号化が中断された場合でも、暗号化を自動的に再開させます。
☐ Synchronize SecureDoc password with Windows password (bi-directional)	チェックを入れると、ユーザーの Windows パスワードが、SecureDoc のキーファイルパスワードと自動的に同期されます。Windows パスワードの変更は自動的に SecureDoc に適用され、SecureDoc パスワードの変更も Windows に適用されます。 プロビジョニングルールを使用する場合は、チェックを入れる必要があります。チェックを入れていない場合、パッケージ作成時にアラートが表示され、プロファイルを変更するよう促されます。
☐ Users can Encrypt File using Windows Explorer context menu	ユーザーは、Windows エクスプローラーのコンテキスト メニューを使用してファイルを暗号化できます。
☐ Users can create SelfExtractor archives using Windows Explorer context menu	ユーザーは、Windows エクスプローラーのコンテキスト メニューを使用して 自己解凍アーカイブを作成できます。
☐ Secure Wipe permits users to Wipe a file the following number of times:	このオプションを選択すると、エクスプローラーの右クリックコンテキストメニューにオプションが追加され、右側にあるドロップリストで指定された回数でディスクからファイルを上書きして消去できます。
☐ Protect device against repeated failed-password attack Windows logon	管理者は、パスワードの試行回数が許可される回数をさらに定義することができます。 Windows ログインに連続して失敗した回数が、ここで設定した回数に達すると、再起動し、プリブート認証（または BitLocker リカバリ）に切り替えます。
Number of Key File in SecureDoc space:	登録するキーファイルの最大数を指定します。規定値：40 変更する場合は 16～200 の間で値を入力します。
Client User Interface Language:	SecureDoc ユーザーインターフェースで使用する言語を選択します。 「System」は、Windows OS に設定されている言語設定に基づき、SecureDoc の言語を設定します。言語を指定すると、OS とは関係なく、SecureDoc の言語が設定されます。
SecureDoc Encryption	
☐ Only encrypt Removable Media (RME) - No hard disks will be encrypted	リムーバブルメディアのみを暗号化する場合に選択します。 HDD や SSD のローカルディスクを暗号化しません。
○ Encryption all disks	全てのディスクを暗号化します。
○ Encryption boot disk only	ブートディスクのみ暗号化します。（初期設定）
○ Encryption boot disk and all fixed disks	ブートディスクと固定ディスク全てを暗号化します。
☐ Encryption partition only	パーティションのみを暗号化します。
☐ Use hardware encryption if available	インストレーションプロセス中に、TCG Opal ドライブを検知した場合、ソフトウェアによる暗号化はおこなわず、Opal モードをアクティブにし、プリブート認証プログラムをインストールします。 チェックを外すと、TCG Opal ドライブであってもソフトウェアで暗号化します。 注　事前に UEFI/BIOS で、HDD パスワードもしくは Block SID の設定を無効にしておいてください。 TCG Opal ハードウェアの仕様で、インストール完了時、シャットダウンが必要です。

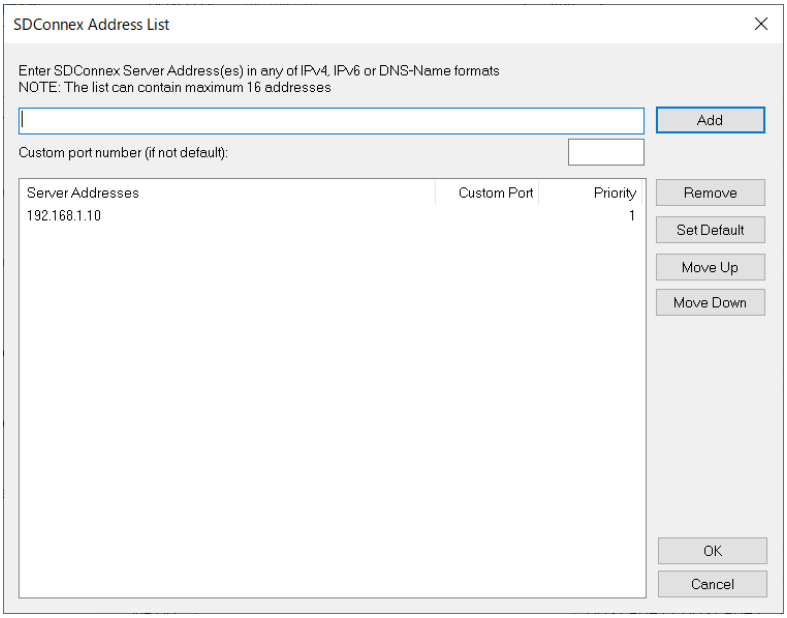
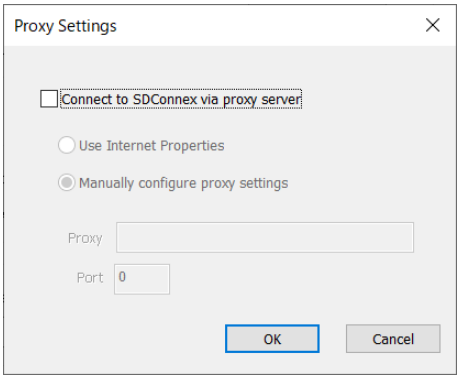
設　定	説　明
☐ If BlockSID enabled force software encryption	UEFI の設定で BlockSID が有効になっている場合、ソフトウェアで暗号化します。UEFI の設定で BlockSID を無効にできないデバイス向けの設定です。
Initial conversion will encrypt:	Every sector : 全てのセクターを暗号化します。既にディスクに重要なデータが保存されている場合はこのオプションを選択します。 Data only(faster) : インストール時、使用済領域のみを暗号化します。その後、データが書き込まれると、そのセクターは自動で暗号化されます。暗号化をユーザーが意識することはありません。(初期設定) 注　既にユーザーが使用している、重要なデータがあるデバイスの場合、このオプションは推奨されません。
☐ No recovery (faster)	暗号化時、万一の不具合に備えてリカバリデータを作成し暗号化しますが、このオプションを選択するとリカバリデータを作成せずに暗号化を実行します。ドライブの暗号化を早く完了させたい場合に役立ちます。 注　既にユーザーが使用している、重要なデータがあるデバイスの場合、このオプションは推奨されません。選択した場合、暗号化が完了するまで、電源コードを接続し、OS のシャットダウンや電源を切らないようにしてください。
Exclude partitions from encryption	[Encryption partition only] を選択した場合に、暗号化を必要としないパーティションを指定します。入力フィールドにはパーティションのラベルを入力します。

[Communication]

SDConnex との通信に関連する設定箇所です。



設　定	説　明
Communication Settings	
☐ Use SDConnex to communicate with SecureDoc client machines	クライアントデバイスは、SDConnex との通信をおこないます。 特別な理由がない限り、この設定は解除しないでください。
Server List	SDConnex がインストールされたサーバーの IP アドレスまたは FQDN 名を入力します。SDCoonex は、最大 16 台設置できます。 クライアントは、ここで指定された SDConnex と通信をおこないます。 複数の SDConnex が設置されている場合、接続先 SDConnex の優先順（Priority）を設定できます。クライアントは、Priority1 の SDConnex と接続できなかった場合、Priority2 の SDConnex との接続を試みます。

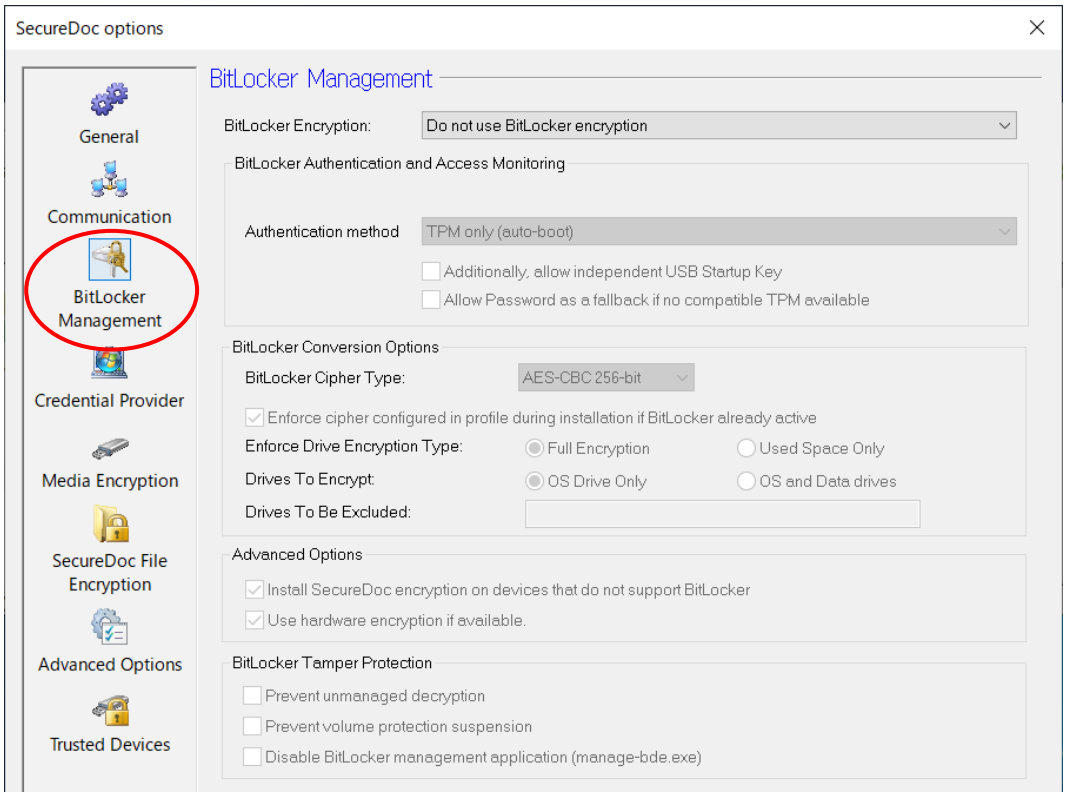
設　定	説　明
	
Port number	クライアントが SDConnex と通信する際のポート番号を指定します。規定値は「7100」です。
Proxy Settings	クライアントがプロキシサーバーを経由して SDConnex と通信する場合に設定します。 
☐ Communicate with random SDConnex Server within priority group	複数の SDConnex で Priority の設定を 1 にし、このオプションを有効にすると、クライアントは Priority の設定が 2 の SDConnex へのアクセスを試みる前に、Priority の設定が 1 の SDConnex へランダムにアクセスを試みます。
Communicate with server every X minute(s)	クライアントは、OS 起動時（サービス開始時）に SDConnex との最初の通信を試みます。その後は、ここで指定された間隔で SDConnex との通信を試みます。規定値は「60」分です。
TLS encryption	
- Disable TLS - Force use of TLS 1,3 - Force use of HTTPS	HTTPS あるいは TLS を使用する場合、暗号化スイートを選択します。 ☐ Validate server certificate ☐ Verify host name in certificate

設　定	説　明
If no communication with server for more than	
X day(s) - disable user’s access to computer	指定した日数内にクライアントが SDConnex と通信しなかった場合、自動的に全てのユーザーのキーファイル（管理者キーファイルを除く）をロックさせます。ロック解除にはチャレンジ&レスポンス機能を使います。
X comm cycles - move device to Exempted Devices folder to prevent PBConnex authentication	SDConnex を使用してデバイスをプリブートネットワーク認証しているクライアントデバイスで、通信サイクルで指定された回数、SDConnex と通信しなかった場合、デバイスを [Exempted Devices] フォルダに移動させます。 このオプションの目的は、非通信デバイスをオートブートを許可しないグループに移動することにより、無人の常時接続のエンドポイントデバイス（IOT デバイス、自動預け払い機/自動販売機、キオスクデバイス等）のセキュリティを強化することです。SDConnex と通信できない場合、デバイスが攻撃を受けているか、または危険にさらされている可能性があります（非通信期間中）。[Exempted Devices] フォルダに移動されたデバイスにはオートブートキーファイルが送信されないため、オートブートは実行されません。
PBConnex	
☐ Enable machine to communicate with SDConnex at preboot	プリブートネットワーク認証（PBConnex）を有効にします。
☐ Enable will locally cache PBConnex autoboot key file for X day(s)	プリブートネットワーク認証でオートブートサービスを利用する場合、それに必要なオートブート用キーファイルはサーバー側で都度作成され、クライアントはネットワーク上でそれを使用することで自動ログインを可能としています。都度作成されるオートブート用キーファイルはクライアントには保存されません。 このオプションは、サーバー側の負荷を軽減する目的のために、クライアントにキーファイルをキャッシュさせ、都度、キーファイルを作成しないようにします。キャッシュさせる日数を設定します。
☐ Use Static IP Configuration from Client at preboot	プリブートネットワーク認証で固定 IP を利用できるようにします。 プリブートネットワーク認証で使用する IP アドレスの設定は、Windows の IP アドレス設定を参照します。Windows の IP アドレス設定が DHCP クライアントの場合、プリブートネットワーク認証をおこなうブートログオンプログラムは DHCP クライアントとして動作します。 このオプションを有効にすると、Windows の設定が DHCP ではなく固定 IP を使用している場合、Windows で設定されている固定 IP アドレスをプリブートネットワーク認証で使用する IP アドレスに設定します。
MagicEndpoint Enterprise	
☐ MagicEndpoint can assist/strengthen authentication	MagicEndpoint を SecueDoc と連携し使用する場合、チェックを入れます。
IdP Lis	MagicEndpoint Identity Provider を使用する場合、URL（ホスト名:ポート番号）を入力します。
MagicEndpoint credential Key is synchronized with SES and SES can share it to user's other devices （MagicEndpoint 認証情報キーは SES にバックアップされず、他のデバイスと共有できません。） MagicEndpoint credential Key will not be backed up to SES and cannot be shared to other devices （MagicEndpoint 認証情報キーは SES と同期され、SES はそれをユーザーの他のデバイスと共有できます。） Users will be prompted to perform FaceID-based authentication （ユーザーは、FaceID ベースの認証を実行するように求められます。）	

設　定	説　明
Silently perform FaceID authnetication for MagicEndpoint Clients whenever possible （可能な限り、MagicEndpoint クライアントの FaceID 認証を実行します。） Users will be authentically logged in to MagicEndpoint using SecueDoc Credentials （SecureDoc 認証情報と同期されている場合でも、ユーザーは常に MagicEndpoint へのログインを求められます。） Users will always be prompted to log in to MagicEndpoint,even where sysnc'ed with SD Credentials （デフォルト設定） （ユーザーは SecueDoc 認証情報を使用して MagicEndpoint に認証的にログインします。 Do not show notification when logging in to a website/services （ウェブサイト/サービスにログインするときに通知を表示しません。） Show notification when logging into a website/services （ウェブサイト/サービスにログインするときに通知を表示します。）	
☐ Validate IdP certificate	IdP 証明書を検証します。
☐ Verify host name in certificate	証明書のホスト名を確認します。
Automatically log out MagicEndpoint key after N minutes (Note: 0 ,means never) N 分後に MagicEndpoint キーを自動的にログアウトします。 注　0 はログアウトしないことを意味します。	

[BitLocker Management]

BitLocker 管理に必要な設定項目です。

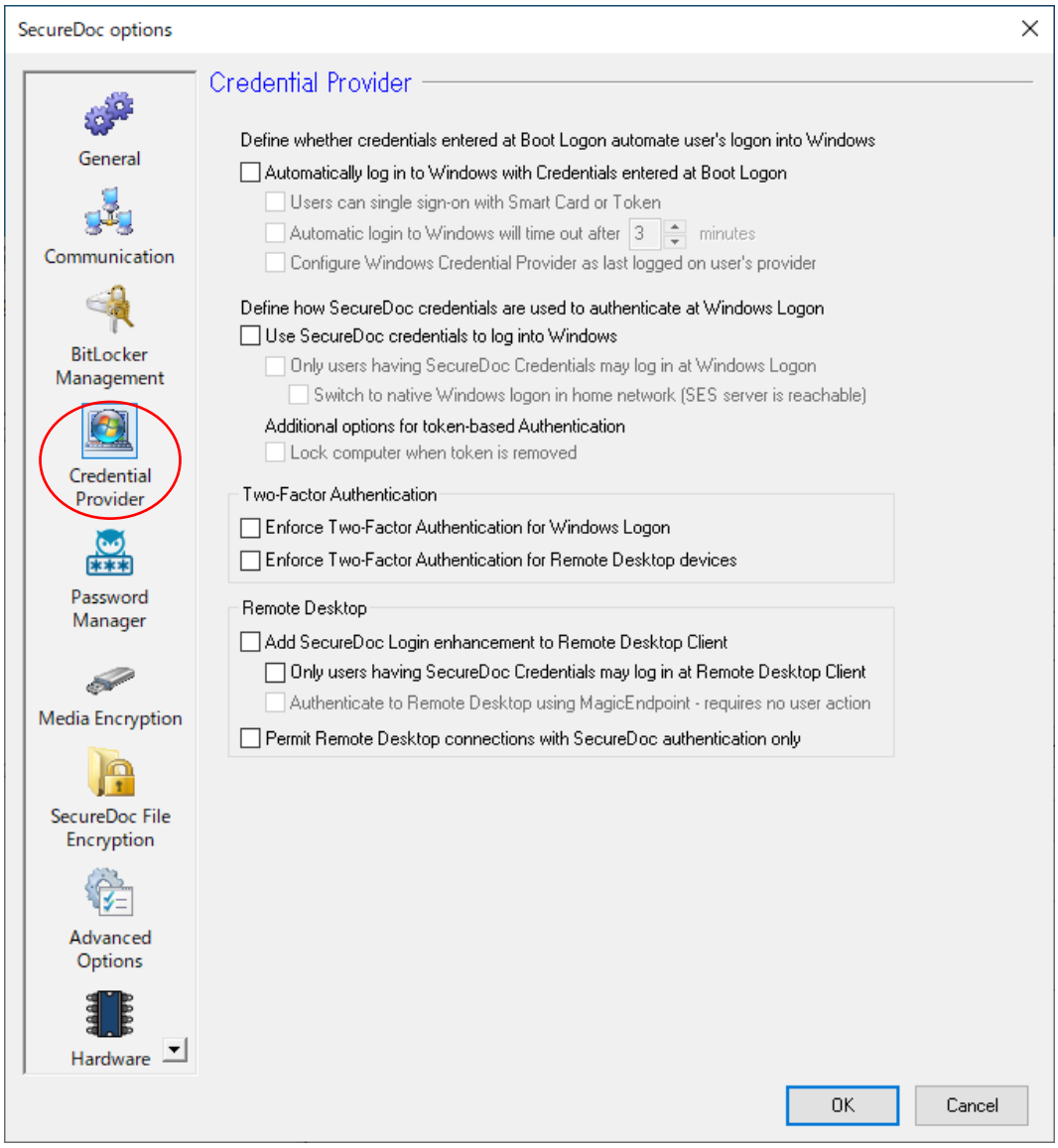


項　目	説　明
BitLocker Encryption	・Do not use BitLocker encryption BitLocker を使用しません。 ・Enable Microsoft BitLocker Pre-boot BitLocker 標準のプリブート認証を使用します。 [Authentication method] のプルダウンメニューで、BitLocker の認証方法を選択します。 ・Enable SecureDoc Pre-boot for BitLocker (推奨) SecureDoc のプリブート認証プログラムを使用します。 SecureDoc プリブート認証によって、細かいパスワードルールでの運用やシングルサインオン（SSO）、ユーザーロック機能、チャレンジ&レスポンス等の機能を使用できます。 また、プリブートネットワーク認証も利用可能です。
BitLocker Authentication and Access Monitoring	
☐ Synchronize BitLocker PIN/Password with SecureDoc device owner user’s password	BitLocker PIN/パスワードを SecureDoc デバイス所有者ユーザーのパスワードと同期します。
Authentication method	BitLocker 標準のプリブート認証を選択した場合、認証方法を選択します。

項　目	説　明
	・TPM only (auto-boot) ・TPM+PIN ・TPM+USB Startup Key ・TPM+PIN+USB Startup Key (incompatible with BitLocker password sync) BitLocker パスワード同期と互換性がありません。 ・USB Startup Key only ・Password (no TPM)
☐ additionally, allow independent USB Startup Key	さらに、独立した USB スタートアップ キーを許可します。
☐ Allow Password as a failback if no compatible TPM available	互換性のある TPM がない場合、パスワードを許可します。
BitLocker Conversion Options	
BitLocker Cipher Type:	暗号化アルゴリズムを選択します。 ・AES-CBC 128-bit ・AES-CBC 256-bit ・XTS-AES 128-bit ・XTS-AES 256-bit
☐ Enable cipher configured in profile during installation if BitLocker already active	既に BitLocker が有効に設定されている場合、インストール中にプロファイルで構成された暗号化アルゴリズムを有効にします。
Enforce Drive Encryption Type:	全セクターを暗号化するか、使用領域のみ暗号化するか選択します。 既にディスク上に重要なデータがある場合は、[Full Encryption]を選択します。
Drives To Encrypt:	OS のインストールされたドライブのみ、あるいはそれ以外のドライブも暗号化するのかを選択します。
Drives To Be Excluded:	暗号化を除外したいドライブ名を入力します。
Advanced Options	
☐ Install SecureDoc encryption on devices that do not support BitLocker	BitLocker をサポートしないデバイスの場合、SecureDoc によるソフトウェア暗号化をおこないます。
☐ Use hardware encryption if available.	ハードウェアレベルの暗号化ドライブ（TCG Opal など）を検知した場合、BitLocker の暗号化アルゴリズムによるソフトウェアでの暗号化はおこなわず、ハードウェアレベルの暗号化機能を利用します。
BitLocker Tamper Protection	
☐ Prevent unmanaged decryption	ユーザーによる BitLocker の削除を禁止します。
☐ Prevent volume protection suspension	デバイスのボリュームレベルで BitLocker をサスペンドさせません。
☐ Disable BitLocker management application (manage-bde.exe)	ユーザーは、manage-bde.exe 実行可能プログラム（BitLocker を無効にしたり変更したりできる Microsoft ツール）を使用できなくなります。

[Credential Provider]

Windows サインインに関する設定で、Windows 標準の Credential Provider（クレデンシャルプロバイダー）から SecureDoc Credential Provider に変更します。シングルサインオン(SSO)に設定変更するには SecureDoc Credential Provider が必要です。

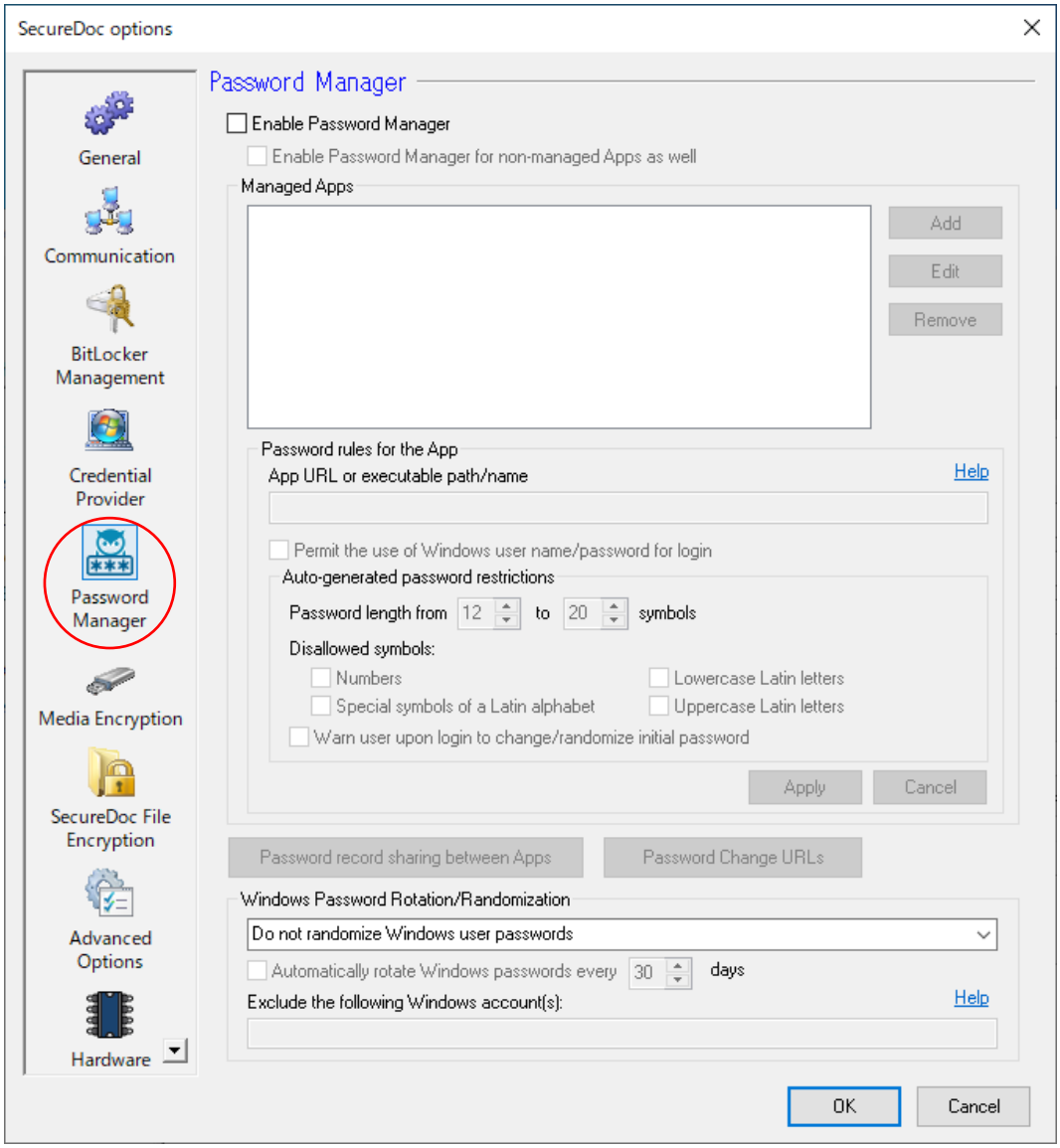


項　目	説　明
Define whether credentials entered at Boot Logon automate user’s logon into Windows	
☐ Automatically log in to Windows with Credentials entered at Boot Logon	プリブート認証での資格情報を使用して Windows に自動的にサインインします。
☐ Users can single sign-on Smart Card or Token	スマートカードまたはトークンを使用することで、シングルサインオンを利用できます。
☐ Automatic login to Windows will time out after X minutes	Windows への自動サインインは X 分後にタイムアウトします。
☐ Configure Windows Credential Provider as last logged on user’s provider	最後にサインインしたユーザーをクレデンシャルプロバイダーの構成に使用します。

項　目	説　明
Define how SecureDoc credentials are used to authenticate ad Windows Logon	
☐ Use SecureDoc Credentials to log into Windows	SecureDoc Credential Provider を使用して Windows にサインインします。Windows サインインへのセキュリティを強化します。
☐ Only uses having SecureDoc Credentials may log in Windows Logon	SecureDoc Credential Provider でのみ、Windows にサインインできます。
☐ Switch to native Windows logon in home network (SES Server is reachalble)	SDConnex と通信可能なネットワーク環境では、Windows 標準のクレデンシャルプロバイダーに切り替えます。
Additional options for token-based Authentication	
☐ Lock computer when token is removed	USB トークンを抜くと、Windows をロックします。
Two-factor authentication	
☐ Enforce Two-factor Authentication for Windows logon	Windows サインインに二要素認証を適用します。 (SecureDoc Credential provider)
☐ Enforce Two-factor Authentication for Remote Desktop devices	リモートデスクトップデバイスに 2 要素認証を適用します。
Remote Desktop	
☐ Add SecureDoc Login emhancement Remote Desktop Client	リモート デスクトップクライアントに SecureDoc ログインの拡張機能を追加します。
☐ Only users having SecureDoc Credental may log in at Remote Desktop Client	SecureDoc 資格情報を持つユーザーのみがリモート デスクトップクライアントにログインできます。
☐ Authenticate to Remote Desktop using MagicEndpoint-requires no user action	MagicEndpoint を使用したリモート デスクトップへの認証。 ユーザーの操作は不要です。
☐ Permit Remote Desktop connections with SecureDoc authentication only	SecureDoc 認証のみでリモートデスクトップ接続を許可します。

[Password Manager]

従来のユーザー名とパスワードを使ったレガシーアプリケーションへの認証をサポートします。

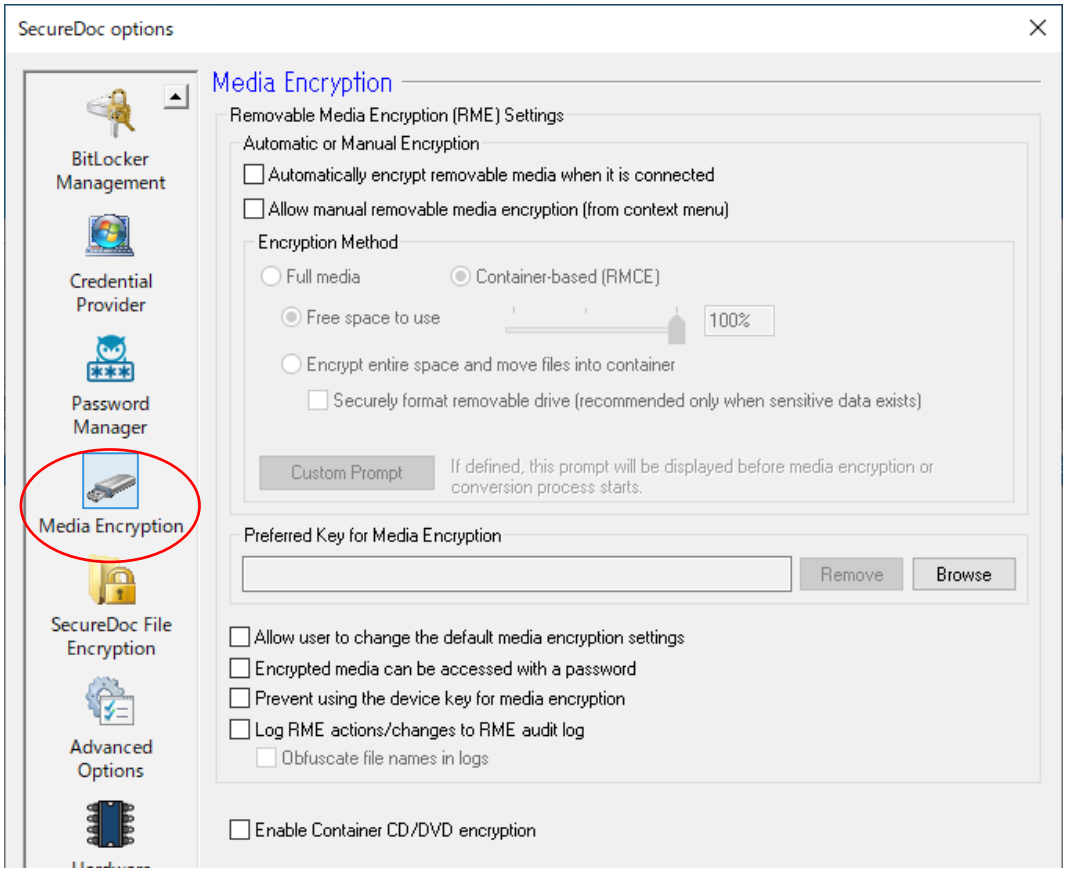


項　目	説　明
☐ Enable Password Manager	パスワードマネージャーを有効にします。
☐ Enable Password Manager for non-managed Apps as well	管理対象外アプリでもパスワードマネージャーを有効にします。
Password rules for the App App URL or executable path/name	<Add>ボタンをクリックして、アプリの URL または実行ファイルのパス/名前を入力します。
☐ Permit the use of Windows user name/password for login	ログインに Windows ユーザー名/パスワードの使用を許可します。
Auto-generated password restrictions Password length from XX to YY symbols	自動生成パスワードの規制 パスワードの長さは XX から YY 文字にします。
Disallowed symbols: ☐ Numbers ☐ Lowercase Latin letters	使用できない記号： 数字 小文字のラテン文字

項　目	説　明
☐ Special symbols of a Latin alphabet ☐ Uppercase Latin letters ☐ Warm user upon login to change/randomize initial password	ラテンアルファベットの特殊記号 大文字のラテン文字 ログイン時に初期パスワードを変更/ランダム化するようユーザーに促します。
Password record sharing between Apps	アプリ間でのパスワード記録を共有します。
Password Change URLs	パスワード変更 URL を追加します。
Windows Password Rotation/Randomization	
Do not randomize Windows user passwords Enable password randomization for users protected by Phone[Bluetooth and Network] Enable password randomization for all users protected by SecureDoc	Windows ユーザーのパスワードをランダム化しません。 スマートフォン[Bluetooth とネットワーク]で保護されているユーザーのパスワードをランダム化します。 SecureDoc で保護されているすべてのユーザーのパスワードをランダム化します。
☐ Automatically rotate Windows password every XX days	Windows パスワードを XX 日ごとに自動的に変更します。
Exclude the following Windows account(s):	除外するアカウントを設定します。

[Media Encryption]

リムーバブルメディアを暗号化する設定

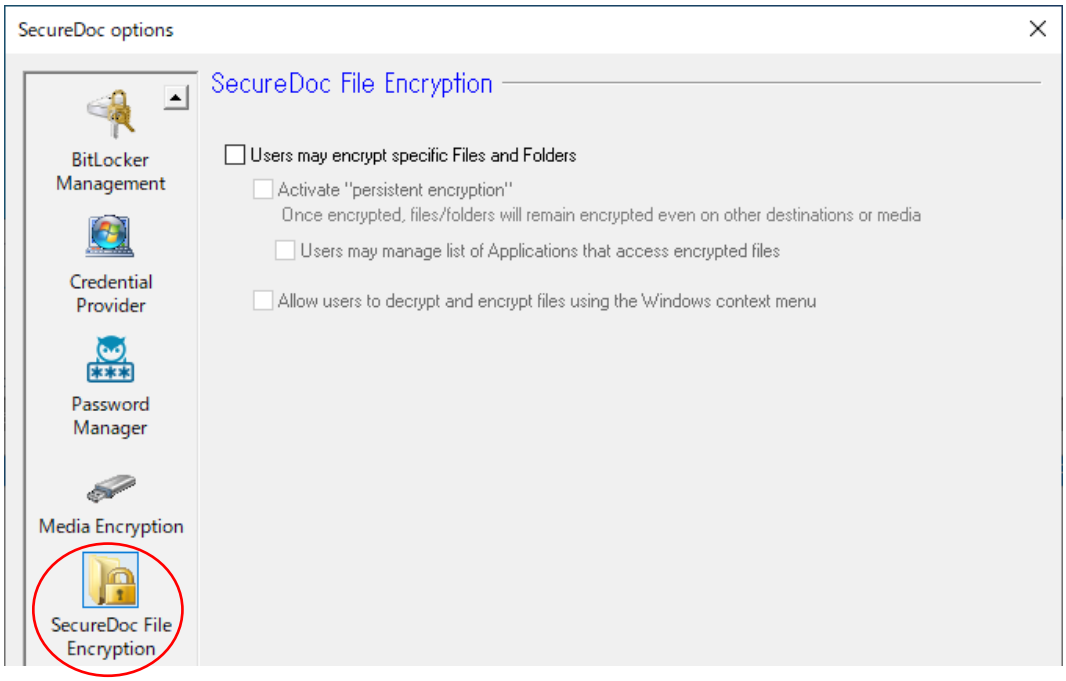


項　目	説　明
Automatic od Manual Encryption	
☐ Automatically removable media when it is connected	リムーバブルメディアが接続されると自動的に暗号化を開始します。
☐ Allow manual removable media encryption (from context menu)	コンテキストメニューを使用してメディアを暗号化します。
Encryption Method	
○ Full media	セクタレベルでメディアを暗号化します。 注 ユーザー間でメディアを共有する場合、次の条件があります。 ・ メディアは共有鍵で暗号化されている、あるいはパスワードで保護されていること。 ・ デバイスには SecureDoc がインストールされていること
○ Container-based (RMCE)	コンテナベースの暗号化をおこないます。 注 ユーザー間でメディアを共有する場合、次の条件があります。 ・ メディアは共有鍵で暗号化されている、あるいはパスワードで保護されていること。

項　目	説　明
○ Free space to use	コンテナ暗号化の領域を指定します。
○ Encrypt entire space and move files into container	全体をコンテナの領域として暗号化します。 暗号化前にデータを退避し、暗号化後、データを暗号化されたメディアに戻します。
☐ Securely format removable drive	コンテナ暗号化を開始する前にメディアを初期化します。
Custom Prompt	暗号化を開始する前に、メッセージを表示できます。
Preferred Key for Media Encryption	メディア暗号に使用する鍵を指定します。
☐ Allow use to change the default media encryption settings	メディア暗号の設定内容の変更を許可します。
☐ Encrypted media can be accessed with a password	暗号化メディアにパスワードでアクセスできるようにします。 注 Full media で暗号化したメディアにアクセスできる条件として、SecureDoc がインストールされている必要があります。
☐ Prevent using the device key for media encryption	ユーザーがメディア暗号に使用する鍵を、ディスクの暗号化に使用した鍵以外にさせます。
☐ Log RME actions/change to RME auditlog	メディアのログを残します。
☐ Obfuscate file names in logs	ログ内のファイル名を難読化します。
☐ Enable Container CD/DVD encryption	コンテナ暗号で、CD/DVD を暗号化できるようにします。

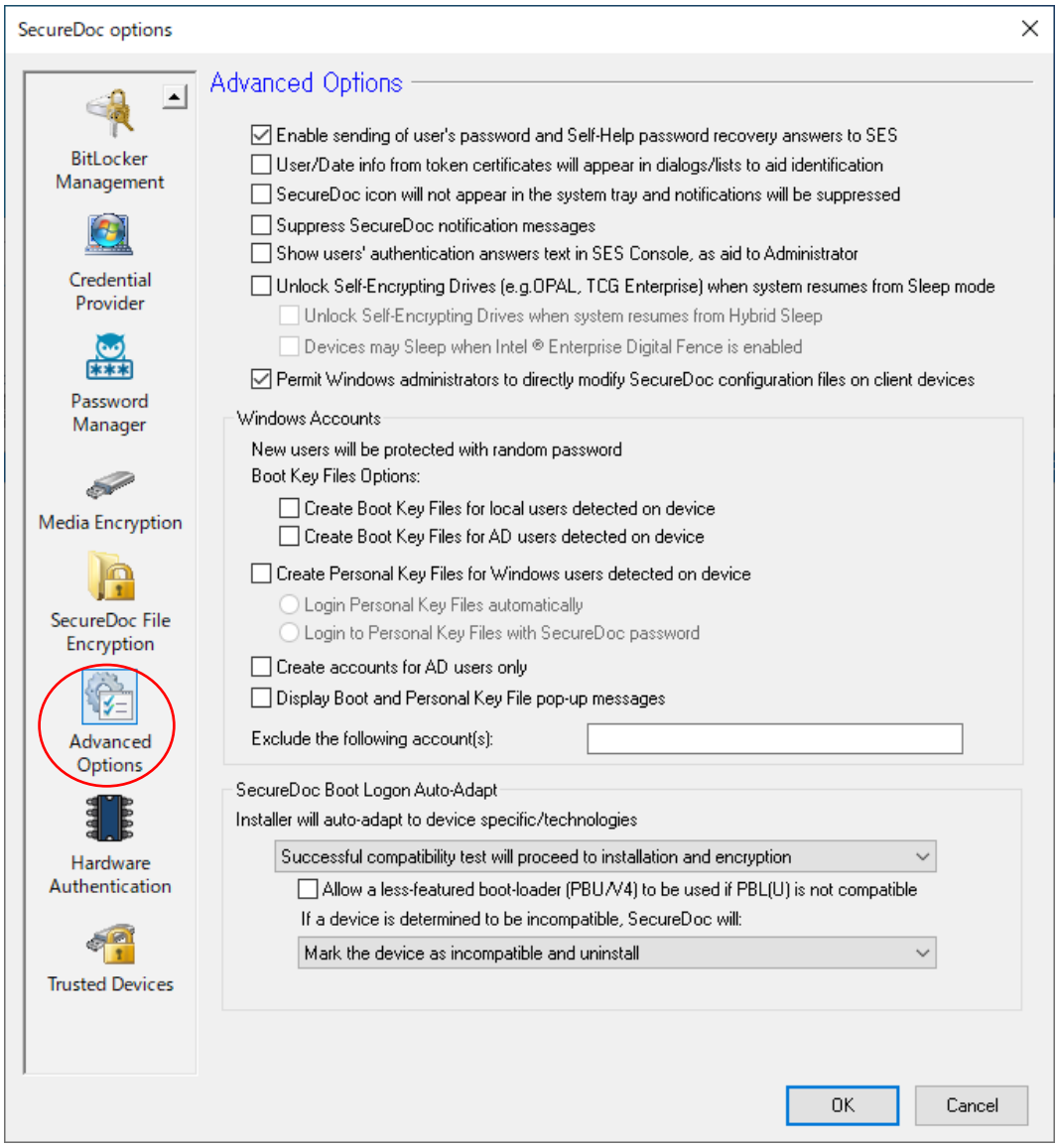
[SecureDoc File Encryption]

フィル・フォルダを暗号化する場合の設定



項　目	説　明
☐ Users may encrypt specific Files and Folders	特定のファイルとフォルダを暗号化できます
☐ Active “persistent encryption”	Persistent encryption（永続的な暗号化）を有効にします。
☐ Uses may manage list of Applications that at access encrypted files	Persistent encryption で保護された暗号化ファイルに、ユーザーは、シームレスに復号化可能なアプリケーションのリストを管理できます。
☐ Allow users to decrypt and encrypt files using Windows contest menu	Windows コンテスト メニューを使用してファイルを復号化および暗号化できるようにします。

[Advanced Options]



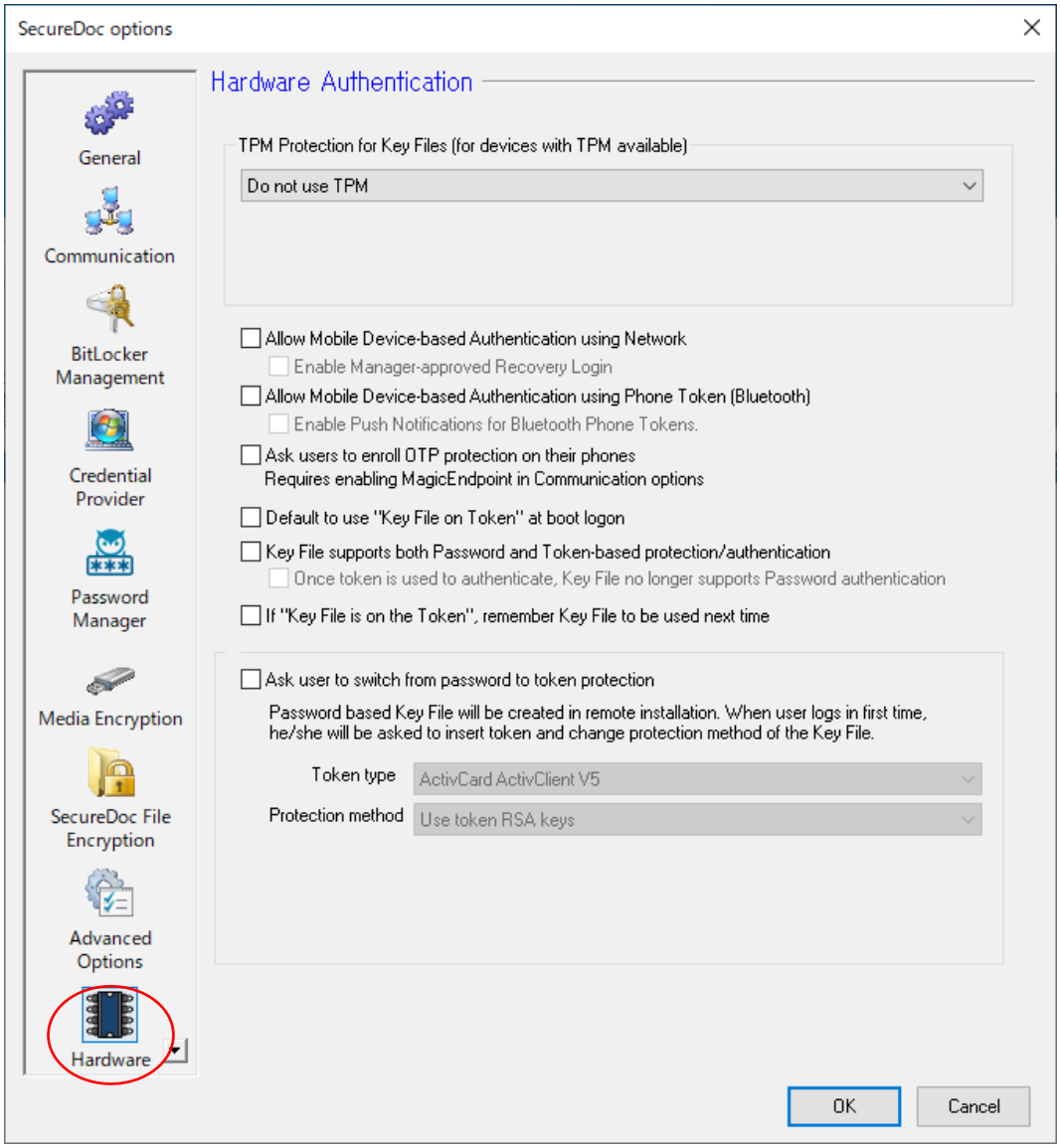
項　目	説　明
☐ Enable sending of user’s password and Self-Help password recovery answers to SES	ユーザーのパスワードとセルフヘルプの回答を SDConnex を介して SES DB に送ります。 セルフヘルプリカバリーは日本語環境ではご利用いただけません。
☐ User/Date info from token certificates will appear in dialog/lists to aid identification	トークン証明書のユーザー/日付情報がダイアログ/リストに表示され、本人確認を容易にします。
☐ SecureDoc icon will not appear in the system tray and notifications will be suppressed	システムトレイに SecureDoc のアイコンを表示させません。 通知も抑止し表示させません。
☐ Suppress SecureDoc notification messages	通知メッセージを抑止し表示させません。
☐ Show user’s authentication answers text in SES Console, as aid to Administrator	管理者の補助として、SES コンソールにユーザーのセルフヘルプの回答を表示させます。 日本語環境ではご利用いただけません。

項　目	説　明
☐ Unlock Self-Encrypting Drives(e.g.OPAL, TCG Enterprise) when system resumes from Sleep mode	自己暗号化ドライブ（TCG Opal）で、スリープモードを利用できるようにします。 注　スリープモードの使用は推奨されません。
☐ Unlock Self-Encrypting Drives when system resumes from Hybrid Sleep	自己暗号化ドライブ（TCG Opal）で、ハイブリッドスリープモードを利用できるようにします。
☐ Devices may Sleep when Intel Enterprise Digital Fence is enabled	Intel Enterprise Digital Fence をサポートします。 Intel Enterprise Digital Fence では、デバイスが信頼できる LAN でウェイクアップすると、スリープが再開されます。しかし、帰宅途中の車内など信頼できる LAN がない場合、休止状態が強制されます。
☐ Permit Windows administrators to directly modify SecureDoc configuration files on client devices	Windows 管理者がクライアントデバイス上の SecureDoc 設定ファイルを直接変更することを許可します。
Windows Accounts	
Boot Key Files Options	
☐ Create Boot Key Files for local users detected on device	デバイス上で検出されたローカルユーザー向けに、ブートキーファイルを作成します。
☐ Create Boot Key Files for AD users detected on device	デバイス上で検出された AD ユーザー向けに、ブートキーファイルを作成します。
☐ Create Personal Key Files for Windows users detected on device	デバイス上で検出された Windows ユーザー向けに、パーソナルキーファイルを作成します。 注　プリブート認証を利用するユーザーでは使用しません。 主に「Only encrypt Removable Media (RME)」向けです。
○ Login Personal Key Files automatically	個人キーファイルに自動でログインします。 注　プリブート認証を利用するユーザーでは使用しません。 主に「Only encrypt Removable Media（RME)」向けです。
○ Login to Personal Key Files with SecureDoc password	SecureDoc のパスワードで個人用キーファイルにログインします。 注　プリブート認証を利用するユーザーでは使用しません。 主に「Only encrypt Removable Media（RME)」向けです。
☐ Create accounts for AD users only	SecueDoc のアカウント作成を AD ユーザーに限定します。
☐ Display Boot and Personal Key File pop-up messages	起動およびパーソナルキーファイルのポップアップメッセージを表示させます。 注　プリブート認証を利用するユーザーでは使用しません。 主に「Only encrypt Removable Media（RME)」向けです。
Excludes the following account(s):	ここで指定したアカウントは作成しません、
SecueDoc Boot Logon Auto-Adapt	
☐ Install will auto-adapt to device specific/technologies ・ Successful compatibility test will proceed to installation and encryption	デバイスに固有の設定が必要な場合、自動でそれを適応してインストールします。 ・　互換性テストに成功すると、インストールと暗号化に進みます。

項　目	説　明
・ Stop after Pre-Boot compatibility test and report results only	・ プリブート互換性テスト後にインストールを停止し、結果のみをレポートします。
☐ Allow a less-featured boot-loader(PBU/V4) to be used if PBL(U) is not compatible	UEFI デバイス向けのブートログオンプログラムの PBL(U)と互換がない場合、旧ブートログオンプログラム PBU V4 を使用できるようにします。
If a device is determined to in compatible, SecureDoc will:	
・ Switch to SecuerDoc BitLocler Management　(SDBM)	・ ブートログオンプログラムの PBL(U)と互換がない場合、BitLocker Management に切り替えます。 事前に、BitLocker Management の設定が必要です。
・ Mark the device as incompatible and uninstall	・ 互換性の無いデバイスとして記録し、アンインストールします。

[Hardware Authentication]

パスワード以外の方法で、キーファイルを保護する設定です。

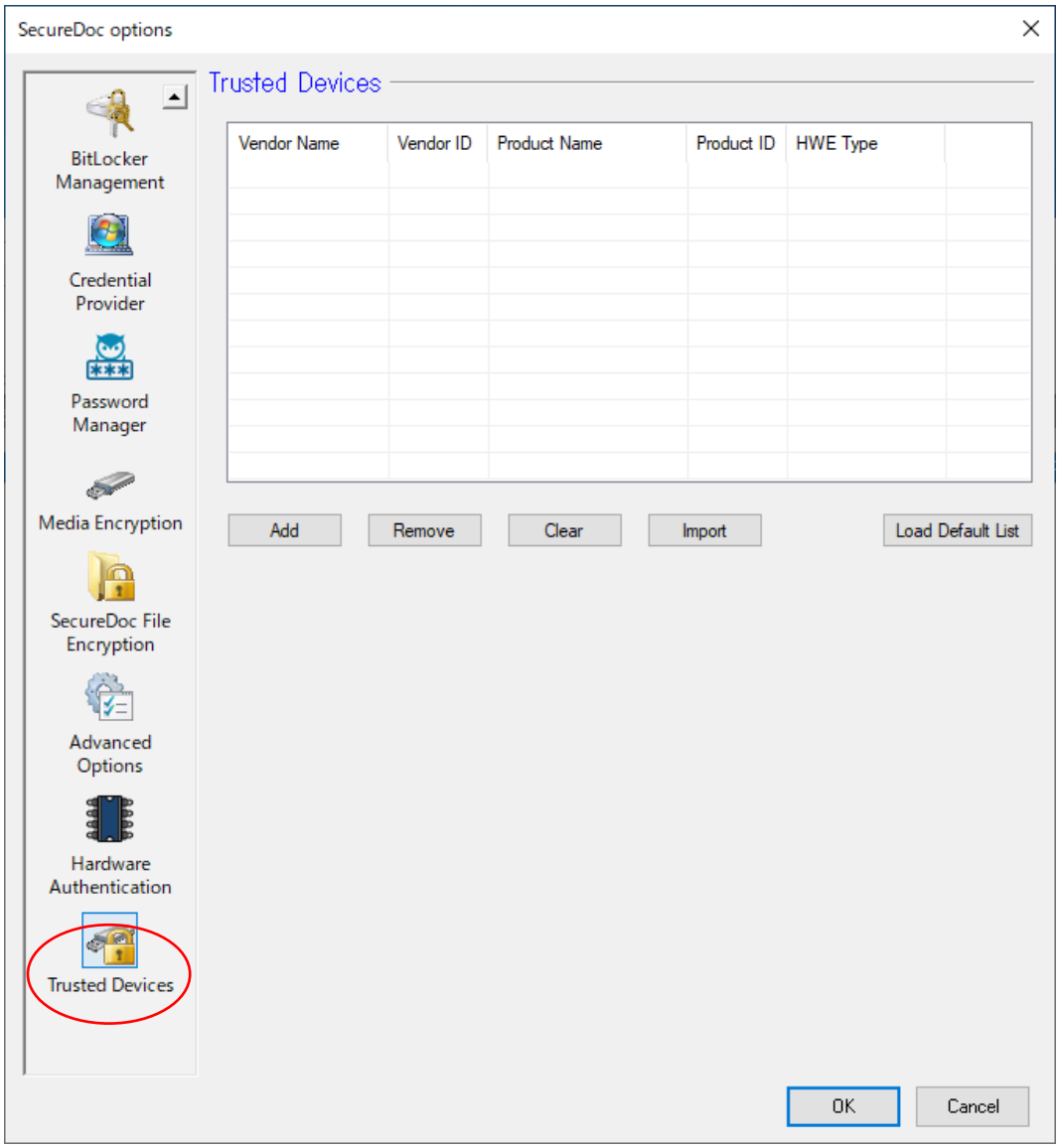


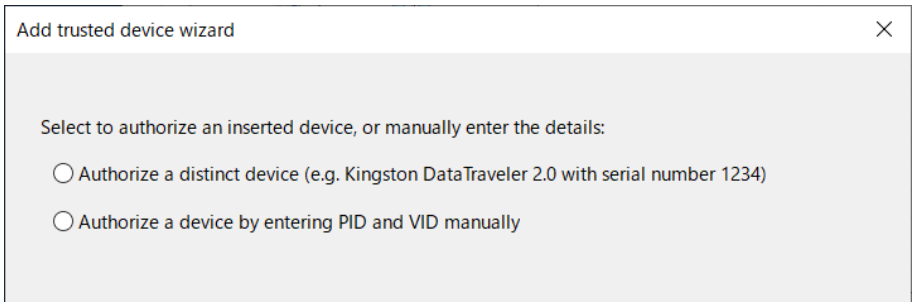
項　目	説　明
TPM Protection for Key Files (for devices with TPM available)	
・ Do not use TPM ・ Automatically TPM-protect Password-protected Key Files ・ Create Key files protected by TPM and PIN instead of a password	・ TPM を使用しません。 ・ パスワードで保護されたキーファイルを自動で TPM 保護に切り替えます。 ・ パスワードの代わりに TPM と PIN で保護されたキー ファイルを作成します。
PIN complexity rules: ☐ Allow alpha characters in PIN Minimum PIN length: X	 PIN に英字を許可します。 PIN の長さ（最小）
☐ Allow Mobile Devices-based Authentication using Network	ネットワークを使用したモバイルデバイスベースの認証を許可します。

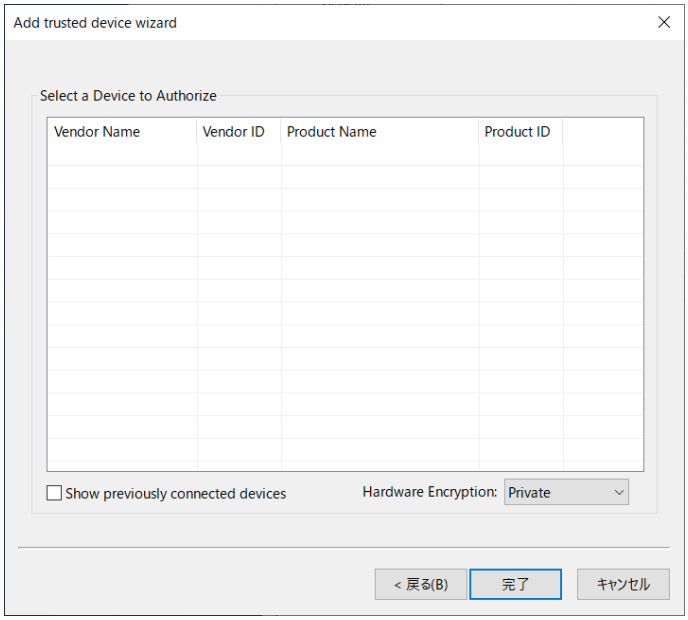
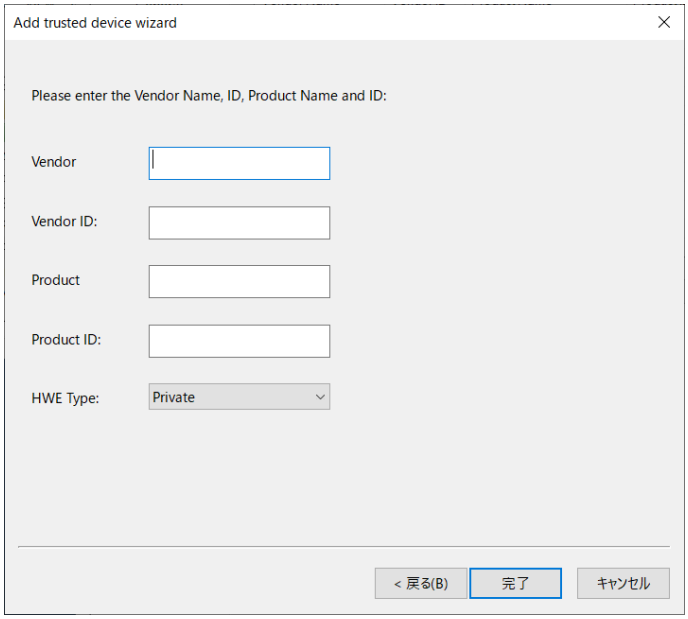
項　目	説　明
☐ Allow Mobile Device-based Authentication using Phone Token (Bluetooth)	スマートフォンによるトークン (Bluetooth) を使用したモバイルデバイスベースの認証を許可する
☐ Ask users to enroll OTP protection on their phone Requires enabling ….	ユーザーに携帯電話の OTP 保護を登録するよう依頼する 通信オプションで MagicEndpoint を有効にする必要があります。
☐ Default to use “Key File on Token-based protect/authentication	デフォルトでは、トークンベースの保護/認証で「キー ファイル」を使用します。
☐ Key File supports both Password and token-based protection/authentication	キーファイルは、パスワードとトークン ベースの保護/認証の両方をサポートします。
☐ Once token is used to authenticate, Key File no longer supports Password	キーファイルの認証にトークンを使用することとし、パスワードによる認証を無効にします。チェックを入れると、プリブート認証時にディスクではなく、トークンを検索します。
☐ If “Key file is on the Token”, remember key file to be used next time	プリブート認証でユーザーが認証情報を入力すると、プリブート認証プログラムはキーファイルをサーチします。キーファイルがディスク内ではなくトークンにある場合、それを記憶させます。
☐ Ask user to switch from password to token protection Token type Protection method	パスワードで保護されたキーファイルをトークンで保護するキーファイルに変換することができます。 このオプションを使用する場合は、適切なトークンタイプを選択しておく必要があります。 [Token type] では、プルダウンメニューから使用するトークンを選択します。 [Protection method] はトークン側の設定にあわせます。 ・Use token RSA Keys ・Token contains PIN ・Use Certificate on token - トークン証明書 ・Use Certificate from windows store - Windows ストアからの証明書

[Trusted Device]

IHV 製・暗号化機能付 USB メモリなどを、SecureDoc の「Media Encryption」で暗号化されたデバイスと同様に、信頼されたデバイスとして扱うように設定します。

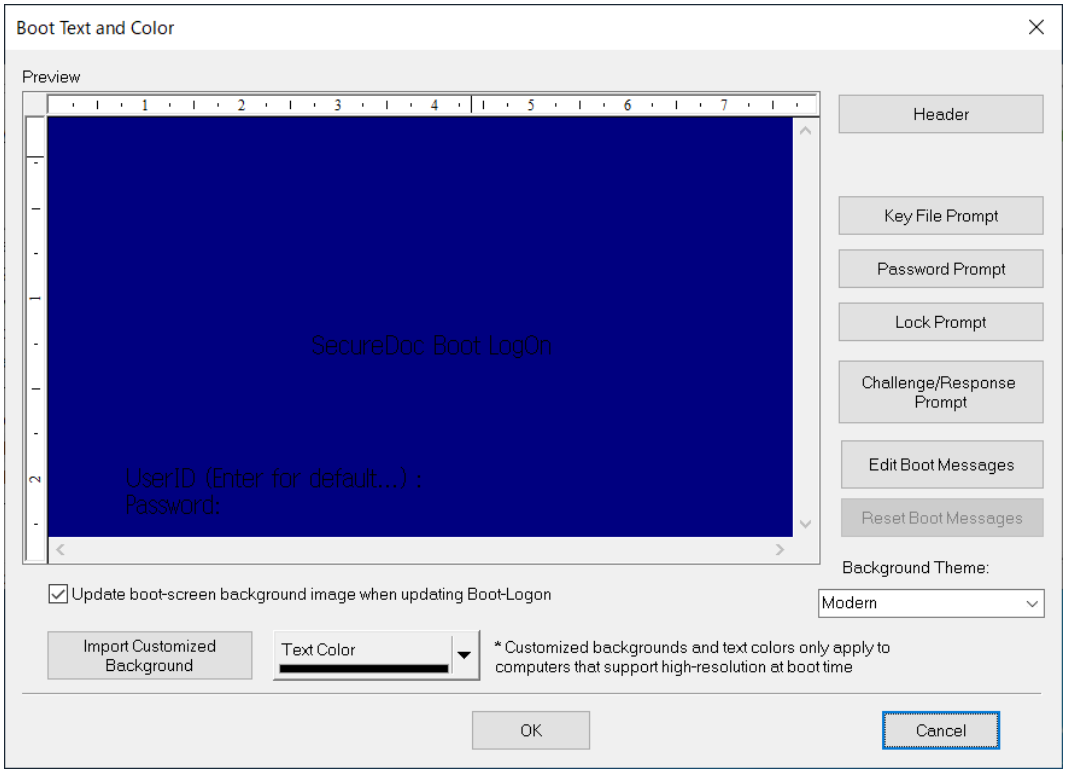


項　目	説　明
<Add> ボタン	<Add> をクリックすると、登録方法を選択できます。 

項　目	説　明
○ Authorize a distinct device (e.g.Kingston Data Traveler 2.0 with serial number 1234)	デバイスを SES コンソールに接続し、表示されたデバイスから目的のデバイスを登録します。 
○ Authorize a device by entering PID and VID manually	手動入力で、デバイスを登録します。 
<Load Default List>	一般的に信頼できる SED のリストを利用するには、<Load Default List> をクリックします。

2.2. Boot Test and Color

プリブート認証画面で表示する項目をカスタマイズできます。



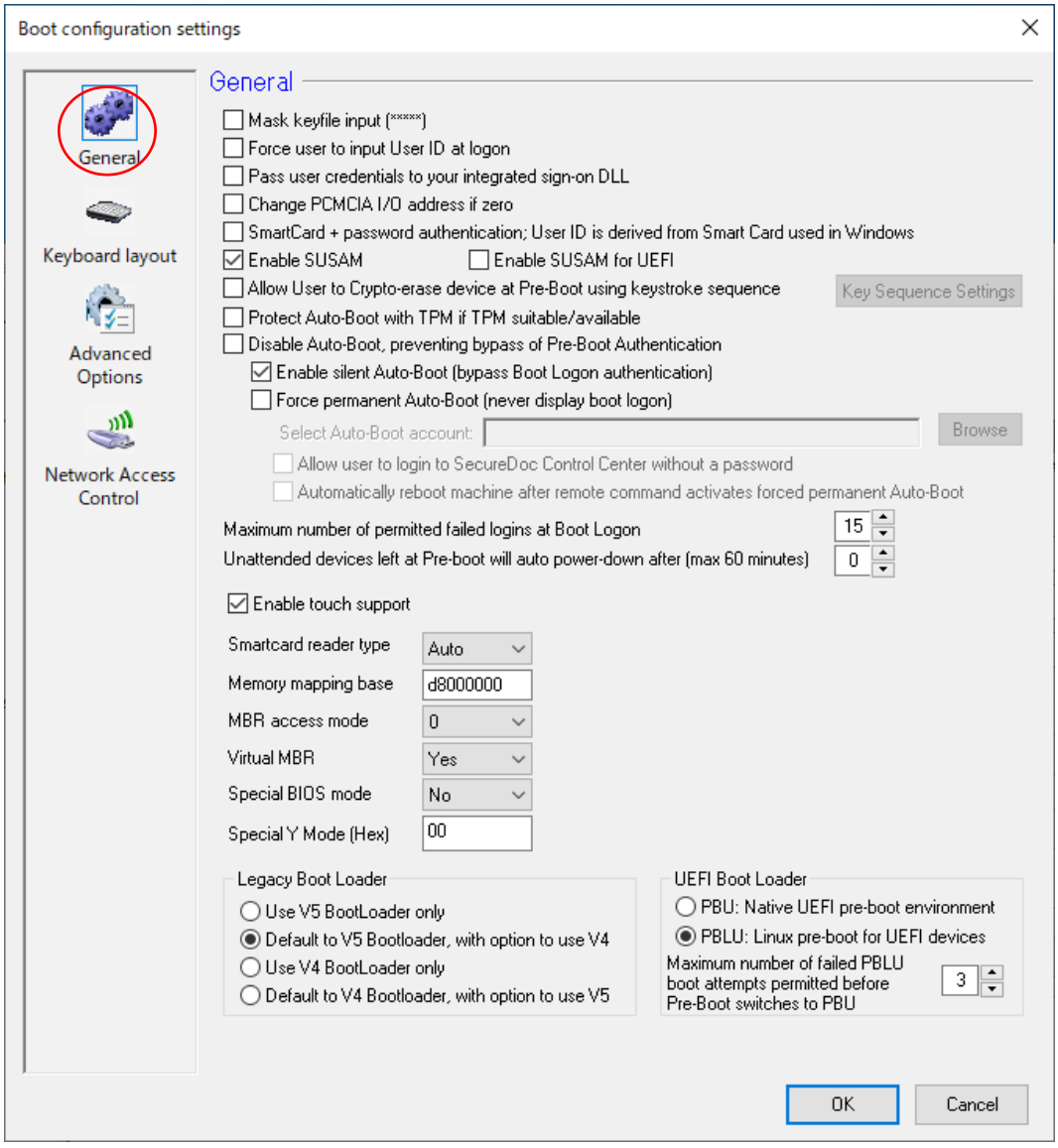
項　目	説　明
Header	初期設定　SecureDoc Boot LogOn
Key File Prompt	ユーザーID を入力する項目に表示する文字を設定します。 初期設定　User ID (Enter for default…) : 設定例　　ユーザーID　:
Password Prompt	パスワードを入力する項目に表示する文字を設定します 初期設値　Password : 設定例　　パスワード :
Lock Prompt	続けて ID またはパスワードの誤入力があった場合に表示する文字を設定します。 初期設定 You have incorrectly logged into the computer. If you know your User ID and password, please press Ctrl+Alt+Del and try again. If you don't know your User ID or Password, please contact your Help Desk for assistance. 設定例 間違った ID もしくはパスワードが入力されました。 Ctrl + Alt + Del を押して、再起動し、入力し直してください。 もし、パスワードを忘れてしまった場合、社内のヘルプデスクに連絡しください。 紛失時、取得者に持ち主を特定されるような情報の記載は推奨しません。会社名等
Challenge/Response Prompt	チャレンジレスポンス時に表示させる文字を設定できます。

項　目	説　明
Edit Boot Message	ブートメッセージを編集できます。 特別な理由が無い限り、通常は使用しません。
☐ Update boor-screen background image when updating Boot-Logon	ブートログオンの更新時に、背景画像を更新します。
Background Theme:	Classic :旧タイプのプリブート認証画面 Modern： 高解像度に対応した新しいプリブート認証画面
Import Customized Background	背景の画像を変更できます。 ファイル形式は、24 ビットの bmp フォーマット
Text Color	文字色を変更できます。

2.3. Boot configuration

[General]

ブートログオンプログラムの設定など



項　目	説　明
☐ Mask keyfile input (******)	ユーザーの入力した文字がアスタリスクに置き換えられます。 （パスワードはデフォルトで常にこの方法で処理されます。）
☐ Force user to input UserID at login	ブートログオン時にユーザーID の入力が必ず必要とする。 選択していない場合、デフォルトのユーザーID は入力を必要としません。
☐ Pass use credential to your integrated sign-on DLL	統合サインオン DLL に使用クレデンシャルを渡します。 SecureDoc からのパラメーターを許容するように設定された DLL があり、その DLL を使用してブートログオンで入力されたユーザー名とパスワードを取得する場合に、このオプションにチェックを入れます。通常は使用しません。

項　目	説　明
☐ Change PCMCIA I/O address if zero	ブートログオンがノート PC の PCMCIA リーダーを検出できない場合、アドレス指定に問題がある可能性があります。また、場合によっては、SecureDoc でアドレスを正しく検出できるように、ノート PC の PCMCIA I/O アドレスをデフォルトアドレスの「D0000000」に変更する必要があります。
☐ SmartCard+psssword authentication; Use ID is derived from Smart Card used in Windows	SmartCard+pssword 認証の場合、ユーザーID は Windows で使用されている Smart Card から取得します。
☐ Enable SUSAM	ハードウェアがプリブート環境にサポートされているかどうか不明な場合にチェックを入れます。
☐ Enable SUSAM for UEFI	UEFI デバイスで、ハードウェアがプリブート環境にサポートされているかどうか不明な場合にチェックを入れます。
☐ Allow Use to Crypto-erase device at Pre-Boot using Keystroke sequence	プリブート認証画面で、Crypto-erase を実行できるようにします。Crypto-erase を実行すると、デバイスから暗号化キーが削除され、アクセス不能になります。
☐ Protect Auto-Boot with TPM if TPM suitable/available	TPM が適切に使用可能な場合、TPM でオートブートを保護します。
☐ Disable AutoBoot preventing bypass of Pre-Boot Authentication	オートブート機能を無効にして、プリブート認証のバイパスを防ぎます。
☐ Enable silent Auto-Boot (bypass BootLogon authentication)	オートブート機能を有効にします。 チェックを入れると、ユーザーがまだブートログオンを通して認証されていない場合でも、オートブートを実行できるようになります。
☐ Force permanent Auto-Boot (never display boot logon)	暗号化されたクライアントのユーザーに対してプリブート認証を表示させません。ユーザーは通常どおりの方法で Windows にサインインします。
Select Auto-Boot account	オートブートで使用するアカウントを指定します。
☐ Allow user to login SecureDoc Control Center without password	認証なしで Secure Doc コントロールセンターにログインできるようにします。常時オートブートが有効なデバイスに適用します。 オートブートの場合、ユーザーのキーファイルを使用せずに実行されるため、ユーザーは SecureDoc コントロールセンターにログインできなくなります。
☐ Automatically reboot machine after remote command activates forced permanent Auto-Boot	SES からリモートコマンドで永続的なオートブート機能を有効にした後、マシンを自動的に再起動します。
Maximum number of permitted logins at Boot Logon	プリブート認証で許可されるログイン失敗回数の最大値を設定できます。累計で設定された回数に達すると、キーファイルは自動的にロックされます。 初期値「15」 デバイスのロックを解除するには、管理者キーファイルまたはパスワードリカバリが必要です。別のキーファイルでログインが成功した場合でも、ロックされたキーファイルは解除されません。
Unatiended devices left at Pre-boot will auto power-down after (max60 minutes)	SecureDoc クライアントの電源をオンにしてから一定時間内にユーザー認証が行われなかった場合、デバイスをシャットダウンします。この機能を使用する場合、指定時間（分）を入力します。
☐ Enable touch support	プリブート認証で、オンスクリーンキーボードを有効にします。
Smart reader type	プリブート認証時、トークンを認識できない場合、ブートログオンプログラムがトークンリーダーを検索できないことが原因の１つとして

項　目	説　明
	考えられます。このような場合、リーダーのタイプ(USB、PCMIA、Serial)を指定することで問題を回避できる場合があります。 （デフォルトは Auto）
Memory mapping base	プリブート認証時、ブートログオンが PCMCIA リーダーを検出できない場合、デバイスのメモリマッピングに問題がある可能性があります。このような場合、デバイスに合わせてメモリマッピングのアドレスを変更します。 WinMagic テクニカルサポートに相談した上で利用してください。
MBR access mode	Master Boot Record へのアクセスに関する制御が可能です。 BIOS 向けの機能です。UEFI デバイス向けの機能ではありません。 [アクセスモード 0] 他のプログラムに MBR を変更させないように保護します。 [アクセスモード 1] MBR の変更を許可します。 [アクセスモード 2] MBR への変更操作をしようとしているプログラムを操作して、MBR が実際には変更されていないのに、変更されていると認識させます。(ほとんど使用されません) [アクセスモード 3] パーティションテーブルの変更を許可します。
Virtual MBR	拡張ブートレコードの設定で、常に初期設定値「Yes」のままにしておきます
Special BIOS mode	ハードウェアのコントローラーがデバイスの起動に影響を与えている場合に使用します。 WinMagic テクニカルサポートに相談した上で利用してください。
Special Y Mode (Hex)	MBR の優先順位を変更する必要がある場合に使用します。 WinMagic テクニカルサポートに相談した上で利用してください。
Legacy Boot Loader	BIOS デバイス向け　ブートログオンプログラムの選択
◎ Use V5 BootLoader only	V5 ブートログオンプログラムのみ設定します。
◎ Default to V5 Bootloader, with option to user V4	V5 ブートログオンプログラムを使用し、それがうまく動作できないときに旧 V4 ブートログオンプログラムをフォールバックとして使用するように設定します。（デフォルト設定）
◎ Use V4 BootLoader only	旧 V4 ブートログオンプログラムのみ設定します。
◎ Default to V4 Bootloader, with option to user V5	旧 V4 ブートログオンプログラムを使用し、それがうまく動作できないときに V5 ブートログオンプログラムをフォールバックとして使用するように設定します。
UEFI Boot Loader	UEFI デバイス向け　ブートログオンプログラムの選択
◎ PBU: Native UEFI pre-boot environment	ネイティブ・プリブートのブートログオンプログラム
◎ PBLU: Linux pre-boot for UEFI devices	Linux プリブートのブートログオンプログラム PBLU では。Linux ベースのサードパーティ製ライブラリやツールを使用する機能を備えており、スマートフォンのサポートに不可欠です。 注　スマートフォンを使用する場合、PBLU を選択してください。

項　目	説　明
Maximum number of failed PBLU boot attempts permitted before Pre-Boot switch to PBU	PBLU の設定で起動に失敗する場合、PBU へ自動的に切り替えることが可能です。PBU へ切り替える前の PBLU での試行回数を設定します。

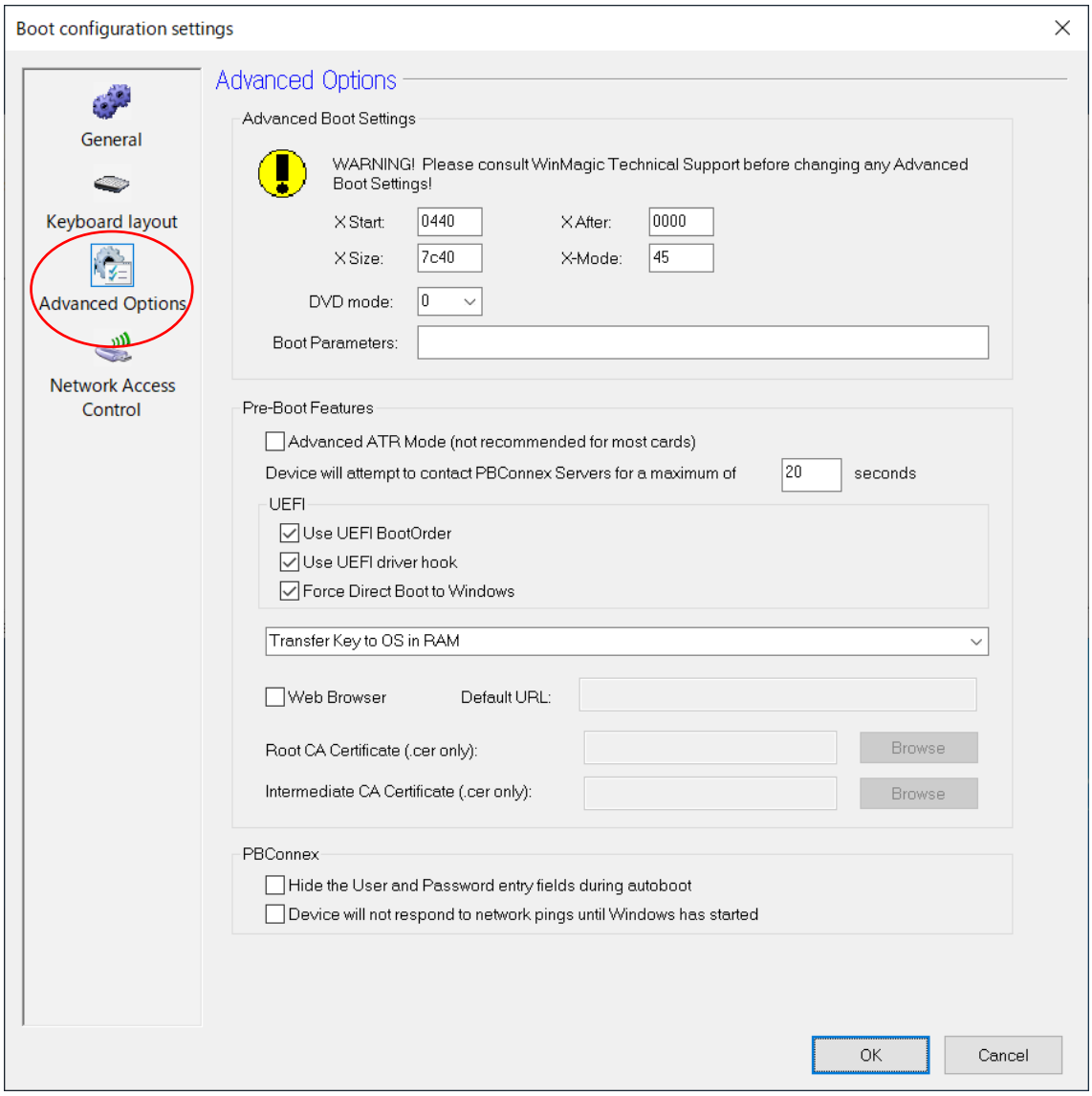
[Keyboard layout]

キーボードレイアウトに関する設定

項　目	説　明
Default Keyboard Layout:	プルダウンメニューより、デバイスに合わせた言語のキーボードレイアウトを選択します。 注　日本語キーボードでは、「Japanese」を選択してください。
☐ Automatically detect keyboard layout when installing Boot Logon	SecureDoc のインストール時に自動的にキーボードレイアウトを検出します。日本語キーボード、US キーボードなど、異なるキーボードレイアウトのデバイスが存在する場合に有効です。 正しいキーボードレイアウトを検出できない場合は、 [Default Keyboard Layout:] で、適切なキーボードレイアウトを選択してください。
☐ Support Foreign keyboards	English（United States）以外の外国語キーボードを使用する場合、チェックを入れます。
☐ Where an On-Screen Keyboard applies, it will begin minimized at Pre-Boot	オンスクリーンキーボードが適用される場合、プリブート認証画面で、最小化します。

[Advanced options]

通常、設定する必要はありません。設定変更する場合は、テクニカルサポートに相談した上でおこなってください。

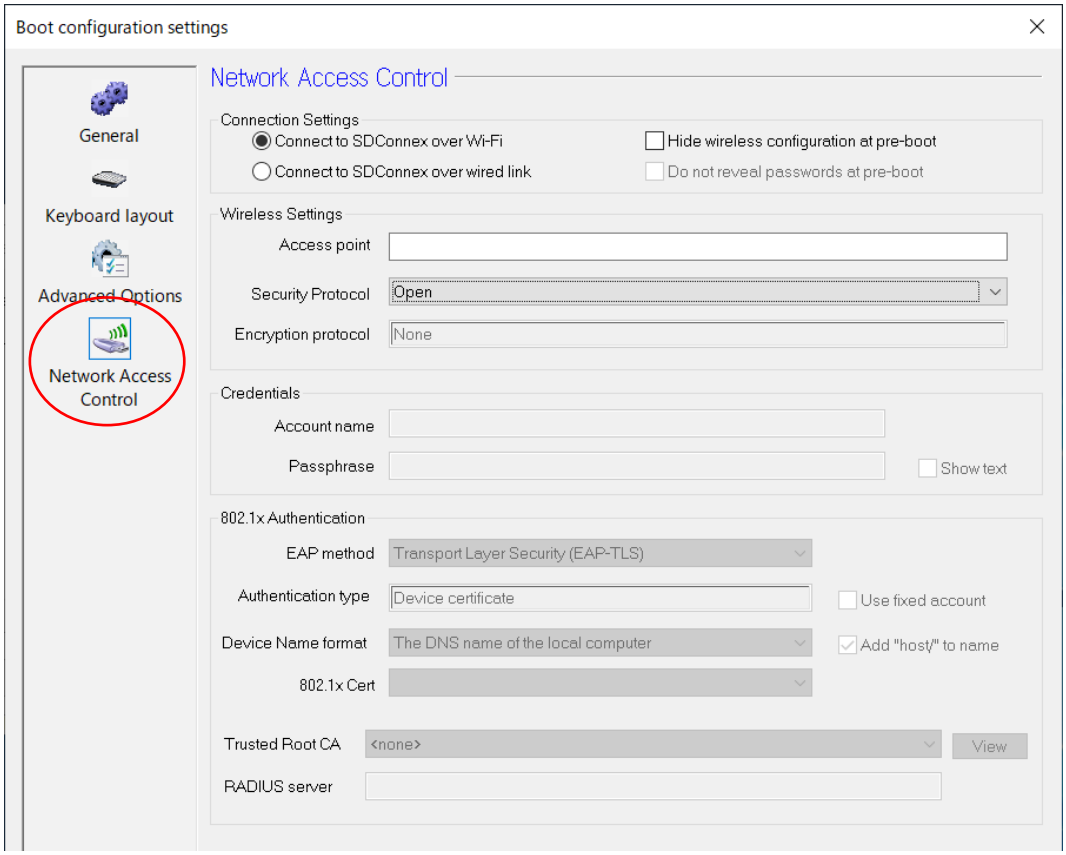


項　目	説　明
Advanced Boot Settings	
X Start:	デフォルト設定；040
X After:	デフォルト設定；0000
X Size:	デフォルト設定；7c40
X-Mode:	デフォルト設定；45
DVD mode:	0
Boot Parameters:	ブートログオンプログラム起動時に、ここで設定したパラメーターを実行します。
Pre-Boot Features	
☐ Advanced ATR Mode (not recommended for most cards)	スマートカードで、Advanced ATR (Answer-To-Reset) 属性を有効にする場合（ほとんどのカードには推奨されません）
Device will attempt to contact PBConnex Service for a maximum of X seconds	PBConnex サービスへの接続を試みる秒数を設定します。

項　目	説　明
UEFI	
☐ Use UEFI BootOrder	UEFI のブートオーダーを使用し、順番 1 から起動します。 1. SecueDoc Boot Logon 2. Windows Boot Loader
☐ Use UEFI Drover hook	UEFI のドライバーバインディングが実装されている UEFI デバイス向けの設定です。UEFI ドライバーバインディングは特別なプロトコルであり、ドライバーを起動および停止するための機能と、特定のドライバーが特定のコントローラーを管理できるかどうかを決定するための機能があります。
☐ Force Direct Boot to Windows	SED 搭載デバイスで、プリブート認証後に Windows を起動できない場合、Windows への強制ダイレクトブートを試みます。
Transfer Key to OS in RAM	デフォルト設定 プリブート認証で認証に成功した後、復号化に必要な鍵はメモリを使って転送し OS を起動します。 ブートオーダーが正しく動作するデバイスの場合、 「1. SecueDoc Boot Logon」で、 認証に成功すると、鍵はメモリ上にロードされ、 「2. Windows Boot Loader」を起動する前に、 鍵を使って暗号化されたディスクを復号化します。
Transfer Key to OS using Persistent Storage	上記の「2. Windows Boot Loader」を起動する際に、メモリ上にロードした鍵をクリアしてしまうデバイスの場合、OS 起動前に暗号化されたディスクを復号化できず、OS を起動することができません。 このような特別なケースでは、鍵の転送にディスクを使用します。 起動に成功すると、鍵は自動でディスクから削除されます。
☐ Web Browser	プリブート認証時、ブラウザを利用できるようにします。
Default URL:	デフォルトの URL を指定します。
Root CA Certificate (.cer only):	URL のアクセスに必要なルート CA 証明書を設定します。
Intermediate CA Certificate (.cer only):	URL のアクセスに必要な中間 CA 証明書を設定します。
PBConnex	
☐ Hide the User and Password entry fields during autoboot	プリブートネットワーク認証によるオートブートを利用するデバイスで、ユーザーが誤って ID とパスワードのフィールドに何らかの文字などを入力すると、オートブートとはなりません。 誤入力を防ぐために、ID とパスワードの入力箇所を非表示にすることができます。
☐ Device will not respond to network pings until Windows has started	Windows が起動するまで、デバイスは Ping に応答しないようにします。

[Network Access Control]

プリブートネットワーク認証を利用する場合のネットワーク設定箇所



項　目	説　明
Connection Settings	
○ Connect to SDConnex over Wi-Fi	ネットワーク認証に、Wi-Fi 接続を使用します。
☐ Hide wireless configuration at pre-boot	プリブート認証画面で、Wi-Fi 設定を表示しません。
○ Connect to SDConnex over wired link	ネットワーク認証に、有線接続を使用します。
☐ Do not reveal password at pre-boot	プリブート認証画面で、パスワードを表示しません。
Wireless Settings	
Access point	デフォルトのアクセスポイントを設定します。 ユーザーは、プリブート認証画面で、別のアクセスポイントをスキャンできます。
Security Protocol	アクセスポイントに接続するために必要なワイヤレスセキュロティプロトコルを選択します。 Open Shared WPA-Personal WPA-Enterprise WPA2-Personal WPA2-Enterprise Wired 802.1x

項　目	説　明
Encryption protocol	上記で選択したセキュリティプロトコルに応じて、暗号化プロトコルが表示されます。 このオプションにはアクセスできません。
Credentials	
User name (Account name) EAP method の選択で、表記が変わります。	802.1x Authentication で、PEAP を固定アカウントで設定する場合など
Passphrase	WPA-Personal 、WPA2-Personal アクセスのログインパスワードまたはパスフレーズを入力します。
☐ Show text	入力したパスワードを表示します。
802.1 x Authentication	
☐ EAP method	EAP 認証方法を選択します。 ・Protected EAP (PEAP) ・Transport Layer Security (EAP-TLS) [Authentication Type]オプションは自動的に選択されます。
☐ Use fixed account	PEAP で、固定アカウントを設定できます。
☐ Device name format	EAP-TLS で、必要とされるデバイス名フォーマット（DNS 名、NetBIOS 名、FQDN）のいずれかを選択します ・ The DNS name of the local computer ・ The NetBIOS name of the local computer ・ The fully qualified DNS name of the local computer
☐ Add “host/” to name	チェックボックスをクリックすると、デバイス名の前に「host /」を含めることができます。
Trusted Root CA	この機能を使用する場合、事前に証明書をインポートします。ドロップダウンリストを使用して、SES にインポートされた証明書の中から目的の証明書を選択します。 SES コンソール　メニューバー ① [Tools] -> [Options] -> [Server’s RSA keys] ② <Import> をクリックし、証明書をインポートします。 [Options]ウィンドウが表示されますので、下部にある<Password rules>ボタンをクリックします。
RADIUS server	RADIUS サーバーを入力します。

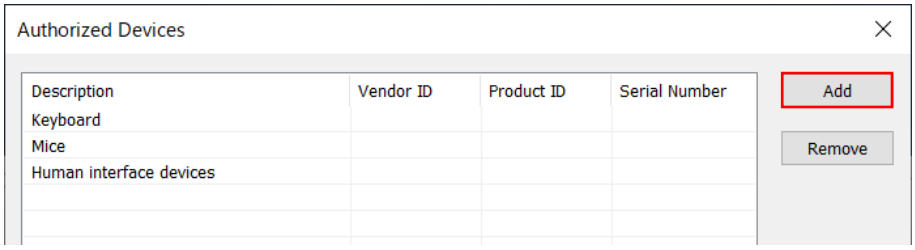
2.4. Port Control

Port Control の機能を使用すると、特定の USB デバイスのみを使用可能にすることができます。

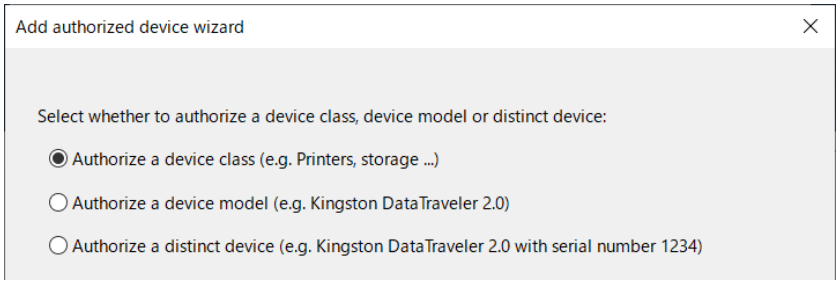
① [Install port control] と、[Block unauthorized USB devices] にチェックを入れ、<Authorized Devices> ボタンをクリックします。

項　目	説　明
Install/Uninstall Port Control	
◎ Install port control	Port Control をインポートします。
Port Control Policy	
○ Manually configure authorized devices	<Authorized Devices>ボタンをクリックし、使用可能とするデバイスを選択します。
○ Automatically build the Authorized Devices list on the client, authorizing currently-inserted devices Security Protocol	クライアントで承認済みデバイスリストを自動的に作成し、現在挿入されているデバイスを承認します。この設定を有効にすると、クライアントデバイスは現在挿入されているデバイスタイプをスキャンして自動的に「ホワイトリスト」に登録し、そのデバイスを将来的に受け入れ可能なデバイスとして挿入を許可できます。この機能追加の利点は、ポートコントロールを一時的に無効にして、デバイス（マウス、キーボード、診断ツール）をポーリングして使用できるようにすることです。1 時間後に、デバイスは通常のデバイスセットのみのサポートするように戻ります。 注　この機能は主に、銀行の ATM やキオスクデバイスなどの IOT デバイスを主にサポートする目的で追加されました。これらの機器に接続される周辺機器は、通常、厳格に制限されますが、厳密に制御された状況で、修理または診断のためにマウス/キーボードや診断デバイスを接続する必要がある場合があります。

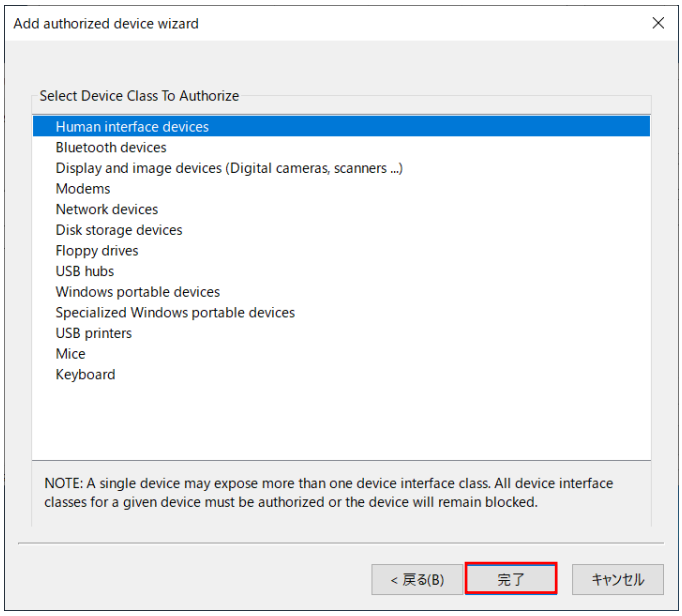
② 次の画面が表示されるので、<Add> をクリックします。



③　特定のデバイスクラス単位で承認する場合は、[Authorize a device class] ラジオボタン、
特定のモデルの USB デバイス単位で承認する場合は、[Authorize a device model] ラジオボタン、
特定の USB デバイスのみを承認する場合は、[Authorize a distinct device] ラジオボタンを
選択し、下部にある <次へ>をクリックします。

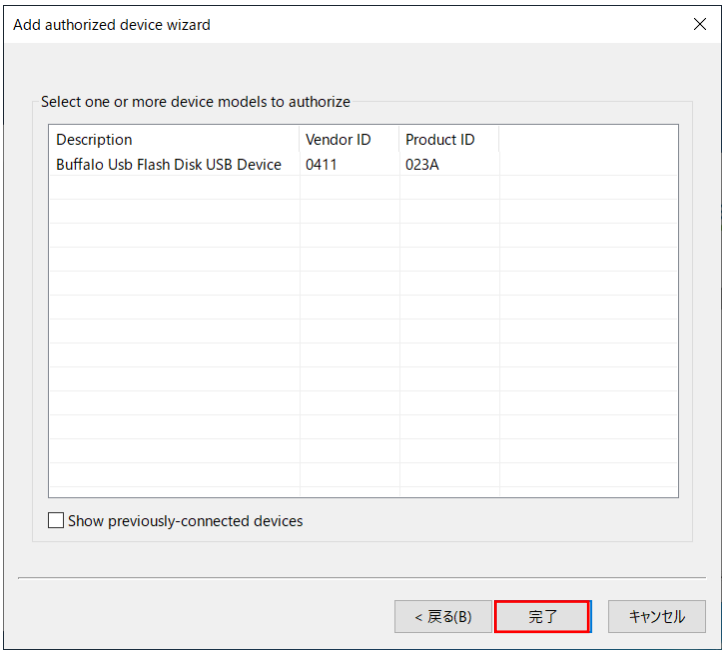


[Authorize a device class] ラジオボタンをクリックした場合、次の画面が表示されます。



デバイスクラスを選択して、<完了> をクリックします。

[Authorize a device model] ラジオボタンをクリックした場合、次の画面が表示されます。
承認させたいデバイスを接続し、SES に認識させます。デバイスが認識されると一覧に表示されますので、承認させたいデバイスを選択します。過去に接続したことのあるデバイスを追加する場合は、
「☐ Show previously-connect devices」のチェックボックスをオンにします。
最後に、<完了> をクリックします。

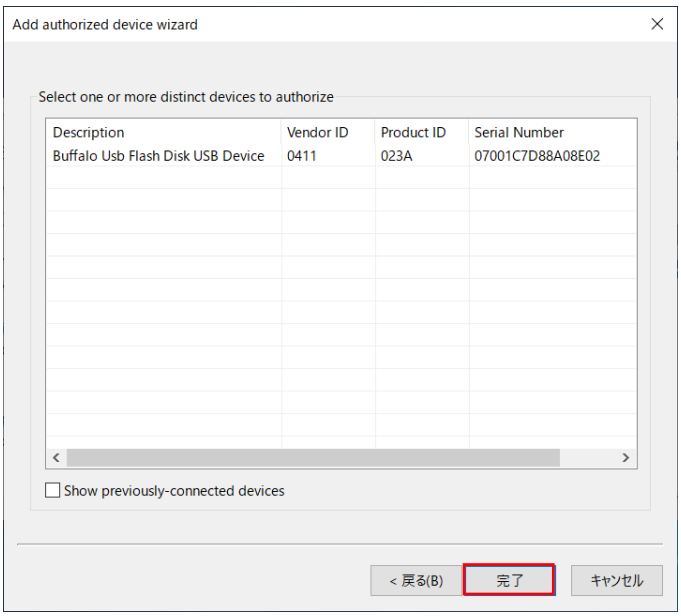


[Authorize a distinct device] ラジオボタンをクリックした場合、次の画面が表示されます。

承認させたいデバイスを接続し、SES に認識させます。デバイスが認識されると一覧に表示されますので、承認させたいデバイスを選択します。過去に接続したことのあるデバイスを追加する場合は、

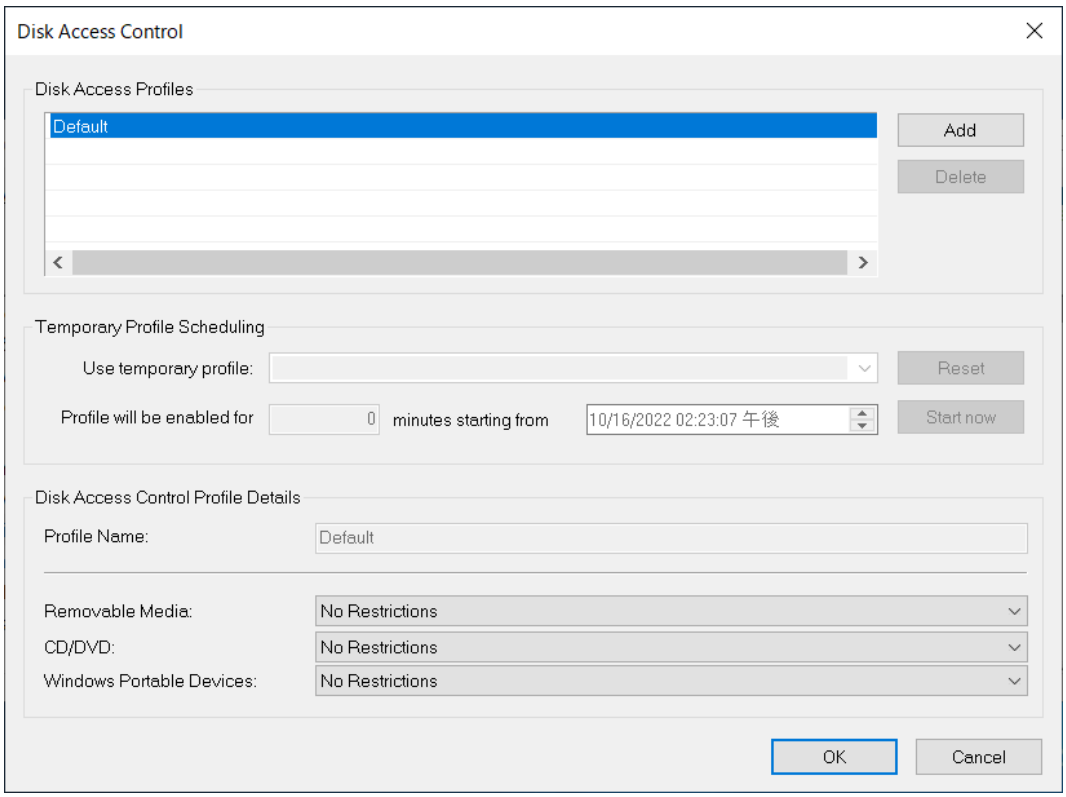
「☐ Show previously-connect devices」のチェックボックスをオンにします。

最後に、<完了> ボタンをクリックします。



2.5. Disk Access Control

Disk Access Control の機能を使用すると、USB 等の方法で接続されるデバイスについて制御することができます。



項　目	説　明
Disk Access Control	
<Add> ボタン	ディスクアクセスコントロール用にデフォルト以外に複数のプロファイルを設定することができます。 <Add>ボタンで、一時プロファイルを作成できます。 一時プロファイルは指定した期間のみ有効なプロファイルです。 それ以外はデフォルトプロファイルの設定が適用されます。
Temporary Profile Schedule	
Use Temporary Profile	一時プロファイルを設定する場合は、プルダウンメニューより<Add>ボタンをクリックして追加したプロファイル名を選択します。
Profile will be enabled for X minutes from xx/xx/xx	一時プロファイルの有効時間（分）および、いつから有効にするかを設定します
Disk Access Control Profile Details	
Profile Name:	設定変更するプロファイル名が表示されます。
Removable Media	リムーバブルメディアへの制御方法を選択します。 ・No Restrictions　（制限なし） ・Read Only, unless Encrypted （暗号化されていない場合は読み取り専用） ・No access, unless Encrypted （暗号化されていないとアクセス不可） ・Read Only access　（読み取り専用アクセス） ・No access　（アクセス不可）

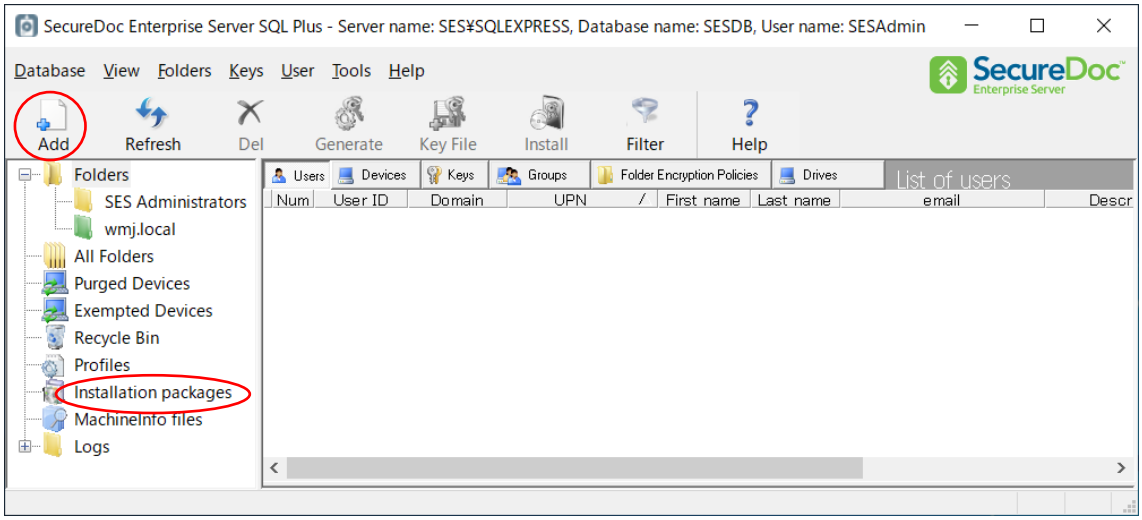
項　目	説　明
CD/DVD	CD/DVD の制御方法を選択します。 ・No Restrictions （制限なし） ・Read Only access （読み取り専用アクセス）
Windows Portable Devices	Windows ポータブルデバイスへの制御方法を選択します。 ・No Restrictions （制限なし） ・Read Only access （読み取り専用アクセス） ・No access （アクセス不可）

3. SecureDoc Enterprise for Windows パッケージ

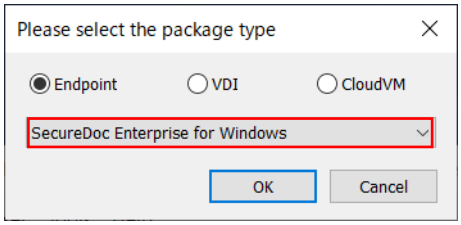
「SecureDoc Enterprise for Windows」のライセンスを使用するインストレーションパッケージの設定項目について解説します。

プロビジョニンルールを使ったインストレーションパッケージの作成方法については、「SecureDoc Enterprise Server Version 9.2 クイックインストールガイド」をご参照ください。

① 左ペインの [Installation packages] アイコンを選択し、<Add> ボタンをクリックするか、右ペインの上で右クリックし、コンテキストメニューから [Add package] をクリックします。



② [Please select the profile type] ウィンドウが表示されますので、[Endpoint] のプルダウンメニューより「SecureDoc Enterprise for Windows」を選択し、<OK> ボタンをクリックします。



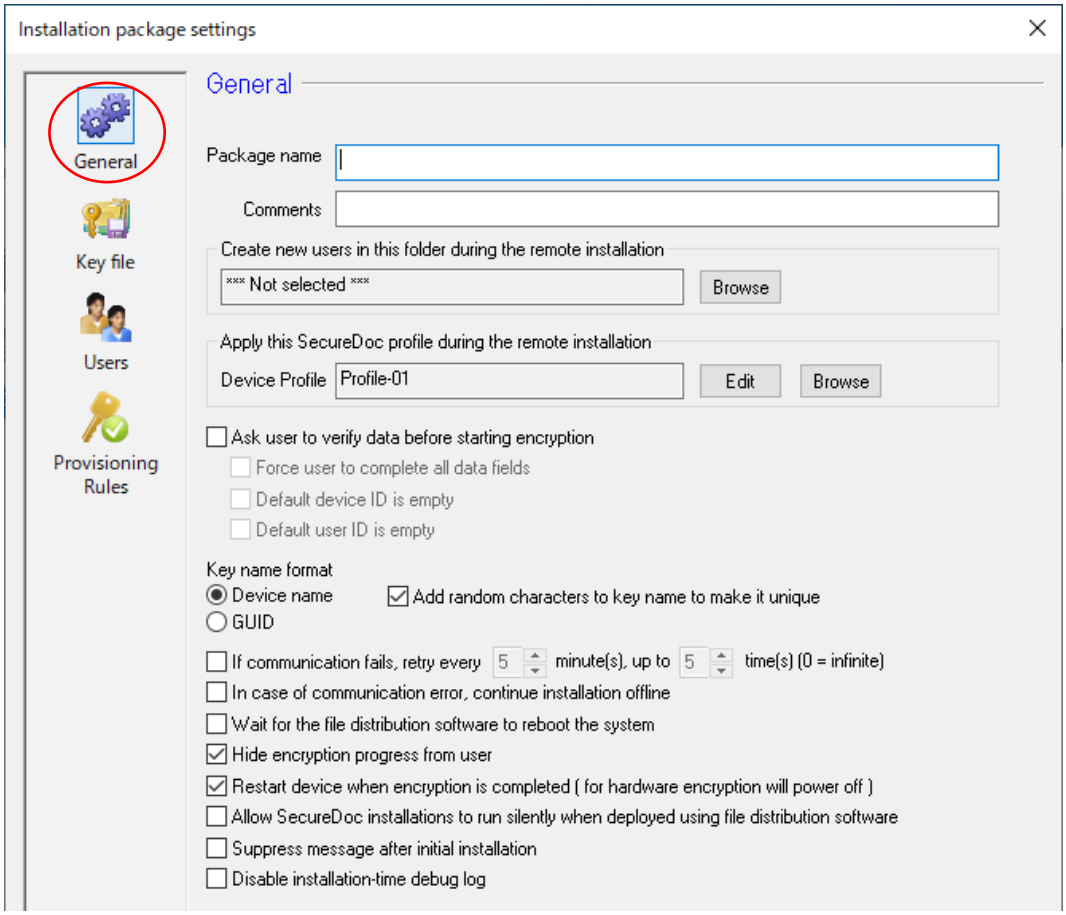
※ 複数のインストレーションパッケージを作成する場合、作成済のインストレーションパッケージを編集することで簡単に作成できます。

作成済のインストレーションパッケージを右クリックして、[Copy Package] を実行します。

[Package name] に新しいパッケージ名を入力し、必要な項目を編集して保存してください。

[General]

プロファイルの指定や暗号化時の設定などが含まれます。



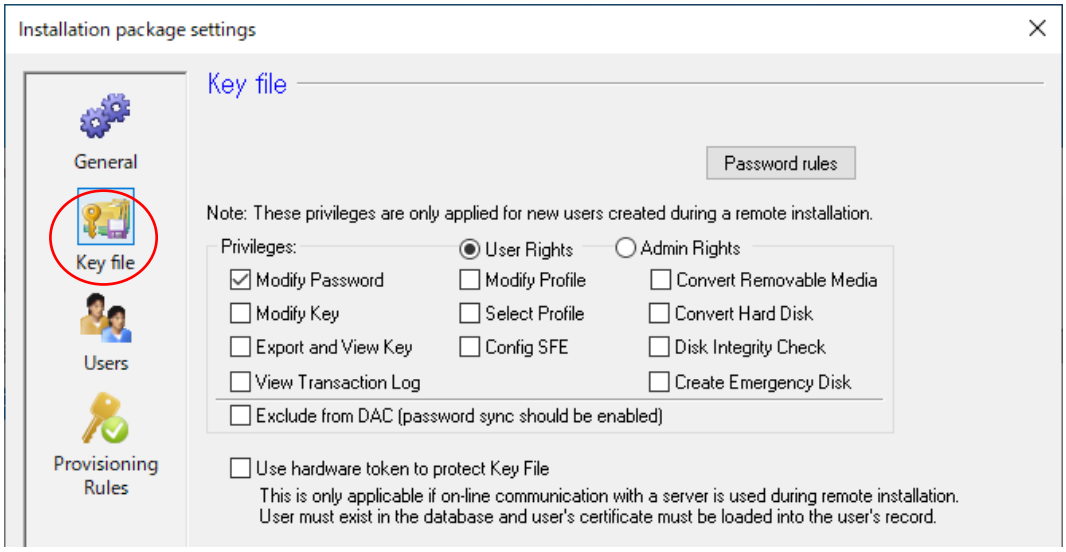
項　目	説　明
Package name	作成するインストレーションパッケージ名を入力します。
Comments	必要に応じて、コメントを入力します。
Create new users in this folder during the remote installation	
*** Not selected ***	<Browse> をクリックし、インストールプロセス中に作成するユーザーの登録先フォルダを指定します。 ADSync を使用している場合、この設定は必要ありません。
Apply this SecureDoc profile during the remote installation	
Device profile	<Browse> をクリックし、デバイスに適用するプロファイルを指定します。

項　目	説　明
☐ Ask user to verify before staring encryption	暗号化を開始する前に、「SecureDoc の登録フォーム」をデスクトップに表示し、ユーザーによるユーザーID 名などの設定を可能とします。 「SecureDoc の登録フォーム」 
☐ Force user to computer all data fields	「SecureDoc の登録フォーム」の全てのフィールドを空白にします。
☐ Default device ID is empty	「SecureDoc の登録フォーム」の「コンピュータ情報」に関するフィールドを空白にします。
☐ Default use ID is empty	「SecureDoc の登録フォーム」の「ユーザー情報」に関するフィールドを空白にします。
Key name format	
◎ Device name	デバイス名と同名の鍵を生成します。
☐ Add random characters to key name to make it unique	鍵名にランダムな文字を追加し、ユニークなものとします。
◎ GUID	GUID と同名の鍵を生成します。
☐ If communication fails, retry every X minute(s), up to X times(s)	通信に失敗した場合、X 分ごとに最大 X 回リトライします
☐ In case of communication error, continue installation offline	通信エラーの場合、オフラインでインストールを続行します。 後に、SDConnex と通信をおこなうと、クライアントデバイスで生成された鍵は SES DB に保存されます。
☐ Wait for the file distribution software to reboot the system	ファイル配布ソフトがシステムを再起動するのを待ちます。
☐ Hide encryption progress from user	注　暗号化の進捗状況をデスクトップ上に表示しません。
☐ Restart device when encryption is completed (for hardware encryption will power off)	暗号化完了後、デバイスを再起動します。 ハードウェア暗号化ドライブを搭載しているデバイスの場合は、シャットダウンします（電源オフ）

項　目	説　明
☐ Allow SecureDoc installations to run silently when deployed using file distribution software	ファイル配布ソフトウェアを使用して展開する場合、SecureDoc のインストールをサイレント モードで実行できるようにします。
☐ Suppress message after initial installation	初期インストール後に、暗号化が完了した時に表示されるメッセージ「暗号化の終了」を非表示にします。

[Key file]

権限の設定箇所

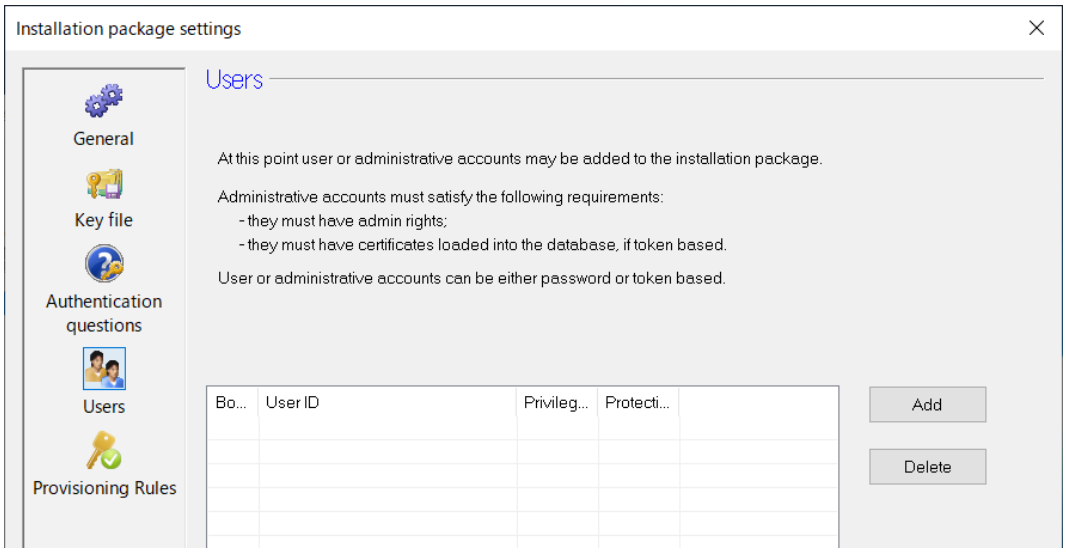


項　目	説　明
<Password rules>ボタン	グローバルオプションで設定されているデフォルトのパスワードルールが表示されます。 [Tools] -> [Options] -> [General] <Password rules> ここで権限の設定を変更できます。
Privileges:	
◎ User Rights	グローバルオプションで設定されている権限が付与されます。 [Tools] -> [Options] -> [Key file options] デフォルト設定では、「Modify Password」のみが付与されています。 権限一覧から、必要な権限を付与できます。
◎ Admin Rights	チェックすると、全ての権限が付与されます。
☐ Modify Password	ユーザーは、パスワードを変更できます。
☐ Modify Profile	ユーザーは、プロファイルを変更できます。
☐ Convert Removable Media	ユーザーは、リムーバブルメディアを暗号化できます。
☐ Modify Key	ユーザーは、鍵を生成、削除、およびインポートできます。
☐ Select Profile	ユーザーはキーを生成、削除、およびインポートできます。

項　目	説　明
☐ Convert Hard Disk	ユーザーは、ディスクの暗号化/復号化をおこなえます。
☐ Export and View Key	ユーザーは、鍵を操作できます。たとえば、キーファイルをエクスポートすることや、鍵を他のキーファイルにエクスポートしたりできます。
☐ Config SFE	ユーザーは、クライアント側で、SecureDoc ファイル暗号化を定義することができます。
☐ Disk integrity Check	ディスクの整合性チェックが失敗した場合でも、ユーザーは作業を続行できます。デバイスを検査し、ディスクの整合性のために新しい署名を再作成します。
☐ View Transaction Log	ユーザーは、Audit Log を見ることができます。
☐ Create Emergency Disk	ユーザーは、エマージェンシーディスクを作成できます。
☐ Exclude from DAC (password sync should be enabled)	DAC を無効にします。（通常は選択しません） インストレーションパッケージのプロファイルの設定にて、ディスクアクセスコントロール（DAC）が有効に設定され、外部メディアへの接続が制限されている場合、外部メディアへのアクセスが行えず、ディスクをアンロックしても、外部メディアなどへデータの移動が行えません。
☐ Use hardware token to protect Key File	このインストールパッケージを実行するクライアントデバイスのユーザーが、暗号化されたデバイスに正常にログインするにはトークンが必要であることを指定する場合にオンにします。 トークンには、ユーザーに関連付けられた証明書が含まれている必要があります。このオプションを使用するには、最初にユーザー証明書情報を Active Directory から SES にインポートする必要があります。

[Users]

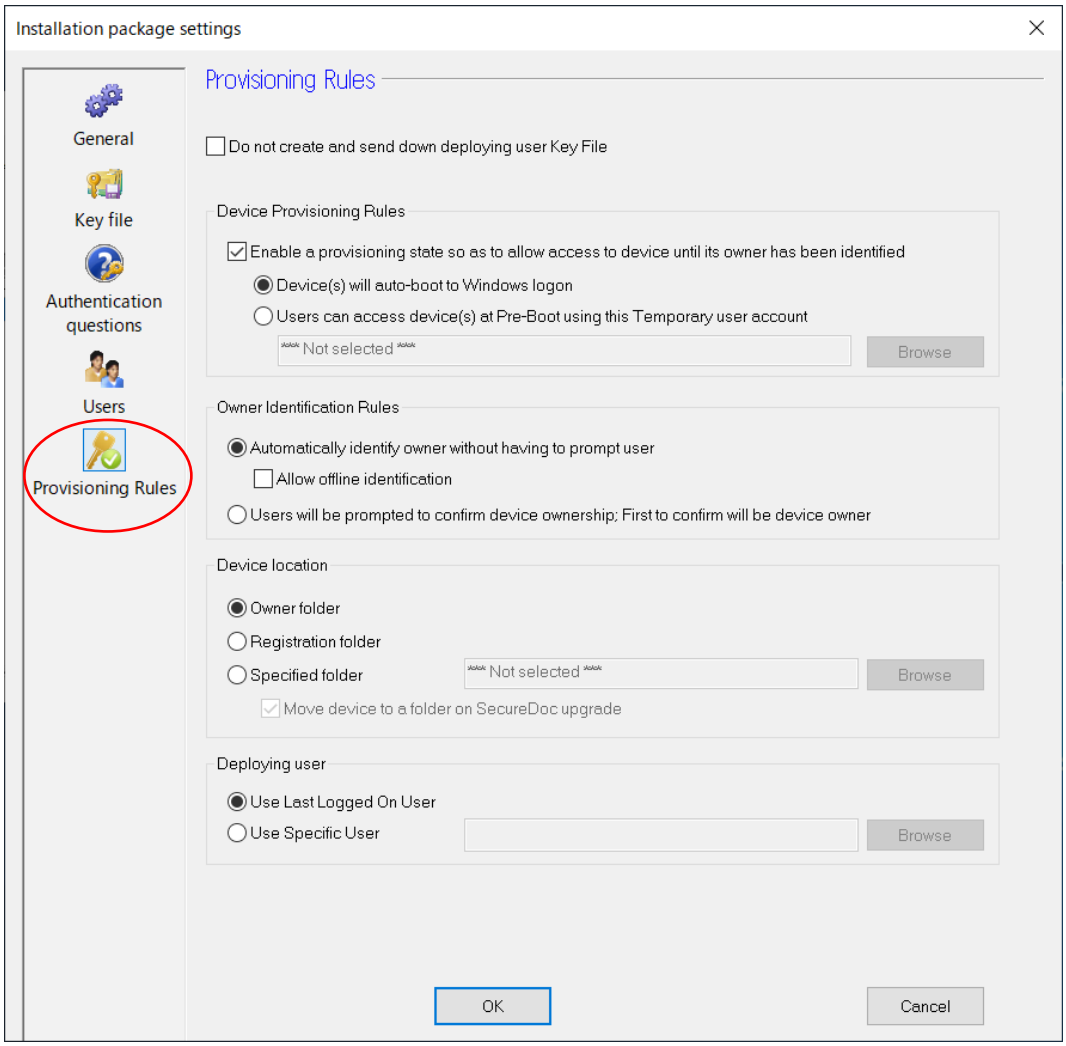
管理者権限の ID をクライアントデバイスに二人目のユーザーとして登録する設定



項　目	説　明
<Add>ボタン	インストールプロセス中に、管理者権限の ID を二人目以降のユーザーとしてクライアントデバイスに登録できます。該当の ID を選択します。
<Delete>ボタン	一覧から、管理者権限の ID を削除します。

[Provisioning Rules]

オーナーID 作成方法の設定など



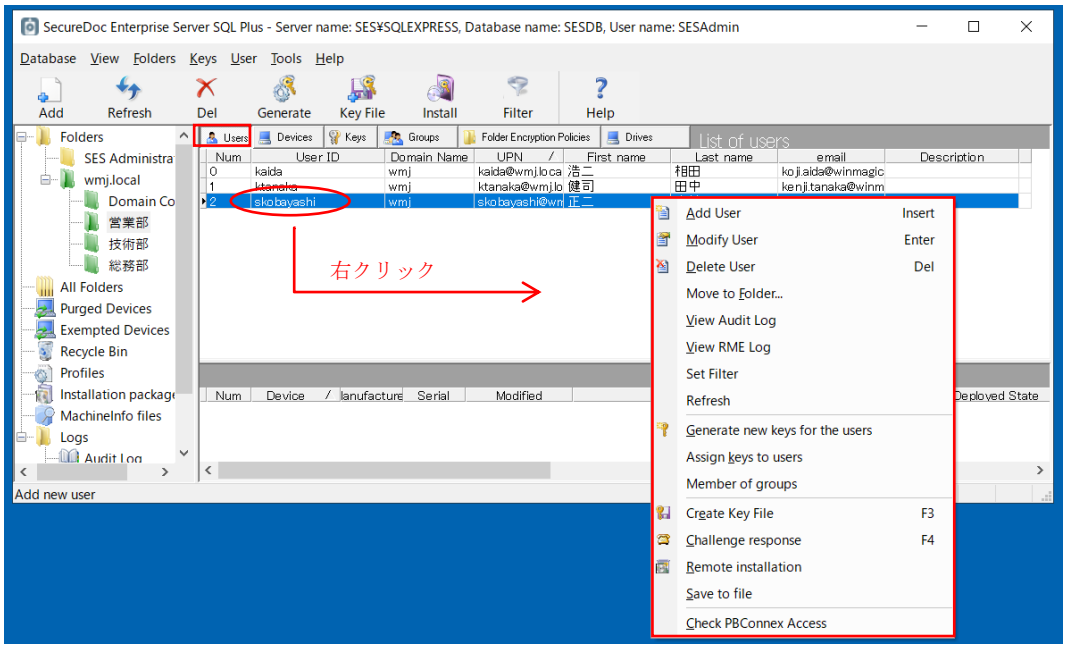
項　目	説　明
☐ Do not create and send down deploying user Key File	ユーザーのキーファイルを作成せず、クライアントデバイスにキーファイルを登録しません。 この設定の目的は、プリブートネットワーク認証を使用するデバイスで、ネットワークを介した認証を必須とし、デバイスにユーザーID を登録しないことです。
Device Provisioning rules	
☐ Enable a provisioning state so as to allow access to device until its owner has been identified	プロビジョニング状態を有効にして、所有者が特定されるまでデバイスへのアクセスを以下の方法で許可します。
○ Device(s) will auto-boot to Windows logon	オートブートによって、プリブート認証はパスされ、Windows を起動できます。
○ User can access device(s) at Pre-Boot using this Temporary user account	オーナーが確定するまで、プリブート認証では、SES コンソールの[Users]タブで事前に作成した Temporary タイプのユーザーID を使ってログインできます。

項　目	説　明
	オーナーが確定すると、ここで指定した Temporary タイプのユーザーID は、クライアントデバイスから自動で削除されます。
<Browse>ボタン	Temporary タイプのユーザーID を指定します。
Owner Identification Rules	
○ Automatically identify owner without having to prompt user	デスクトップに何も表示せず。自動でオーナーID を作成します。 それにより、サイレントインストールが可能です。 オーナーID の作成方法は、下記の「Deploying user」の設定に従います。
☐ Allow offline identification	オフライン状態で、オーナーID の作成を許可します。 「Deploying user」の設定で、「Use Last Logged On User」を選択してください。
○ Users will be prompt to confirm device ownership; First confirm will be device owner	デスクトップに「**SecureDoc プライマリアカウントの設定**」ダイアログを表示し、デバイス所有者であることについて確認を求めます。 <OK>をクリックすると、そこに表示されている Windows ユーザー名が、オーナーID として登録されます。表示されている Windows ユーザー名は、その時、Windows にサインインしている ID です。 オーナーID が確定すると、デバイス起動時のプリブート認証を利用できるようになります。  デバイス所有者でない場合、例えば、IT 担当者やキッティング作業をおこなっている業者がインストールをおこなっており、ユーザーの Windows ID でサインインしていない場合は、<後で>をクリックします。 <OK> をクリックするまで（オーナーID が確定するまで）、OS 起動後、常に「**SecureDoc プライマリアカウントの設定**」が表示されます。
Device location	
○ Owner folder	デバイスは、オーナーID と同じフォルダに登録します。
○ Registration folder	[General] -> [Create new users in this folder during the remote installation] で、指定したフォルダにデバイスを登録します。
○ Specified folder	<Browse> ボタンで、デバイスの登録先を指定します。
☐ Move device to a folder on SecureDoc upgrade	SecureDoc のアップグレード時、デバイスを指定したフォルダ先に移動します。
Deploying user	
○ Use Last Logged On User	インストール実行時に、Windows へサインインしている ID を使います。
○ Use Specific User	ここで指定した ID を使います。

4. SES コンソールメニュー

4.1. ユーザーに関する操作メニュー

[Users] タブで、ユーザーを選び、コンテキストメニュー（マウスの右クリックメニュー）で表示される機能は、下記のテーブルを参照してください。

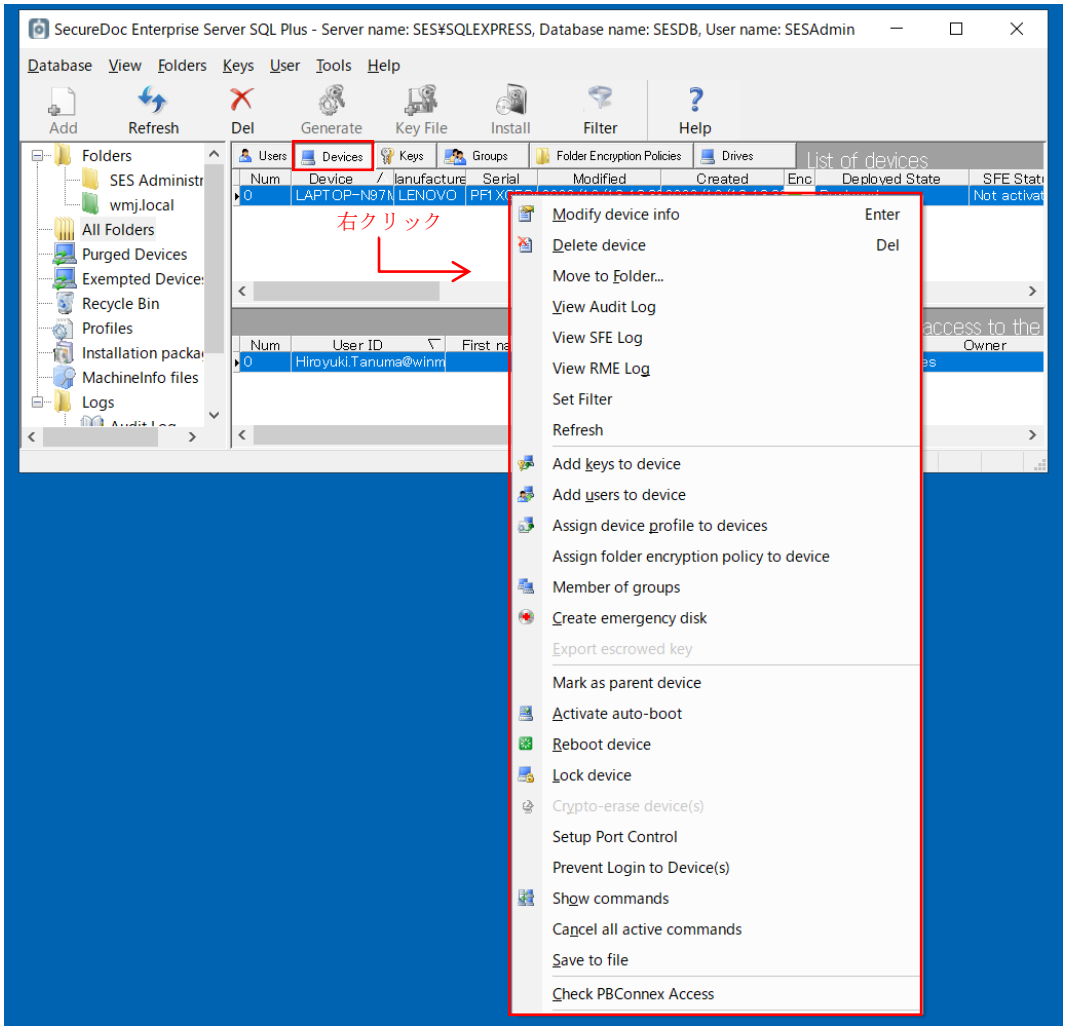


項　目	説　明
Add User	フォルダにユーザーを新規作成します。
Modify User	選択しているユーザーの情報を編集します。 ※　ここで編集して保存しても、デバイスには配信されず、デバイスに登録されているユーザーのキーファイルは上書きしません。
Delete User	選択しているユーザーをフォルダから削除します。 ユーザーは、Recycle bin に移動します
Move to Folder…	選択しているユーザーを別のフォルダに移動します。
View Audit Log	ユーザーの認証に関するログ「Audit Log」を閲覧できます。
View RME Log	ユーザーの RME に関するログ「RME Log」を閲覧できます。
Set Filter	フィルター機能で、一覧から情報を抽出できます。
Refresh	一覧表示をリフレッシュします。
Generate new keys for the users	ユーザーの為に新たに鍵を生成します。例えば、メディア暗号用の鍵。
Assign keys to users	SES から鍵をユーザーのキーファイルに追加できます。 例えば、ユーザーの為に鍵を生成し、ユーザーに配信することが可能。
Member of groups	グループへの参加を設定できます。

項　目	説　明
Create Key File	ユーザーのキーファイルを作成できます。 .dbk ファイルの形式で作成されるので、プリブート認証画面で、USB メモリに保存した.dbk ファイルを使ってログインすることが可能です。 ※　デバイスには配信されず、デバイスに登録されているユーザーキーファイルは上書きしません。
Challenge response	チャレンジレスポンス機能。ユーザーのパスワード忘れに対応します。
Remote installation	オフラインインストレーションパッケージを作成できます。
Save to files	ユーザーの情報をテキスト形式で書き出せます。
Check PBConnex Access	PBConnex の利用可能なデバイスを確認できます。

4.2.デバイスに関する操作メニュー

「Devices」タブで、デバイスを選び、コンテキストメニューで表示される機能は、下記のテーブルを参照してください。

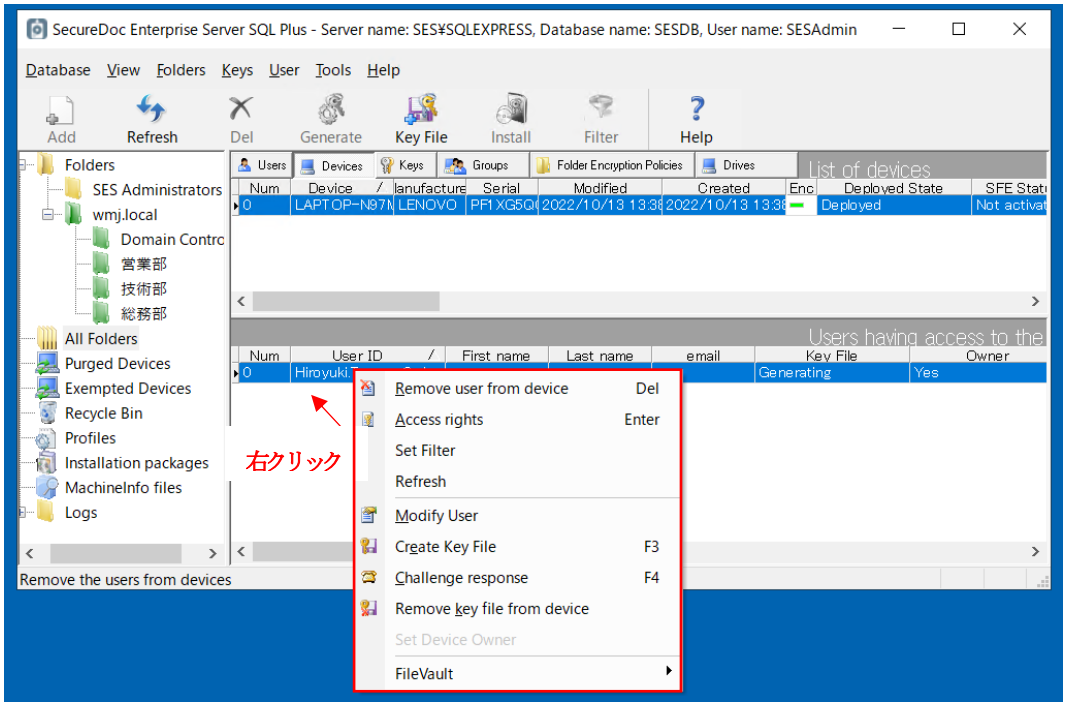


項　目	説　明
Modify device info	デバイスの情報を編集できます。
Delete device	選択しているデバイスをフォルダから削除します。 デバイスは、[Recycle bin] に移動します。
Move to Folder…	選択しているデバイスを別のフォルダに移動します。
View Audit Log	デバイスに関するログ「Audit Log」を閲覧できます。
View SFE Log	SFE に関するログ「RME Log」を閲覧できます。
View RME Log	RNE に関するログ「RME Log」を閲覧できます。
Set Filter	フィルター機能で、一覧から情報を抽出できます。
Refresh	一覧表示をリフレッシュします。
Add Keys to device	鍵をユーザー単位ではなく、デバイスに配信できます。
Add users to device	ユーザーをクライアントデバイスに追加できます。
Assign device profile to devices	SES 上で、編集した既存のプロファイルをデバイスに再適用する場合や、他のプロファイルに変更することができます。

項　目	説　明
Assign folder encryption policy to device	フォルダ暗号のポリシーを適用します。 別途、ライセンスが必要です。
Member of groups	グループへの参加を設定できます。
Create emergency disk	クライアントデバイスのプリブート認証プログラムに異常が発生した場合の対処時に必要なエマージェンシーディスクを作成できます。
Export escrowed key	エスクローキーのエクスポート。 通常は利用できません。
Mark as parent device	通常は使用しません。 parent と child device の関係を持つデバイスの場合、parent device としてマークします。
Active auto-boot	設定した一定期間・回数のみ、オートブートを有効にできます。
Reboot device	クライアントデバイスを再起動します。
Lock device	クライアントデバイスの Windows OS をスクリーンロックします。
Crypto-erase device(s)	ディスクの復号化に必要な鍵をリモートで削除します。 実行されるタイミングは、クライアントが SDConnex と通信し命令を受け取った際で、鍵を削除されることで、ユーザデータは破壊されたのと同様です。 このコマンドを受け取ったデバイスは、プリブート認証プログラムも正常に動作しなくなります。
Setup Port Control	ポートコントロールの有効・無効を設定できます。
Prevent Login to Device(s)	デバイスへのログインを禁止します。 解除するためにはチャレンジレスポンスによるリカバリが必要です。
Show commands	SES からの操作したコマンドの状態を確認できます。
Cancel all active commands	アクティブなコマンドを全てキャンセルします。
Save to files	デバイスの情報をテキスト形式で書き出せます。
Check PBConnex Access	PBConnex の利用可能なデバイスを確認できます。

4.3. デバイスに登録されているユーザーへの操作メニュー

「Devices」タブで、デバイスを選ぶと、下のパネルにはデバイスに登録されているユーザーID が表示されます。
そのユーザーID を右クリックして表示されるコンテキストメニューの機能は、下記のテーブルを参照してください。



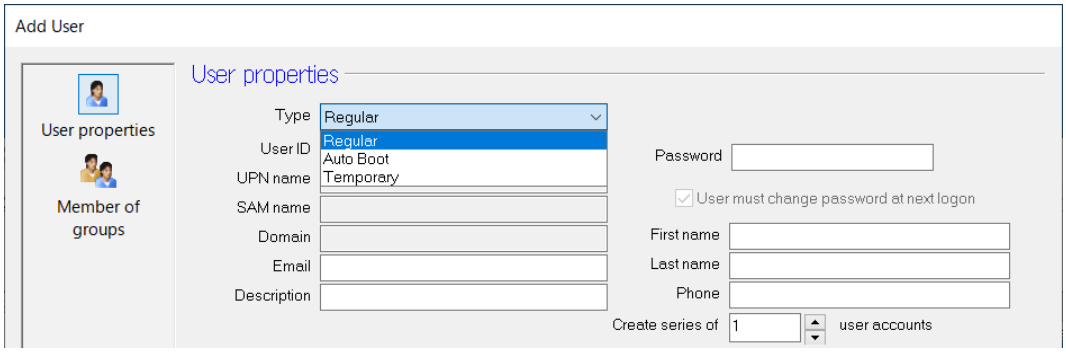
項　目	説　明
Remove user from device	デバイスからユーザーを削除します。
Access rights	アクセス権を変更します。
Set Filter	フィルター機能で、一覧から情報を抽出できます。
Refresh	一覧表示をリフレッシュします。
Modify User	ユーザーを編集できます。
Create Key File	権限変更や鍵の追加など、ユーザーのキーファイルを再作成できます。 クライアントは SDConnex 経由で、新しいキーファイルを受け取り、次回のプリブート認証時には新しいキーファイルでログインすることになります。
Challenge Response	ユーザーのパスワード忘れ時に、16 進数のやりとりで、一度だけログインを許可します。ユーザーは、Windows サインイン後に、自身による新しいパスワード設定を求められます。
Remove key from device	デバイスから鍵を削除します。
Set Device Owner	デバイスオーナーを変更する場合、該当のユーザーを選択して実行します。
File Vault	mac デバイス向けのメニューです。

5. ユーザープロパティのタイプについて

ユーザープロパティには、「Type」の設定があります。

ADSync を使ってユーザーを Active Directory からインポートする場合、「Regular」が設定されています。

手動でのユーザー作成時には、目的にあわせて設定します。



Regular： 通常どおり使用するためのユーザーID

Auto Boot： プリブート認証画面で、認証を必要とせず、自動ログイン（オートブート）とするユーザーID です。
このユーザーID をクライアントデバイスに追加すると、他に Regular タイプのユーザーID が登録されていてもオートブートとなるので、注意が必要です。

Temporary： プロビジョニングルール「パターン C」、「パターン D」で使用します。
オーナーが確定すると、Temporary のユーザーID はデバイスから削除されます。

6. プリブートネットワーク認証（PBConnex）

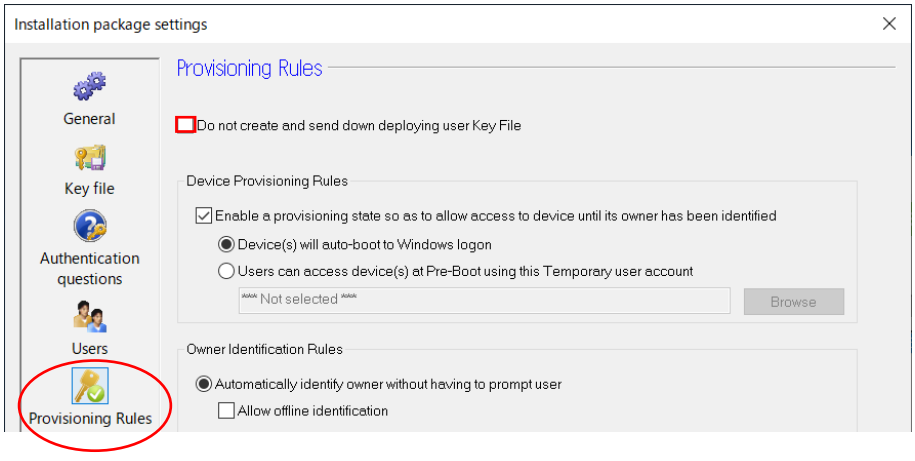
SecureDoc クライアントは、有線 LAN あるいは無線 LAN を使ったネットワーク認証の機能（PBConnex）を提供します。プリブート時の認証において、ローカルデバイスに登録されているユーザーID を使うのではなく、SES 側に登録されているユーザーID を使ってログインする仕組みです。ユーザーが入力した ID がローカルデバイスに存在しない場合、ブートログオンプログラムは、SDConnex を経由して SES に登録されている ID への認証を試みます。
PBConnex を使用するためには、プロファイルの設定と対象のデバイスとユーザーを指定する必要があります。

特長１：共有 PC でのユーザー管理の負担軽減

プリブートネットワーク認証の機能を使うと、SecurDoc のエンドポイントユーザーは複数のデバイスにアクセスできるようになります。共有 PC など複数のユーザーが利用するデバイスにおけるユーザー管理の負担を軽減することができます。

特長２：全ての認証情報をローカルデバイスに登録しないことも可能

常にプリブートネットワーク認証を利用するデバイスの場合、ローカルに認証情報を登録しない SecueDoc クライアントのインストールも可能です。
プロビジョニングルールの設定で、
「☑ Do not create end send down deploying user Key File」
のチェックボックスをオンにしたインストレーションパッケージを使って、クライアントに SecureDoc クライアントをインストールすると、ローカルデバイスにキーファイルは登録されません。キーファイルが登録されていないため、復号化するのに必要なキーファイルを利用するための ID/PW が存在しません。



特長３：オートブート機能

PBConnex は、オートブート機能もサポートします。SecureDoc クライアントが SDConnex と接続すると、SES でオートブートに定義されたデバイスはプリブートでの認証を必要とせず、自動ログインさせることが可能です。
SDConnex が設置された LAN 以外にデバイスが持ち出された場合、オートブートとはならず、認証が必要となります。

6.1. プロファイルの設定

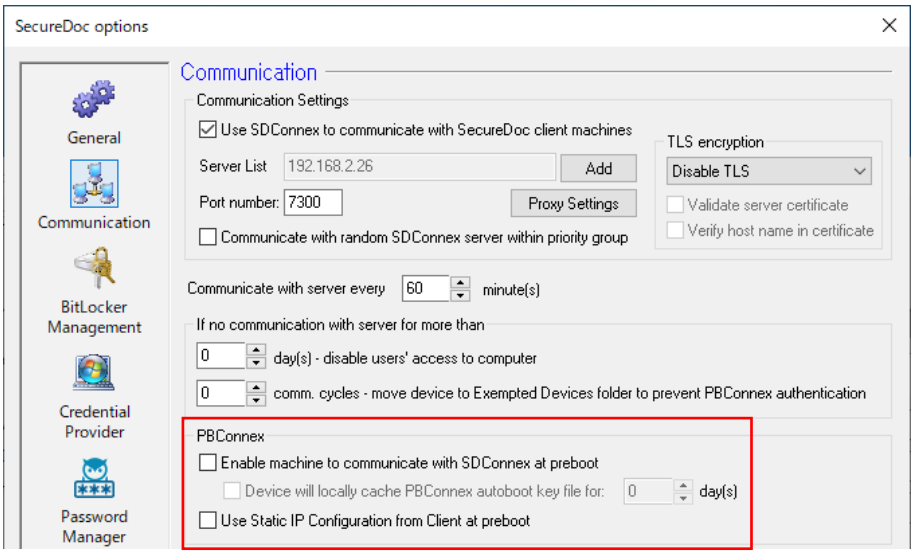
PBConnex を使用するデバイスでは、プロファイルに以下の設定が必要です。

・「 ☐Enable machine to communicate with SDConnex at preboot 」 を有効にします。

設定箇所：<General options> -> [Communication] -> [PBConnex]

☐Enable machine to communicate with SDConnex at preboot

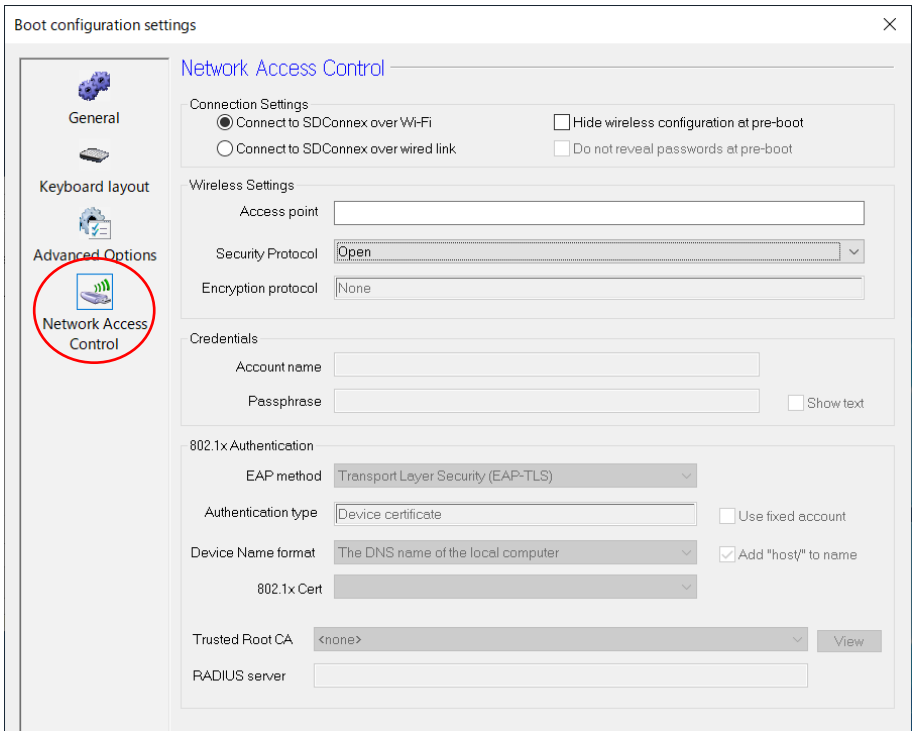
前述の「Communication 設定」をご参照ください。



・有線あるいは無線 LAN の設定

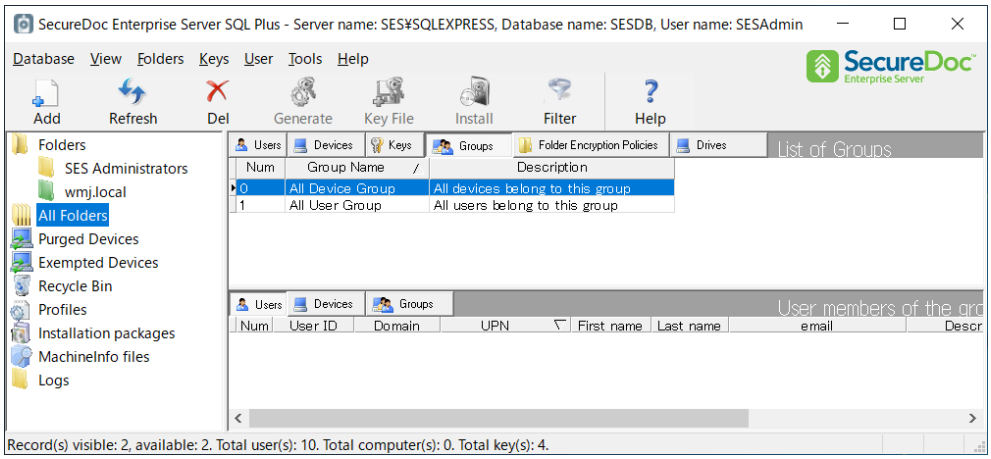
設定箇所：<Boot configuration > -> [Network Access Control]

前述の「Network Access Conteol 設定」をご参照ください。

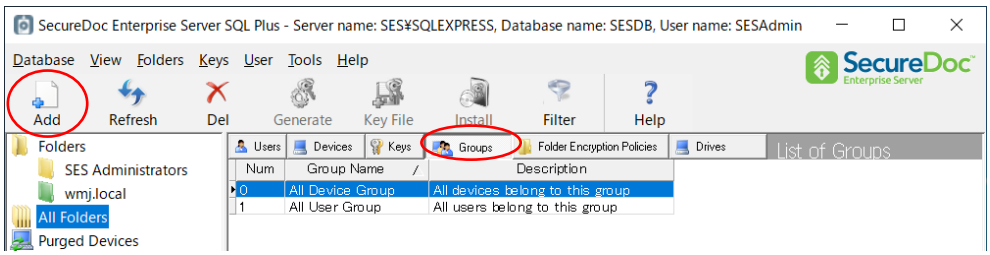


6.2. グループの作成

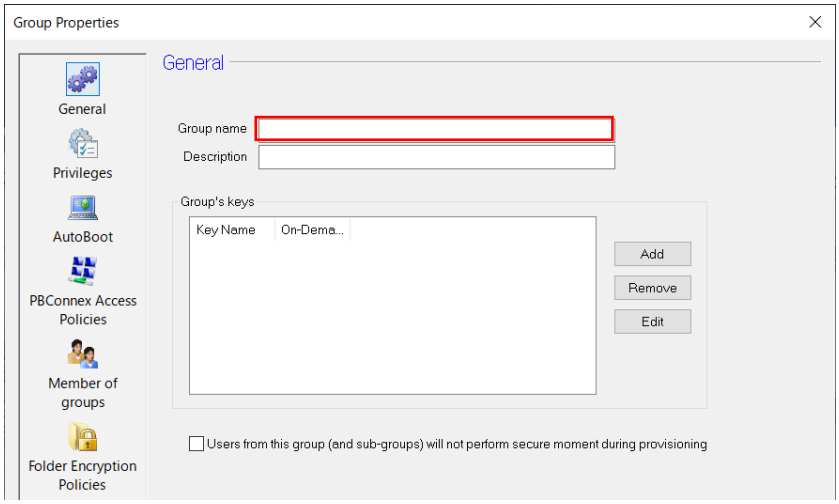
All Folders には、既存で「All Device Group」と「All User Group」が設定されています。これらのグループを使用すると、全てのデバイスと全てのユーザーに PBConnex の利用を設定することができます。
ここでは、PBConnex を利用するユーザーとデバイスを管理する為のグループを新規に作成し、対象とするデバイスとユーザーを登録する方法を説明します。



① SES の左ペインより、グループを作成する場所（フォルダ）を選択します。次に、右ペインにある [Groups] タブをクリックし、<Add> ボタンをクリックします。

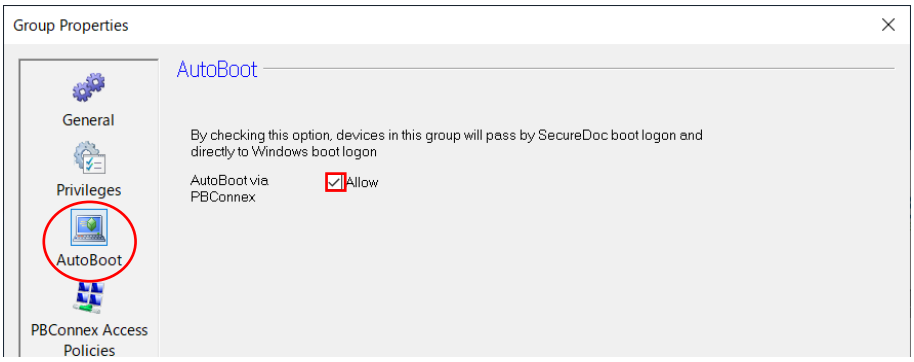


② 次の画面で、 [Group name] 欄にグループ名を、必要に応じて [Description] 欄に説明を入力します。



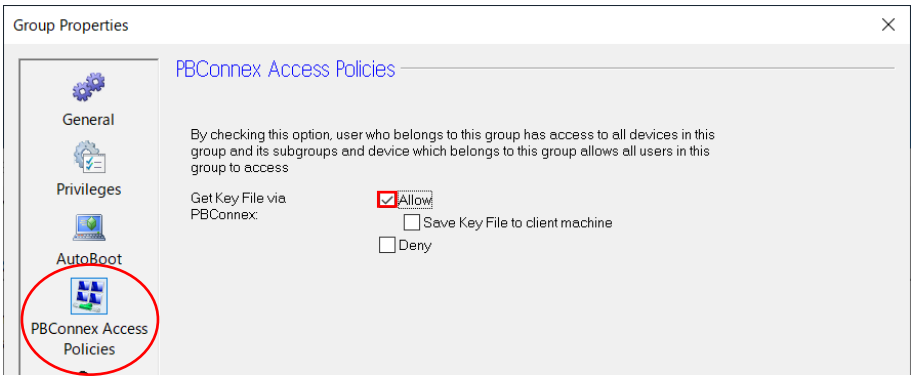
③ オートブートを設定する場合は、

左ペインより、[AutoBoot] アイコンをクリックし、[AutoBoot via PBConnex] の [Allow] にチェックを入れ、画面下部にある <OK> ボタンをクリックします。



SES に登録されている ID をネットワーク認証で使用する場合は、

左ペインより、[PBConnex Access Policies] アイコンをクリックし、[Get Key File via PBConnex] 欄の [Allow] チェックボックスにチェックを入れ、画面下部にある <OK> ボタンをクリックします。



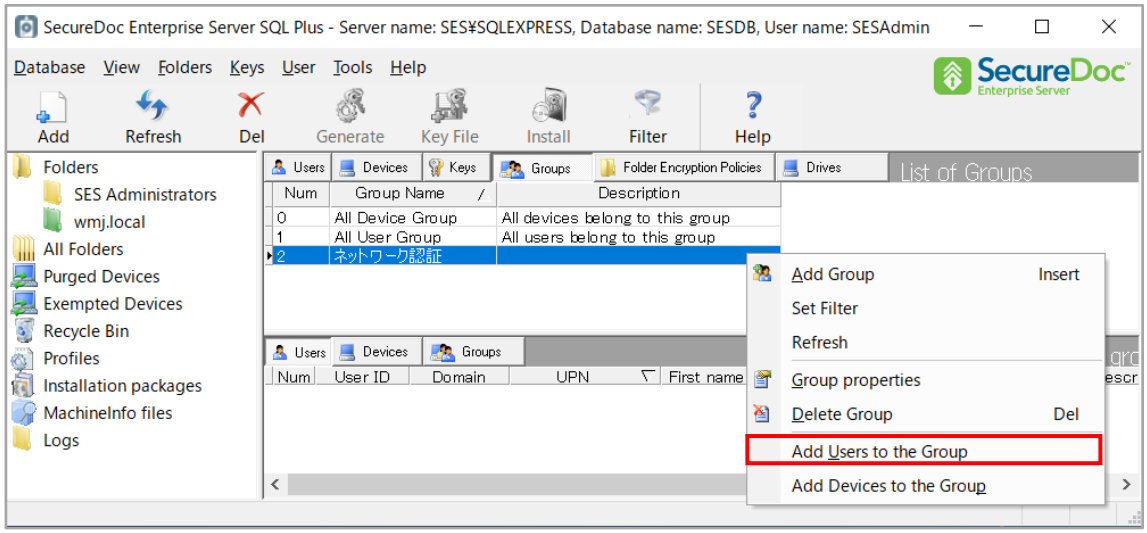
項　目	説　明
Get Key File via PBConnex	
☐ Allow	許可する。
☐ Save Key File to client machine	プリブートネットワーク認証に成功した後、使用した ID（キーファイル）をクライアントデバイスに登録します。 常にネットワーク認証を使用する場合は、チェックしません。 ※ 次回、同じ ID を使ってログインを試みると、キーファイルはクライアントデバイスに登録されている為、ネットワーク認証とならず、ローカル認証となります。
☐ Dey	拒否する

6.3. グループへのユーザー登録

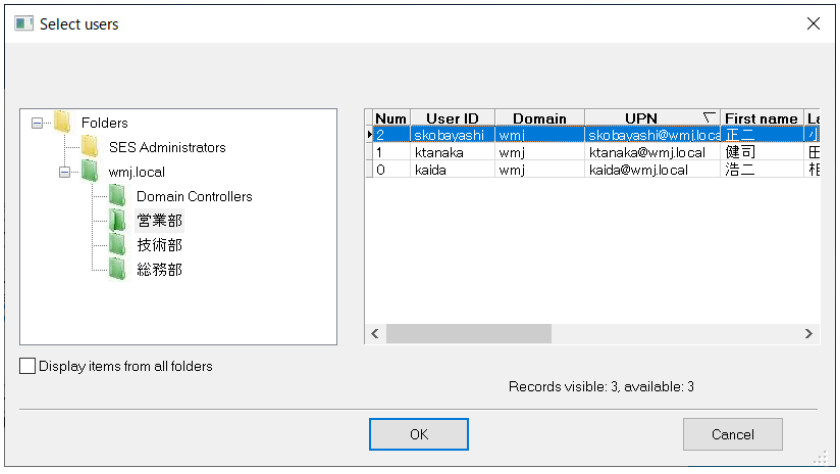
ネットワーク認証で使用するユーザーをグループに追加します。

※　オートブートを利用する場合、この設定は不要です。

①　前項で作成したグループを選択し、コンテキストメニューから [Add Users to the Group] をクリックします。



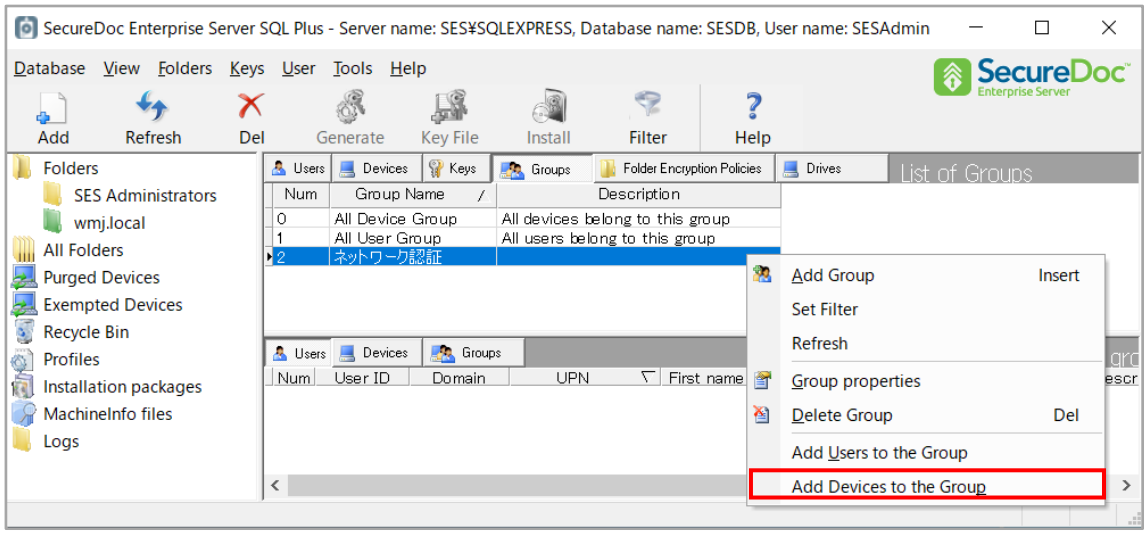
②　次のような画面が表示されます。左ペインより、グループに追加したいユーザーが所属するフォルダを選択します。
右ペインより、ユーザーを選択し、下部にある <OK> ボタンをクリックします。



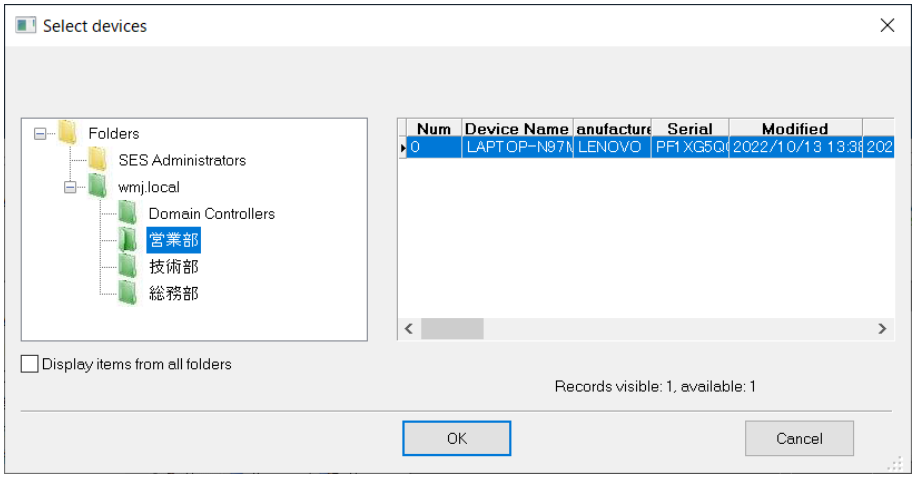
6.4. グループへのデバイス登録

ネットワーク認証機能を利用するデバイスをグループに登録します。同じグループに所属するユーザーがグループ内のデバイスにアクセスできるようになります。

① 作成したグループを選択し、コンテキストメニューから [Add Users to the Group] をクリックします。



② 次のような画面が表示されます。左ペインより、グループに追加したいデバイスが所属しているフォルダを選択します。右ペインよりデバイスを選択し、下部にある <OK> ボタンをクリックします。



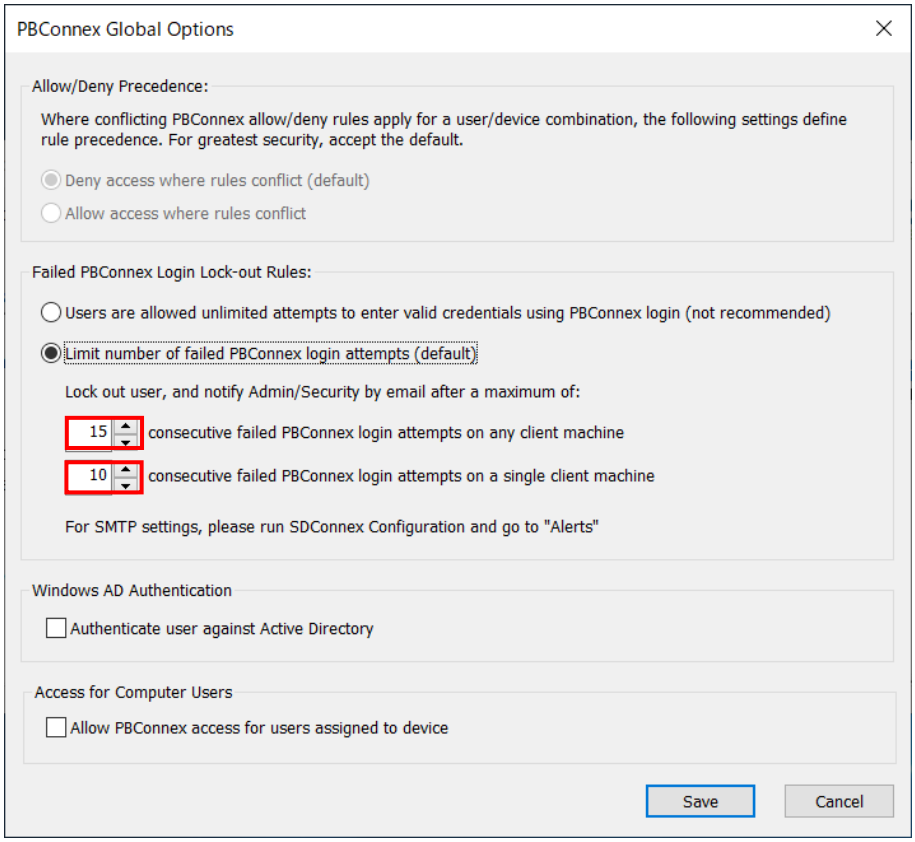
以上の設定により、
同一グループに所属しているユーザーは、プリブート認証時にネットワーク経由で SES に登録されている ID を使ってログインできるようになります。オートブート設定の場合は、SDConnex と接続後、自動ログインとなります。

6.5. 連続ログイン失敗回数の設定

プリブートネットワーク認証にて、連続ログイン失敗回数がしきい値を超えた場合、そのアカウントをロックできます。連続ログイン失敗回数のしきい値を変更する手順について説明します。

① SES のメニューバーより、
[Tools] -> [Preboot Network(PBConnex)] -> [PBConnex Global options]
をクリックします。

② 任意のデバイスおよび単一のデバイスで、連続ログイン失敗回数を超過したら ID をロックする回数を指定します。
最後に、<Save> ボタンをクリックします。



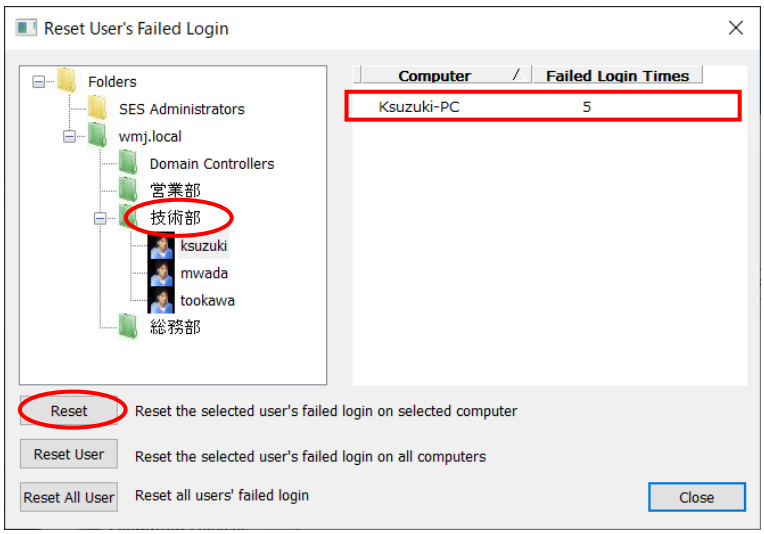
項　目	説　明
Failed PBConnex Login Lock-out Rules:	
○ Users are allowed unlimited attempts to enter valid credentials using PBConnex login (not recommends)	資格情報（ID/パスワード）の入力を無制限に試行できます。（推奨しません）
◎ Limit number of failed PBConnex login attempts (default)	ログイン試行の失敗回数を制限します。（デフォルト）
Lock out user, and notify Admin/Security by email after a maximum of:	
XX consecutive failed PBConnex login attempts on any client machine	任意のデバイスで連続ログイン失敗回数を超過したら ID をロックする回数を指定します。

項　目	説　明
XX consecutive failed PBConnex login attempts on a single client machine	単一デバイスで連続ログイン失敗回数を超過したら ID をロックする回数を指定します。
Windows AD Authentication	
Authenticate use against Active Directory	デフォルト設定のオフでは、ユーザーの ID/パスワードは SES によってのみチェックされます。 このオプションを有効にすると、ユーザーの ID/パスワードは、SES と Active Directory の両方でチェックされます。 ユーザーの ID は SES データベースに登録されているだけでなく、Windows ドメインでも有効である必要があります。
Access for Computer Users	
Allow PBConnex access for users assigned to device	このオプションを使用すると、AutoBoot はグループの設定ではなく、ユーザー/デバイスの関係に基づくことができます。

6.6. ユーザーのロック解除

① SES のメニューバーより、
[Tools] -> [Preboot Network(PBConnex)] -> [Reset User’s Failed Login]
をクリックします。

② 下記のような画面が表示されます。左ペインより、ロックされたユーザーが登録されているフォルダを展開し、該当ユーザーを選択します。右ペインにデバイス名とログイン失敗回数が表示されます。単一のデバイスでロックされた場合、左下にある <Reset> ボタンをクリックすると、ID のロックが解除されます。



ロック解除については、下記のテーブルを参照してください。

項　目	説　明
<Reset> Reset the selected user’s failed login on selected computer	単一のデバイスで、選択したユーザーのログイン失敗回数をリセットし、ロックを解除します。
<Reset User> Reset the selected user’s failed login on all computer	すべてのデバイスで、選択したユーザーのログイン失敗回数をリセットし、ロックを解除します。
<Reset All User> Reset all user’s failed login	すべてのユーザーのログイン失敗回数をリセットし、ロックを解除します

③ [Confirm: Reset failed login number on the selected computer to zero for the selected user?] というダイアログが表示されますので、<はい> をクリックします。

④ 右ペインに表示されていたデバイス名がクリアされます。該当ユーザーのロックが解除されているので、正しいパスワードでログインできるか確認します。

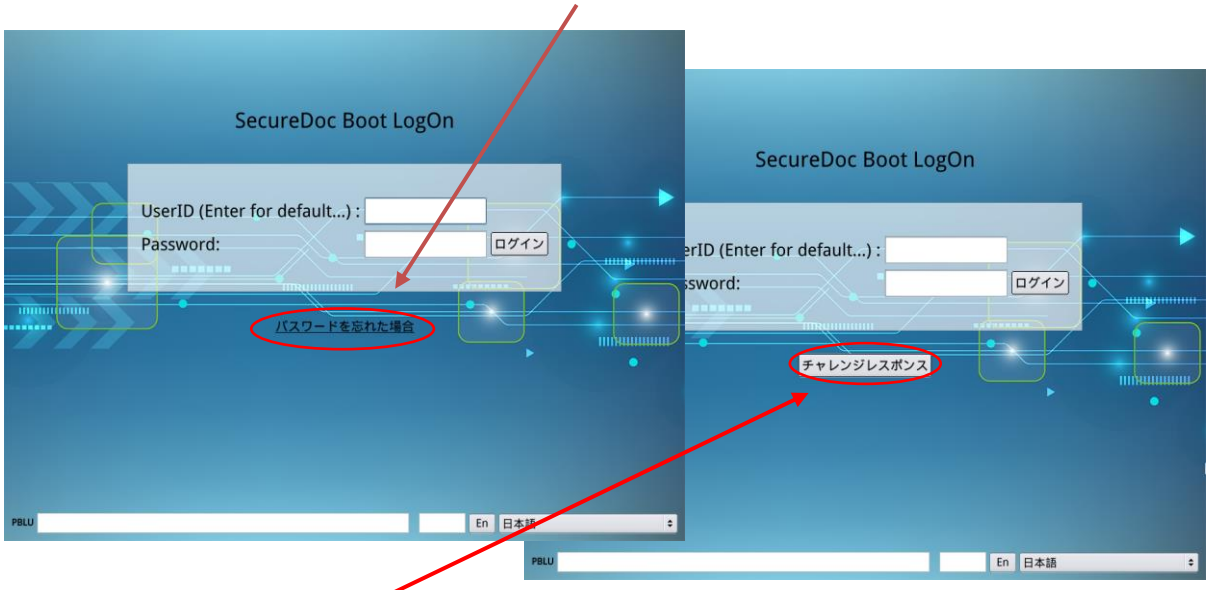
7. よくある質問と回答（SES）

7.1. ユーザーサポート

■ ユーザーのパスワード忘れへの対処方法（チャレンジレスポンス機能）

ユーザーがパスワードを失念してしまった場合、チャレンジ&レスポンス機能によって、リカバリが可能です。デバイスがネットワークに接続されている必要はなく、電話によるパスワードリカバリのサポートが可能です。

① ユーザーに、プリブート認証画面で、［パスワードを忘れた場合］をクリックするように伝えます。

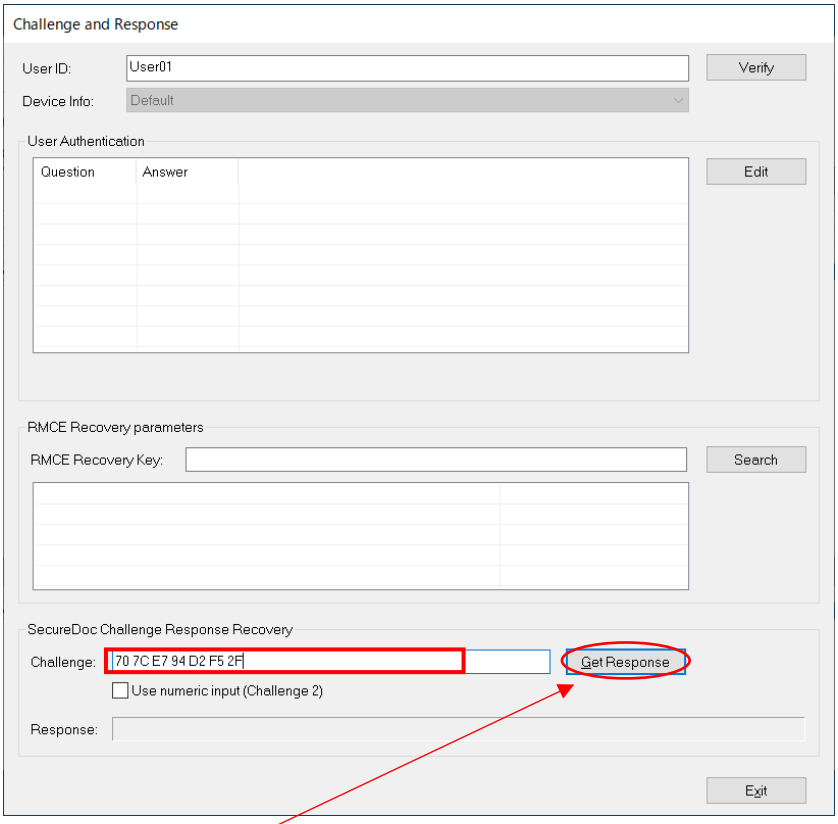


② 続けて<チャレンジレスポンス> ボタンをクリックしてもらい、チャレンジ値を表示させます。

③ SES 管理者は、ユーザーから、画面に表示されている「ユーザーID」を聞き、SES コンソールの［Users］タブで、その ID を探します。

④ 該当ユーザーを右クリックし、[Challenge response] をクリックします。

⑤　チャレンジ&レスポンス画面が表示されます。②で表示されているチャレンジ値をユーザーに読み上げてもらい [Challenge] 欄に入力します。



⑥　続けて、<Get Response> ボタンをクリックすると、[Response] 欄にレスポンス値が表示されます。

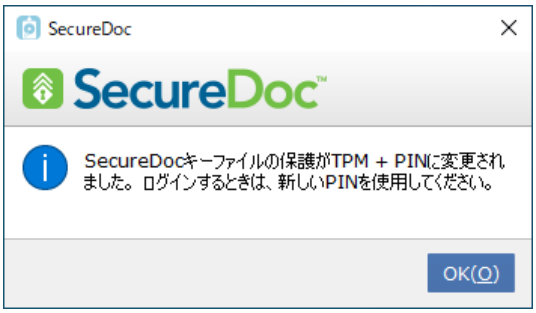
⑦　ユーザーにレスポンス値を伝え、入力後に <ログイン> をクリックしてもらいます。

⑧ Windows にサインインすると、パスワードあるいは PIN の変更を促すダイアログが表示されます。
<OK> をクリックします。

⑨ パスワードあるいは PIN を設定するための画面が表示されます。
ユーザー自身によって、新しいパスワードあるいは PIN を入力し、<OK> をクリックします。
ユーザーによる設定であり、管理者は関与しません。

※ 設定されている認証方法によって、表示される画面が異なります。

⑩ パスワードが変更されたというダイアログメッセージが表示されますので、<OK> をクリックします。
次回ログイン時より、新しいパスワードを入力します。



※ 設定されている認証方法によって、表示される画面が異なる場合があります

■ パスワードの誤入力を繰り返し、ロックされてしまいました

ユーザーがパスワードを失念してしまった場合と同じ「チャレンジ&レスポンス機能」を使うことで、リカバリが可能です。パスワードの再設定と、正しい時刻に修正してください。

■ UEFI/BIOS の時刻ずれが原因で、ロックされてしまいました

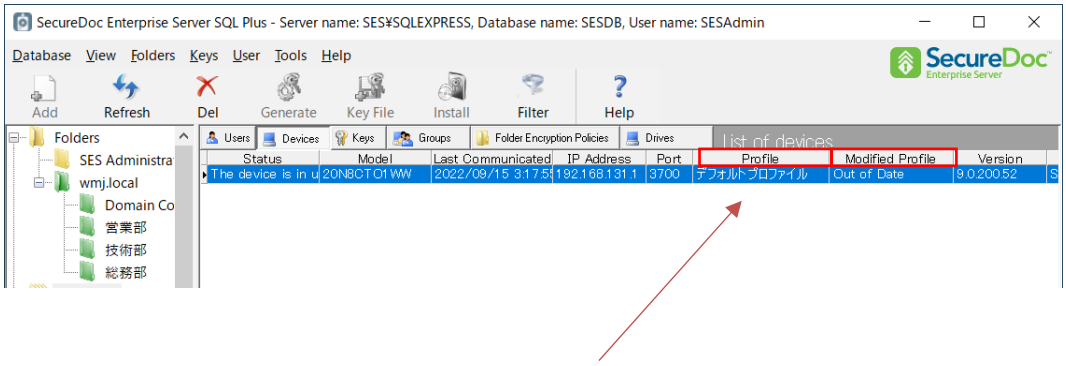
時差を超えて大幅に時刻がずれると、SecureDoc は不正な行為とみなして、ユーザーID をロックします。
時刻ずれによるロックの場合、ユーザーがパスワードを失念してしまった場合と同じ「チャレンジ&レスポンス機能」を使うことで、リカバリが可能です。パスワードの再設定と、正しい時刻に修正してください。

7.2. SecureDoc クライアントデバイスの管理

■ デバイスに適用されているプロファイルを確認したい

SES コンソールでは、それぞれのクライアントデバイスに適用されているプロファイルを確認できます。SES で既存プロファイルの設定を変更した場合、それぞれのクライアントデバイスに適用されているプロファイルが変更前のものか、変更後のものかも SES コンソールで確認できます。

SES の [Devices] タブで、確認したいデバイスを選択します。



[Profile] のタブに表示されてプロファイル名が現在クライアントデバイスに適用されているプロファイルです。

[Modified Profile] のタブに表示される内容については、下記のとおりです。

「Up to Date」 ： SES にあるプロファイルと同じ最新のものが適用されています。

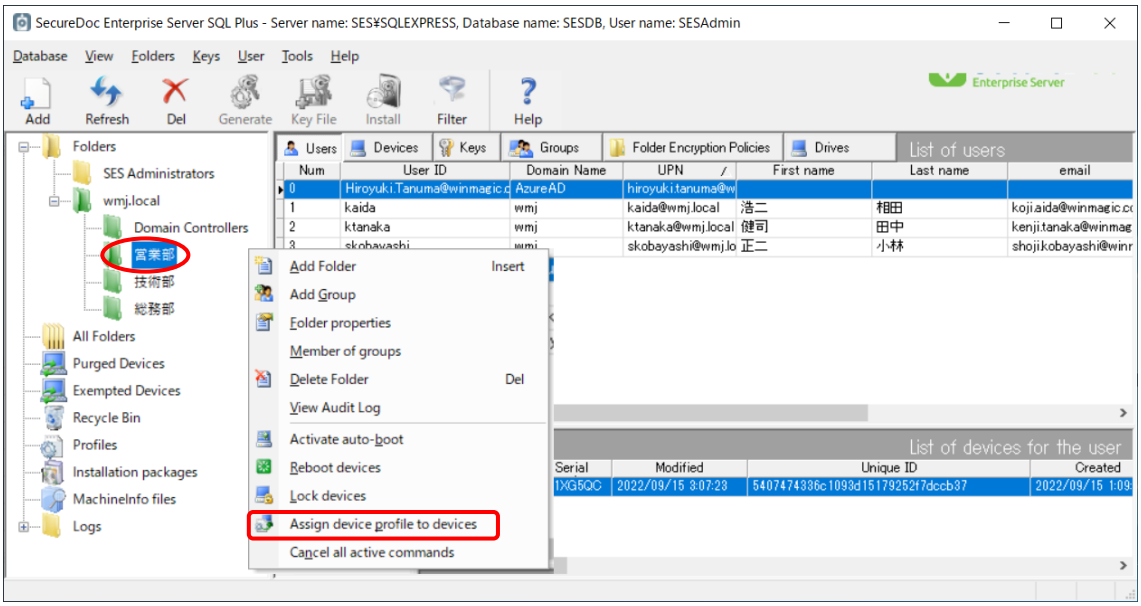
「Out of Date」： SES にあるプロファイルよりも古いプロファイルがそのデバイスには適用されています。
SES 上でプロファイルを更新したが、それがクライアントに適用されていない状態です。
プロファイルの設定を何も変更していない場合でも、プロファイルで <Save> をクリックすると、クライアントに適用されているプロファイルとは作成日時が異なるので「Out of Date」なります。

■ デバイスに適用しているプロファイルを変更したい（フォルダ単位）

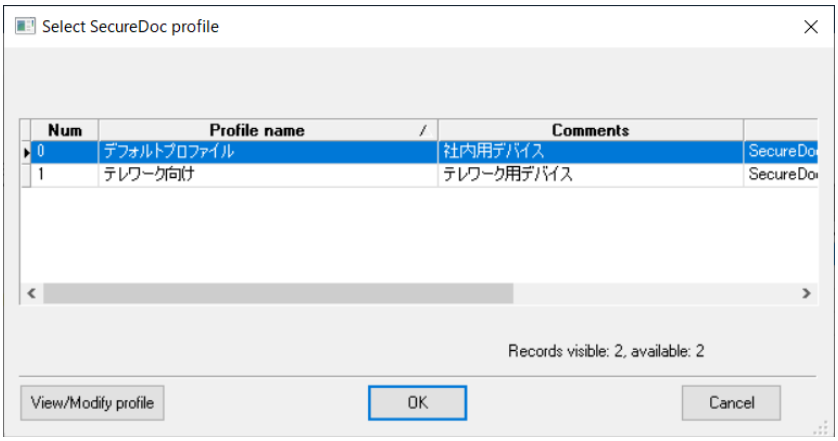
フォルダに所属しているデバイス全てに、別のプロファイルの適用や、変更した既存のプロファイルを更新する場合

※ フォルダ単位で、そこに所属しているデバイスは全て同じプロファイル設定を使用する場合の変更方法です。

① SES の左ペインより、プロファイルを変更したいデバイスが所属するフォルダを選択後、マウスのコンテキストメニューから、[Assign device profile to devices] をクリックします。



② プロファイル選択画面が表示されます。適用したいプロファイルを選択し、<OK> ボタンをクリックします。

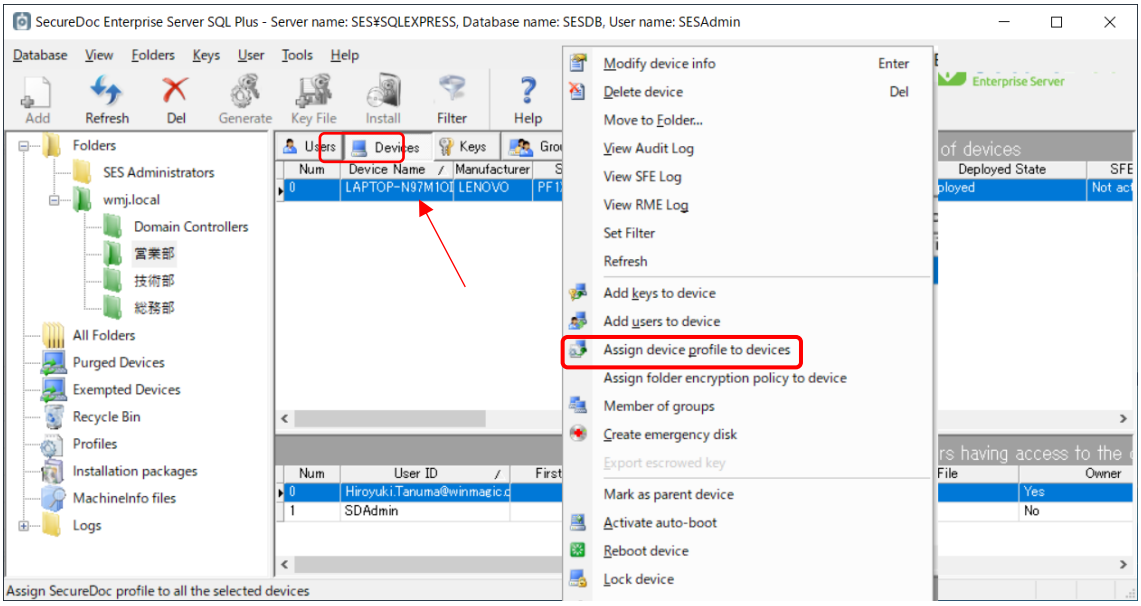


③ フォルダ内の SecureDoc クライアントは、次回、SDConnex との通信時にプロファイルを受け取ります。

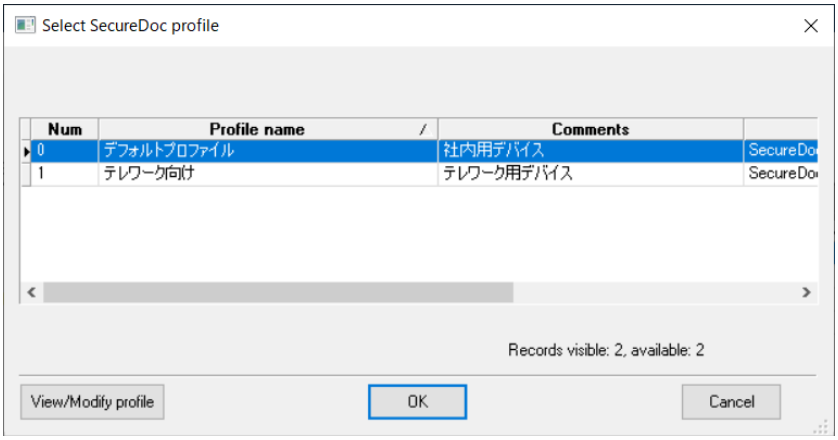
■ デバイスに適用しているプロファイルを変更したい（デバイス単位）

デバイス単位で、別のプロファイルを適用したり、変更した既存のプロファイルを適用したりする場合

① SES の [Devices] タブで、プロファイルを変更したいデバイスを選択後、マウスのコンテキストメニューから、[Assign device profile to devices] をクリックします。



② プロファイル選択画面が表示されます。適用したいプロファイルを選択し、<OK> ボタンをクリックします。



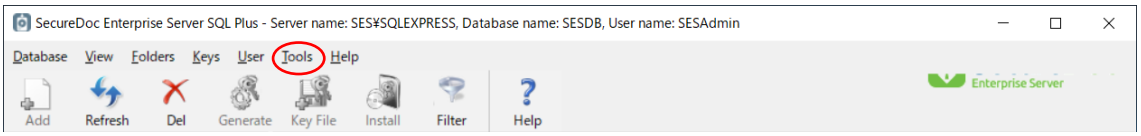
③ SecureDoc クライアントは、次回、SDConnex との通信時にプロファイルを受け取ります。

■ デバイスに適用しているプロファイルを自動で更新したい（全デバイス）

クライアントデバイスに適用済プロファイルを SES で設定変更した場合、該当する全クライアントデバイスのプロファイルを自動で更新させる場合

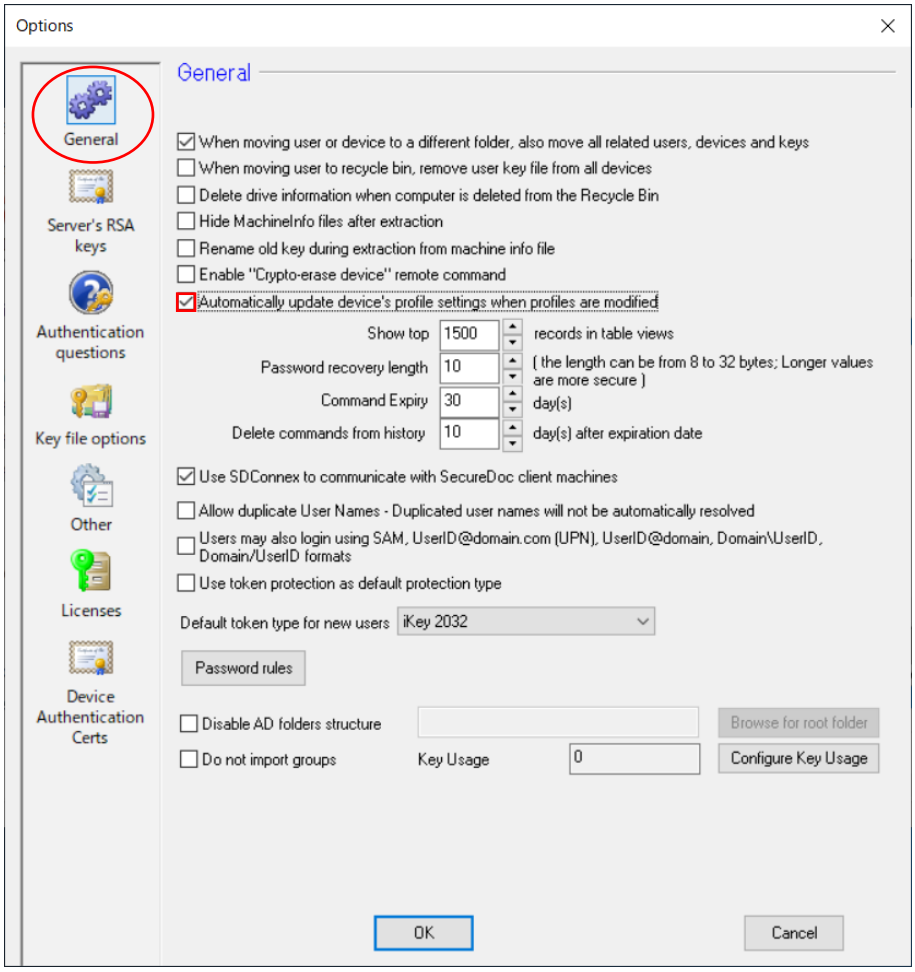
注　設定変更する前のプロファイルが適用されている全てのデバイスに影響があるので、十分な注意が必要です。

①　既存のプロファイルを設定変更する前に、次の設定をおこないます。
SES のメニューバーから、[Tools] -> [Options] を実行します。

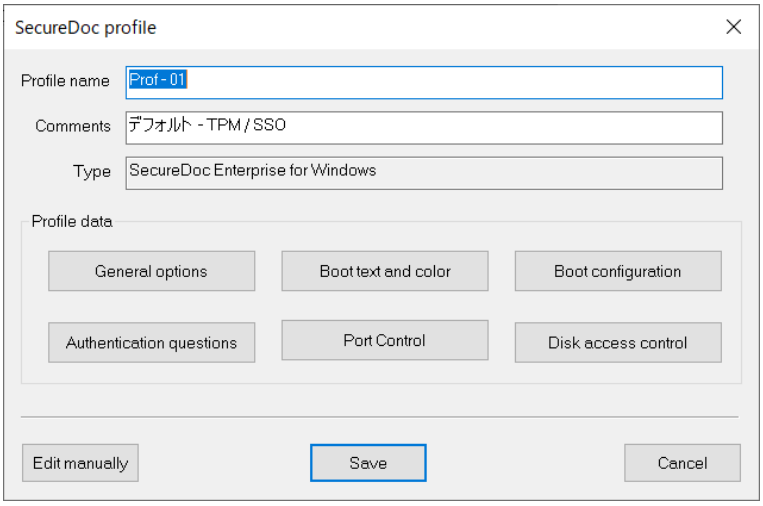


②　[General] を開きます。

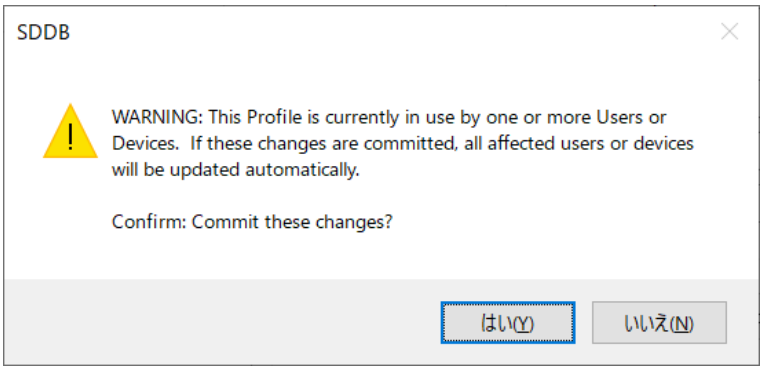
「☐ Automatically update device’s profile settings when profile are modified」にチェックを入れ、<OK> をクリックします。



③　既存のプロファイルを設定変更したら、<Save>をクリックします。



④　このプロファイルは、既にエンドユーザーのデバイスで使われているので、次のように更新確認のアラート画面が表示されます。
<はい>をクリックします。



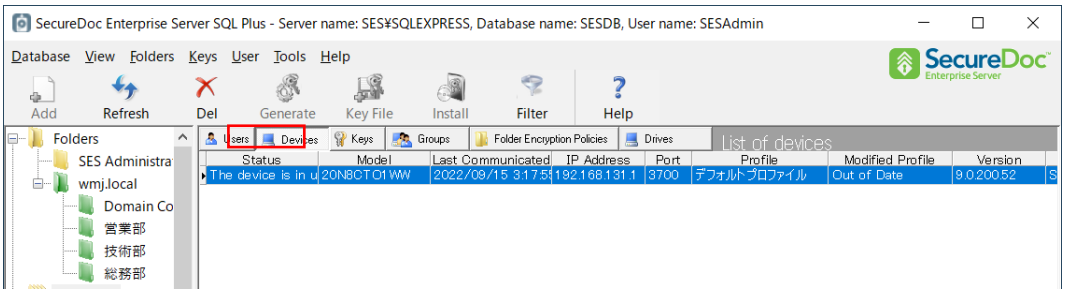
※　「☐ Automatically update device’s profile settings when profile are modified」にチェックを入れていないデフォルトの設定では、プロファイルの設定を変更して<Save>をクリックしてもこのアラートは表示されず、クライアントデバイスに適用されているプロファイルは自動で更新されません。

⑤　SecureDoc クライアントは、次回、SDConnex と通信した際に更新されたプロファイルを受け取ります。

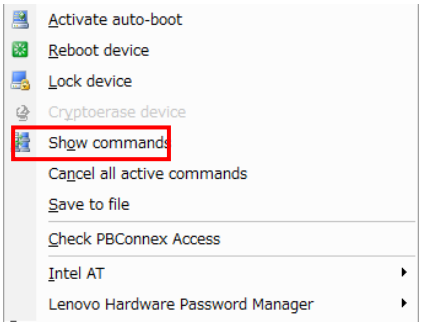
■ SES でクライアントデバイスにおこなった操作の結果を確認したい

管理者が SES コンソールで、クライアントデバイスのプロファイル変更や、ユーザーを追加した場合など、クライアントデバイスに対しておこなった操作の結果を確認することができます。

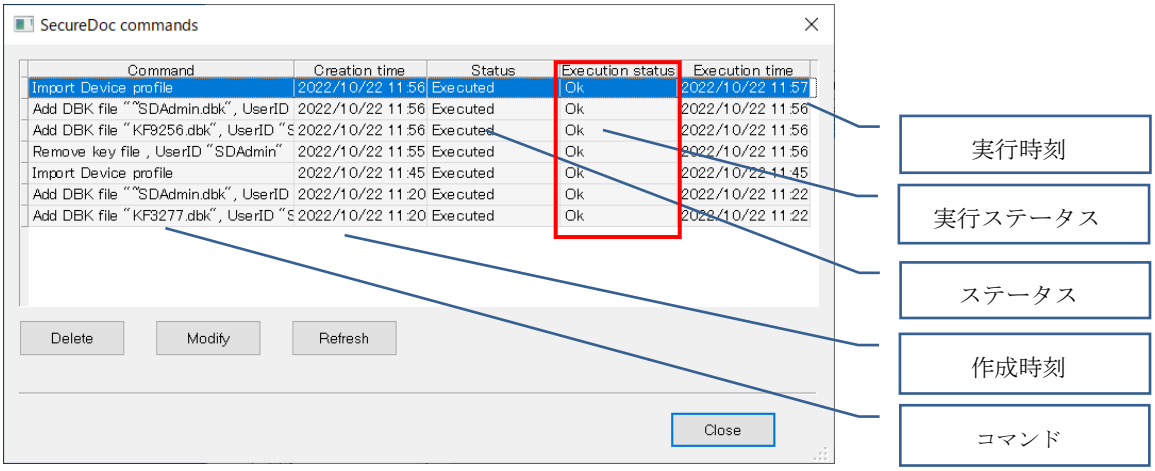
① SES の [Devices] タブで、確認したいデバイスを選択します。



② マウスの右クリックによるコンテキストメニューから、[Show commands] をクリックします。



③ コマンド一覧が表示されます。[Command] 欄にクライアントへのコマンドが表示されます。



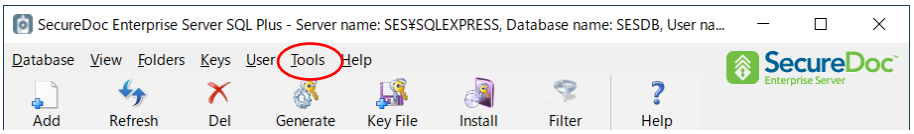
④ クライアントデバイスがコマンドを受け取り実行されると、[Status] 欄が「Executed」と表示され、そのコマンドの結果が成功すると、[Execution status] 欄に「OK」と表示されます。

⑤ ウィンドウを閉じるには、<Close> をクリックします。

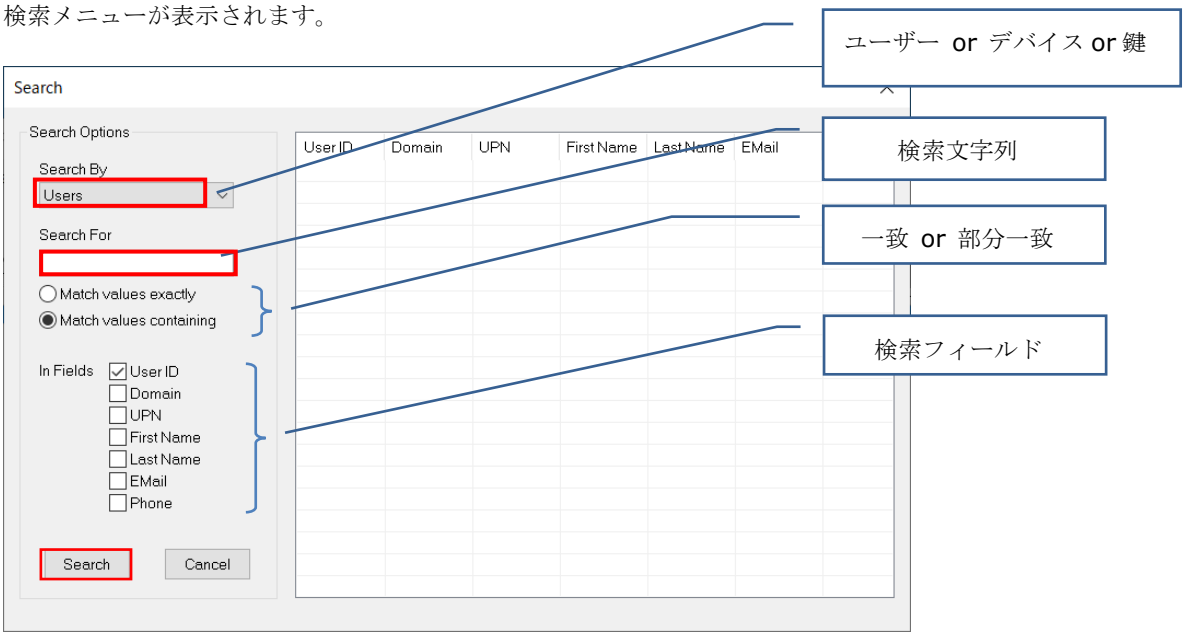
■ SES に登録されているユーザーもしくはデバイスを検索したい

[Search] 機能で、SES に登録されているユーザーやデバイスを検索できます。

① SES のメニューバーから、[Tools] -> [Search] をクリックします。



② 検索メニューが表示されます。



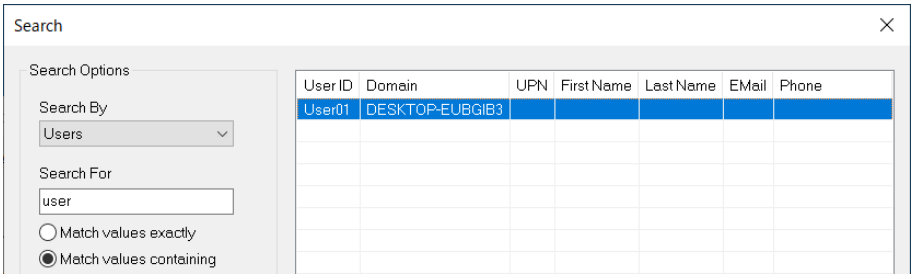
③ [Search By] 欄で、検索対象を [Users]、「Devices」、「Keys」から選択します。

④ [Search For] 欄に検索したい文字列を入力します。

⑤ 完全一致または部分一致を選択し、<Search> をクリックします。

- ○ Match values exactly ・・・完全一致
- ○ Match values containing ・・・ 部分一致

⑥ 下図のように、検索結果が表示されます。

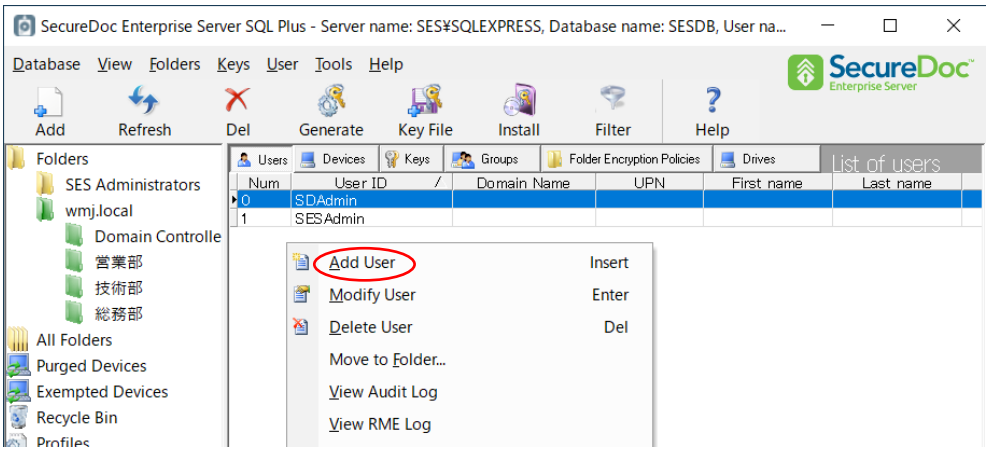


⑦ 表示された、例えばユーザーをダブルクリックすると、SES の右ペインに検索結果が表示されます。
[x] ボタンをクリックして、検索ボックスを閉じます。

■ クライアントデバイスに管理者権限ユーザーを追加したい

① 事前に管理者権限ユーザーを作成します。

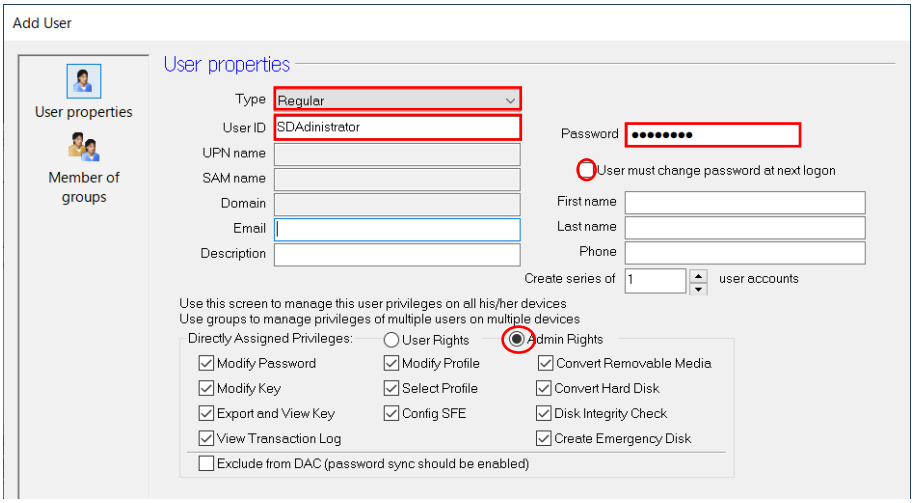
左ペインで登録するフォルダを選んだ後、右ペインの上でマウスの右クリックでコンテキストメニューを表示し、[Add User] をクリックします。



② Type は、「Regular」を選び、User ID と Password を入力します。

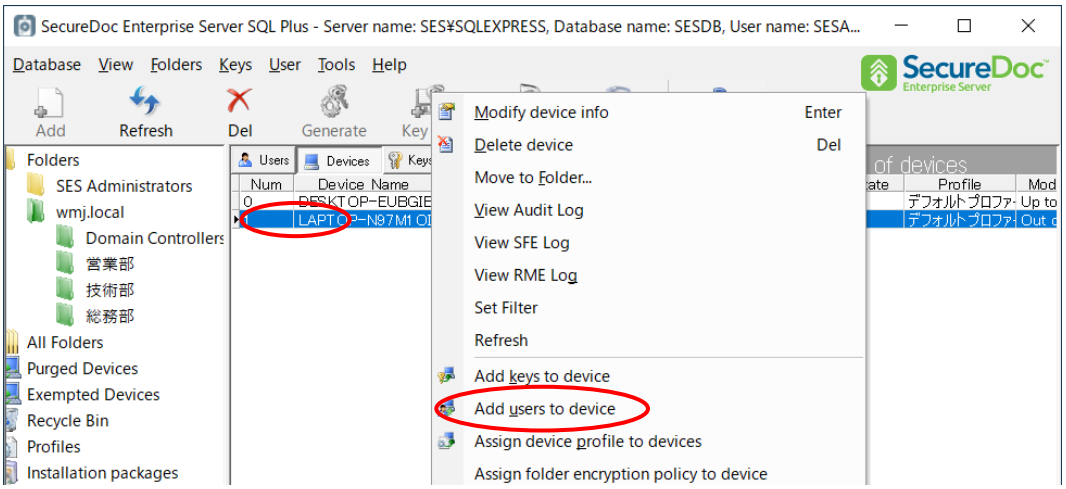
「☐User must change password at next logon」は、パスワードの変更要求です。
変更を望まない場合はチェックを外します。

権限設定で、「Admin Rights」を選びます。

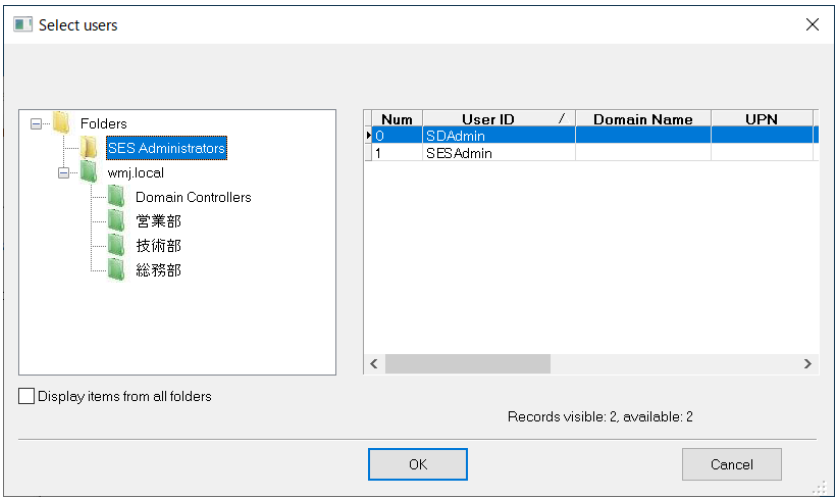


デバイス単位で、管理者ユーザーを追加する場合

① [Devices] タブから、該当デバイスを右クリックします。
コンテキストメニューから、[Add users to device] をクリックします。



② ユーザーの選択画面が表示されます。管理者権限ユーザーを選択し、<OK> をクリックします。



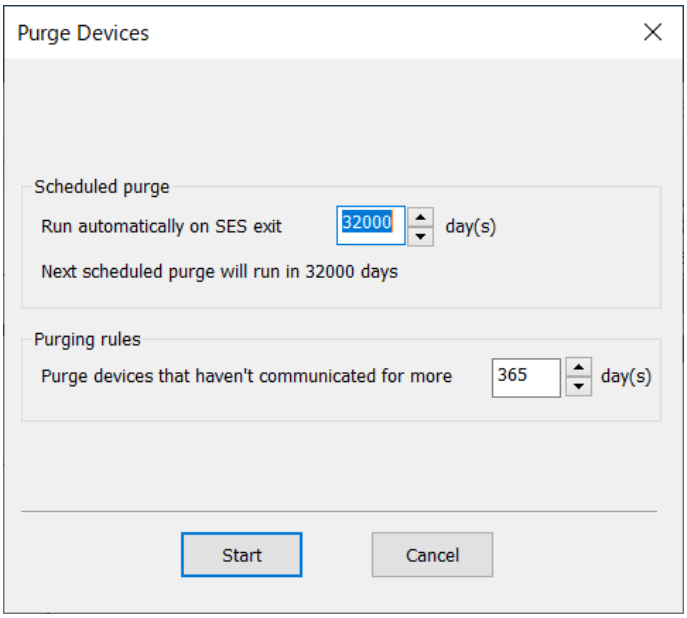
複数のデバイスに、管理者ユーザーを追加する場合

「SecureDoc Enterprise Server Version x.x クイックインストールガイド」
「12.8. フォルダの機能を使って管理者 ID の配備や共有鍵の追加」をご参照ください。

■ 長期間、通信していないデバイスを管理したい

指定した期間中に、デバイスが SDConnex と一度も通信されない場合、デバイスに通信していないフラグを立て、SES 管理コンソールの [Purged Devices] に移動します。
この機能により、紛失、盗難、または再フォーマットされた可能性のあるデバイスを特定できます。
[Purged Devices] 内のデバイスは、SecureDoc ライセンスを使用していないと見なされ、他のデバイスのためにそれらのライセンスを解放します。

① SES のメニューバーより、[Tools] -> [Purge Devices] をクリックします。
Purge Devices の設定画面が表示されます。



② 下記のテーブルを参照して設定してください。

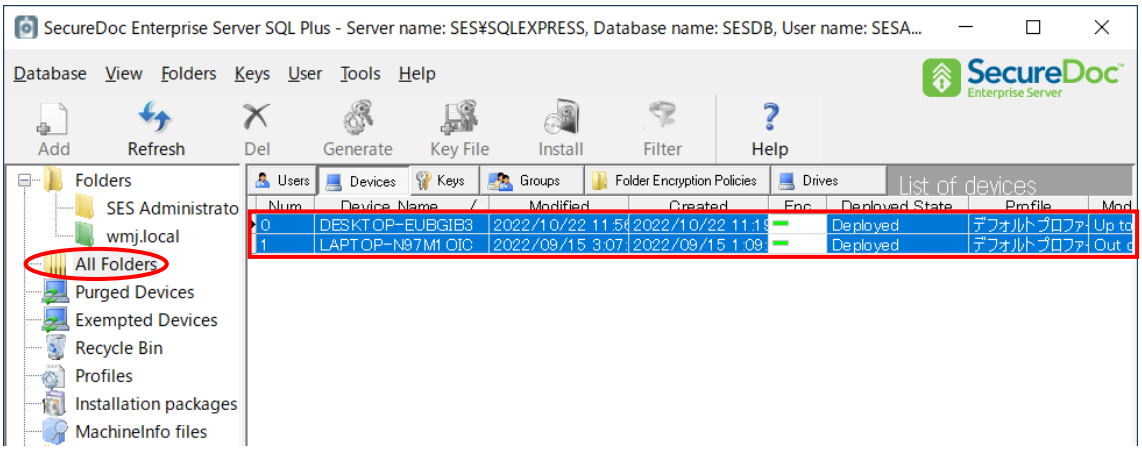
項　目	説　明
Scheduled purge	
Run automatically on SES exit X day(s)	SES コンソールの終了時、 XX 日毎にパージを実行するようにスケジュールします。
Purging rules	
Purge devices that haven’t communicated for more the X day(s)	X X 日以上通信していないデバイスを Purge Device フォルダへ移動します。
<Start>ボタン	開始します。

※ デバイスが Purge Device として識別されたが、その必要がない場合、そのデバイスを復元できます。
[Purge Devices] からデバイスを右クリックし、[Restore selected device(s)] をクリックします。
復元されたデバイスは、ライセンスの使用を再開します。

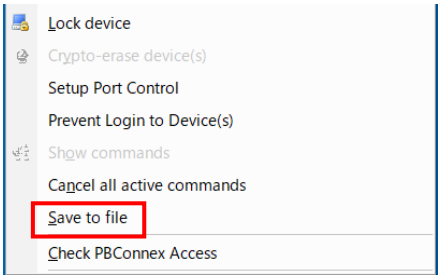
■ SES から各種一覧を出力したい

SES より、ユーザーやデバイス情報などの一覧を出力することができます。

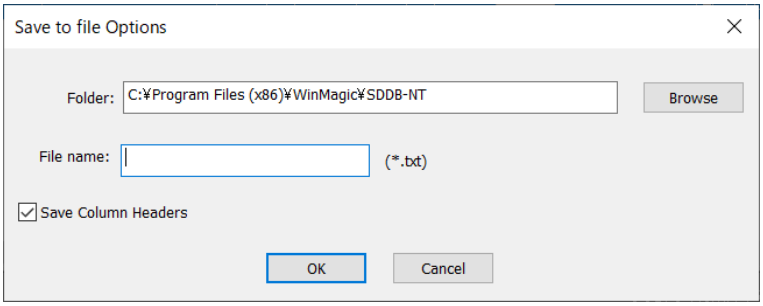
① SES の左ペインより、出力したい情報が含まれるフォルダをクリックします。次に、出力したい情報が含まれるタブ（ここでは、[Devices] タブ）をクリックします。出力したい行を選択します。



② 出力したい行を選択した状態で、右クリックして、コンテキストメニューから [Save to file] をクリックします。



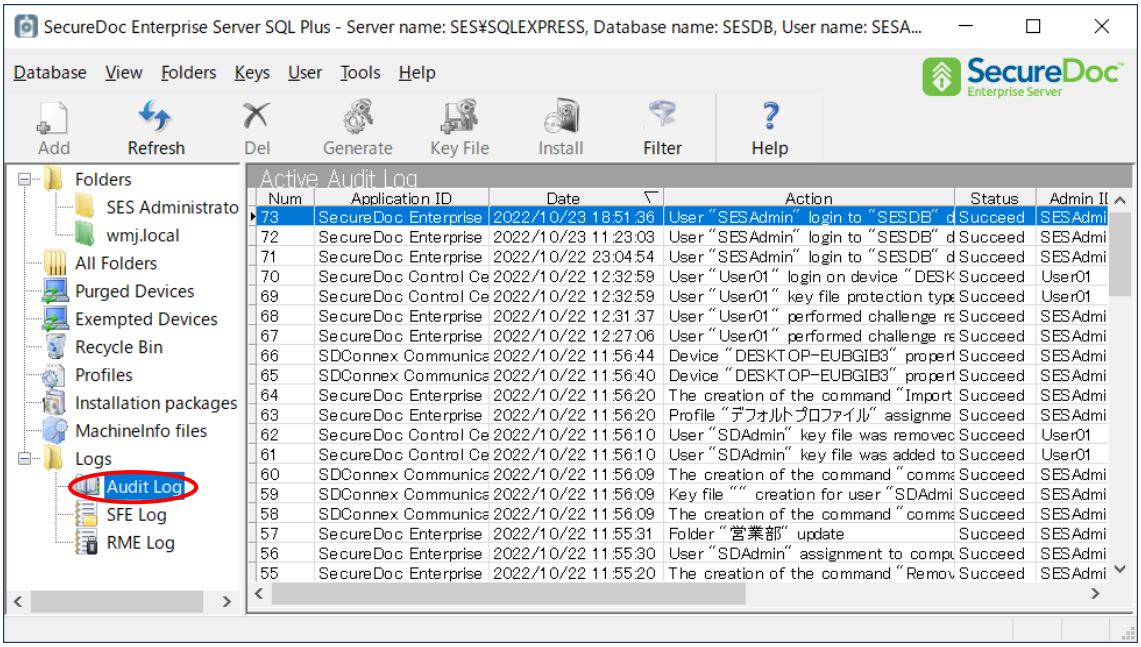
③ 保存先と選び、ファイ名を入力して <OK> をクリックします。



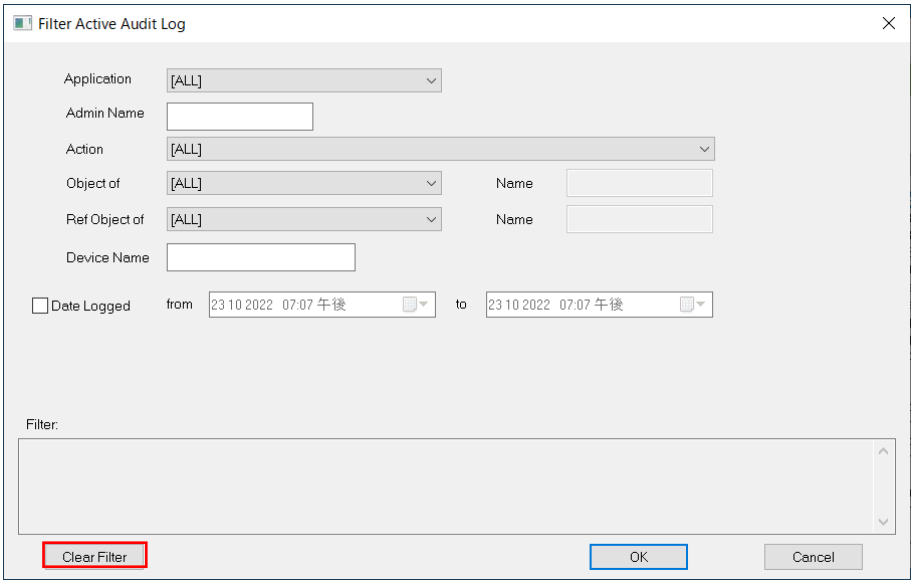
■ 監査ログを確認したい

SES 左ペインの [Audit Log] では、クライアント及び SES の操作ログが保存されます。

① SES の左ペインより、[Audit Log] アイコンをクリックします。右ペインにログが表示されます。



② 画面上部のメニューバーより、<Filter> 機能を使用すると、ログを選別することができます。



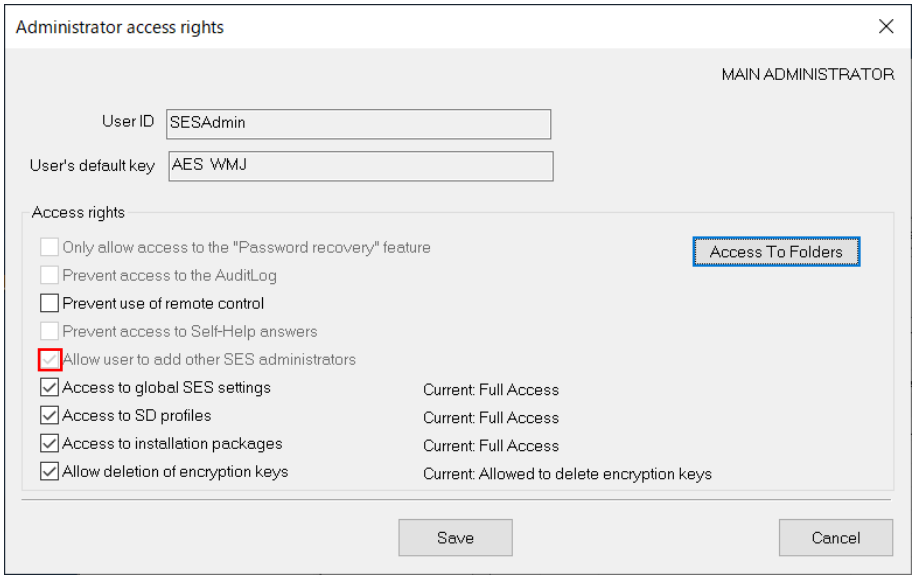
③ [Application] 欄から「SecureDoc Control Centre」を選択した場合、「暗号化完了」や「ログオン失敗」といったイベントが抽出されます。

注 <Clear Filter> をクリックするまで、SES コンソールの表示はフィルター機能によって条件が設定されたままになっていることに注意してください。

■ SES 管理者 ID を追加したい　（例：パスワードリカバリのみの管理者）

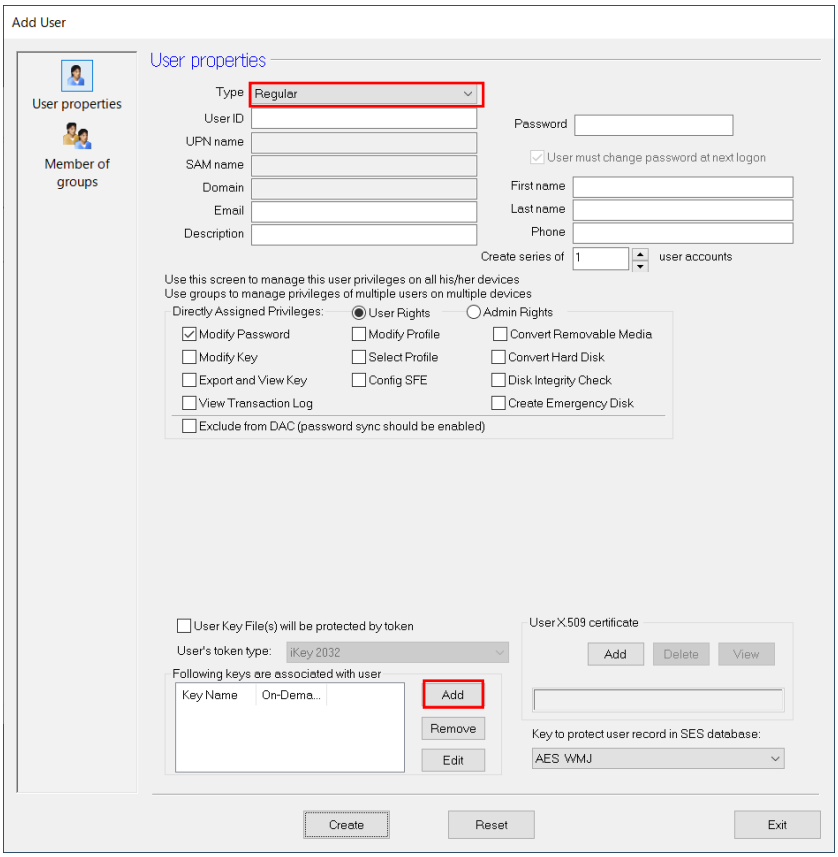
主とする SES 管理者以外に、別の管理者を作成することができます。
パスワードリカバリのみを実施できる管理者、特定のフォルダのみの管理者などを作成することができます。

注　条件として、SES インストール後の、最初の管理者キーファイルを作成する際に、
「☑ Allow user to add other SES administrators」にチェックを入れており、別の SES 管理者作成の権限を持っている必要があります。この設定がされていない場合、別の SES 管理者を作成することができません。

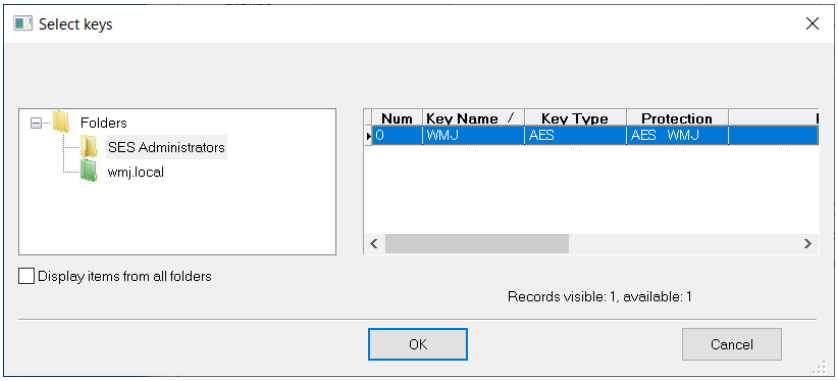


① SES の左ペインより、[SES Administrators] フォルダを選択します。
[Users] タブで、ツールバーの [Add] をクリックして、新規にユーザーを作成します。

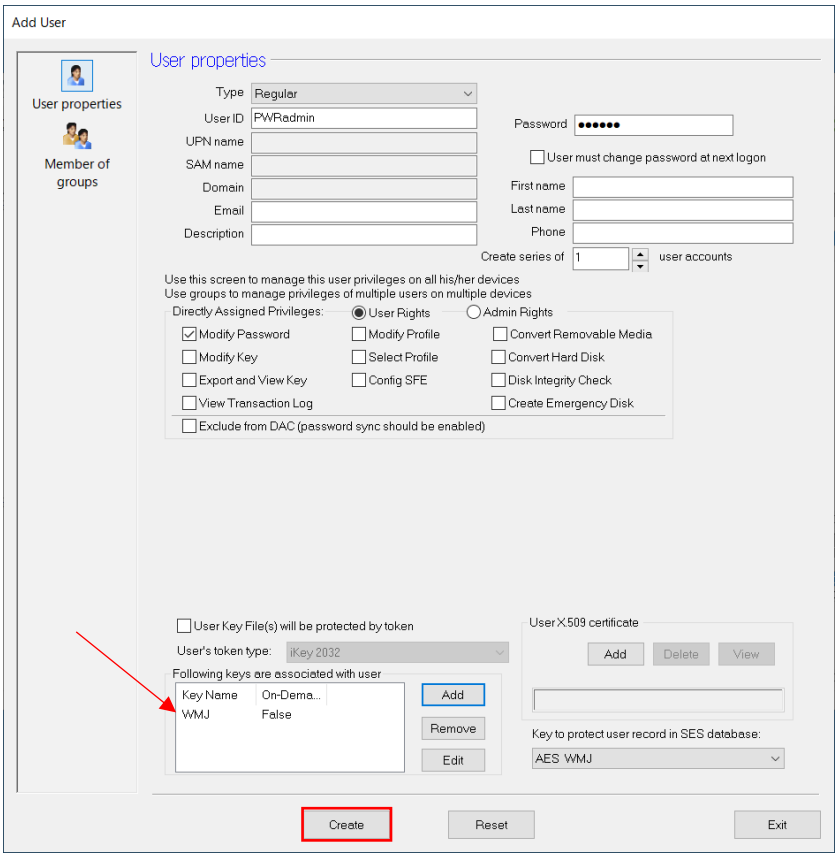
② ユーザーのプロパティ画面が表示されます。
[Type] は、Regular を選択し、[User ID] と [Password] を入力します。
[Following keys are associated with user] 欄で、<Add> をクリックします。



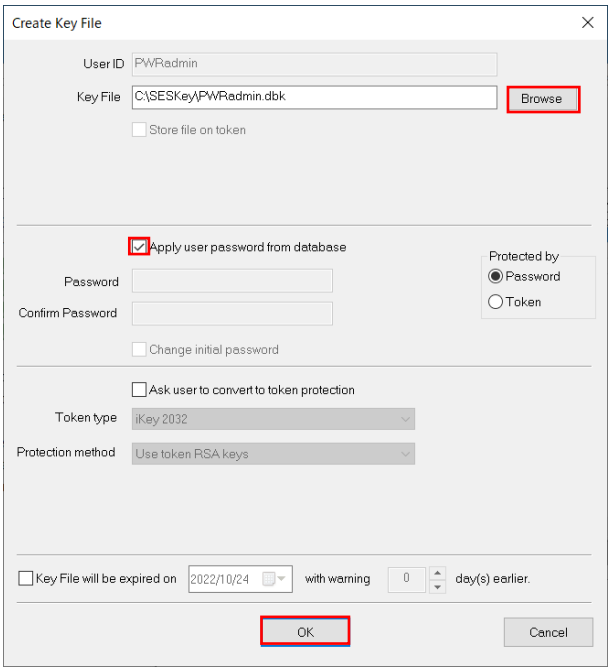
③ [SES Administrators] フォルダにある SES の鍵を選択して、<OK> をクリックします。



④　鍵が追加されたことを確認して、<Create> ボタンをクリックします。

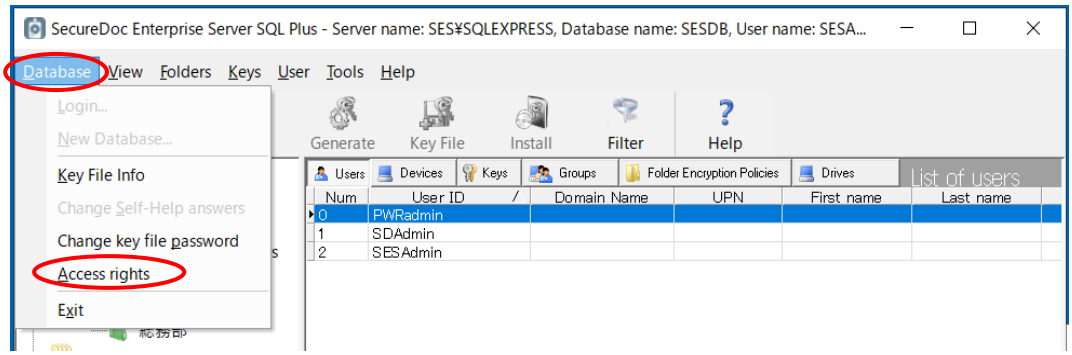


⑤　作成したユーザーを右クリックして、コンテキストメニューから [Create Key File] をクリックします。<Browse>ボタンをクリックしてキーファイルの保存場所を指定します。パスワードは DB に設定済のものをそのまま使用するために、「☐ Apply use password from database」をチェックし、<OK> をクリックします。

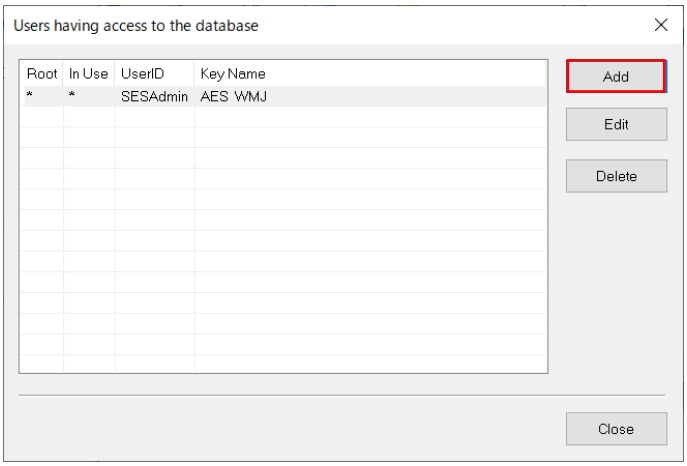


⑥　「Key File successfully created.：（キーファイルが作成された）というダイアログが表示されますので、<OK>　をクリックします。

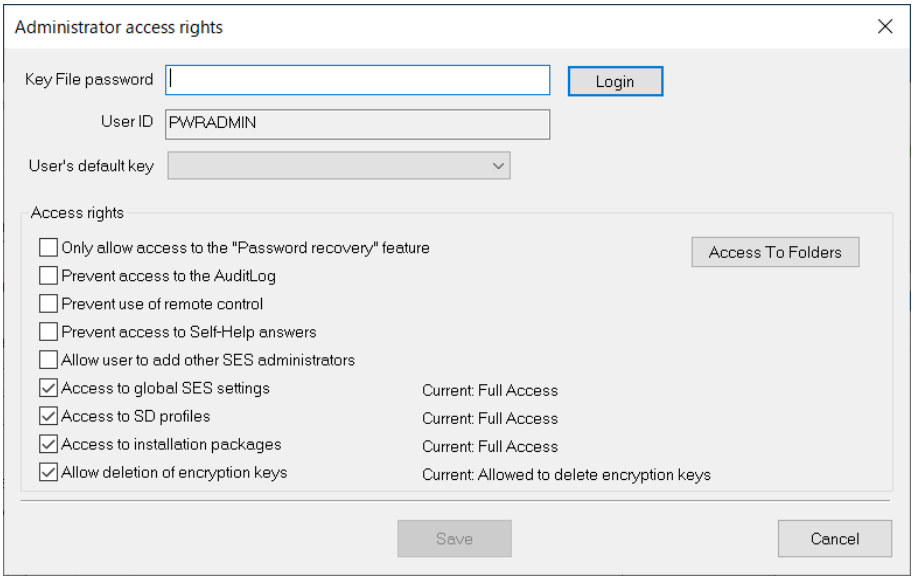
⑦ SES のメニューバーより、[Database] -> [Access rights] をクリックします。



⑧ <Add>ボタンをクリックし、先に作成したキーファイルを選択します。



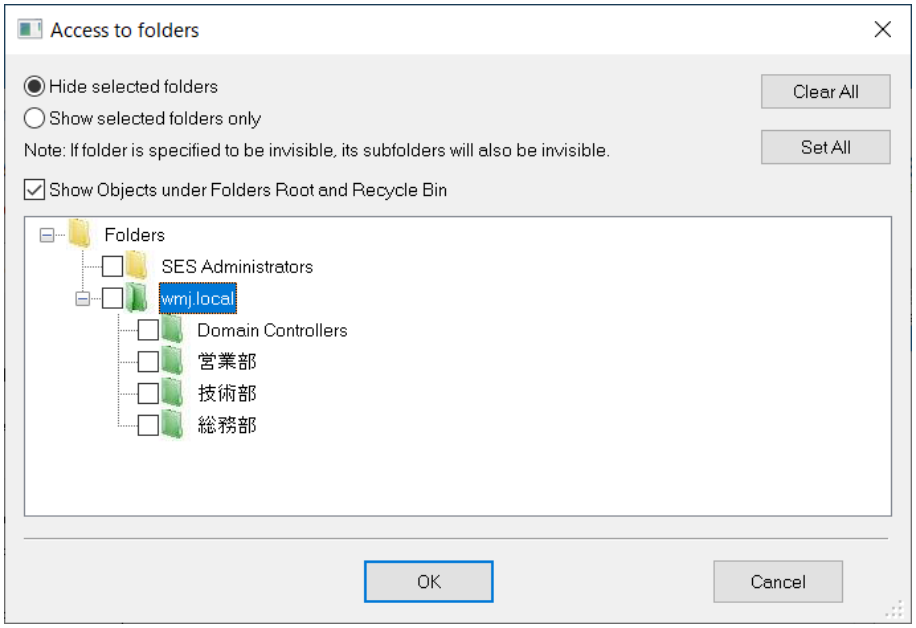
⑨ [Key file password] 欄にパスワードを入力して、<Login> をクリックします。
必要に応じて権限を制限した後、<Save> をクリックします。



権限の設定については、次のテーブルを参照してください。

項　目	説　明
Access rights	
◎ Only allow access to the “Password recovery” feature	パスワードリカバリ機能へのアクセスのみ許可
<Access to Folders>	アクセス可能とするフォルダを指定します。
☐ Prevent access to the Audit Log	[Audit Log] へのアクセスを制限
☐ Prevent user of remote control	リモートコントロールを制限
☐ Prevent access to Self-Help answers	「セルフヘルプの回答」へのアクセスを禁止 日本語環境では、ご使用いただけません
☐ Allow user to add other SES administrators	他の SES 管理者を作成・追加できるようにします。
☑ Access to global SES settings	グローバル SES 設定へのアクセス
☑ Access to SD profiles	[Profiles] へのアクセス
☑ Access to installation packages	[Installation packages] へのアクセス
☑ Allow deletion on encryption keys	鍵の削除を許可

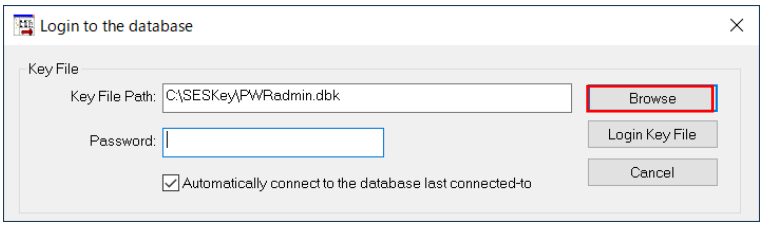
<Access to Folders> の設定について



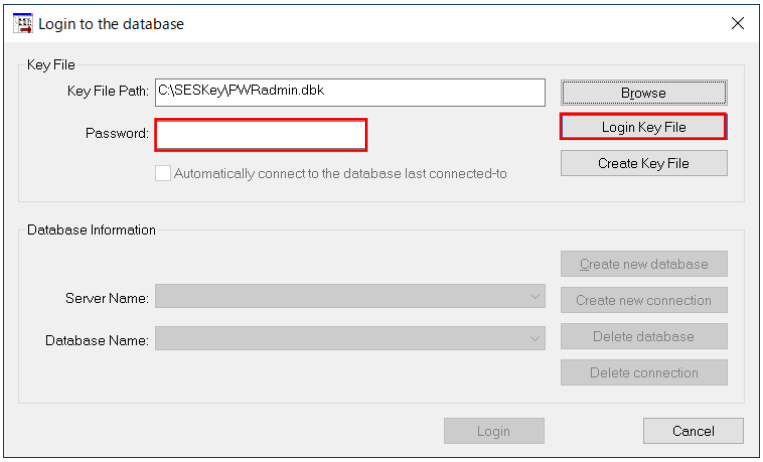
項　目	説　明
○ Hide selected folders	選択したフォルダをコンソールに表示しません。 アクセス不可とするフォルダを選択します。
○ Show selected folders only	選択したフォルダのみ表示し、アクセス可能
☐ Show objects under Folders Root and Recycle Bin	フォルダのルートと Recycle Bin の下にあるオブジェクトを表示します。

例：パスワードリカバリのみ のキーファイルを作成した場合

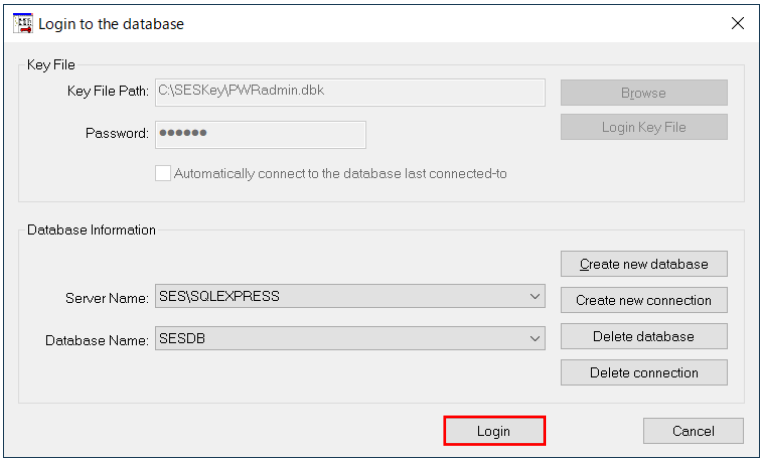
①　<Browse> をクリックして、先に作成したキーファイルを選択します。



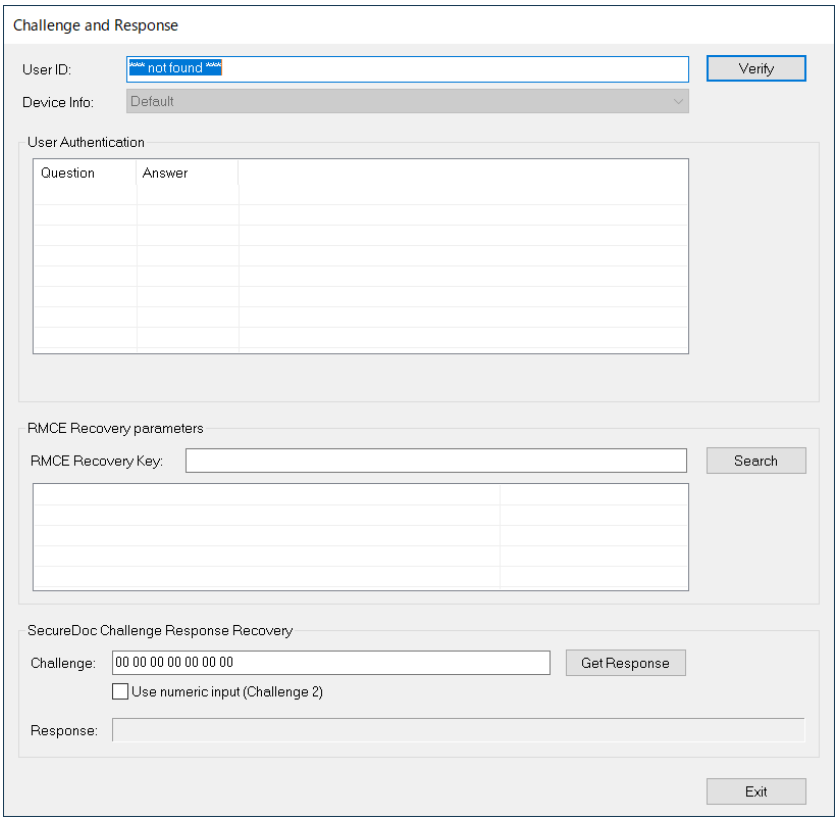
② 下記の画面が表示されたら、パスワードを入力し、<Login Key File> をクリックします。



③ <Login> をクリックします。



④　SES 管理コンソールは、チャレンジ&レスポンス 専用のコンソールとなります。



■　不要なライセンスを解放したい

SecueDoc をアンインストールせずに、OS をリカバリした場合、SES 上に OS リカバリ前のデバイス情報が残り、ライセンスが使用されたままの状態です。SES の［Device］ タブから古いデバイスを削除するとライセンスが解放されます。

①　SES の［Devices］タブから該当のデバイスを選び、右クリックします。コンテキストメニューから［Delete device］をクリックしてデバイスを削除します。

②　デバイスは、［Recycle Bin］に移動します。
ライセンスが解放されます。

■ クライアントの認証をシングルサインオンの設定にしたい

① 既存のプロファイルを編集するか、既存のプロファイルをコピーして新しくプロファイルを作成します。

② プロファイルで、Credential Provider を設定します。

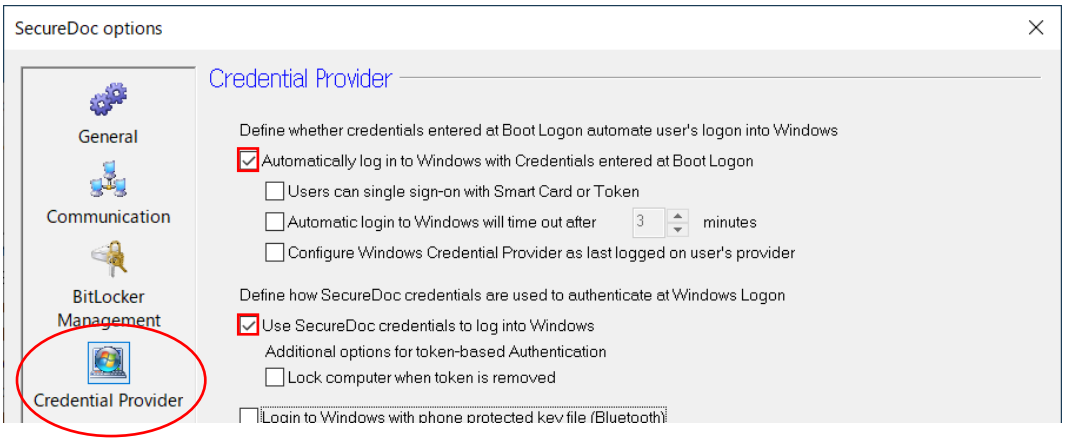
[General options] -> [Credential Provider]

「☐ Automatically log in to Windows with Credentials entered at Boot Logon」にチェックを入れます。

③ スクリーンロックからの解除に、SecueDoc Credential Provider を使う場合は、

「☐ Use SecureDoc Credentials to log into Windows」にチェックを入れます。

SecueDoc Credential Provider を設定すると、スクリーンロックの解除（Windows へのサインイン）には、SecureDoc プリブート認証で設定しているプリブート認証で許可されるログイン失敗回数の最大値が設定されます。



項　目	説　明
Define whether credentials entered at Boot Logon automate user’s logon into Windows	
☑ Automatically log in to Windows with Credentials entered at Boot Logon	プリブート認証での資格情報を使用して Windows に自動的にサインインします。
Define how SecureDoc credentials are used to authenticate ad Windows Logon	
☑ Use SecureDoc Credentials to log into Windows	SecureDoc Credential Provider を使用して Windows にサインインします。

プロファイルを保存します。

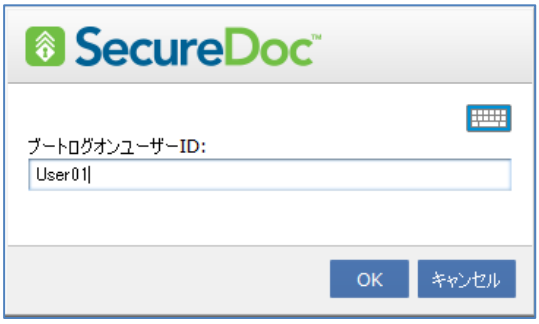
④ [Devices] タブで、目的のデバイスを右クリックし、コンテキストメニューから [Assign device profile to devices] をクリックします。プロファイル一覧が表示されるので、先に作成したプロファイルを選択し、<OK> をクリックします。

※ フォルダに対してプロファイルをアサインすることも可能で、フォルダ内の全てのデバイスに適用されます。

⑤ クライアントデバイスは、定期的な通信で、SDConnex を介して、プロファイルを受け取ります。

⑥ 次回、プリブート認証を通過すると、シングルサインオンの設定により、Windows へ自動でサインインとなります。

⑦ 「☐ Use SecureDoc Credentials to log into Windows」にチェックを入れていた場合、スクリーンロックの解除時には、最初に ID の確認画面が表示されます（複数のユーザーID が登録されている場合）。



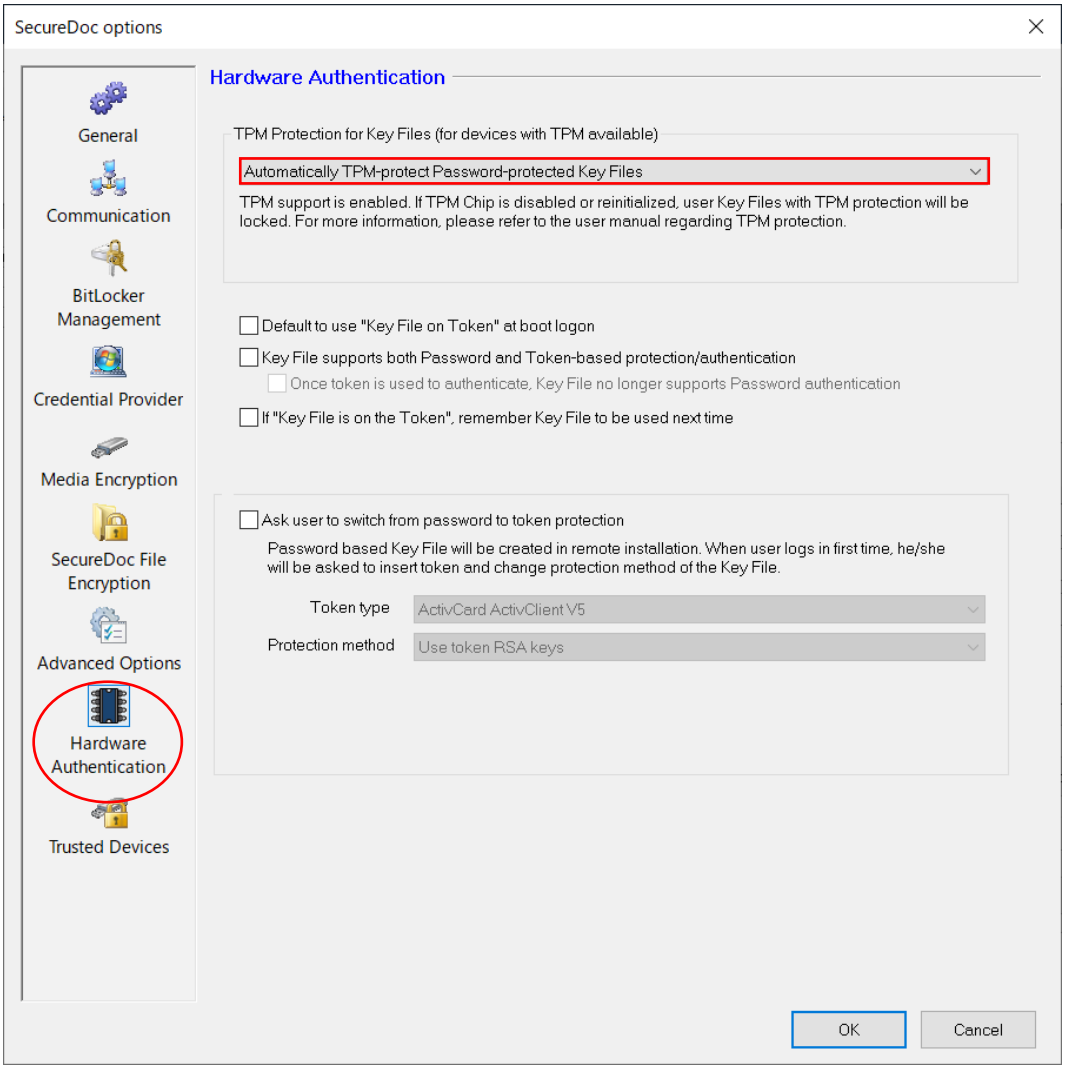
⑧ <OK> をクリックすると、画面が変わり、パスワードを求められます。
このパスワードは SecureDoc プリブート認証と同じパスワードです。正しいパスワードを入力して <ログイン> をクリックすると、Windows へサインインできます。

■ TPM によって、デバイスのセキュリティを高めたい

TPM を使うとデバイスと紐づけられ、ストレージをデバイス本来から抜かれた場合のセキュリティ保護が可能です。

① 既存のプロファイルを編集するか、既存のプロファイルをコピーして新しくプロファイルを作成します。
TPM の設定が含まれるプロファイルを全てのクライアントに適用した場合、UEFI / BIOS で TPM が有効になっていないデバイスでは、TPM の設定は無視され、エラーとはなりません。

② プロファイルで、TPM の使用を設定します。
[General options] -> [Hardware Authentication]
[TPM Protection for Key Files (for devices with TPM available)] の設定項目で、プルダウンメニューから「Automatically TPM-protect Password-protected Key Files」を選択します。



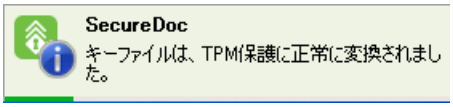
プロファイルを保存します。

設　定	説　明
TPM Protection for Key Files (for devices with TPM available)	
・Do not use TPM	・TPM を使用しません。
・Automatically TPM-protect Password-protected Key Files	・パスワードで保護されたキーファイルを自動で TPM 保護に切り替えます。
・Create Key files protected by TPM and PIN instead of a password	・パスワードの代わりに TPM と PIN で保護されたキー ファイルを作成します。

③　[Devices] タブで、目的のデバイスを右クリックし、コンテキストメニューから [Assign device profile to devices] をクリックします。プロファイル一覧が表示されるので、先に作成したプロファイルを選択し、<OK> をクリックします。

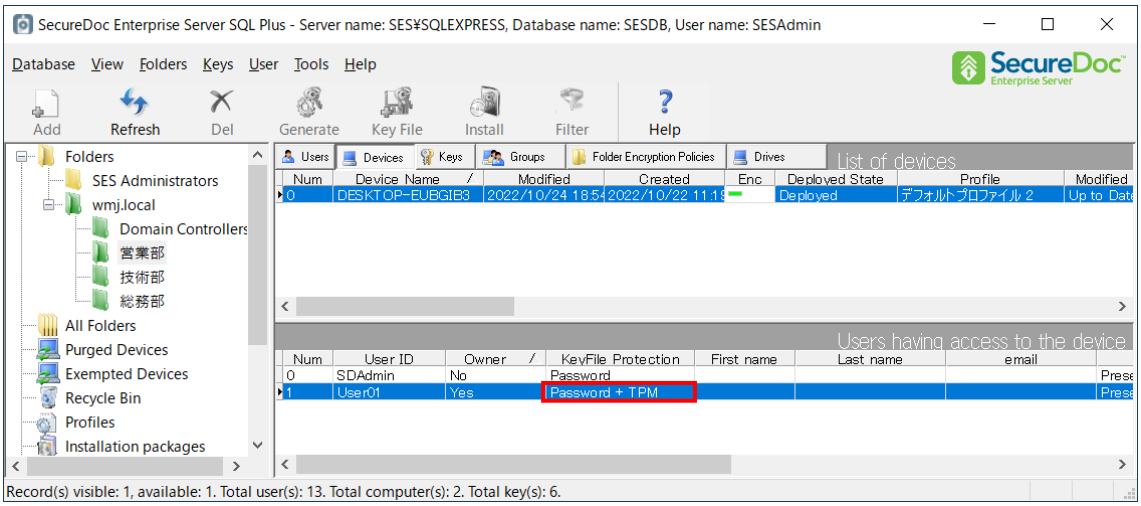
④　クライアントデバイスは、定期的な通信で、SDConnex を介して、プロファイルを受け取ります。

⑤ 次回、プリブート認証を通過し、Windows サインインの後に「キーファイルは TPM 保護に正常に変換されました」と表示されます。



ユーザーのキーファイルは、パスワード保護から TPM 保護に切り替わりましたが、ユーザーがおこなうプリブート認証での方法や入力するパスワードに変わりはありません。

⑥ クライアントで、プリブート認証を PIN で認証し、Windows にサインイン後、SDConnex と通信すると、クライアントの情報が SES に送られます。SES の [Devices] タブより、該当ユーザーの [KeyFile Protection Type] 欄を確認すると、「Password + TPM」と表示されており、TPM で保護されていることが確認できます。



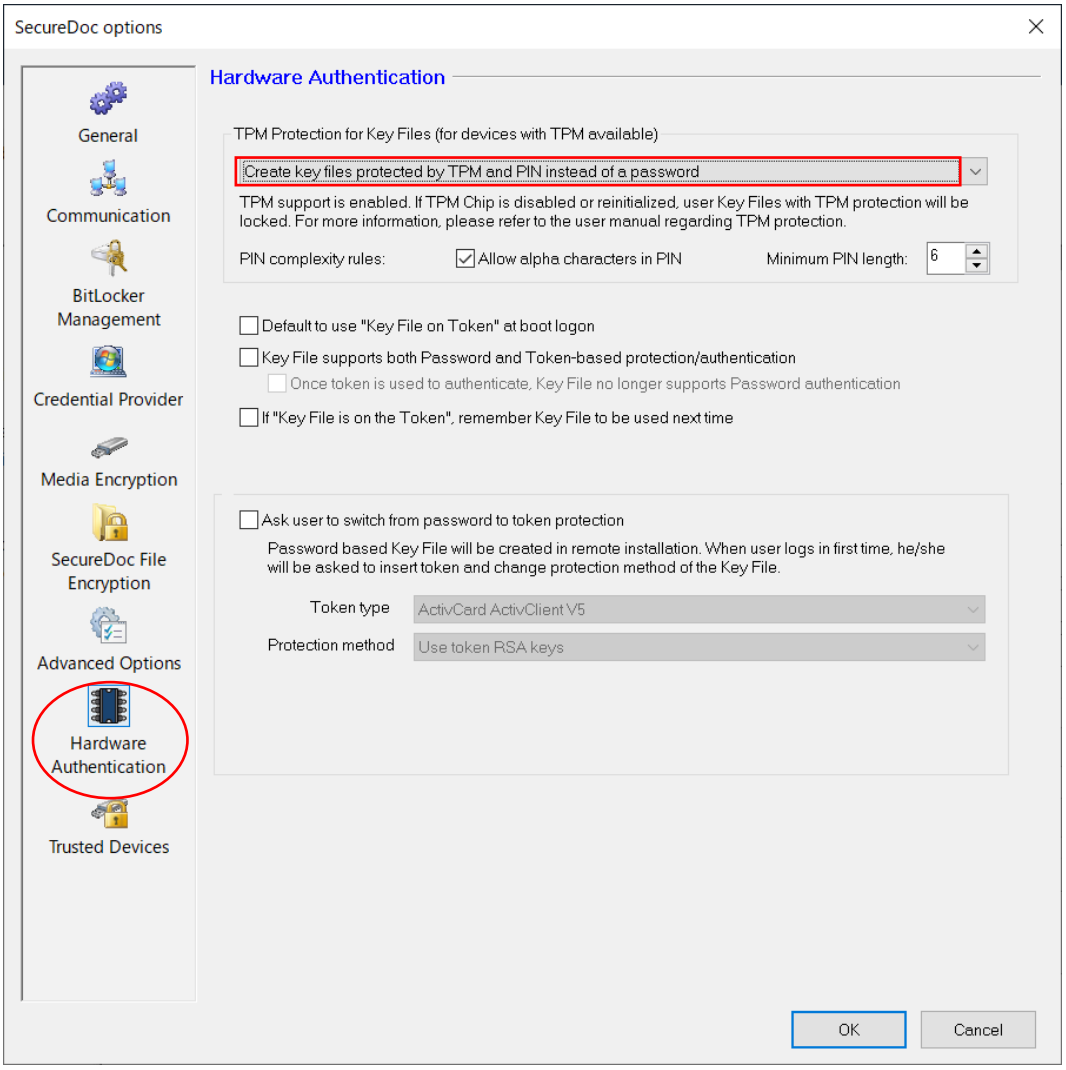
注 デバイスの UEFI/BIOS 設定で、TPM を無効あるいはクリアすると、プリブート認証で正しい ID/パスワードを入力してもログインできなくなります。

■ TPM+PIN によって、デバイスのセキュリティを高めたい

V9.0 で追加された新機能です。TPM と PIN を使うと、完全にデバイスと紐づけられたセキュリティ保護方法となります。PIN を使うことで、複雑な長いパスワードを使用する必要がなくなります。

① 既存のプロファイルを編集するか、既存のプロファイルをコピーして新しくプロファイルを作成します。
TPM の設定が含まれるプロファイルを全てのクライアントに適用した場合、UEFI / BIOS で TPM が有効になっていないデバイスでは、TPM の設定は無視され、エラーとはなりません。

② プロファイルで、TPM の使用を設定します。
[General options] -> [Hardware Authentication]
[TPM Protection for Key Files (for devices with TPM available)] の設定項目で、プルダウンメニューから「Create Key files protected by TPM and PIN instead of a password」を選択します。



設　定	説　明
TPM Protection for Key Files (for devices with TPM available)	
・Do not use TPM ・Automatically TPM-protect Password-protected Key Files ・Create Key files protected by TPM and PIN instead of a password	・TPM を使用しません。 ・パスワードで保護されたキーファイルを自動で TPM 保護に切り替えます。 ・パスワードの代わりに TPM と PIN で保護されたキー ファイルを作成します。
PIN complexity rules: ☐ Allow alpha characters in PIN Minimum PIN length: X	 PIN に英字を許可します。 PIN の長さ（最小）

③　[Devices] タブで、目的のデバイスを右クリックし、コンテキストメニューから [Assign device profile to devices] をクリックします。プロファイル一覧が表示されるので、先に作成したプロファイルを選択し、<OK> をクリックします。

④　クライアントデバイスは、定期的な通信で、SDConnex を介して、プロファイルを受け取ります。

⑤　次回、プリブート認証を通過し、Windows サインインの後に、PIN を設定するためのポップアップメニューが表示されます。

[キーファイルパスワード：] 欄には、プリブート認証でこれまで使用していたパスワードを入力し、[SecureDoc TPM PIN:] 欄に、画面に下に表示されているルールにそって PIN を入力します。[TPM PIN を確認します：]欄は、確認のためのものなので、同じ PIN を入力し、<OK> をクリックします。

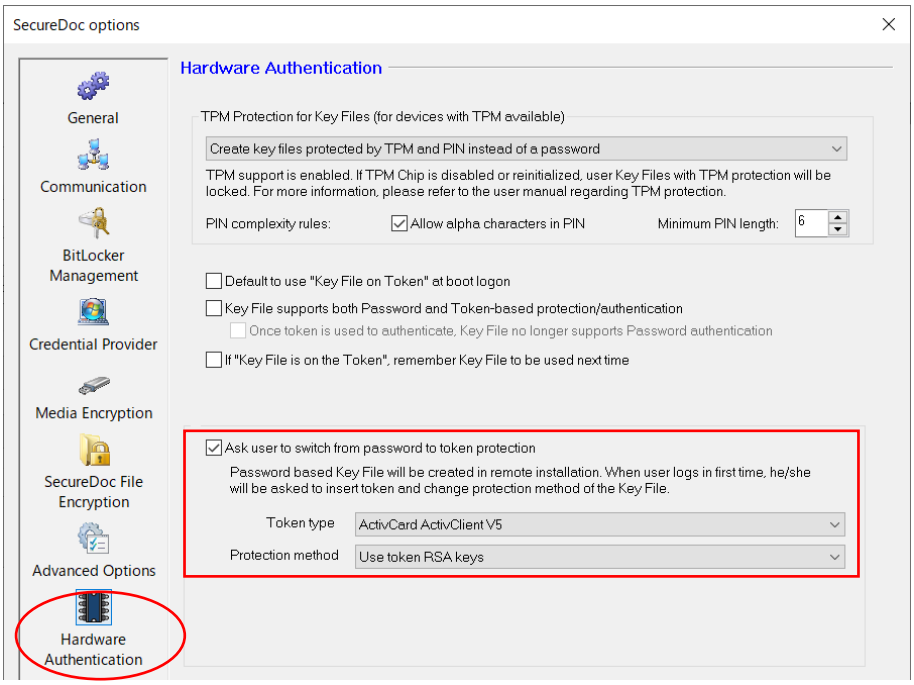
⑥　正しく設定が完了すると、「SecureDoc キーファイルの保護が TPM + PIN に変更されました。ログインするときは、新しい PIN を入力してください。」と表示されます。

■ トークンを使用して、二要素認証とする設定にしたい（プロファイルでの設定）

設定（ご購入）前に、SecureDoc がサポートしているトークンであるかを確認してください。

① トークンの初期設定を予め済ませておき、トークンが Windows 上で認識される状態に準備しておきます。
初期設定方法は、トークンのマニュアルを参照してください。

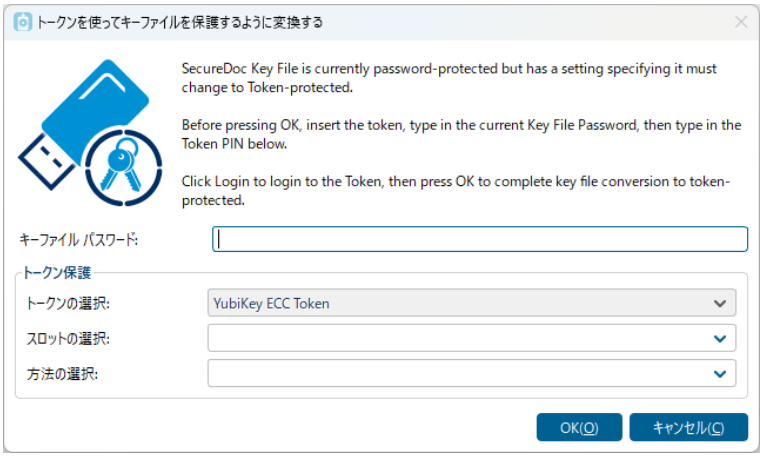
② プロファイルの<General options>で、使用するトークンを選択します。



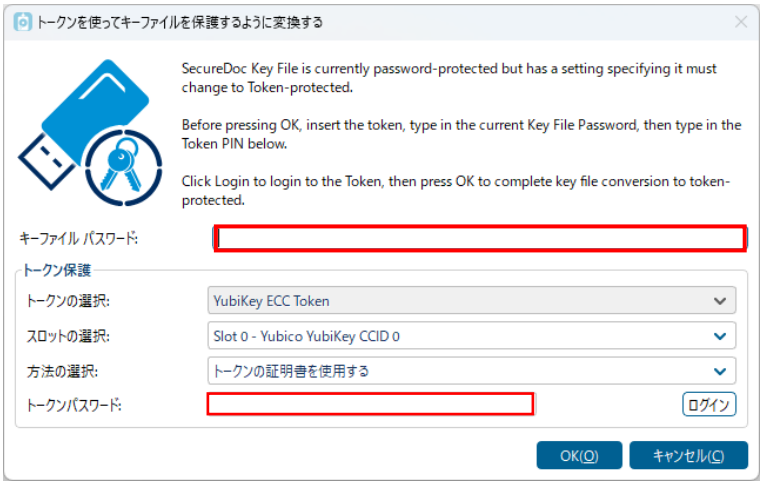
項　目	説　明
☐ Ask user to switch from password to token protection Token type Protection method	パスワードで保護されたキーファイルをトークンで保護するキーファイルに変換します。 [Token type] では、プルダウンメニューから使用するトークンを選択します。 [Protection method] はトークン側の設定にあわせます。 トークンによって選択できる方法は異なります。 ・Use token RSA Keys ・Token contains PIN ・Use Certificate on token - トークン証明書 ・Use Certificate from windows store - Windows ストアからの証明書

③ クライアントデバイスに、作成したプロファイルを適用します。

④ クライアントデバイスで、トークンを接続します。プリブート認証をパスワードで通過し、Windows サインイン後、Windows デスクトップにトークン保護に切り替えるためのポップアップが表示されます。



⑤ トークンを認識すると、「スロットの選択：」に接続したトークンが表示されます。
トークンを認識していない場合、<キャンセル> をクリックし、SecureDoc コントールセンターを実行します。
再度、トークン保護に切り替えるための設定画面が表示されます。



「方法の選択：」はトークンの設定に合わせます。

⑥ キーファイルのパスワードとトークンのパスワード（PIN）を入れて、<ログイン>をクリックします。

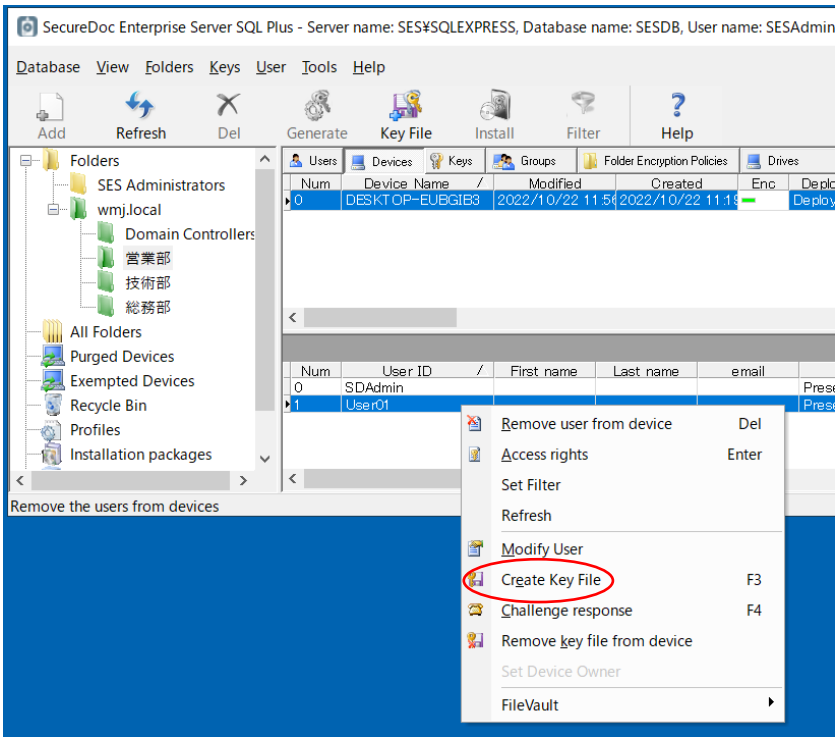
⑦ トークンのパスワード（PIN）が正しい場合、[データオブジェクトラベル]が表示されます。
<OK>をクリックすると、「キーファイルのキー保護方法がトークンに正常に変換されました」と表示されます。
次回以降、プリブート認証時にトークンと、トークンのパスワード（PIN）が必要になります。

■ トークンを使用して、二要素認証とする設定にしたい（キーファイルでの設定）

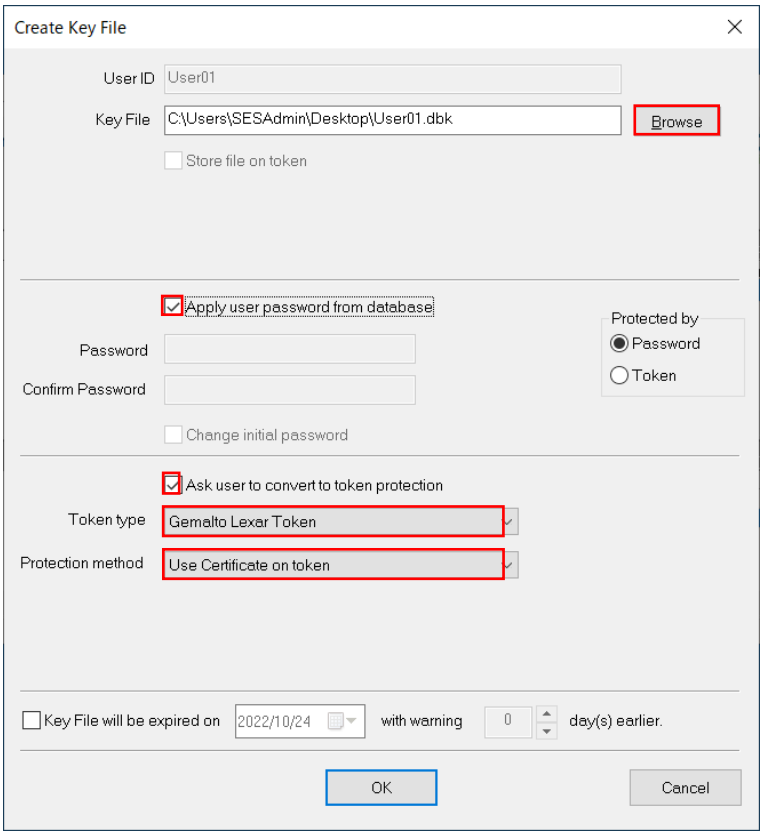
設定（ご購入）前に、SecureDoc でサポートしているトークンであるかを確認してください。

① トークンの初期設定を予め済ませておき、トークンが Windows 上で認識される状態に準備しておきます。
初期設定方法は、トークンのマニュアルを参照してください。

② [Devices] タブで、デバイスに登録されているユーザーを選択し、マウスの右クリックによるコンテキストメニューから [Create Key File] をクリックします。



③ キーファイルの作成画面が表示されます。
[Key File] 欄で、<Browse> をクリックし、一時的に使用するキーファイルの場所を指定します。
トークンへの切り替えが完了したら削除することができます。

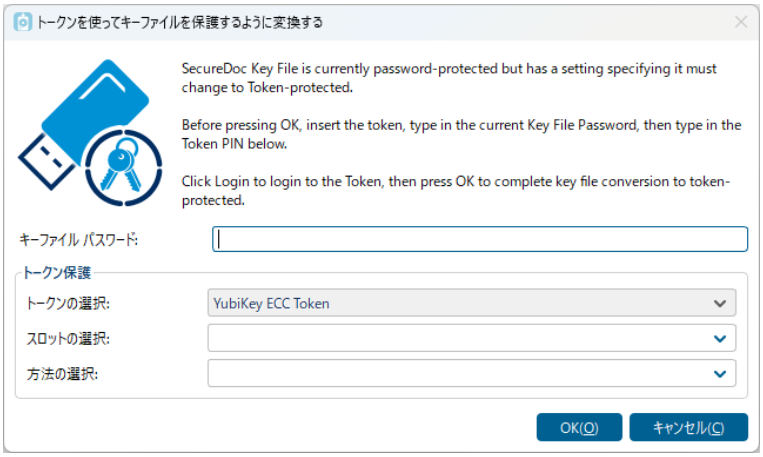


④ パスワードの設定は、SecureDoc の認証パスワードからトークンに切り替える際に使用するものです。
「☐ Apply use password from database」
にチェックを入れると、データベースに保存されているユーザーが設定したパスワードを利用できます。SES 管理者がパスワードに関与する必要がありません。

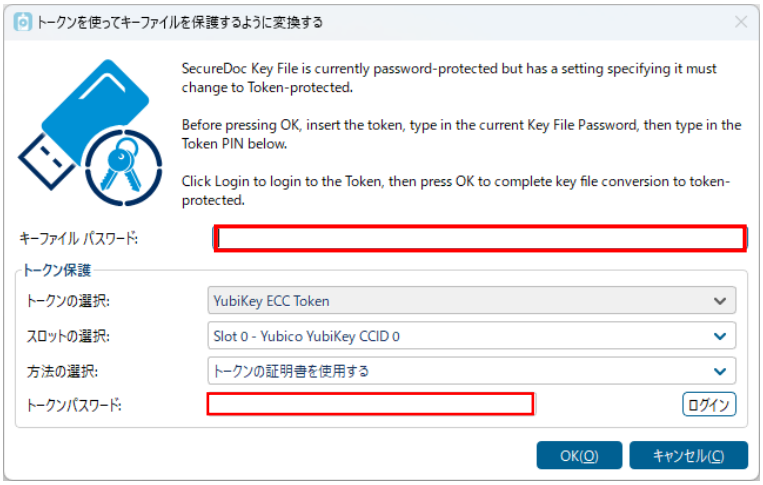
⑤ 「☐ ask user to switch from password to token protection」にチェックを入れます。
[Token type] で目的のトークンを選択し、 [Protection method] はトークン側の設定にあわせます。

⑥ <OK>をクリックします。クライアントデバイスは定期的な通信で、このコマンドを受け取ります。

⑦ クライアントデバイスで、プリブート認証を通過し、Windows にサインインすると、Windows デスクトップにトークン保護に切り替えるためのポップアップが表示されるので、トークンを接続します。



⑧　トークンを認識すると、「スロットの選択：」に接続したトークンが表示されます。
トークンを認識していない場合、<キャンセル> をクリックし、SecureDoc コントールセンターを実行します。
再度、トークン保護に切り替えるための設定画面が表示されます。



「方法の選択：」はトークンの設定に合わせます。

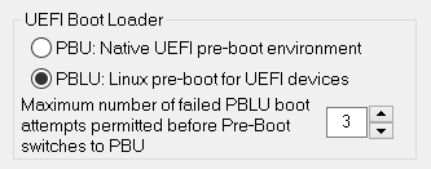
⑨　キーファイルのパスワードとトークンのパスワード（PIN）を入れて、<ログイン>をクリックします。

⑩　トークンのパスワード（PIN）が正しい場合、[データオブジェクトラベル]が表示されます。
<OK>をクリックすると、「キーファイルのキー保護方法がトークンに正常に変換されました」と表示されます。
次回以降、プリブート認証時にトークンと、トークンのパスワード（PIN）が必要になります。

■ プリブートでの認証に、スマートフォンを使いたい

注　V9.2 では、スマートフォンに MagicEndpoint2 が必要です。

① SES で、ブートログオンプログラムに PBLU を使うインストレーションパッケージを作成します。
プロファイル内の「UEFI Boot Loader」の設定で、PBLU を選択したプロファイルを作成します。
[General options] -> [Boot configuration]

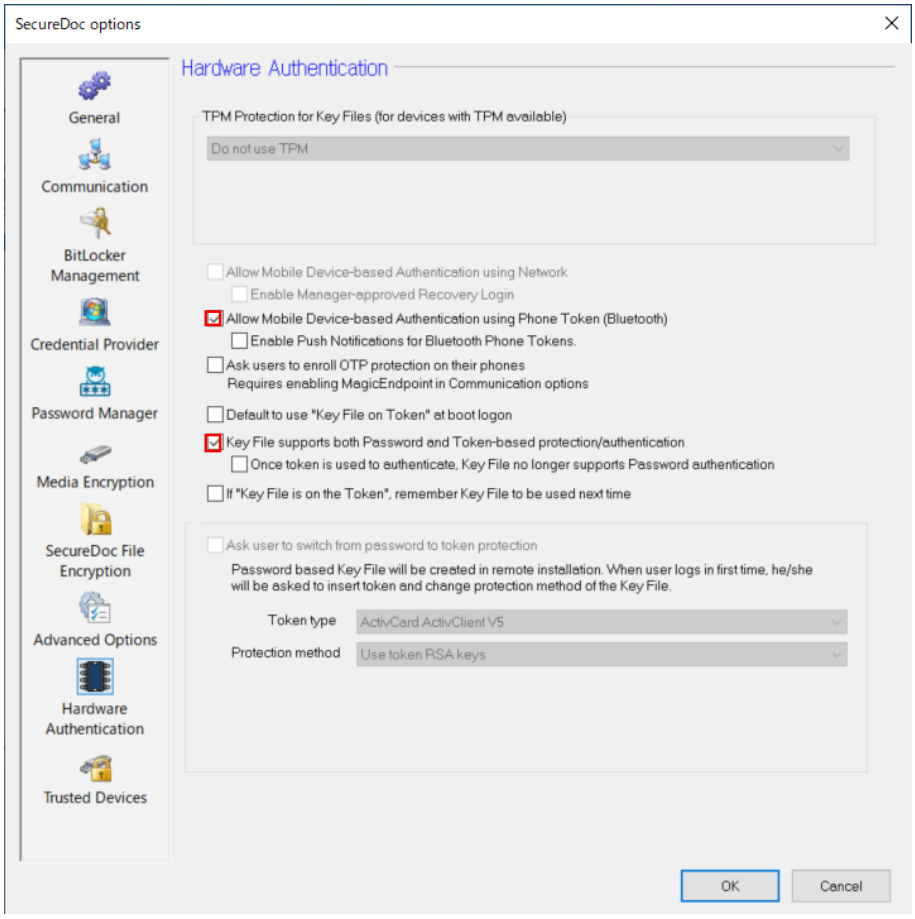


PBLU に設定したプロファイルを選択して。インストレーションパッケージを作成します。

② SecureDoc をクライアントにインストールし暗号化します。

③ クライアントデバイスの UEFI/BIOS 及び Windows で、Bluetooth が利用可能な状態であることを確認します。

④ SES で、プリブート認証でスマートフォンを使用するためのプロファイルを作成します。
インストールに使用した既存のプロファイルを右クリックして、[Copy profile]の機能を使うと、必要な個所のみ編集できます。
[General options] -> [Hardware Authentication]



⑤ 「☑ Key File supports both Password and Token-bsed protection/authentication」のチェックボックスをオンにすると、スマートフォンの充電切れなど、スマートフォンを使えない場合、パスワードで認証できます。

⑥ SES から作成したプロファイルをクライアントデバイスに適用します。

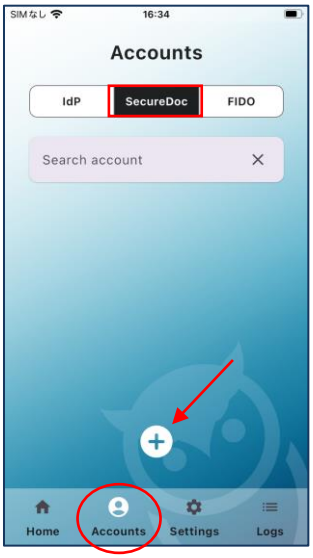
⑦ クライアントデバイスでは、プロファイル受信後の再起動時、パスワード保護からスマートフォンによる認証に切り替えるためのポップアップメッセージが表示されます。

⑧ 続いて、キーファイル保護方法の変更画面が表示されます。

⑨ WinMagic Authenticator（MagicEndpoint2）がスマートフォンにインストールされていない場合、QR コードをスキャンしてインストールします。v9.2 では、MagicEndpoint2 が必要です。
MagicEndpoint2 を起動し、画面に従って設定してください。
例えば、iPhone の場合、MagicEndpoint2 を実行すると、「”MagicEndpoint2”で Bluetooth デバイスを探すことを許可しますか？」、「”MagicEndpoint2”は通知を送信します。よろしいですか？」と表示されるので、
<許可> をクリックします。

⑩ [キーファイルパスワード:]欄にプリブート認証で使用しているパスワードを入力して、<OK>をクリックします。

⑪ 次の画面が表示されるので、スマートフォンの MagicEndpoint2 で、「Accounts」で「SecureDoc」を選び「+」をクリックします。「”MagicEndpoint2”がカメラへのアクセスを求めています」と表示されるので、
<許可> をクリックし、QR コードをスキャンします。



⑫ パスワード保護から切替えに成功すると、次のメッセージが表示されます。
クライアントの再起動後、スマートフォンによる認証が可能となります。

⑬ プリブート認証画面で「Bluetooth を利用したスマートフォン認証」の画面が表示されます。
スマートフォンで MagicEndpont2 の画面を表示してください。Bluetooth 接続に成功すると、スマートフォンにログインの許可を求めるメッセージが表示されます。<Approve> をクリックします。
この後、生体認証、あるいはスマートフォンのパスワードを入力して認証をおこなってください。

⑭ プリブート認証画面で「Bluetooth を利用したスマートフォン認証」の画面が表示されます。
スマートフォンで MagicEndpont2 の画面を表示してください。Bluetooth 接続に成功すると、スマートフォンに

ログインの許可を求めるメッセージが表示されます。<Approve> をクリックします。

この後、生体認証、あるいはスマートフォンのパスワードを入力して認証をおこなってください。

※ ユーザーがスマートフォンを使用できない場合、設定により代替パスワードでログインすることができます。

ユーザーがパスワードを失念している場合、チャレンジレスポンスによってパスワードリカバリが可能です。

設定しているスマートフォンの故障などで、使用できなくなった場合、パスワードによる認証に戻し、プロファイルの設定もスマートフォンによる認証を無効にしたプロファイルをクライアントデバイスに適用する必要があります。

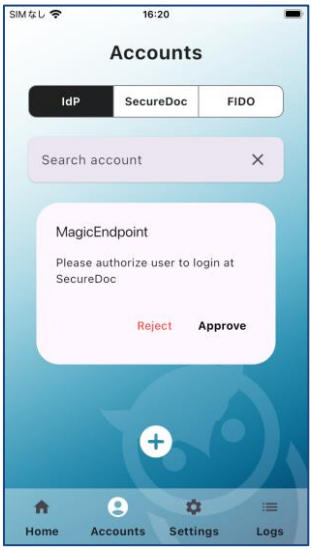
■ 認証に設定しているスマートフォンを別のスマートフォンに変更したい

注　スマートフォンに MagicEndpoint2 が必要です

① クライアントで、SecureDoc コントールセンターを起動し、ログインします。
[開始ページ] で、”トークン保護” をクリックします。

② 次の画面が表示されます。スマートフォンで MagicEndpont2 を開きます。

③ スマートフォンの MagicEndpont2 に、ログインの許可を求めるメッセージが表示されます。
<Approve> をクリックすると、トークン保護に切り替える画面が表示されます。



④ 「QR コードからアプリをダウンロード」をクリックし、これから設定するスマートフォンに MagicEndpoint2 をインストールします。「"MagicEndpoint2"で Bluetooth デバイスを探すことを許可しますか？」、「"MagicEndpoint2"は通知を送信します。よろしいですか？」と表示されたら、<許可> をクリックします。

⑤ MagicEndpoint2 の「Accounts」で「SecureDoc」を選び「+」をクリックします。「"MagicEndpoint2"がカメラへのアクセスを求めています」と表示されたら、<許可> をクリックし、QR コードをスキャンします。

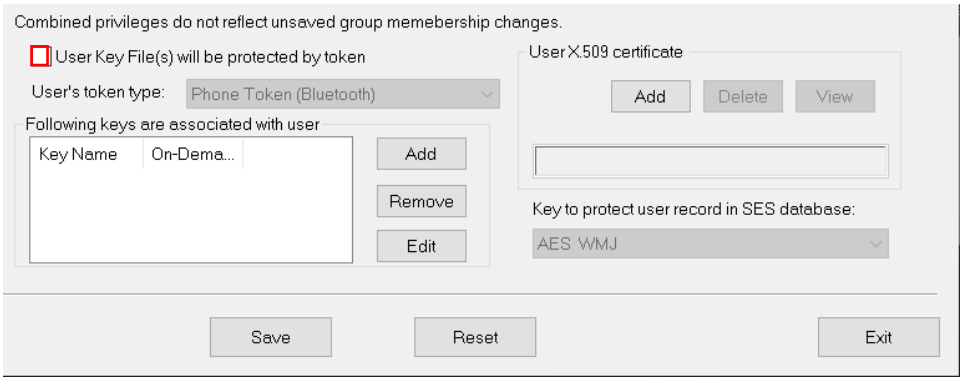
⑥ 切替えに成功すると、次のメッセージが表示されます。
クライアントの再起動後、新しいスマートフォンによる認証が可能となります。

■ 現在、設定されているスマートフォンによる認証からパスワードによる認証へ変更する方法

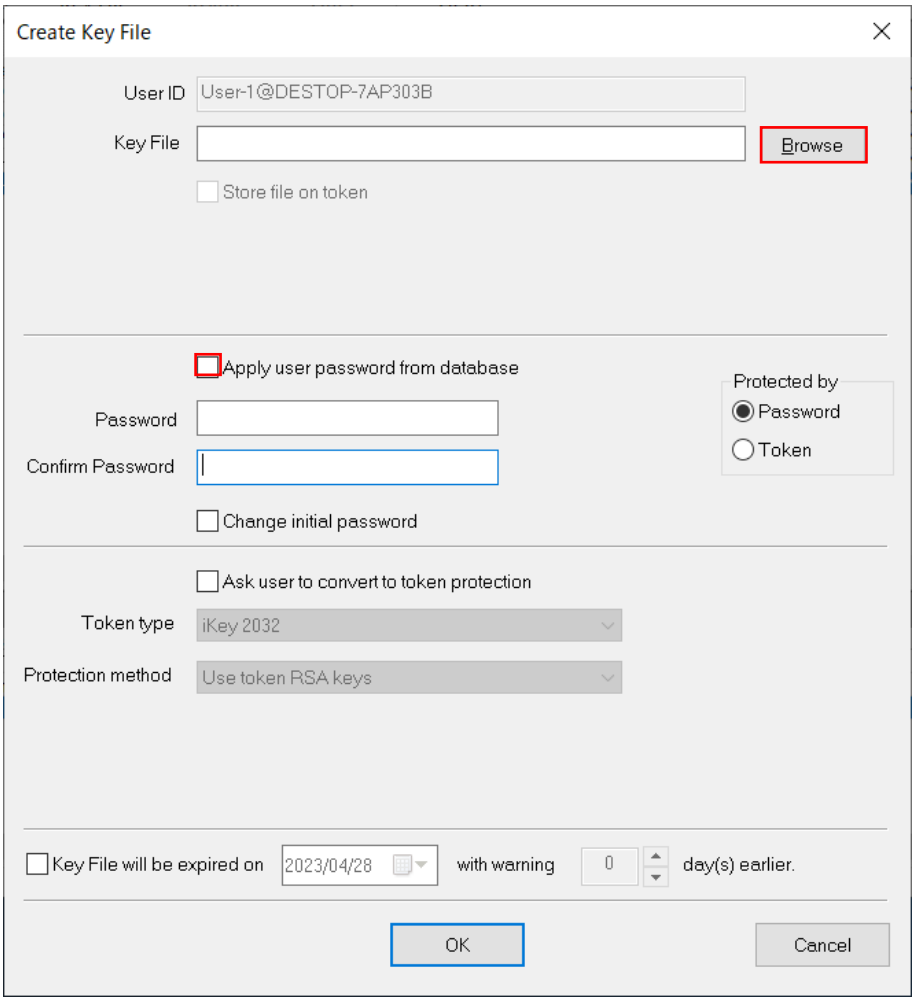
キーファイルを再作成します。

① スマートフォンを使用しないプロファイルをクライアントデバイスに適用します。

② SES の[Devices]タブで、ユーザーのデバイスを選び、下段に表示される該当のユーザーを右クリックします。[Modify User]を実行します。
下段にある「☑ User Key File(s) will be protected by token)」のチェックボックスをオフにし、<Save>をクリックします。



③ 再度、ユーザーを右クリックし、コンテキストメニューから[Create Key File]を実行します。



④ <Browse>ボタンをクリックしてキーファイルの保存場所を指定します。

⑤ 「☐ Apply use password from database」のチェックボックスをオンにすると、プリブート認証でユーザーが設定していたパスワードで、認証できます。（管理者は SES コンソールを使ってユーザーのパスワードを知ることはできませんが、ユーザーのパスワード情報は SES の DB に保存されています。）

⑥ ユーザーがパスワードを失念している場合は、[Password]フィールドにパスワードを入力し、「☑ Change user password」のチェックボックスをオンにします。ユーザーにパスワードの変更を要求します。

⑦ <OK> をクリックします。

⑧ 「Key File successfully created.」というダイアログが表示されますので、<OK>をクリックします。

⑨ クライアントデバイスは、SDConnex との通信で新しいキーファイルを受け取ります。
再起動後は、パスワードによる認証となります。

⑩ 設定が完了したら、④で指定した先に保存されているキーファイル（*.dbk）は削除できます。

7.3. SecureDoc クライアントのインストール設定・方法について

■ SecureDoc クライアントのインストール・展開を簡単にしたい

プロビジョニングルールを使用すると、ほぼサイレントインストールが可能ですが、既にエンドユーザーが使用しているデバイスに SecureDoc クライアントを展開する場合は、ユーザーによるインストール操作が必要になります。
ユーザーに負担をかけずに、SecureDoc クライアントをインストールする方法としては、Active Directory のグループポリシーを利用してソフトウェアをリモートでインストールする方法があります。その場合、Windows インストーラーパッケージ「SecureDoc_64.msi」を使用します。

詳しくはマイクロソフト社のサイトをご参照ください。
参考：Microsoft ドキュメント「グループ ポリシーを使用してソフトウェアをリモートでインストールする」
https://learn.microsoft.com/ja-jp/troubleshoot/windows-server/group-policy/use-group-policy-to-install-software

■ 認証 ID を Windows サインインアカウント名以外で設定したい

これまでウィンマジックは、多くのお客様からのフィードバックをいただき、プロビジョニングルールによる ID の作成方法を実装してきました。プロビジョニングルールによって、Windows サインインアカウント名から SecureDoc のユーザーID を自動で作成することができ、インストール及び設定を簡易に済ませることができます。SecureDoc のブートログオンプログラムは、Windows OS ではないため、Windows サインインアカウント名をユーザーID とパスワードに使用しても、Windows のパスワードクラックなどの攻撃対象とはなりません。これらの理由により、Windows サインインアカウント名を SecureDoc のユーザーID として使用するようにデザインされています。

ここでは、企業ポリシーによって Windows サインインアカウント名以外のユーザーID を使用する必要がある場合のインストレーションパッケージの作成方法を説明します。

事前に ID を準備し、SES にインポートします。

① Excel 等を使って、SecureDoc のユーザーとして使う ID を作成します。
必ず、パスワードを入力してください。イニシャルパスワードとして使用します。
クライアントで使用する Windows のサイン ID も必ず含めてください。これにはパスワードを入力する必要はありません。エンドユーザー以外の IT 部門やキッティング業者がインストールする場合で、作業用の Windows ID を使って Windows にサインインする場合は、その Windows ID だけを含めてください。

例）下記のようにタイトル行とパスワードを含めます。

ユーザーID	イニシャルパスワード	苗字	名前	メールアドレス
PC-11	12345678			
PC-12	12345678			
PC-13	12345678			
PC-14	12345678			
PC-14	12345678			
User01				
User02				
Uesr03				
User04				
User04				

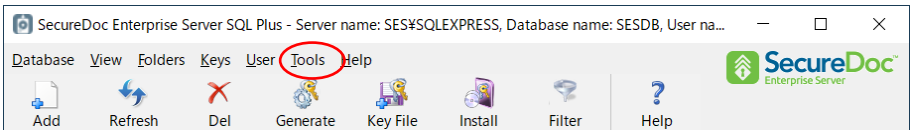
SecureDoc の ID として使用

Windows の ID

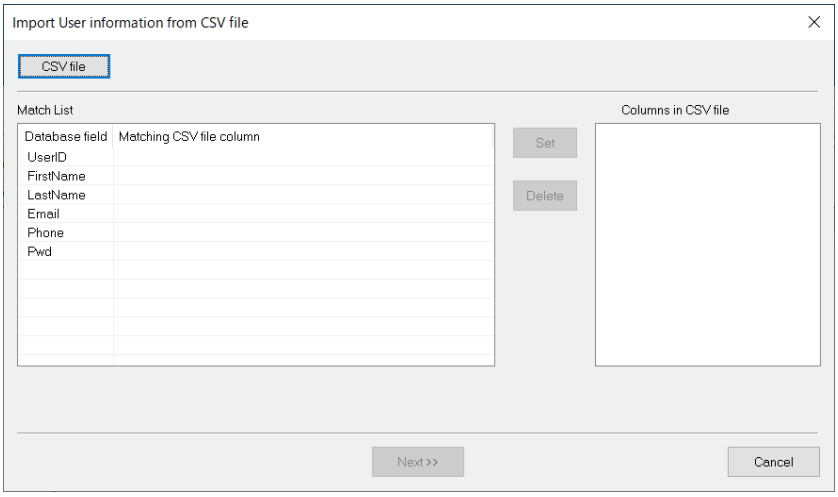
CSV（CSV UTF-8 コンマ区切り）形式で保存します。

② SES に、事前に、ユーザーをインポートするフォルダを作成しておきます。

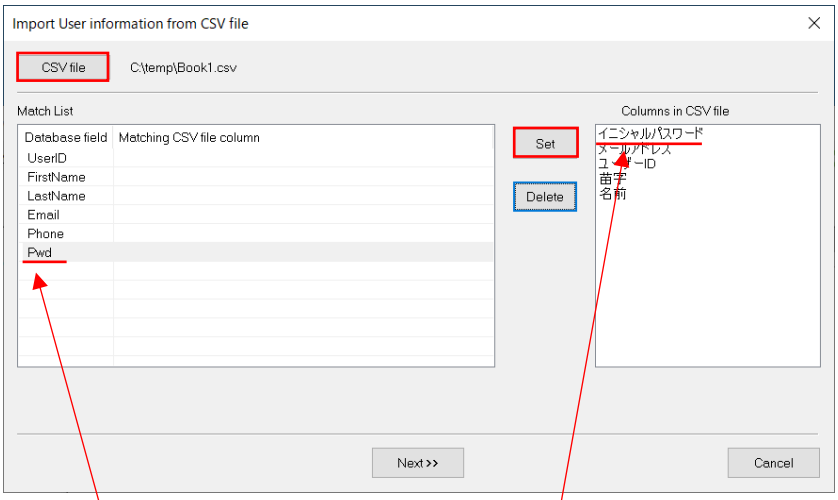
③ SES のメニューバーから、
[Tools] - > [Import from…] -> [Import users into from CSV file] をクリックします。



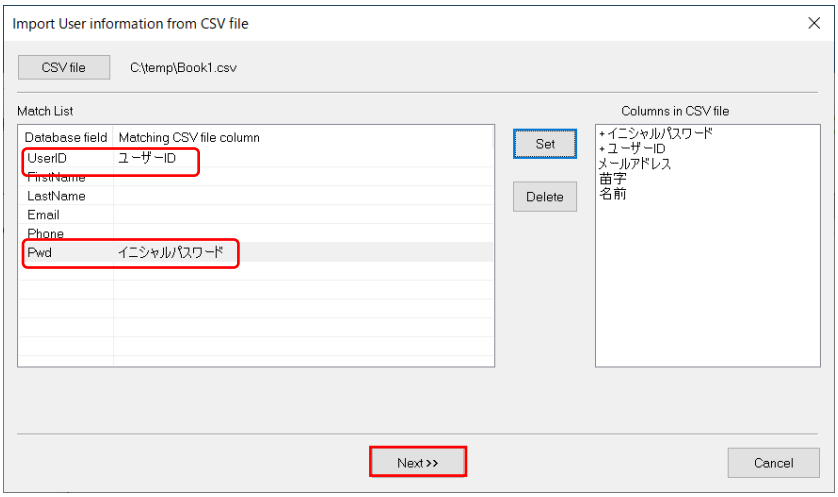
④ SES DB のフィールドと一致させるための画面が表示されます。



⑤ CSV file をクリックし、先に作成した CSV ファイルを読み込みます。

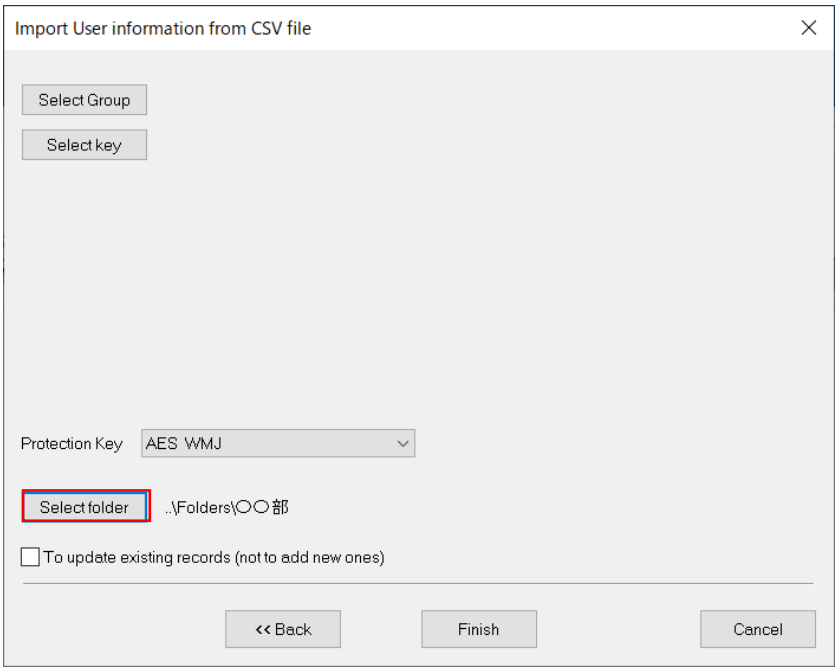


⑥ 左に表示されている項目と読み込んだファイルのタイトルを選び <Set> をクリックします。



User ID と PWD は必ず設定します。一致させるものを繰り返し、設定が済んだら、<Next> をクリックします。

⑦　次の画面で、<Select folder>でインポート先フォルダを指定し、最後に、<Finish> をクリックします。

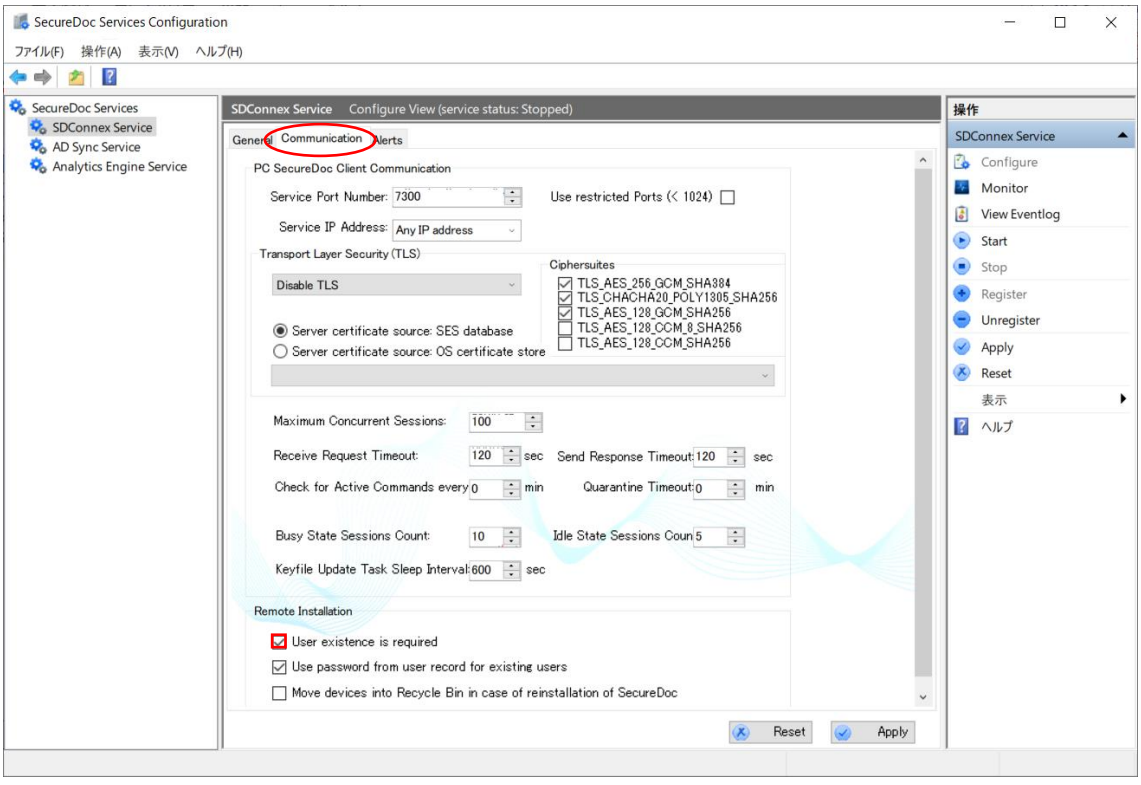


⑧　確認を求められるので、<OK> をクリックします。

⑨　SES のフォルダに、ユーザーID がインポートされていることを確認します。

SDConnex の設定を変更します。

①　SDConnex の [Communication] タブを開きます。



② 「☑ User existence is required」にチェックを入れます。

※ この設定によって、先にインポートしたユーザーID 以外の ID を誤って作成することを防げます。

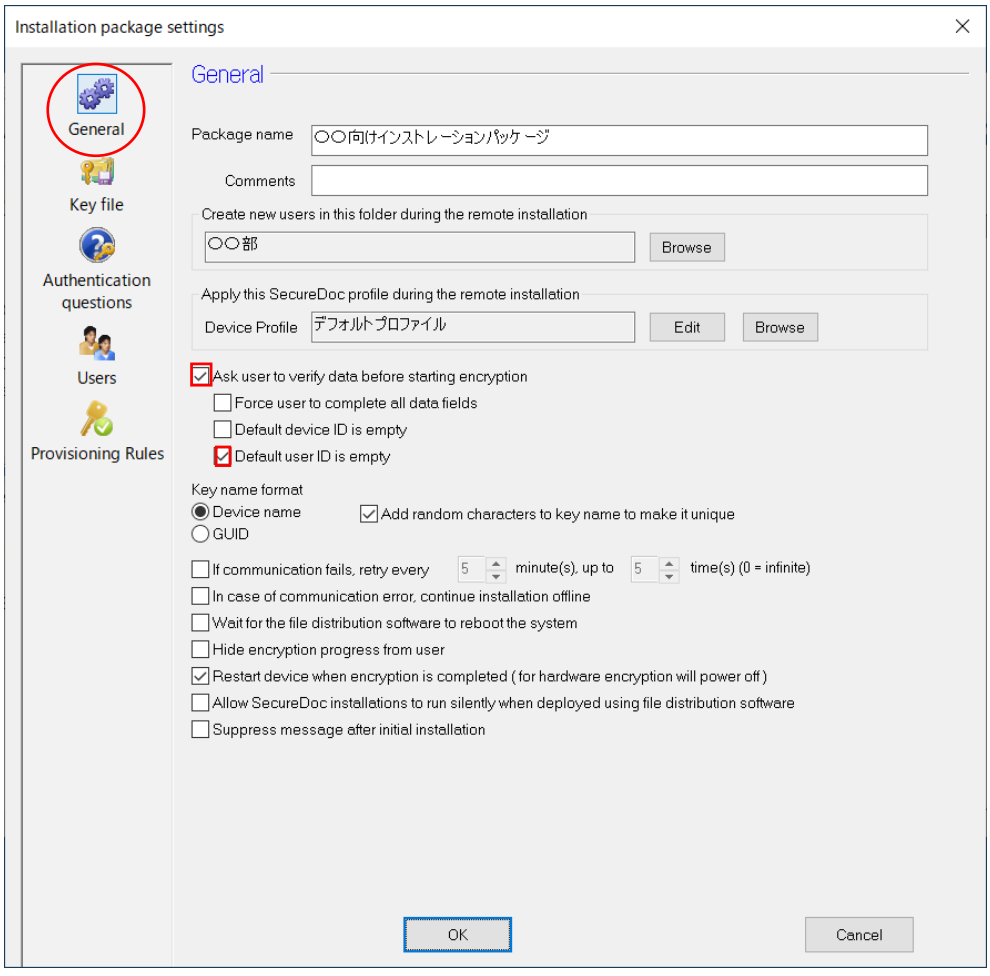
③ 右の操作パネルで、[Stop]をクリックし停止させ、[Start] をクリックして起動してください。
一瞬の操作ですので、既存のクライアントに影響があることはほとんどありません。

インストレーションパッケージの作成

① 「SecureDoc Enterprise Server v9.2 クイックインストールガイド」を参照して、プロビジョニングルールの設定「パターン A」 で、インストレーションパッケージを作成します。

② 作成したインストレーションパッケージをダブルクリックして、設定画面を開きます。
[General] アイコンで、次の設定を変更します。

下記の設定箇所にチェックを入れて、<OK> をクリックします。
☑ Ask user to verify data before starting encryption
☑ Default Use ID is empty



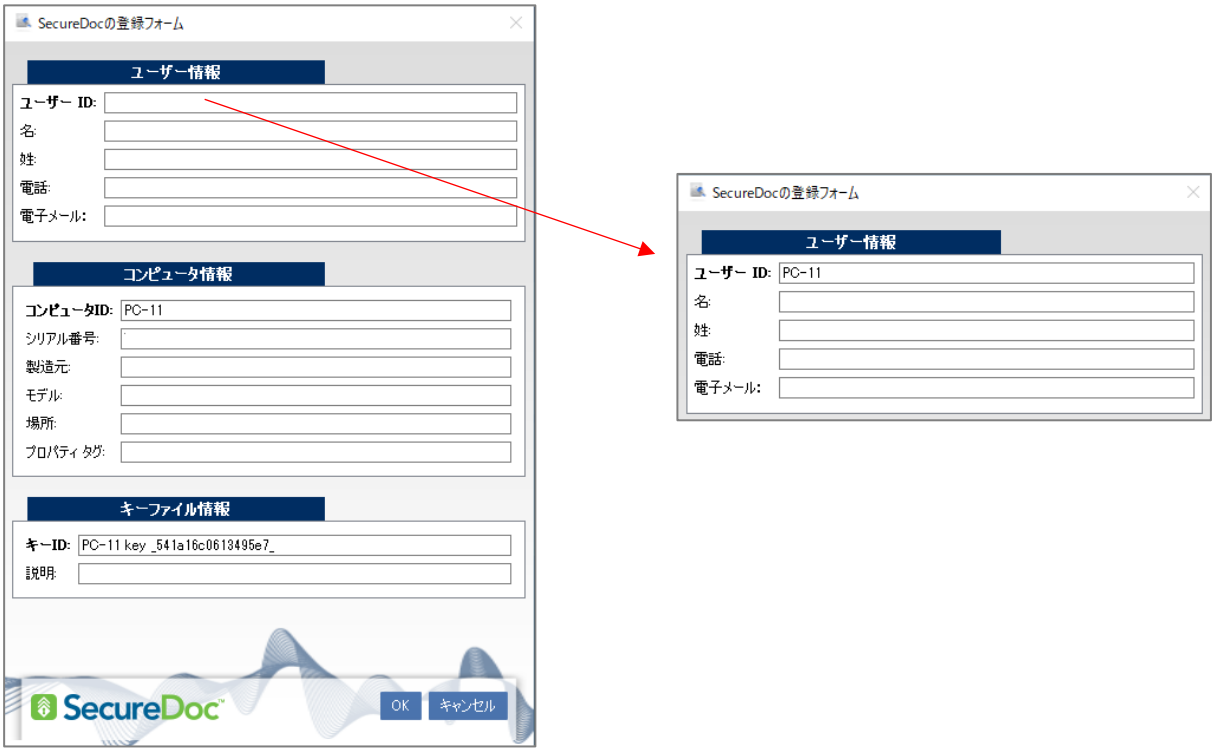
③ <OK> をクリックします。

④　作成したインストレーションパッケージを右クリックし、[Create package files] をクリックします。

クライアントへのインストール

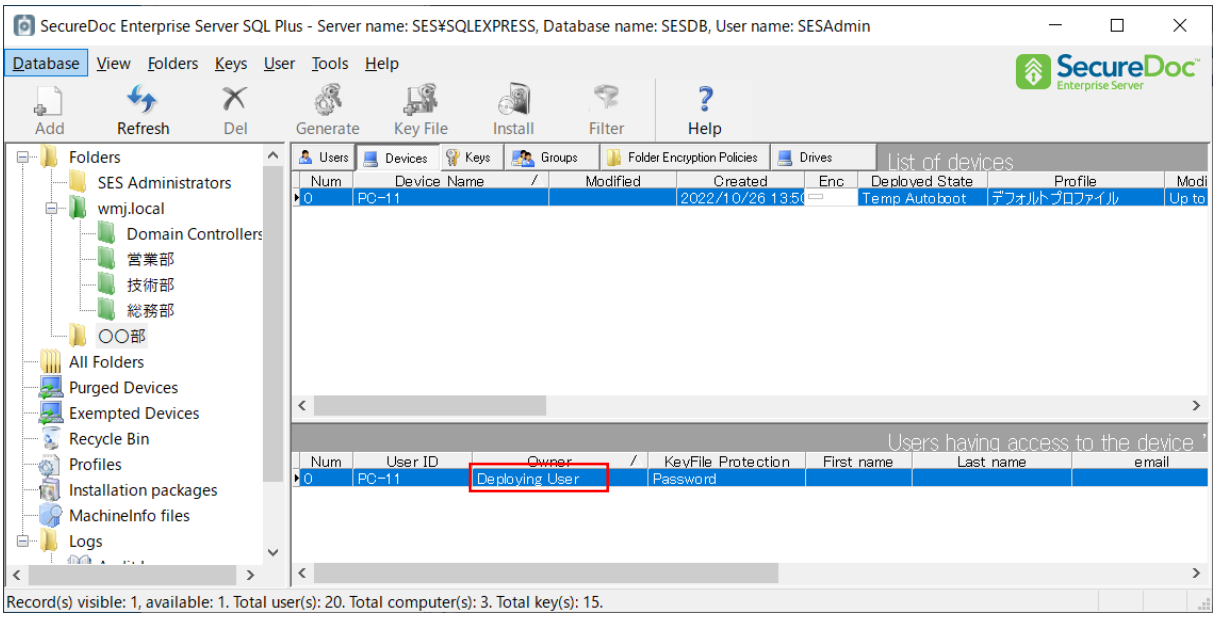
①　作成したインストレーションパッケージを使って、インストールします。

②　暗号化が開始する前に、「SecureDoc の登録フォーム」が表示されます。



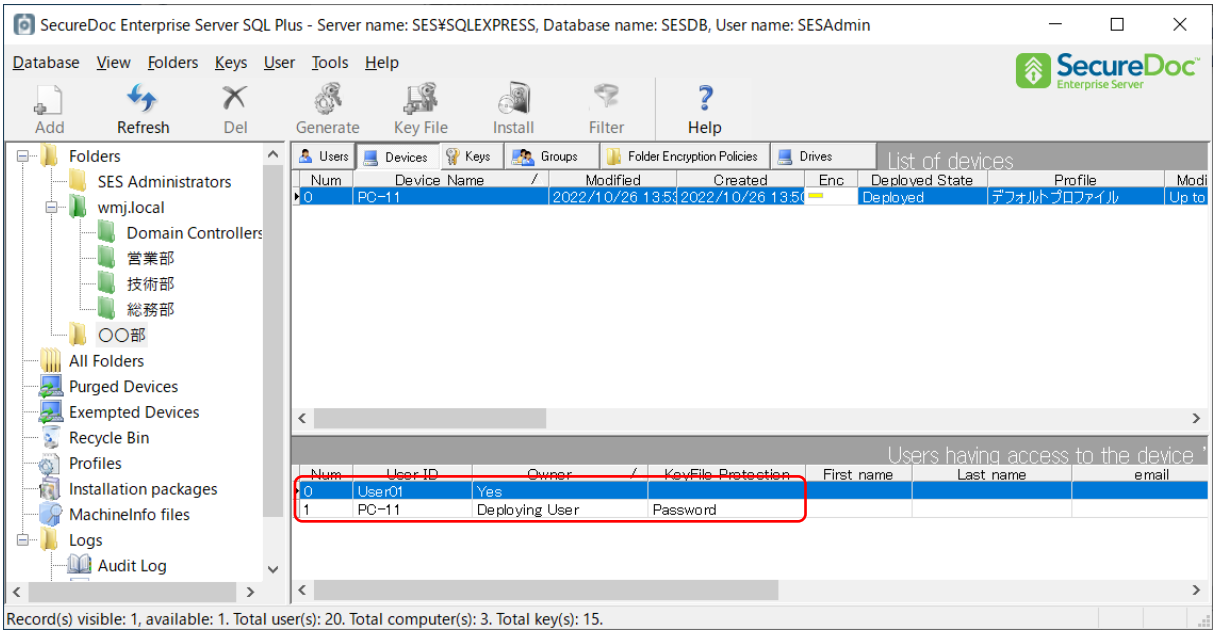
⑤　「ユーザーID」欄に、事前に SES に登録済のユーザーID を入力して、<OK> をクリックします。
事前におこなった SDConnex の設定変更により、SES に登録されていない ID を使ってインストールを継続することはできません。
例として、ここでは、「PC-11」を入力します。

⑥　SES に、Deploying User として、ユーザーID「PC-11」が作成されます。

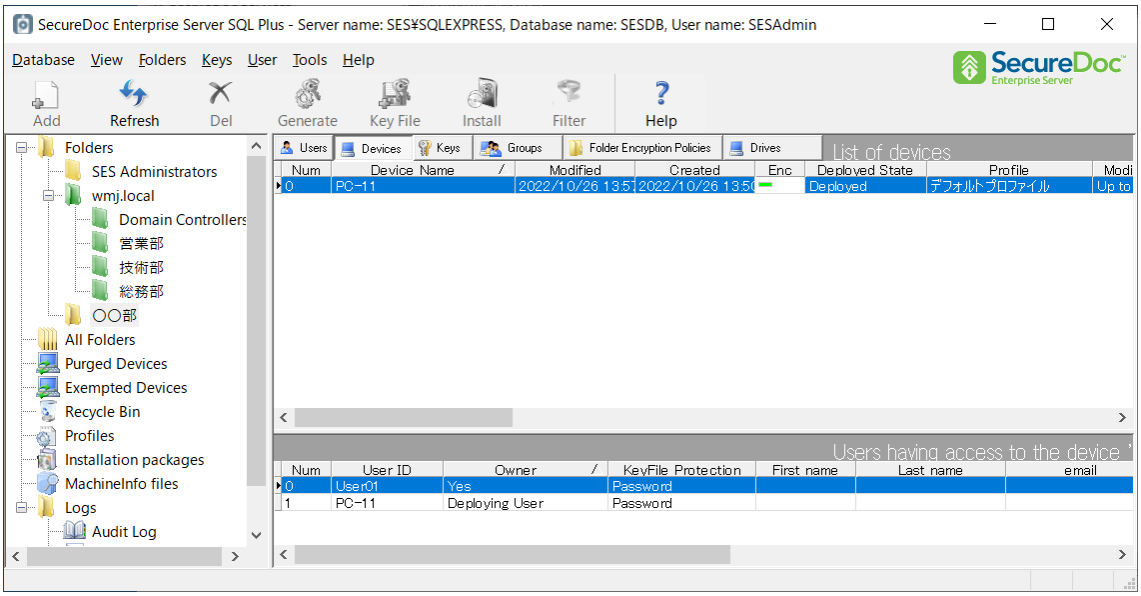


⑦　クライアントは再起動となり、暗号化が開始されます。

⑧　クライアントでは、この時に Windows へサインインしている Windows ID 名と同じ名前の ID を自動でオーナーの ID として作成します。その ID は、SES にも登録されます。

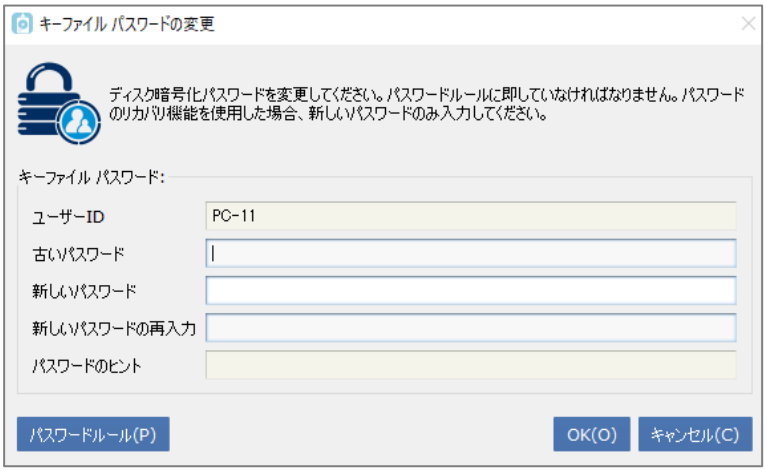


⑨　クライアントへのインストール・暗号化が完了すると、「User01」と「PC-11」が登録されており、どちらでもログインすることができます。



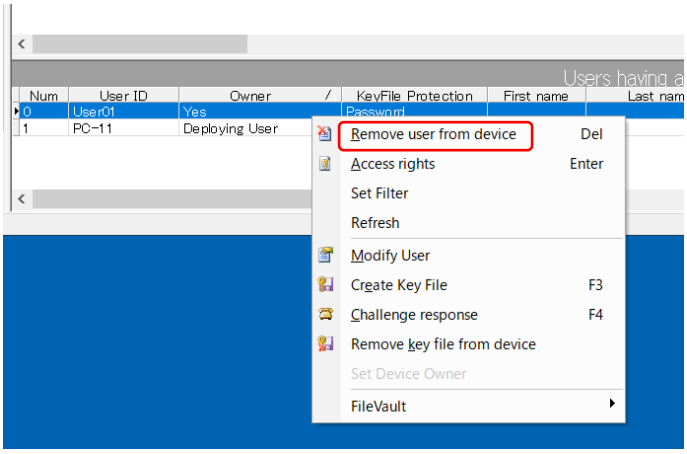
⑩ 「PC-11」を使って、ログインします。

パスワードの変更要求があるので、イニシャルパスワードとして設定済のパスワードを［古いパスワード］欄に入力し、新しいパスワードを設定します。



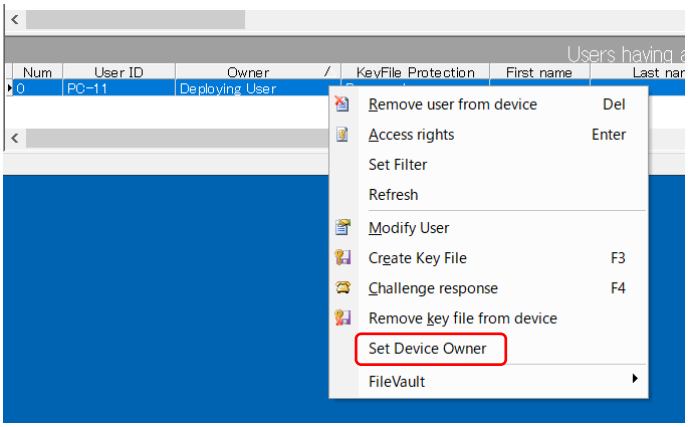
次回から、プリブート認証で、変更したパスワードを使ってログインできます。

⑪ 「User01」が不要であれば、右クリックし、[Remove use from device] をクリックします。
クライアントは、定期的な通信で、この命令を受け取ります。



PC-11」は、Deploying User のままですが、そのまま利用することができます。

⑫ オーナーとして、設定する場合は、[Set Device Owner] をクリックします。



※ インストール時、全ての Windows へのサインインに、キッティング用の同じ ID を使った場合は、[Users] タブでその ID を選ぶと、下段のパネルに登録されているデバイス一覧が表示されます。
複数のデバイスはシフトキーを使って選択し、右クリックで [Remo use from device] をクリックします。
全てのデバイスから、その ID は削除されます。

8. 旧バージョンからの SES アップグレード

ウィンマジックは SES 及び SecureDoc クライアントを最新のバージョンにアップグレードして使用することを推奨しています。SES は旧バージョンのクライアントも包括的に管理することが可能です。
SES のアップグレードは、既存の SES へ上書きインストールが可能ですが、アップグレード前に下記の注意事項を必ず読んでから実行してください。

注　「SDConnex Service」、「ADSync Service」、「Analytics Engine Service」を SES と同じサーバーで実行している場合、上書きインストールの前にそれぞれのサービスを停止する必要があります。
それぞれのサービスは、マイクロソフト管理コンソール（Microsoft Management Console）の上で実行されており、上書きインストールをおこなっても、それまで設定されていた内容は引き継がれずクリアされます。
右ペインの「操作」メニューから<Configure>をクリックして、現在の設定内容をメモする、あるいは画面コピーなどをおこって、アップグレード後の設定に役立つようにしてください。
また、起動に使用するアカウントも同様に現在の設定をメモする、あるいは画面コピーなどをおこってください。
アップグレード後の再設定をスムーズに完了するために役立ちます。

注　SESWeb の設定もクリアされますので、ログインの為の再設定が必要になります。

注　SQL に作成されている SES のデータベースは、アップグレードプロセス中にバックアップを取ることができます。
アップグレード前に、データベースのバックアップを取る。仮想環境に構築している場合はスナップショットを取るなど、予期せぬ不具合などに備えてから実行してください。
SQL Server Management Studio を使って、既存のデータベースをバックアップできます。

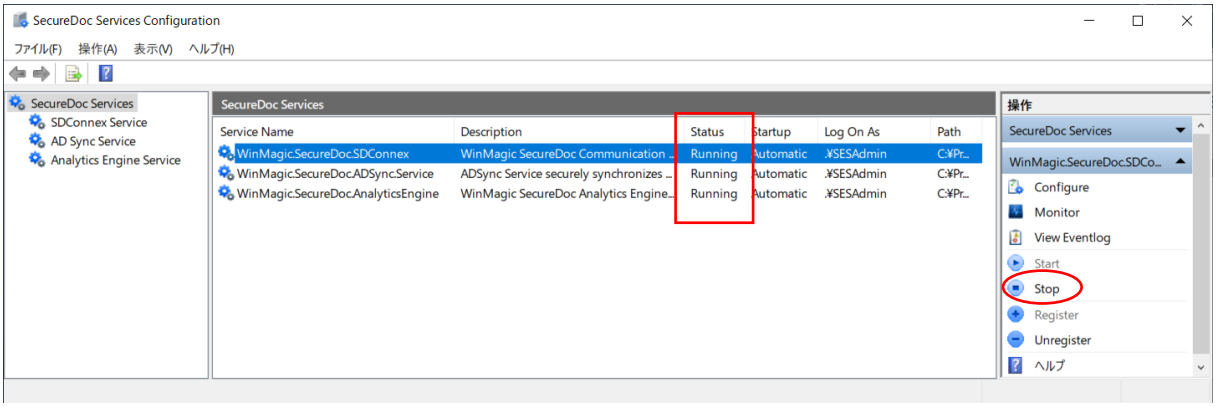
詳しくは、SQL Server Management Studio 開発元のサイトでご確認ください。
データベースの完全バックアップの作成
https://learn.microsoft.com/ja-jp/sql/relational-databases/backup-restore/create-a-full-database-backup-sql-server?view=sql-server-ver16

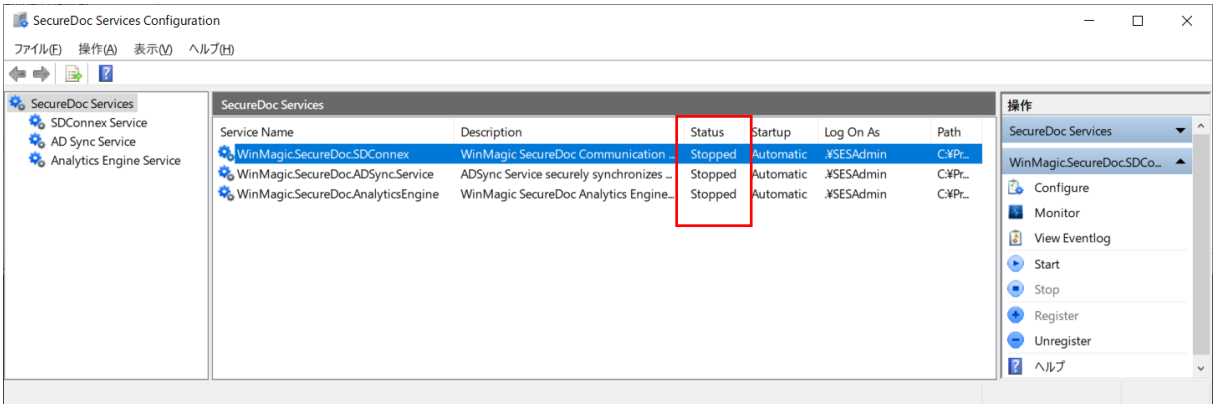
注　V8.6 SR1 HF2 より古いバージョンや既に EOL となっているバージョンから、最新バージョンへのアップグレードの場合、特定の中間アップグレード（V8.6 SR1 HF2 にアップグレード）が必要になる場合があります。

SES を別のサーバーに移行する場合の手順は、次のとおりです。

① [スタート] > [SecureDoc Enterprise Sever] > [SecureDoc Service Configuration] を実行します。

全てのサービスを右ペインの「操作」メニューから<Stop>をクリックして停止します。



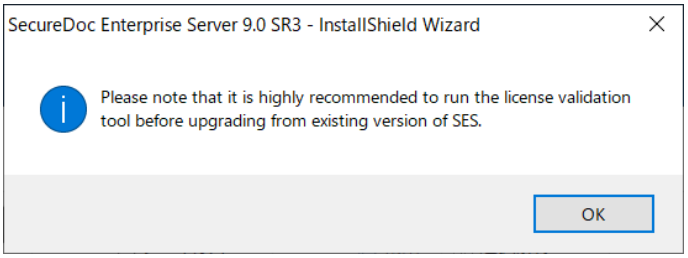


② 「SecureDoc Enterprise Server Version 9.2 クイックインストールガイド」を参照して、インストールを実行してください。

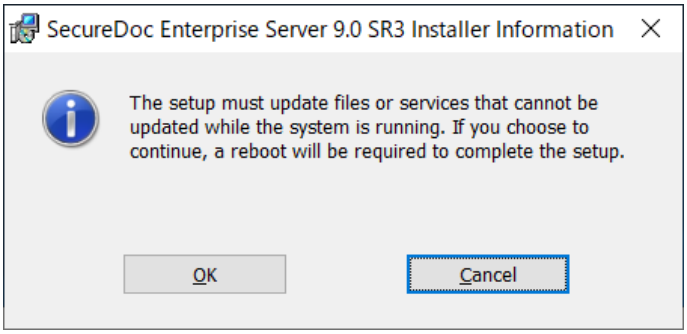
③ インストールプロセスの途中で、下記のポップアップメッセージが表示されます。

V6.5 以前のバージョンを使用しているお客様は、SES のアップグレード前に License validation tool を使って、現在所有しているライセンスが正しく引き継がれるのかを確認する必要がありました。しかし、v6.5 は既に EOL となっておりサポートが終了しているため、今後のバージョンではこのメッセージは表示しないように変更されます。

<OK>をクリックして、進めてください。



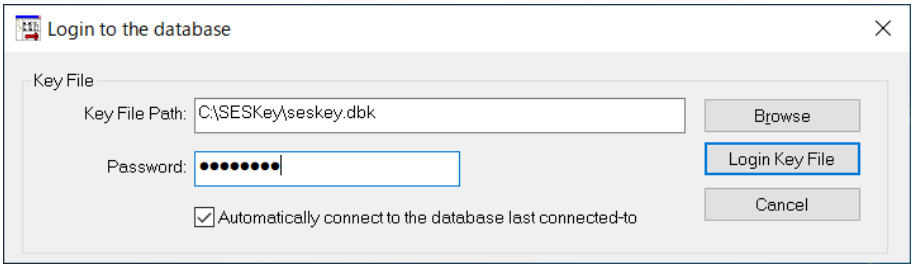
④ SES が終了しておらず、実行されたままの場合、インストールプロセス中に下記のポップアップメッセージが表示されます。SES のプログラムを終了し、<OK>をクリックしてください。



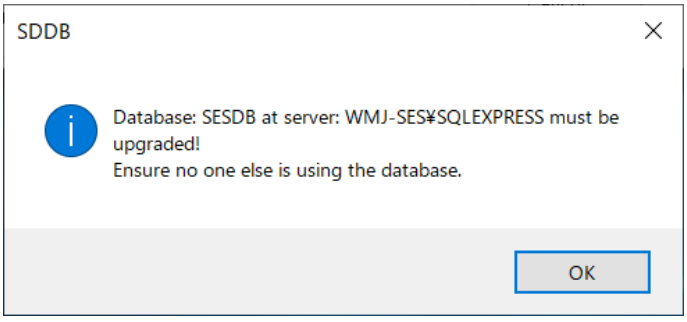
⑤ 画面に従って、インストールを完了させます。
詳細は「SecureDoc Enterprise Server Version 9.2 クイックインストールガイド」を参照してください。

⑥ [スタート] > [SecureDoc Enterprise Server] > [SecureDoc Enterprise Server] を実行します。

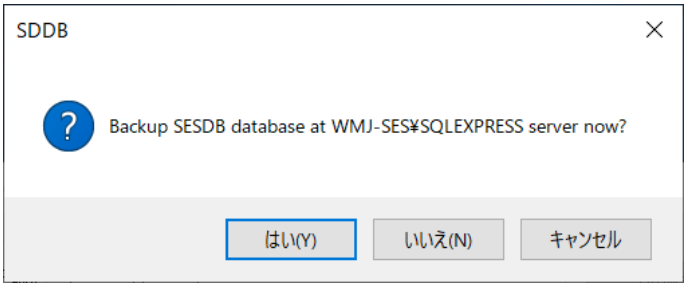
⑦ ログイン画面が表示されます。
管理者用キーファイルのパスワードを入力し、<Login Key File>ボタンをクリックします。



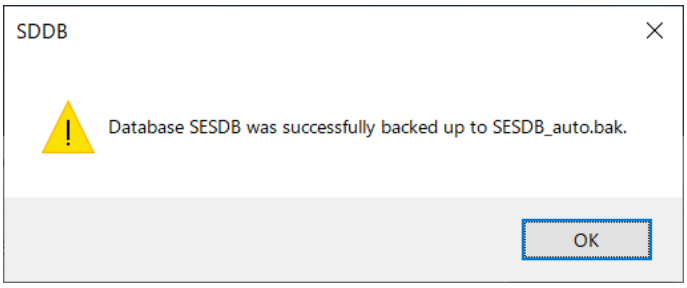
⑧ データベースのアップグレードが必要であることを示すメッセージが表示されます。<OK>をクリックします。



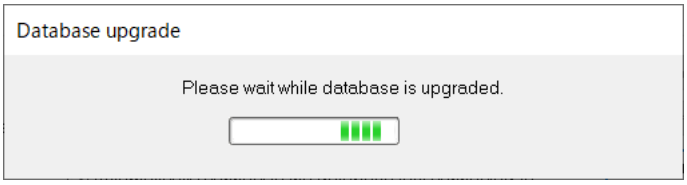
⑨ データベースのバックアップをおこなうことの確認を求められます、必ず、<はい>をクリックします。



⑩　データベースのバックアップに成功すると、次の画面が表示されます。<OK>をクリックします。



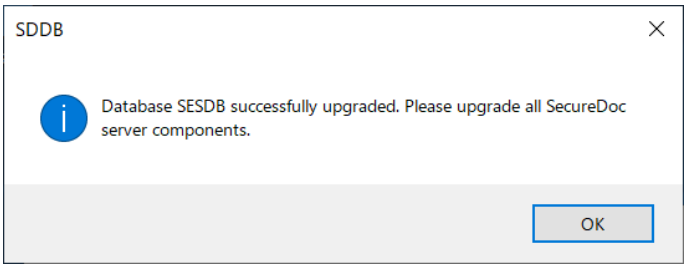
⑪　データベースのアップグレードが開始されます。



⑫　データベースのアップグレードに成功すると、次の画面が表示されます。

<OK>をクリックすると、SES が起動します。

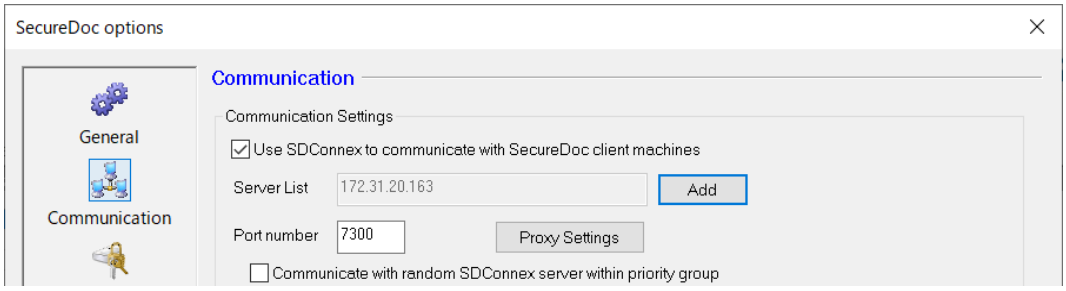
「SDConnex Service」、「ADSync Service」、「Analytics Engine Service」を再設定してください。



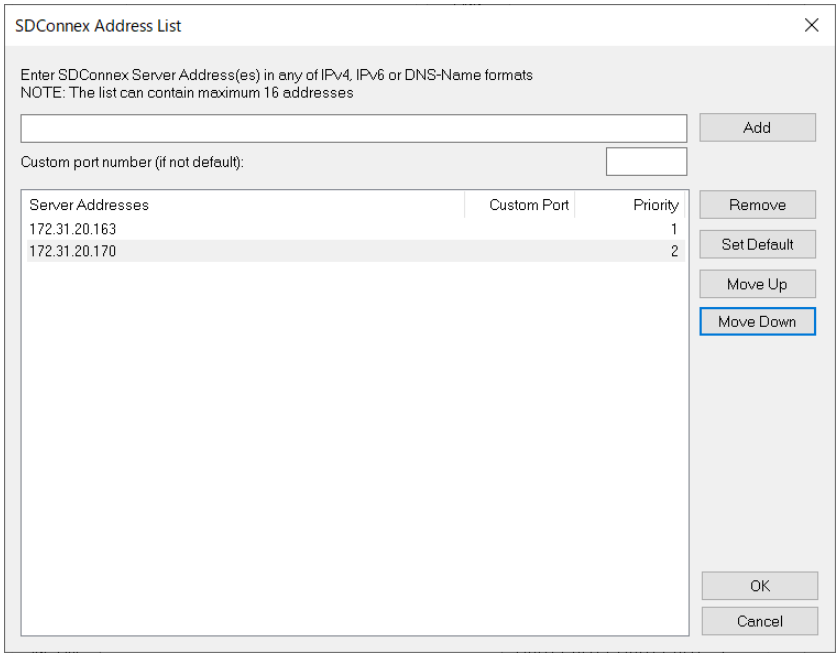
9. SES を別のサーバーに移行する場合

既存の SES 環境が SES コンソールと SDConnex が同じサーバーにインストールされており、新たに SES をインストールする環境で SDConnex の IP アドレスがこれまでと異なると、クライアントは既存の SDConnex との通信を続けようとします。IP アドレスが変更になる場合は、既存の SES 環境で、クライアントデバイスに適用しているプロファイルに新しくインストールする環境の IP を追加し、全てのクライアントにプロファイルを再適用しておく必要があります。

[General options] -> [Communication]



<Add>をクリックし、IP アドレスを追加します。
追加した後、<Move Up>、<Move Down>をクリックすると、Priority を変更できます。
クライアントは Priority の順番で、SDConnex との通信を試みます。新しくインストールする SDConnex の IP を Priority 1 とし、既存の SDConnex の IP を 2 とした場合、新規に SDConnex がインストールされるまで、クライアントは Priority 1 の SDConnex と通信できないため、Priority 2 の既存の SDConnex との通信をおこないます。



クライアントにプロファイルを再適用します。
[Devices]で一覧を表示し、全てのクライアントデバイスで、[Modified Profile]の表示が「Up to Date」となったことを確認し、既存の SDConnex サービスを停止します。

SES を別のサーバーに移行する場合の手順は以下のとおりです。

① SES にログインするためのキーファイル（拡張子は、dbk）を新たにインストールするサーバーに移動（コピー）します。

② SQL Server Management Studio を使って、既存のデータベースをバックアップします。

詳しくは、SQL Server Management Studio 開発元のサイトでご確認ください。
データベースの完全バックアップの作成
https://learn.microsoft.com/ja-jp/sql/relational-databases/backup-restore/create-a-full-database-backup-sql-server?view=sql-server-ver16

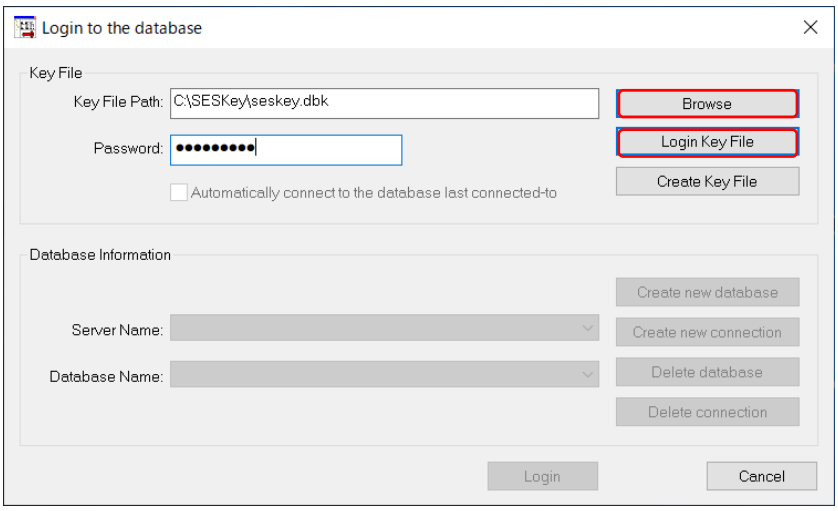
③ 新たに SES をインストールするサーバーに、Microsoft SQL Server、SQL Server Management Studio をインストールします。

④ SQL Management Studio を使って、バックアップ済のデータベースをレストアします。

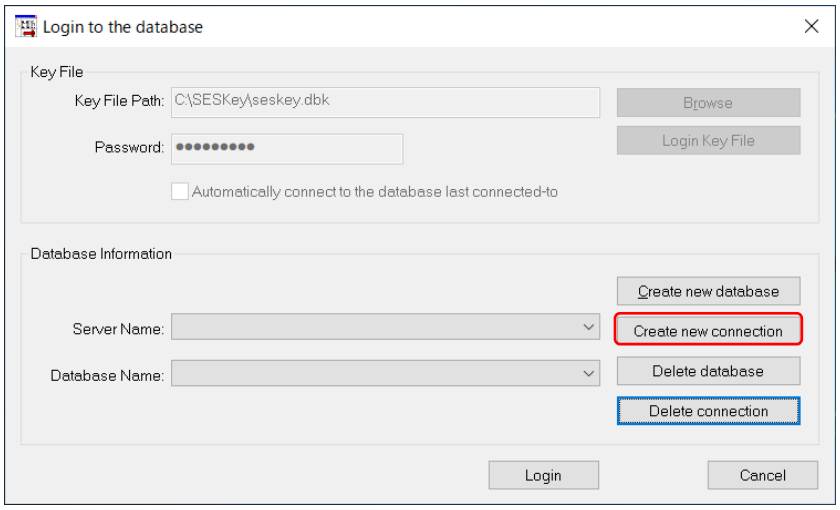
⑤ SecureDoc Enterprise Server をインストールします。
詳細は「SecureDoc Enterprise Server Version 9.2 クイックインストールガイド」を参照してください。

⑥ [スタート] > [SecureDoc Enterprise Server] > [SecureDoc Enterprise Server] を実行します。

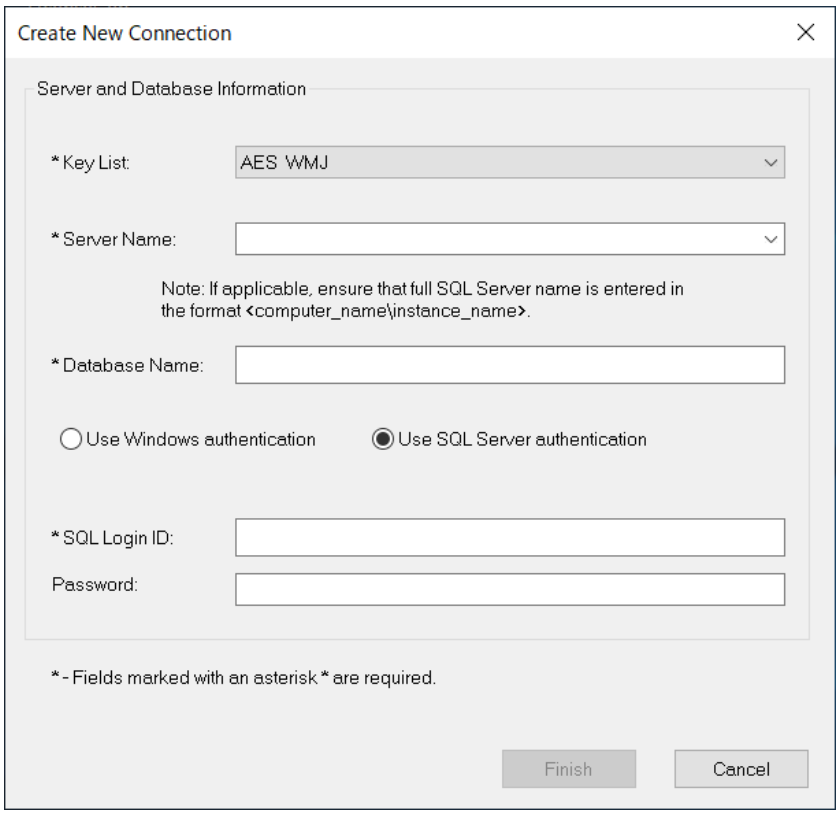
⑦ ログイン画面が表示されたら、<Browse>をクリックしてキーファイルを選択し、パスワードを入力後、<Login Key File>ボタンをクリックします。



⑧ <Create new connection>をクリックします。



⑨ データベースに接続するための設定をします。



⑩ 接続に成功すると、SES が起動します。

⑪ 「SDConnex Service」、「ADSync Service」、「Analytics Engine Service」を再設定してください。

[スタート] > [SecureDoc Service Configuration] > [SecureDoc Service Configuration] を実行します。

各サービスの設定方法は、「SecureDoc Enterprise Server Version 9.2 クイックインストールガイド」を参照してください。

10. SecueDoc クライアント・アンインストール手順

クライアントから SecureDoc をアンインストールする場合は、予め復号化およびブートログオン（プリブート認証プログラム）のアンインストールが必要です。復号化するためには、[Convert Hard disk] の権限が必要です。
クライアントデバイスに管理者権限のユーザーID が登録されていない場合、SES からクライアントに管理者のユーザーID を追加してください。

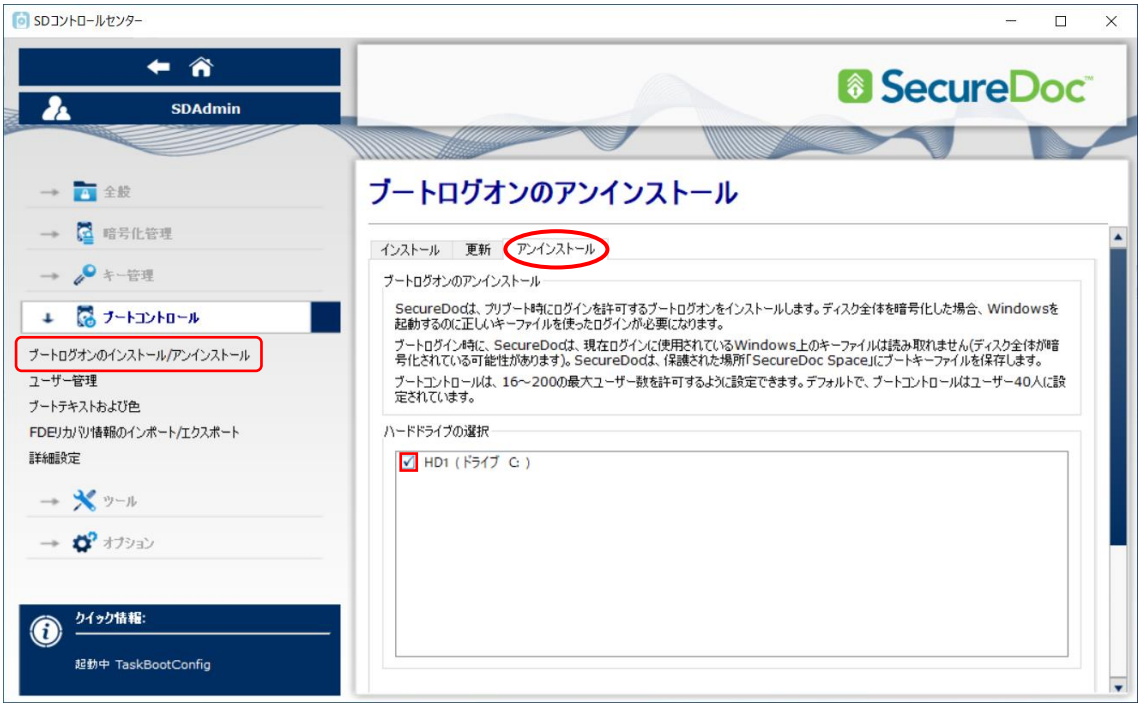
① 「SecureDoc コントロールセンター」を起動し、[Convert Hard disk] の権限を持っているユーザーID でログインします。

② SD コントロールセンターの左ペインで、[暗号化管理] のプルダウンメニューから [暗号化管理] をクリックします。右ペインで、ディスクを選択し、下部にある [操作] 欄より、「復号化」、「完全」を選択し、<開始> ボタンをクリックします。

③　復号化するディスクを正しく選択できていなかった場合、「先にディスクを選択してください」と表示されますので、<OK> をクリックし、やり直します。

④　復号化が開始されたら、完了するまで待ちます。

⑤　復号化完了後、ブートログオンをアンインストールします。
[ブートコントロール] のプルダウンメニューから [ブートログオンのインストール/アンインストール] をクリックします。次に、右ペインの [アンインストール] タブで、ブートディスクを選択し、画面をスクロールして下部にある <アンインストール> をクリックします。



⑥　警告が表示されますので、<OK>ボタンをクリックします。

⑦　アンインストール後に再起動する警告が表示されます。内容を確認して、<OK> をクリックします

⑧　OS 再起動後、「SecureDoc Disk Encryption」をアンインストールできます。

⑨　「SecureDoc Disk Encryption」をアンインストール後、OS の再起動を求められます。
再起動後、ディスクに残されている下記のプログラムを削除することができます。
C:¥Program Files¥WinMagic

注　SecureDoc を再インストールする場合は、SecueDoc のアンインストール後、必ず OS を再起動してから実行してください。OS の再起動することで、SecueDoc のアンインストールが完全に完了します。再起動せずに、再インストールを実行すると、予期せぬ不具合の原因となります。