# SafeCrypt ユーザーガイド

DataLocker Inc.

2019 年 6 月


## SafeCrypt

# 内容

# SafeCrypt について

SafeCrypt は、ネイティブシステムインターフェースで機密ファイルを管理できるソフトウェアベースの暗号化プラットフォームです。Windows では、暗号化された仮想ドライブはドライブ文字です。 macOS では、ストレージボリュームです。 この暗号化された仮想ドライブに保存されたファイルは、FIPS 140-2 承認アルゴリズムを使用して自動的に暗号化され、システムストレージの場所に保存されます。 このシステムストレージの場所は、ローカルメディア、ネットワーク共有、クラウドゲートウェイなど、コンピューターからアクセス可能な任意のストレージデバイスにすることができます。
最大 3 つの SafeCrypt インストールを同じシステムストレージに接続できるため、異なるマシンの SafeCrypt ドライブにアクセスできます。 基礎となる暗号化はファイルレベルで実行されるため、暗号化された仮想ドライブで変更が行われたときにネットワークを効率的に使用できます。
注：この製品を使用するには、SafeConsole サーバーが必要です。 会社に SafeConsole サーバーがない場合は、dl@itdirect.co.jp までご連絡ください。

## ハイライト

単に安全：

- •ユーザーが自分の暗号化を制御できる Cloud Encryption Gateway ソフトウェアプラットフォーム。
- •パスワードを入力してから、ファイルを仮想ドライブ文字にドラッグアンドドロップします。
- •ランサムウェア攻撃から安全。これらの攻撃は、ローカルドライブで一般的に使用されているファイルタイプをスキャンし、それらを暗号化します。機密ファイルはすでに暗号化されており、識別できません。

軍用グレードの暗号化：

- •暗号化エンジンは、OpenSSL 証明書＃2768 を使用して FIPS 140-2 認定されています。
- •すべての暗号化はローカルで行われるため、クラウドサーバーがハッキングされてもデータは安全です。

一元管理：

- •すべての SafeCrypt 管理エンドポイントを中央コンソールからインベントリ、監査、制御します。
- •ユーザーとその居場所を追跡します。
- •すべてのユーザーのファイルアクティビティを監査します。
- •無効化、強制終了、およびパスワード回復アクションをリモートで実行して、ユーザーファイルへのアクセスを制御します。

## 必要条件

- •SafeConsole 接続トークン
- •互換性のあるオペレーティングシステム：
  - Windows 7 または 10
  - macOS 10.12 から 10.14
- •1GB の RAM
- •200MB のハードディスク空き容量
- •SafeConsole Server への接続

## ライセンス

作成される暗号化された仮想ドライブごとに SafeCrypt ライセンスが必要です。 1 つのライセンスにより、3 つのシステム上の 1 人のユーザーが暗号化仮想ドライブにアクセスできます。 SafeCrypt を使用するには、アクティブな SafeConsole サーバーが必要です。 会社にまだ SafeConsole がない場合は、sales@datalocker.com に連絡して、購入に関する詳細情報を入手してください。

# 入門

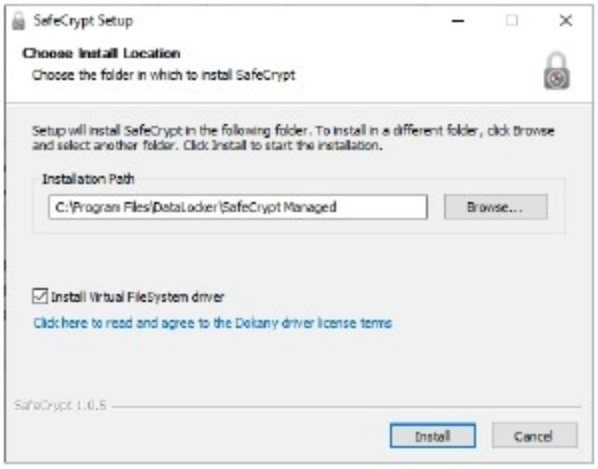
## ダウンロードとインストール

SafeCrypt の最新バージョンは、常にここから入手できます。

- Windows：https://media.datalocker.com/downloads/safecrypt/SafeCrypt-Setup-win64.exe
- macOS：https://media.datalocker.com/downloads/safecrypt/SafeCrypt-mac.dmg

### Windows

SafeCrypt を Windows コンピューターにインストールするには、SafeCrypt-Setup-win64.exe を起動し、インストールウィザードに従ってインストールパスを選択します。インストール中に Virtual FileSystem ドライバー（デフォルトでチェックされている）をインストールすることをお勧めします。 このドライバーを使用できない場合、SafeCrypt Virtual Drives はネイティブ Windows ファイルシステムとしてマウントされず、サードパーティ製アプリケーションのファイルにアクセスする際の動作が遅くなり、機能が制限されます。




### macOS

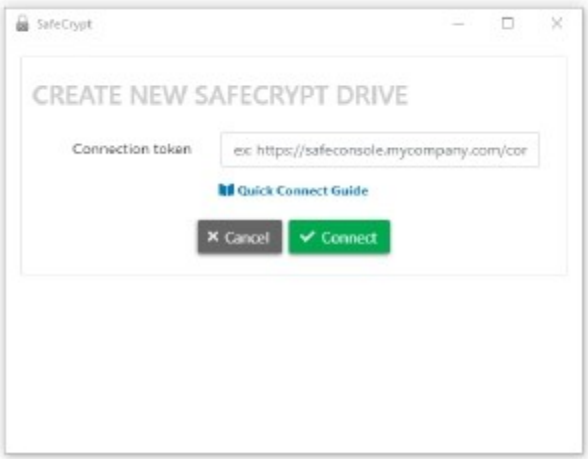
SafeCrypt を macOS コンピューターにインストールするには、SafeCrypt-mac.dmg ファイルを起動します。 次に、SafeCrypt アイコンをアプリケーションフォルダにドラッグするか、アイコンをダブルクリックして実行します。

# 暗号化された仮想ドライブの作成

SafeCrypt を初めて開くと、メールアドレスの入力が求められ、ライセンス条項に同意する必要があります。 入力したら、以下に概説する手順に従って、暗号化された仮想ドライブを作成します。

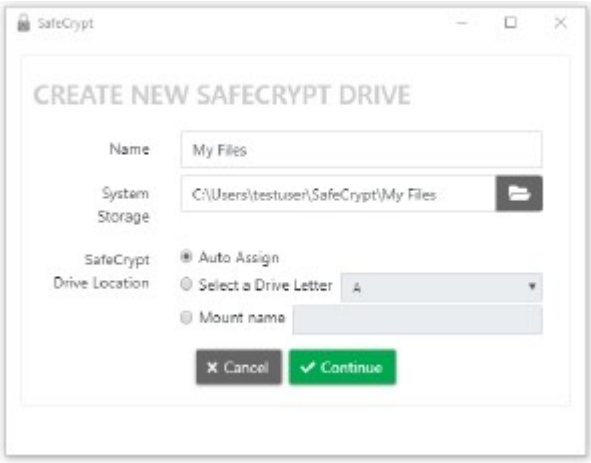
1. [+]アイコンをクリックして、新しいドライブの作成を開始します。
2. SafeConsole 管理者から提供された SafeConsole 接続トークンを入力します。 接続トークンがメールで送信された可能性があります。

注：現在の SafeCrypt ドライブが既に存在する場合、以前に使用した接続トークンを選択するか、新しい接続トークンを入力するかの 2 つのオプションがあります。





3. [名前]ボックスに、暗号化された仮想ドライブの名前を入力します。 この名前は、SafeCrypt ドライブを識別するために使用されます。 この名前は、ドライブがロック解除されたときにボリューム名としても使用されます。



4. [システムストレージ]セクションで、暗号化されたファイルを保存する場所を選択します。使用するフォルダを選択します。デフォルトでは、これは上記のユーザーのプロファイルフォルダー内に入力された名前と一致するフォルダーになります。例：
C：¥ Users ¥ John ¥ SafeCryptDrive
警告：暗号化された仮想ドライブを作成すると、その中のすべてのファイルが削除されるため、選択するフォルダーは空にする必要があります。
注：ファイルは、SafeCrypt の外部のこのフォルダーに直接保存しないでください。に追加されたファイル
SafeCrypt アプリケーションの外部にあるこのフォルダーは暗号化されません。

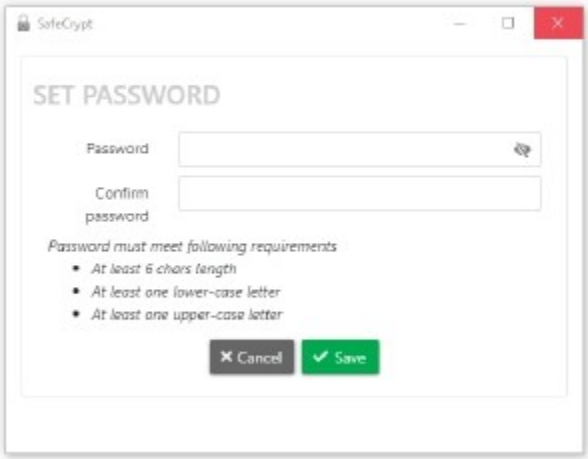
5. SafeCrypt ドライブの場所を選択します（Windows のみ）。 SafeCrypt ドライブの場所には 3 つのオプションがあります。

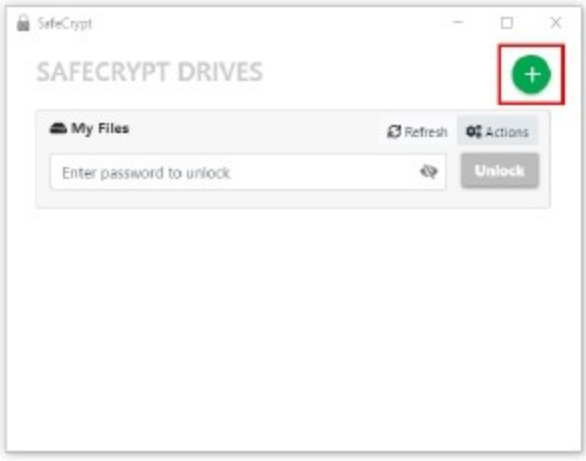
- 自動割り当て：最初の空きドライブ文字が暗号化された仮想ドライブに割り当てられます（推奨）
- ドライブ文字の手動選択：使用可能なドライブ文字のリストから暗号化された仮想ドライブの特定のドライブ文字を選択します。
- マウント名：ドライブ文字としてマウントできない場合、マウント名を選択できます。
  ドライブはネットワーク共有ドライブのように動作します。注：これにより、特定のアプリケーションとの互換性が制限されることがあります。

6. SafeConsole Administrator によってオプションで有効にされた設定がいくつかあります。有効になっている場合、この時点で暗号化された仮想ドライブの作成が表示されます。

- ユーザー固有のトークン：SafeConsole 管理者は、暗号化された仮想ドライブを SafeConsole に登録するために Unique Token の入力を要求する場合があります。管理者がこのトークンをメールで提供する場合があります。
- 承認保留中：SafeConsole 管理者は、SafeConsole に登録する前に、暗号化された仮想ドライブの承認を要求する場合があります。管理者に連絡して承認を取得してください。管理者がドライブを承認したら、アクティベーション保留ボタンをクリックします。

7.パスワードを作成して確認します。パスワード要件は SafeConsole Administrator によって設定されます。パスワードが要件を満たせば、ドライブが作成されます。



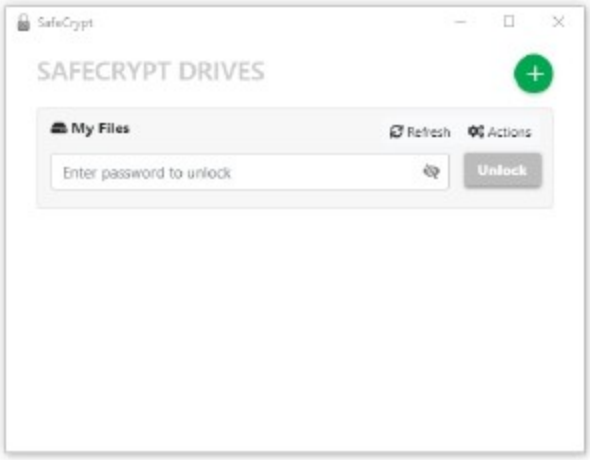

暗号化された仮想ドライブをさらに作成するには、右上隅の[＋]をクリックして同じ手順に従います。

# SafeCrypt 暗号化ファイルへのアクセス

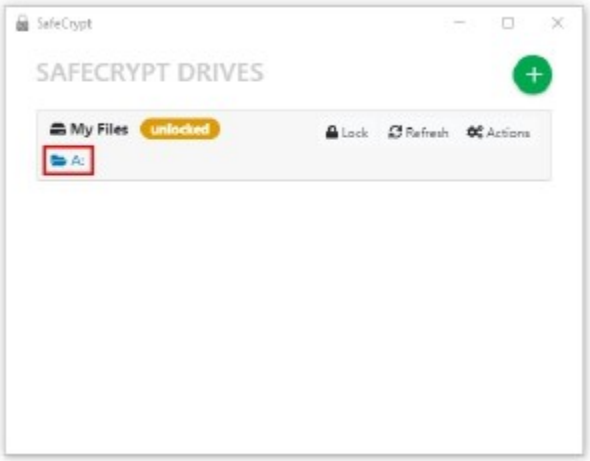
SafeCrypt ドライブのロックを解除するには、SafeConsole への接続が常に必要です。
注：ドライブが[アクセスを拒否]または[無効]で表示されている場合、SafeConsole 管理者がドライブのステータスを復元するまで、ドライブのロックを解除することはできません。

## SafeCrypt ドライブのロック解除

1. SafeCrypt を開きます。 ファイルにアクセスするには、SafeCrypt が常に実行されている必要があります。
2.ロックを解除するドライブのパスワードを入力します。 パスワードが正しく入力されると、ドライブはロック解除された状態で表示されます。



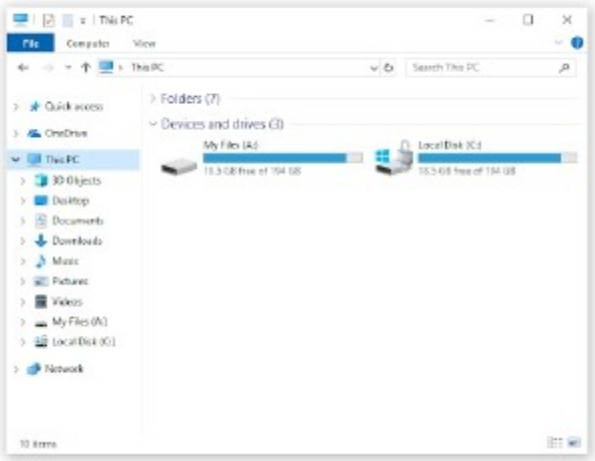

3.フォルダアイコンをクリックして、オペレーティングシステムファイルブラウザでファイルを開きます。




アプリケーションは、標準のストレージドライブのように、暗号化された仮想ドライブと対話できます。
SafeCrypt ドライブは、ロックアイコンをクリックするか、SafeCrypt を終了することにより、いつでもロックできます。

## Windows でのファイルアクセス

Windows マシンでは、ドライブはネットワークロケーションとして表示され、最初に利用可能なドライブ文字またはドライブの作成時に定義された特定のドライブ文字が割り当てられます。 SafeCrypt に割り当てられたドライブ文字を見つけるには、Windows エクスプローラーを開き、Windows 7 のコンピューターまたは Windows 10 のこの PC に移動します。ファイルは、このドライブ文字に転送するか、プログラムの[名前を付けて保存]ダイアログボックスで直接保存できます。



## macOS でのファイルアクセス

macOS マシンでは、ドライブはローカルホストの場所に接続されたボリュームとして表示されます。
最初のドライブのロック解除で、SafeCrypt から Finder へのアクセスを許可するように求められます。 これにより、Finder 内でお気に入りのショートカットを作成して、ロック解除された SafeCrypt ドライブにすばやくアクセスできます。 このショートカットは、ドライブのロックが解除されている間のみ利用できます。 Finder の[お気に入り]セクションまたはアプリケーションの保存ダイアログボックスで SafeCrypt ドライブ名を探して、ファイルを[SafeCrypt ドライブ]にコピーして保存します。


# SafeCrypt アクション

SafeCrypt ドライブがロックされている間、以下にリストされたオプションが利用可能です


## ドライブを編集

名前、システムストレージ、および SafeCrypt ドライブの場所は、ドライブが最初に作成されたときから変更できます。
System Storage を変更する場合、ファイルを新しい場所に手動で移動する必要があります。
SafeCrypt は、ファイルの移動を試みません。

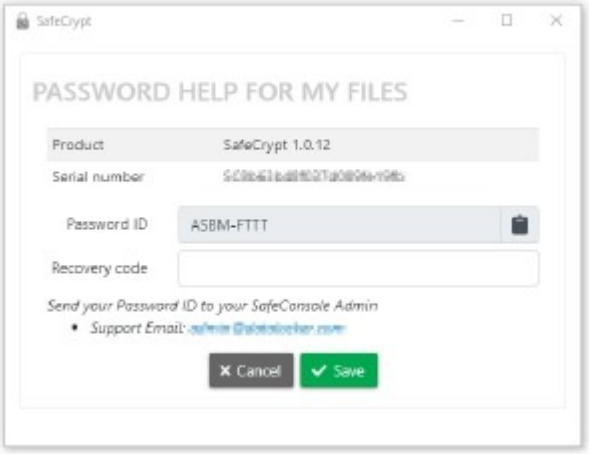
## バックアップセキュリティトークン

セキュリティトークンのバックアップにより、SafeCrypt ドライブをインポートして、暗号化されたファイルにアクセスできます。このインポートは、SafeCrypt ドライブへの同時アクセスを許可する新しいマシンで行うことも、将来必要に応じて同じマシンで行うこともできます。
選択すると、セキュリティトークンを SCM ファイルとして保存する場所を選択するよう求められます。
このファイルは、SafeCrypt®ドライブをインポートしてその内容にアクセスするために必要なので、SafeCrypt ボリューム内に保存しないでください。このファイルは安全に保管する必要があります。

注：新しいファイルを追加した後、セキュリティトークンを再度バックアップする必要はありません。
セキュリティトークンとともに、システムストレージのバックアップも作成する必要があります。これには、SafeCrypt ドライブに保存されているファイルの暗号化されたコンテンツが含まれます。 SafeCrypt Drive のファイルを変更または追加した後、システムストレージをバックアップする必要があります。

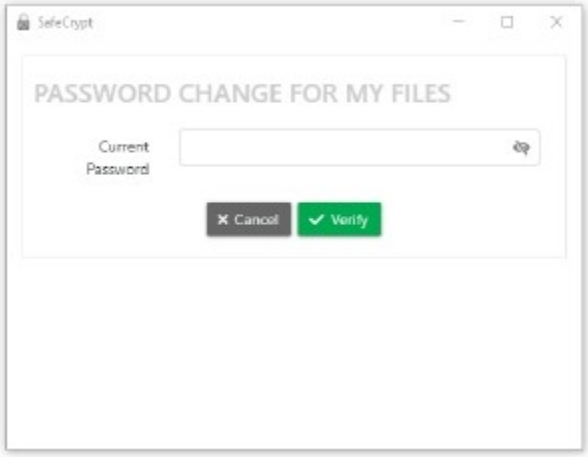
## パスワードヘルプ

SafeCrypt ドライブのパスワードを思い出せない場合は、SafeConsole Administrator がパスワードヘルプを使用して新しいパスワードの設定を支援します。 選択すると、ドライブのシリアル番号とパスワード ID が表示されます。 パスワードリセットを実行するには、この情報を SafeConsole Administrator に提供する必要があります。 サポートのメールリンクをクリックすると、システムのメールクライアントに SafeConsole 管理者へのメールが事前に入力されます。
SafeConsole 管理者から受け取った回復コードを入力します。 正しい場合は、現在のパスワードポリシーに適合する新しいパスワードを作成するよう求められます。




## パスワードを変更する

現在の SafeCrypt Drive のパスワードを知っている場合は、いつでもパスワードを変更できます。 新しいパスワードは、SafeConsole 管理者が設定したパスワードポリシーの現在の要件を満たす必要があります。




## 削除する

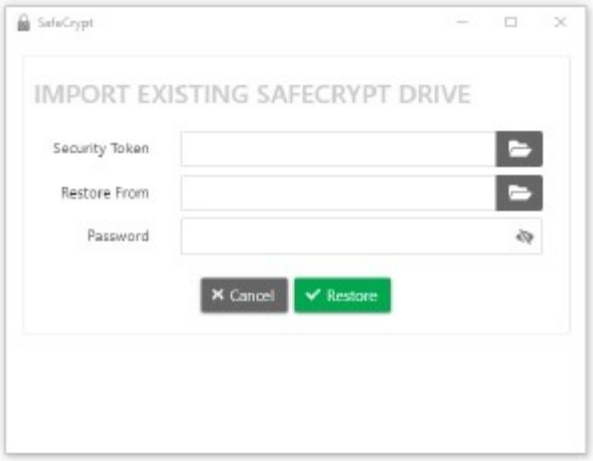
オプション：この設定は、SafeConsole 管理者によって無効にされている場合があります。このオプションを使用できない場合は、SafeConsole 管理者に連絡して、ドライブをリモートで削除してください。

警告：これにより、SafeCrypt ドライブに保存されているすべてのデータが削除され、元に戻すことはできません！
この操作により、ドライブとその内容がコンピューターから削除されます。また、SafeConsole からドライブを削除し、ライセンスシートを解放します。確認されると、ドライブはなくなり、セキュリティトークンのバックアップがあっても再インポートできなくなります。

# SafeCrypt ドライブのインポート

セキュリティトークンとシステムストレージの両方が利用可能で、パスワードがわかっている場合、SafeCrypt ドライブをバックアップからインポートできます。 SafeCrypt ドライブは、SafeConsole でも利用できる必要があります。 SafeCrypt ドライブがアクションまたはアンインストール中に削除されると、ドライブをインポートできなくなります。
このプロセスは、新しいコンピューターまたは 2 台目のコンピューターにドライブをインポートする場合でも同じです。 2 台目のコンピューターでは、同じ SafeCrypt ドライブを同時に使用できます。
SafeCrypt ドライブをインポートするには：

1. マシンに SafeCrypt をインストールします。詳細については、ダウンロードとインストールを参照してください。
2. システムストレージをコンピューターにインポートします。 System Storage がクラウド同期アプリケーションにリンクされている場合、これはクラウドエージェントを新しいコンピューターに再インストールするのと同じくらい簡単です。
3. システムトレイで SafeCrypt アイコンを見つけて、[ドライブのインポート]をクリックします。




セキュリティトークンのフォルダアイコンをクリックして、バックアップセキュリティトークンセクションの手順に従って作成された SCM バックアップファイルに移動します。
SafeCrypt は、以前のコンピューターの設定に基づいて、System Storage Location に自動的に入力します。これが新しいコンピューターで異なる場合は、[インポート元]で新しい場所を指定します。

4. ドライブのパスワードを入力し、[インポート]をクリックします。 これで、ドライブが SafeCrypt リストに追加されます。
注：SafeCrypt は、使用を 3 つのドライブに制限します。 別のコンピューターでファイルにアクセスする前に、開いているアプリケーションからファイルを閉じてください。

# 設定

ユーザー設定にアクセスするには、システムトレイを右クリックして[設定]をクリックします。

## プロキシ

プロキシ設定を使用するには、ネットワーク管理者から提供された設定を入力します。

## デバッグを有効にする

デバッグモードを有効にする必要があるのは、DataLocker テクニカルサポートから要求された場合のみです。この設定を完全に有効にするには、SafeCrypt を再起動する必要があります。
デバッグログは、システムトレイの SafeCrypt アイコンを右クリックし、[バージョン情報]、[ログファイルの表示]の順にクリックして見つけることができます。 SafeCrypt のインストールで問題が発生した場合、作成されたログは support@datalocker.com にメールで送信できます。

# 更新情報

SafeCrypt は、Windows システムと macOS システムの両方で自動的に更新されます。 SafeCrypt が開始されるたびに、アプリケーションは新しい更新をチェックします。新しいバージョンが利用可能な場合、SafeCrypt を更新するように求められます。インストールする前に、Web ブラウザで新しいリリースノートを表示できます。
更新を手動で確認するには、システムトレイの SafeCrypt アイコンを右クリックし、[バージョン情報]、[更新の確認]の順にクリックします。

# アンインストール

コンピューターから SafeCrypt をアンインストールするには、オペレーティングシステムのアンインストール方法を使用します。

- Windows：[プログラムの追加と削除]に移動し、SafeCrypt を見つけます。
- macOS：SafeCrypt をアプリケーションリストからゴミ箱にドラッグします。

## アンインストールオプション

これらのオプションは Windows でのみ使用可能です。

**すべての SafeCrypt 設定をクリア**
このオプションは、すべてのローカル SafeCrypt 設定を削除します。システムストレージの場所にある実際のデータファイルは削除されません。設定をクリアする前にセキュリティトークンがバックアップされていれば、ドライブを再度インポートできます。

**SafeCrypt ドライブの登録解除**
SafeCrypt アプリケーションの登録を解除すると、リモート SafeConsole Server 上のドライブが削除され、ライセンスシートが解放されます。成功した場合、セキュリティトークンのバックアップが利用可能であっても、ドライブをインポートできません。

# ヘルプはどこで入手できますか？

このマニュアルを参照してもソフトウェアに未解決の問題がある場合は、メールでお問い合わせいただくか、次の場所で詳細をご確認ください。

- support.datalocker.com：情報、知識ベースの記事、およびビデオチュートリアル
- support@datalocker.com：フィードバックと機能のリクエスト
- datalocker.com：一般情報
- datalocker.com/warranty：保証情報

システムトレイの SafeCrypt アイコンを右クリックして、[ヘルプ]をクリックすることもできます。
サポートに連絡する前にデバッグモードをオンにし、デバッグモードセクションの手順に従うことで、テクニカルサポートチームが支援するのに必要な時間を短縮できます。