SafeConsole Admin Guide

version 5.2.0

コンテンツ

    - ポリシー　ファイル制限
    - ポリシー　デバイス監査
    - ポリシー　カスタムメイドのデバイス情報
    - ポリシー　ZoneBuilder
    - ポリシー　パブリッシャー
    - ポリシー　ジオフェンス
    - ポリシー　信頼されたデバイスゾーン
- サーバー設定　デバイス登録とジオロケーション編集
    - デバイス登録設定
    - ジオロケーション編集
- 監査ログ　デバイスの使用と管理者アクション
    - デバイス監査ログ
    - システムメッセージ
    - SIEM およびその他の外部ログ収集統合
- SafeConsole の管理スタッフの設定
    - 管理者アカウントのプロファイル設定
    - 管理者スタッフのアクセスレベル
    - 新しい管理者スタッフの設定
    - 管理者スタッフの消去
    - 管理情報の表示をカスタマイズする
    - 管理者スタッフの情報をエクスポートする
    - 管理者スタッフの 2 段階認証を設定する
- デバイスを SafeConsole に接続する
    - デバイスを SafeConsole にすばやく接続する
    - 組織のデバイスを SafeConsole に登録する
    - デバイス登録のトラブルシューティング
- ライセンスのインストール
    - SafeConsole On-Prem のライセンス
- サポート
    - トラブルシューティングのベストプラクティス

イントロダクション

This guide provides SafeConsole administrative users with the knowledge required to configure and handle the SafeConsole on a day-to-day basis.

このガイドでは、SafeConsole の管理ユーザーに、SafeConsole を日常的に設定および処理するために必要な知識を提供します。

The guide is applicable for both SafeConsole Cloud and On-Prem – it does not cover cloud setup or on-prem installation.

このガイドは、SafeConsole クラウドと On-Prem の両方に適用されます。クラウドセットアップや On-Prem インストールについては説明していません。

SafeConsole とは？

The SafeConsole is a web server and a database that is accessible for authenticated administrators through a web browser to enable administration of registered SafeConsole Ready secure USB devices.

SafeConsole は、登録された SafeConsole 対応セキュア USB デバイスの管理を可能にする Web ブラウザと、認証された管理者がアクセスできるデータベースです。

The SafeConsole Ready Devices connect to the SafeConsole server through HTTP over SSL (TLS 1.2 over a configurable port – with 443 set as the default) to register and to fetch their policies and configurations.

SafeConsole 対応デバイスは、ポリシーと設定を登録および取得するために、HTTP over SSL（設定可能なポートを介して TLS 1.2 – デフォルトで 443 が設定されている）を介して SafeConsole サーバーに接続します。

SafeConsole の目的

SafeConsole offers organizations control of portable storage device usage while it supports the device users with password resets and more. Learn more at:
SafeConsole はポータブルストレージデバイスの使用を制御し、パスワードリセットなどのデバイスユーザをサポートします。https://datalocker.com/safeconsole/

SafeConsole ではどのようにデバイスを管理するのか

Devices are registered to SafeConsole, using the standalone device software on the read only partition, either by:

デバイスは SafeConsole に登録され、読み取り専用パーティションのスタンドアロンデバイスソフトウェアを使用して、次のいずれかの方法で SafeConsole に登録されます。

- The device software recognizing a deployed registry key that contains the SafeConsole Connection Token – this prompts the device software to enter the setup and prefills the **Connection Token** from the registry key contents. ・SafeConsole Connection Token を含む展開されたレジストリキーを認識する

デバイスソフトウェア – デバイスソフトウェアにセットアップを入力し、レジストリキーの内容から接続トークンを事前に入力するように求められます。

- The user entering a server common SafeConsole **Connection Token** in the device software, optionally complemented with a **unique registration token**, that they can be emailed through SafeConsole together with the **Quick Connect Guide**.

  デバイスソフトウェアにサーバー共通の SafeConsole 接続トークンを入力し、必要に応じて一意の登録トークンを追加して、SafeConsole 経由でクイック接続ガイドと共に電子メールで送信できるようにする。

Once registered, the devices have the server information embedded in a hidden area of the device and can be used on any computer – if allowed to do so.

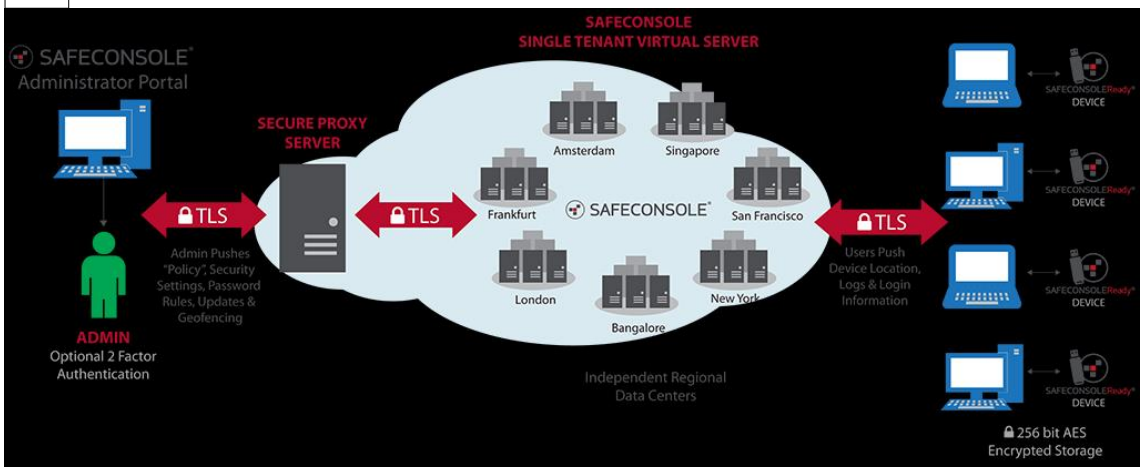
登録されたデバイスは、デバイスの隠し領域に埋め込まれたサーバー情報を持ち、許可されていれば、どのコンピュータでも使用できます。

Devices can be **reassigned** in the SafeConsole if you wish to register devices on behalf of your end users.

エンドユーザーに代わってデバイスを登録する場合は、SafeConsole でデバイスを再割り当てすることができます。

The process for device communication and setup is the same for SafeConsole Cloud and SafeConsole On-Prem.

デバイスの通信とセットアップのプロセスは、SafeConsole Cloud と SafeConsole On-Prem で同じです。



SafeConsole Cloud network schematic SafeConsole クラウドネットワークの回路図

SafeConsole の基礎

SafeConsole スタッフアクセス

- **SafeConsole Cloud** access is setup using one's email address to receive an invitation with an activation link. The invitation also contains the URL to the SafeConsole Server. The first invitations are sent by the super admin, which is the admin registered with the server license.

  SafeConsole クラウドへのアクセスは、自分のメールアドレスを使用してアクティベーションリンク付きの招待を受け取るように設定されます。招待状には、SafeConsole Server の URL も含まれています。最初の招待状は、サーバーライセンスに登録されている管理者であるスーパー管理者によって送信されます。

- **SafeConsole On-Prem** can be accessed either using credentials setup in the SafeConsole Configurator or Active Directory credentials assigned to a configured Security Group. The URL for the SafeConsole Server is visible in the last step of the SafeConsole Configurator.

  SafeConsole On-Prem は、SafeConsole コンフィグレータの資格情報設定または設定されたセキュリティグループに割り当てられた Active Directory 資格情報を使用してアクセスできます。SafeConsole Server の URL は、SafeConsole コンフィグレータの最後の手順で表示されます。

- There are three levels of access for SafeConsole staff: ·SafeConsole スタッフには、3 つのレベルのアクセス権があります。
  - **Administrators** – *Can purchase licenses, add administrators, configure devices, monitor audit logs and perform device actions. o 管理者 – ライセンスの購入、管理者の追加、デバイスの設定、監査ログの監視、デバイスアクションの実行が可能です。*
  - **Managers** – *Can configure devices, monitor audit logs and perform device actions. マネージャー – デバイスを設定し、監査ログを監視し、デバイスアクションを実行できます。*
  - **Support team** – *Can perform a limited number of device actions, such as password resets. Cannot change device configurations. サポートチーム – パスワードリセットなどの限られた数のデバイスアクションを実行できます。デバイスの設定を変更することはできません。*

SafeConsole のベストプラクティス

Follow this approach and you will efficiently get ready to deploy the SafeConsole solution to your organization:

このアプローチに従うと、組織に SafeConsole ソリューションを効率的に導入する準備が整います。

1. **Review** the short Basics section of this guide. このガイドの短い基本事項を確認します。
2. **Configure** – Try configuring some policies that apply to all devices. 2.設定 – すべてのデバイスに適用されるポリシーを設定します。
3. **Connect** – Register your device and see the policies enforced. 3.接続 – デバイスを登録し、施行されたポリシーを確認します。
4. **Manage** your device. Try to do a Factory Reset or a Password reset. デバイスを管理します。ファクトリリセットまたはパスワードリセットを実行してください。
5. **Reports** – Review and Export Reports. You will be asked to answer questions about the system by your organization. Familiarize yourself with the Exported XML or CSV in Excel. レポート – レポートのレビューとエクスポート。組織のシステムに関する質問に答えるように求められます。Excel でエクスポートされた XML または CSV に慣れてください。

SafeConsole クリックスルーツアー

To the left SafeConsole has the main menu and at the right a top drop-down menu for Profile Settings and Logout. In the Profile Settings Two-factor Authentication can be activated by each individual SafeConsole staff member, SafeConsole administrators can verify that two-factor authentication has been activated under the Staff Settings in the main menu.

SafeConsole の左側にはメインメニューがあり、右側にはプロファイル設定とログアウトのトップドロップダウンメニューがあります。プロファイル設定では、SafeConsole スタッフごとに 2 要素認証を有効にすることができます。SafeConsole 管理者は、メインメニューのスタッフ設定で 2 要素認証が有効になっていることを確認できます。

In short, these are the Main menu items. これらはメインメニュー項目です。

ダッシュボード

The landing page of SafeConsole. It provides a birds-eye view of the server.
SafeConsole のランディングページ。サーバーの全体図を提供します。

マネージ

The Manage page of SafeConsole lets you edit and configure Policies, Users, and Devices. Clicking a blue link in one of the fields will filter viewable entries based on the selected link. For example: clicking on a User's Path will show the policy for that path. Or clicking Users on a Policy will show the corresponding users and devices registered those users. You can use these filters to help you find related entries.
SafeConsole の[管理]ページでは、ポリシー、ユーザー、およびデバイスを編集および設定できます。いずれかのフィールドで青色のリンクをクリックすると、選択したリンクに基づいて表示可能なエントリがフィルタリングされます。たとえば、ユーザーのパスをクリックすると、そのパスのポリシーが表示されます。ポリシーのユーザーをクリックすると、対応するユーザーとそのユーザーが登録されたデバイスが表示されます。これらのフィルタを使用すると、関連するエントリを見つけるのに役立ちます。

ポリシー

Modify the default policy or set configurations of registered devices based on the user's path. **Paths** directly relate to the user's placement in a directory service such as Microsoft's Active Directory. A path can include multiple users. Edit the Path's policy by selecting its active policy version. All policy configurations will appear listed in a popup. Click **Save** to apply the new policy. There are blue inline help texts and *More info* icons that can expand and will explain each policy. Policies are checked and applied each time the device unlocks where it can achieve a connection to SafeConsole. To remove and reset all policies open up the Policy Editor and click **Danger Zone** at the very bottom.

既定のポリシーを変更するか、ユーザーのパスに基づいて登録済みデバイスの構成を設定します。パスは、Microsoft の Active Directory などのディレクトリサービスでのユーザーの配置に直接関係します。パスには複数のユーザーを含めることができます。アクティブなポリシーバージョンを選択して、パスのポリシーを編集します。すべてのポリシー設定がポップアップで表示されます。[保存]をクリックして新しいポリシーを適用します。青いインラインヘルプテキストと、各ポリシーを展開して説明する More アイコンがあります。SafeConsole への接続が可能な場所でデバイスがロック解除されるたびにポリシーがチェックされ、適用されます。すべてのポリシーを削除してリセットするには、ポリシーエディタを開き、一番下の「危険ゾーン」をクリックします。

ユーザー

Displays your device users and their registered devices when you expand them using the +−sign in the second left column. Here you can also delete device users from the system and perform actions on their devices. In the wrench−menu next to the

user name in the User column you edit/remove the user. When expanded the options in the Devices section are available here also.

2 番目の左の列に+記号を使用して拡張したときに、デバイスのユーザーとその登録済みのデバイスを表示します。ここでは、システムからデバイスユーザーを削除し、そのデバイスでアクションを実行することもできます。[ユーザー]列のユーザー名の横にあるレンチメニューで、ユーザーを編集/削除します。展開すると、[デバイス]セクションのオプションもここで使用できます。

At the top right, you manage which columns to display and trigger Export of all registered data to CSV or XML. In the dropdown menu, select the columns of data you want to display or remove. Click away from the dropdown menu to close it. The data will be updated according to your selections. To easily scroll the columns on the horizontal axis press *Shift+Mouse wheel*, this applies to all data tables in SafeConsole.

右上に表示する列を管理し、登録されたすべてのデータを CSV または XML にエクスポートします。ドロップダウンメニューで、表示または削除するデータの列を選択します。ドロップダウンメニューからクリックして閉じます。選択した内容に従ってデータが更新されます。簡単に列を水平にスクロールするには、Shift +マウスホイールを押します。これは、SafeConsole のすべてのデータテーブルに適用されます。

You can import users in a standard CSV format if you don't have a live connection to your Active Directory. The Import CSV popup contains needed instructions.
Active Directory へのライブ接続がない場合は、標準 CSV 形式でユーザーをインポートできます。Import CSV ポップアップには、必要な指示が含まれています。

デバイス

Displays all registered devices and all their metadata. Allows you to perform Actions on devices:

登録されているすべてのデバイスとすべてのメタデータを表示します。デバイスに対してアクションを実行できます。

- Restore status ステータスの回復
- Approve (displayed only when pending staff approval) 承認（保留中のスタッフ承認がある場合のみ表示されます）
- Disapprove (displayed when approved) Disapprove（承認されたときに表示されます）
- Mark as lost 紛失としてマーク
- Reset password (displayed when activated under Policies) パスワードのリセット（[ポリシー]でアクティブにしたときに表示されます）

- Disable 無効
- Factory reset 工場出荷状態リセット

In the wrench-menu you can also edit data server side (these do not affect the device):

レンチメニューでは、データサーバー側を編集することもできます（これらはデバイスには影響しません）。

- Edit Custom Data (edit the column rows with custom collected data) カスタムデータの編集（カスタム収集データを使用して列の行を編集）
- Delete (removes the device from the server, leaves the device as is) 削除（デバイスをサーバから削除し、デバイスをそのまま残します）

監査ログ

Contains a submenu for *Device Audit Logs* and *System Messages*. Device Audit Logs contains all device actions, usage and if activated file audits. System Messages shows SafeConsole administrative staff actions.

デバイス監査ログとシステムメッセージのサブメニューが含まれています。デバイス監査ログには、すべてのデバイスアクション、使用状況、およびアクティブ化されたファイル監査が含まれます。[システムメッセージ]には、SafeConsole 管理スタッフの操作が表示されます。

リポート

Displays three dynamic report templates for: connections, device inventory and geolocation.

接続、デバイスインベントリ、ジオロケーションの 3 つのダイナミックレポートテンプレートを表示します。

サーバー設定

Set server behavior for device registration, device password reset and geolocation customization.

デバイス登録、デバイスパスワードリセット、ジオロケーションのカスタマイズのためのサーバー動作を設定します。

スタッフ設定

The SafeConsole Admins page provides a geographic overview of admin logins. Here you can add administrators with privileges and manage their access. Two-factor authentication is available as an option for staff and is activated in the top right profile menu. Administrators can verify that staff have activated two-factor authentication in the 2-Factor Login column.

SafeConsole Admins ページには、管理ログインの地理的概要が表示されます。ここでは、特権を持つ管理者を追加してアクセス権を管理できます。2 要素認証は、スタッフのオプションとして利用でき、右上のプロファイルメニューで有効になります。管理者は、2-Factor Login（2-Factor ログイン）列でスタッフが 2 要素認証を有効にしていることを確認できます。

ヘルプ

Help contains a submenu with: Deployment Wizard, Quick Connect Guide, Support, and License.

ヘルプには、展開ウィザード、クイック接続ガイド、サポート、およびライセンスのサブメニューが含まれています。

- The Deployment Wizard allows you to send the Quick Connect Guide to device users.

  デベロップメントウィザードでは、クイック接続ガイドをデバイスユーザーに送信できます。

- The Quick Connect Guide takes device users step by step through the process of registering a device to SafeConsole using the Connection Token that is displayed here in a textbox in the fourth step. At the top right under Legacy Devices, you find generated registry keys and an ADM file for mass deployment.

  クイック接続ガイドでは、デバイスユーザーは、第 4 ステップのテキストボックスに表示されている接続トークンを使用して SafeConsole にデバイスを登録するプロセスを順を追って説明します。レガシーデバイスの右下には、生成されたレジストリキーと一括展開用の ADM ファイルがあります。

- The Support page lists links to the helpdesk, the manual, release notes, and the latest device software update packages.

  サポートページには、ヘルプデスク、マニュアル、リリースノート、最新のデバイスソフトウェアアップデートパッケージへのリンクが一覧表示されます。

- The License page displays license information and allows you to enter new licenses.

  ライセンスページにライセンス情報が表示され、新しいライセンスを入力することができます。

初めて SafeConsole にデバイスを接続する

Navigate to the *Quick Connect Guide* under the *Help* section in the main menu. Follow the steps.

メインメニューの[ヘルプ]セクションにある[クイック接続ガイド]に移動します。手順に従ってください。

SafeConsole へのデバイス登録を確認する

Click Devices in the main menu. Your device should now be visible. **Note that the devices fetch new configurations and policies each time they are unlocked.**

メインメニューの[デバイス]をクリックします。あなたのデバイスが表示されるはずです。デバイスは、ロックが解除されるたびに新しい設定とポリシーを読み込みます。

デバイスアクション – パスワードのリセットとその他

Actions can be taken on a device in the *Users* or *Devices* section in the main menu. **Note that the device checks for Actions to apply each time the device software starts up.**

メインメニューの[ユーザー]または[デバイス]セクションのデバイスでアクションを実行できます。デバイスは、デバイスソフトウェアが起動するたびに適用されるアクションを確認します。

These are the Actions:これらがアクションです

状態回復

Sets the Device in a neutral state, removing any pending Actions.

デバイスをニュートラル状態に設定し、保留中のアクションをすべて削除します。

承認

Allow the device to become managed and take up a seat in the license. Activate the approval process under Server Settings

デバイスが管理され、ライセンスに準拠します。サーバー設定の承認プロセスを有効にする

非承認

Revokes the registration and the usage of a seat license of the device. The device will become unmanaged. Activate the approval process under Server Settings

デバイスのシートライセンスの登録と使用を取り消します。デバイスはアンマネージドになります。サーバー設定の承認プロセスを有効にする

紛失としてマーク

The device will, if setup in the Device State policy, display a message to the person trying to use the device.

スタッフがデバイスの保存されたデータに影響を与えずにパスワードをリセットできるようにします。忘れたパスワードは決して公開されず、スキームは暗号的に安全であり、デバイスのハードウェアブルートフォース保護を弱めません。

パスワード初期化

Enables the staff to help a device user reset their password without affecting the stored data of the device. The forgotten password is never exposed and the scheme is cryptographically secure and does not weaken the hardware brute force protection of the device.

スタッフがデバイスの保存されたデータに影響を与えずにパスワードをリセットできるようにします。忘れたパスワードは決して公開されず、スキームは暗号的に安全であり、デバイスのハードウェアブルートフォース保護を弱めません。

A password reset can only be performed provided that the Remote Password Reset policy has been applied and activated on the device prior to prompting the Reset password action.

パスワードのリセットは、パスワードのリセット操作を促すメッセージが表示される前に、デバイスでリモートパスワードリセットポリシーが適用され、有効になっている場合にのみ実行できます。

These are the steps to perform a password reset:パスワードリセットの手順

1. Open the device software. Get the eight character Client Request Code (Password ID). Found under Help > Forgot password in the main screen of the device software or displayed when the wrong password is entered more than two times in sequence.

   デバイスソフトウェアを開きます。8 文字のクライアント要求コード（パスワード ID）を取得します。デバイスソフトウェアのメイン画面で[ヘルプ]> [パスワードを忘れました]の順にクリックするか、誤ったパスワードを 2 回以上順番に入力すると表示されます。

2. In SafeConsole search to find the device under Devices or Users. The Device ID or serial number is under About in the device software. Verify at least the last four numbers.

   SafeConsole の検索で、デバイスまたはユーザーのもとにあるデバイスを検索します。デバイス ID またはシリアル番号は、デバイスソフトウェアの[バージョン情報]の下に表示されます。少なくとも最後の 4 つの数字を確認してください。

3. Select the Reset password Action in SafeConsole for the device.

   SafeConsole でデバイスの[パスワードのリセット]アクションを選択します。

4. Enter the Client Request Code (Password ID) in the SafeConsole prompt.

   SafeConsole プロンプトにクライアント要求コード（パスワード ID）を入力します。

5. The 24 character long Server Response Code will be displayed, and you can click to email it to the registered device user email address. You can also read the string to the device user. Make sure to get the string right as a faulty code can destroy all stored data. We suggest employing a phonetic alphabet.

   24 文字の長さのサーバー応答コードが表示されます。クリックすると、登録されたデバイスユーザーの電子メールアドレスに電子メールで送信できます。また、文字列をデバイスユーザーに読み取ることもできます。問題のあるコー

ドはすべての格納されたデータを破壊する可能性があるので、文字列を正しく取得してください。表音アルファベットを使用することをお勧めします。

6. The device user enters the Response Code in the device software and will now be prompted to enter a new device password.

   デバイスユーザーがデバイスソフトウェアに応答コードを入力すると、新しいデバイスパスワードを入力するよう求められます。

無効化

Disables the ability to unlock the device. A password reset can still be performed provided that the Remote Password Reset policy had been applied and activated on the device prior to prompting the Disable action. If left disabled the device cannot be used and is to be considered “bricked”.

デバイスのロックを解除する機能を無効にします。無効にするアクションを促すメッセージが表示される前に、デバイス上でリモートパスワードリセットポリシーが適用され、有効化されている場合は、パスワードリセットを実行することができます。無効のままにしておくと、デバイスは使用できなくなります。

工場出荷時リセット

The Factory reset action, sometimes referred to as *a remote kill*. The action erases the crypto keys and all stored data irrecoverably from the device on the next connect. The device can be reused and connected anew.

工場出荷時リセットおよびリモート強制終了は次の接続時に暗号キーと格納されたすべてのデータをデバイスから回復不能に消去します。このデバイスは再利用して新たに接続することができます。

サーバー上のデバイスとユーザーデータを編集する

デバイスデータ

In the main menu option Devices in the Serial column under the wrench-menu you are able to edit the devices data on the server.

デバイスオプション内の「シリアル」にあるレンチメニューではサーバー上のデバイスデータの編集が可能です。

消去

This removes the device from the server. The device becomes unmanaged and untouched. This is mainly used to release the seat license occupied of a destroyed or irrecoverably lost device.

ここでは、デバイスをサーバーから消去することができます。一度消去されたデバイスは管理不可能になり、再使用も不可能になります。この機能は主に破壊されたもしくは完全に紛失されたデバイスに占有されているライセンスを開放するために使用されます。※消去したデバイスを再使用する場合は必ず工場出荷リセットを行ってから消去してください。

再割り当て

This will allow you to appoint a new user as the device owner. It is possible to assign a device to any other registered user.

これにより、新しいユーザーをデバイスの所有者として指定することができます。他の登録ユーザーにデバイスを割り当てることも可能です。

カスタムデータ編集

Allows the administrator to edit data collected during the device setup – if configured under Custom Information in Policies.

管理者は、デバイスの設定中に収集されたデータを編集できます（ポリシーのカスタム情報で設定されている場合）。

ユーザーデータ

ユーザーデータ編集

In the main menu option Users in the User column under the wrench-menu you are able to edit the user data on the server, you can also remove the user here.

ユーザーオプション内の「ユーザー」にあるレンチメニューではユーザーデータの編集、ユーザーの削除が可能です。

ユーザーデータを含む CSV をインポートする

Note that users will be asked to enter their computer credentials as part of the connection of the device to the server, this behavior can be configured under Server Settings. With this option the database will populate with the directory structure as users connects devices. If you only have one policy and/or will not setup and reassign devices to end users this is the preferred option, to have the database self-populate.

デバイスのサーバーへの接続の一環としてユーザーにコンピュータの資格情報を入力するよう求められますが、この動作は[サーバーの設定]で構成できます。このオプションを使用すると、ユーザーがデバイスを接続すると、データベースにディレクトリ構造が設定されます。ポリシーを 1 つしか持たない場合や、エンドユーザーにデバイスを設定して再割り当てしない場合は、データベースを自動入力することをお勧めします。

It is however possible to import a standardized CSV with your users and groups if you lack a connection to your Active Directory. This imported structure can then be used to apply policies prior to users connecting to the server.

ただし、Active Directory への接続が困難な場合は、ユーザーとグループで標準化された CSV をインポートすることは可能です。このインポートされた構造を使用して、ユーザーがサーバーに接続する前にポリシーを適用することができます。

- Your CSV file should contain the following fields: DistinguishedName and EmailAddress

  CSV ファイルには、次のフィールドが含まれている必要があります。DistinguishedName および EmailAddress

- Recommended maximum entries per import: 1000

  インポートごとの推奨最大エントリ数：1000

Windows PowerShell command to create csv file:

csv ファイルを作成する Windows PowerShell コマンド：

```
Get-ADUser -Filter * -Properties DisplayName,EmailAddress |export-csv ad_users.csv
```

Once you have your csv file generated from your Active Directory you can import it by clicking Import CSV from the Users tab found under Manage. This will populate your SafeConsole Server by placing users in the path according to which Organization Unit they belong to in Active Directory.

Active Directory から CSV ファイルを生成したら、[管理]の[ユーザー]タブから[CSV のインポート]をクリックして CSV ファイルをインポートできます。これにより、Active Directory 内のどの組織ユニットに属しているかに応じて、ユーザーをパスに配置することで、SafeConsole Server に移行します。

For additional help with the Get-ADUser command, Visit Microsoft's KB

Get-ADUser コマンドの詳細については、Microsoft の KB にアクセスしてください

Please refer to this support article for additional help with this process: Exporting Active Directory Users as a CSV

このプロセスの追加のヘルプについては、このサポート記事を参照してください。
Active Directory ユーザーを CSV としてエクスポートする

You are required, prior to completing the import, to provide the character encoding of your CSV-file (US-ASCII, UTF-8 or UTF-16).

インポートを完了する前に、CSV ファイル(US-ASCII、UTF-8 または UTF-16)の文字エンコードを提供する必要があります。

ポリシー – パスワードポリシー設定とその他機能

The *Policies* section is reached through the main menu located under Manage.

「ポリシー」セクションはメインメニュー「マネージ」にあります。

Policies are checked and applied each time the device unlocks where it can achieve a connection to SafeConsole.

ポリシーは、デバイスが SafeConsole へ接続され、ロック解除されるたびにチェックされ、適用されます。

There are blue inline help texts and *More info* icons that will explain each option in each policy option. These are reiterated in this manual.

青いインラインヘルプテキストと、各ポリシーオプションの各オプションについて説明する詳細情報アイコンがあります。これらはこのマニュアルで再掲されています。

ポリシーセクションの概要

- The default policy can be modified by clicking the **Modify Default Policy** button in the top bar. The Default Policy is the fallback base that all other policies are based off. You must click, confirm and Save your default policy to complete the setup of the server. New registrations will use the geolocation and Trusted Network from the Default Policy unless unique tokens are enabled on the server.

  デフォルトポリシーは、上部バーの[Modify Default Policy]ボタンをクリックして変更できます。デフォルトポリシーは、他のすべてのポリシーに基づいているフォールバックベースです。サーバーの設定を完了するには、クリック、確認、およびデフォルトポリシーの保存が必要です。新しい登録は、サーバー上で一意のトークンが有効になっていない限り、デフォルトポリシーからジオロケーションとトラステッドネットワークを使用します。

- You can edit a path under the wrench-menu of in the Path column. Here it is possible to:

  [パス]のレンチメニューでパスを編集できます。ここで可能なこと:

  - **Add New User** - 現在のパスにユーザーを追加します。
  - **Add New Group** - 現在のパスの子パスを作成します。
  - **Import CSV** - Adds multiple users to the current path. CSV requires a specific format. For more information see: Adding users from CSV.

    複数のユーザーを現在のパスに追加します。CSV には特定の形式が必要です。詳細については、CSV からのユーザの追加を参照してください。

  - **Edit Path** - Changes the current path.現在のパスを変更します。
  - **Delete Path** - Deletes the current path if there are no users in the path.ユーザーがいないパスを消去します。

ポリシーエディタ

- The **Policy Editor** pops up when the button **Modify Default Policy** is clicked or when you select to *Create* or *Modify* a policy in the menu for the Path in the Policy column.

  [Modify Default Policy]ボタンをクリックするか、[Policy]列の[Path]メニューのポリシーを作成または変更するを選択すると、Policy Editor がポップアップします。

The policy editor displays all policy configurations in separate sections, each policy is covered in detail in this manual. In each section of the policy editor you can verify which policy version number the change will apply to. There is the *default* which is the base and fallback, and then when the default is modified a *custom #running-number* is created, for example *custom: #56*. The custom policies can be applied to Paths that have sub-paths that therefore inherit their configurations from the main Path and these are named *inherit: #custom-running-number* for example *inherit #56*. The inherited policies in their turn can be modified and will then become custom policies.

ポリシーエディタは、すべてのポリシー設定を別々のセクションに表示します。各ポリシーについては、このマニュアルで詳しく説明しています。ポリシーエディタの各セクションでは、変更が適用されるポリシーバージョン番号を確認できます。ベースとフォールバックであるデフォルトがあり、デフォルトが変更されるとカスタム＃running-number が作成されます（例：custom＃56）。カスタムポリシーは、サブパスがメインパスから設定を継承しているパスに適用でき、継承名は＃custom-running-number です（例：継承＃56）。順番に継承されたポリシーは変更でき、カスタムポリシーになります。

- It is also possible to click **Add New Path** to add a new path to the overview in the top bar. **Add New Path** をクリックして、上部バーの概要に新しいパスを追加することもできます。

パスにポリシーを割り当てる

In the Path column you can see the domain path and then in the Policy column you can modify or create a new policy for the Path in the menu, the **policy editor** will pop up when an option is selected.

パス列にはドメインパスが表示され、[ポリシー]列ではメニューの[パス]の新しいポリシーを変更または作成できます。オプションが選択されると、ポリシーエディタがポップアップします。

You can click the number in the the Users or Devices column to confirm which the policy applies to.

[ユーザーまたはデバイス]列の番号をクリックして、ポリシーが適用されることを確認できます。

ポリシー　ユーザーデフォルト

Available in the Policy Editor popup ポリシーエディタのポップアップで設定できます。

The **User defaults** policy allows you to manage the device software behavior.

ユーザーのデフォルトポリシーにより、デバイスソフトウェアの動作を管理できます。

The following configurations are available: 以下の設定が利用可能です

- **Pre-Selected Language**
    - Preset device software language to avoid user confusion on foreign systems as the device will use the host machine default.

      外部システムへのユーザーの混乱を避けるためにデバイスソフトウェアの言語をあらかじめ設定することができます。

    - Use this setting to specify a default language for all registered users. この設定を使用して、登録されているすべてのユーザーの既定の言語を指定します。Users may change this setting on the device if needed. Leave the "System Default"(English) if you do not wish to define a language.

      デバイス側でも言語設定が可能です。変更の必要がなければデフォルト（英語）のままにしてください。

    - English, Japanese, Korean, Spanish, French and Russian are available (if the language is not available in the device software version it will default back to English).

      英語、日本語、韓国語、スペイン語、フランス語、ロシア語が利用可能です（言語がデバイスソフトウェアのバージョンで利用できない場合、デフォルトの英語に戻ります）。

- **Disable users from resetting device.**
    - Disable users from resetting their devices. After a reset, a device can become unmanaged or managed by a different SafeConsole server. This option allows you to tie the devices to your server. Administrators can still perform the factory reset action. **Be advised that if the server is uninstalled while devices are registered these devices cannot be reset and cannot become managed by any other server**, Take extra care if using On-Prem to save copies of your server certificate, the password for the server certificate and ensure that IP can be assigned to a new server if the old goes down.

      ユーザーからのデバイスのリセットを無効にします。。リセット後、デバイスは管理対象外になるか、別の SafeConsole サーバーによって管

理される可能性があります。このオプションを使用すると、デバイスをサーバーに結び付けることができます。管理者は工場出荷時のリセット操作を実行できます。デバイスが登録されているときにサーバーをアンインストールするとデバイスをリセットすることもほかのサーバーに登録することもできなくなりますのでご注意ください。On-Prem を使用してサーバー証明書のコピーを保存する場合は、サーバー証明書のパスワードと IP ををを確認してください。古いものがダウンする IP を新しいサーバに割り当てることができます。

- **Disable password hints.**
    - Disables the user from setting a password hint. Use for extra security. The new NIST best practice preview suggests that you should not allow password hints as it might expose the devices password if poorly constructed hints are used.

      セキュリティ強化のためにユーザーのパスワードヒント設定を無効にします。新しい NIST のベストプラクティスではヒントからパスワードが漏れる可能性があるためパスワードヒントを許可するべきではないと勧めています。

- **Disable desktop notifications.**
    - Disables desktop notifications from appearing on the users device. This option ensures that the device software is “silent” after unlocked. This option is not advised to use unless special circumstances apply.

      ユーザーのデバイスに表示されるデスクトップ通知を無効にします。このオプションを使用すると、ロック解除後にデバイスソフトウェアが「サイレント」になります。特別な状況以外でのこのオプションの利用はお勧めしません。

ポリシーデバイスのユーザーインタラクション

The user cannot interact with the policy configuration and they are not alerted that the policy is activated. Any configurations will be forced upon the device.

ユーザーはポリシー構成に触れることはできず、ポリシーがアクティブになっていることは通知されません。すべての構成が強制的にデバイスに適用されます。

ポリシー アンチマルウェア

Available in the Policy Editor popup

Protect your devices from malware automatically and all the times with the on-board Anti-Malware protection. When devices unlock, the malware signature definition data is updated automatically when an internet connection is available. The feature is powered by Intel Security McAfee technology.

オンボードのマルウェア対策の保護機能を使用して、デバイスをマルウェアから自動的かつ常に保護します。デバイスのロックが解除され、インターネット接続が利用可能になるとマルウェア定義データは、自動的に更新されます。この機能は、Intel Security McAfee テクノロジによって提供されます。

The on-board Anti-Malware protection is only available for device clients running version 4.8.30 and higher. An Anti-Malware license will need to be purchased for each device.

オンボードのマルウェア対策保護は、バージョン 4.8.30 以降を実行しているデバイスクライアントでのみ使用できます。各デバイスにアンチマルウェアのライセンスを購入する必要があります。

The following configurations are available: 以下の設定が利用できます。

- **Enable Anti-Malware protection**
    - Enables the on-board Anti-Malware protection on the device. デバイス上のオンボードのマルウェア対策保護を有効にします。
    - Threat detections, remedations and signature updates will be visible in the Device Audit Logs 脅威の検出、修復、シグネチャの更新は、デバイス監査ログに表示されます

ポリシーデバイスのユーザーインタラクション

The user is not alerted that the policy is activated. The device software will automatically download the latest configurations from the McAfee server the next time it is unlocked and has a network connection. During this time of the initial download the device may be experience abnormal delay until the signature database is download, roughly 200MB. Once the database is downloaded the device will initiate the scanner in the background each time the device is unlocked, the scanner runs continuously and scans any files that are added during the session. Infected files are removed and the user is prompted with a notification that this has happened.

ポリシーがアクティブであることをユーザーに警告しません。デバイスソフトウェアは、次のロック解除時のネットワーク接続されているときに、McAfee サーバーから最新の設定を自動的にダウンロードします。初期ダウンロード際に、デバイスは、約 200MB のシグネチャデータベースがダウンロードされるまで、遅延を経験することが

あります。データベースがダウンロードされると、デバイスのロックが解除されるたびにデバイスはバックグラウンドでスキャナを起動し、スキャナは継続的に実行され、セッション中に追加されたファイルをスキャンします。感染したファイルは削除され、ユーザーにはこれが発生したという通知が表示されます。

The user can interact with the anti-malware once the device is unlocked in the Main Menu under the button **Anti-Malware**, when the button is clicked the Anti-Malware screen is brought forward. In the Anti-Malware screen the user can verify the status of the protection, the time of the last scan and the last file that was scanned. The user can also manually initiate an additional scan. Furthermore the user can verify the version of the engine and malware database and also the time of the last update. The user can also manually initiate a update of the malware database, this is not necessary to trigger under normal operation as the updates occur automatically.

ユーザーはデバイスのロックが解除されるとメインメニューにある Anti-Malware をクリックすることで操作できます。アンチマルウェア画面では、保護の状態、前回のスキャンの時刻、最後にスキャンされたファイルを確認できます。ユーザーは手動で追加のスキャンを開始することもできます。さらに、ユーザは、エンジンおよびマルウェアデータベースのバージョンおよび最後の更新の時刻を確認することができる。ユーザーは、マルウェアデータベースの更新を手動で開始することもできます。更新が自動的に行われるため、通常の操作でトリガーする必要はありません。

ポリシー デバイスの状態

Available in the Policy Editor popup

The Device state policy enables automatic inventory management of your devices.
デバイス状態ポリシーは、デバイスの自動管理を有効にします。

The following configurations are available:以下の設定が利用できます。

- **Lost drive message to user** text message 紛失状態時のユーザーへのメッセージ
    - Use this setting to enter a custom message to display to users when their device enters a lost state.

      デバイスが紛失状態になった時にユーザーに表示するメッセージを設定できます。

    - The message that will display when the device gets the Action **Mark as lost**. This text could say, please post to address or a contain a general notice or disclaimer.

デバイスが紛失としてマークされたときに表示されるメッセージです。。このテキストは、アドレス宛てに送信するか、または免責事項の一般的な通知を含むことができます。

- **Require devices to connect to the SafeConsole Server** checkbox

  デバイスを SafeConsole に接続するように要求するチェックボックス

  - Select this checkbox to require devices to connect to SafeConsole periodically. (Connections are indicated in the "Last Seen" column on the Registered Devices page.). You can also define the maximum number of days a device can maintain in-use status without connecting to SafeConsole and the status to enforce on any device that does not connect within the specified number of days(lost,access denied or disabled).

    デバイスが SafeConsole に定期的に接続するようにするには、このチェックボックスを選択します。（接続は、「Registered Devices」ページの「Last Seen」列に表示されます）。また、SafeConsole に接続せずにデバイスが使用中の状態を維持できる最大日数と、指定した日数（紛失、アクセス拒否または無効）で接続しないデバイスに適用するステータスを定義することもできます。

  - These are the available options:
    - **Periodically**, configure *Maximum # of days without connection* numerically in number of days. Also configure selector *After maximum # of days reached, set status* to either:

      定期的に、接続なしの最大日数を数値で数値で設定します。また、最大日数に達した場合の状態を次のいずれかに設定します：

      - **紛失**（紛失メッセージのみ表示）
      - **アクセス拒否**（デバイスのアクセス禁止）※デバイスアクションの状態を復元で解除可能
      - **無効**（パスワードリセットが必要）リモートパスワードリセットが無効になっている場合は工場出荷リセットが必要になります。
    - **Always**, requires device v4.8.25+. You may use ZoneBuilder's Restricted Device Access feature to provide greater control over offline usage. デバイス v4.8.25 +が必要です。ZoneBuilder

の制限付きデバイスアクセス機能を使用して、オフラインでの使用をより詳細に制御できます。

ポリシーデバイスのユーザーインタラクション

The user cannot interact with the policy configuration and they are not alerted that the policy is activated. Any configured messages will be displayed at the set time and the states will be forced upon the device without warning (beyond the set message).

ユーザーにはポリシーが設定されたことは通知されません。設定されたすべてのメッセージが指定の条件のもと表示され、警告されずにデバイスの状態は強制的に変更されます。

ポリシー　休止ロック

Available in the Policy Editor popup

When enabled the policy activates a configurable device timer lockdown. This option should be enabled as devices are often forgotten unlocked in host machines. Without the Inactivity Lock, you risk a data breach.

ポリシーを有効にすると、設定した時間の経過後にデバイスがロックされます。この機能は、PC 接続中にロックが解除されたままのデバイスからデータが流出するのを防ぎます。

The following configurations are available:

- **ユーザー設定可能** –デバイスのロック解除後にユーザー自ら設定できます。
- **ポリシーによる強制** – SafeConsole で設定します。
    - **デバイスに Inactivity Lock を使用させる** – Inactivity Lock の設定を有効にするには、この設定を有効にします。また、デバイスがロックされるまでの非アクティブ時間（分）と、デスクトップ警告メッセージをユーザーに表示するときの非アクティブロックまでの秒数を定義することもできます。このポリシーを完全に無効にする場合は、チェックをはずしておきます。
        - **タイムアウト（分）**– 数字を入力します。
        - **デスクトップ警告メッセージ（秒）** – 数字を入力します。

ポリシーデバイスのユーザーインタラクション

ユーザーにはポリシーが設定されたことは通知されず、警告も表示されません。ポリシーで**ユーザー設定可能**を選択した場合はユーザーが自ら設定することも、無効にすることもできます。

ポリシー 許可された自動実行

Available in the Policy Editor popup

The following configurations are available:

- **すべてのデバイスに許可されたオートラン設定が可能**

  Use this setting to specify a command to run on all devices after the user authenticates. Enter the specific command to run in the text field provided. Authorized autorun allows SafeConsole managed devices to run portable software or other security tools upon authentication, providing added protection for the drive while it is unlocked.

  この設定を使用して、ユーザーの認証後にすべてのデバイスで実行するコマンドを指定します。 指定したテキストフィールドに実行する特定のコマンドを入力します。 認可されたオートランにより、SafeConsole 管理対象デバイスは、ポータブルソフトウェアやその他のセキュリティツールを認証時に実行できるようになり、ロックが解除されている間にドライブを保護することができます。

  - **Command to run** text box, type in your command you want to run.

    コマンドを実行するには、テキストボックスに実行するコマンドを入力します。

  - Tokens allow you to perform integration against the portable software that you can deploy to your device using the Publisher policy. These are the tokens that can be used in the **Command to run**:

    トークンを使用すると、パブリッシャポリシーを使用してデバイスにデプロイできるポータブルソフトウェアとの統合を実行できます。コマンドで実行するために使用できるトークンは次のとおりです。

    - {store-path} –デバイス暗号化ストレージパーティションボリューム
    - {serial} – デバイスの ID
    - {login-path} – デバイスの CD-ROM パーティションボリューム
    - {user-name} – デバイスユーザの登録ユーザ名

- デバイスのロックが解除されたときに、デフォルトのブラウザで起動するために http://www.example.com という Web サイトを入力します。

複数のコマンドを一度に実行する例

It is possible to specify several commands to run by entering them in a *.cmd batch file. Tokens can be sent to the script and set as local variables.

＊.cmd バッチファイルに複数のコマンドを入力して実行するコマンドを指定することが可能です。トークンをスクリプトに送信し、ローカル変数として設定することができます。

Example of a **Command to run**:

```
{store-path}/Applications/cmd/scr.cmd {serial} {store-path}
```

These are example lines of the *.cmd file, in this case, we run the Allway Sync'n'Go application with parameters, the locally set variables are utilized by the Allway application to locate local and target directories.

これらは* .cmd ファイルのサンプル行です。この場合、Allway Sync'n'Go アプリケーションをパラメータとともに実行し、ローカルに設定された変数は Allway アプリケーションでローカルディレクトリとターゲットディレクトリを検索するために使用されます。

```
@ECHO OFF

SET SCRID=%1 && SET SCRVOLUME=%2
```

The first line makes the process silent. The second line fetches the serial of the device and storage path from the authorized autorun command to run.

最初の行はプロセスを無音にします。2 行目は、実行を許可自動実行コマンドからのデバイスとストレージパスのシリアルを取り出します。

```
START /D ^"%2Applications¥Allway^" AllwaySync'n'Go.exe -m
```

This example line specifically starts the Allway portable sync application. The -m parameter is Allway specific and means that the application starts as minimized.

この例の行は、Allway ポータブル同期アプリケーションを開始します。-m パラメーターは Allway 固有であり、アプリケーションが最小化された状態で開始することを意味します。

```
START /D ^"%2Applications¥Example^" Example.exe"
```

This last line is to demonstrate that we also can run additional applications from this batch file.

最後の行は、このバッチファイルから追加のアプリケーションを実行できることを示しています。

ポリシーデバイスのユーザーインタラクション

The users cannot interact with the policy configuration and they are not alerted that the policy is activated. The user can of course see any software or files that are prompted by the **Command to run**.

ユーザーにはポリシーが設定されたことは通知されませんが、実行するコマンドによってはファイルを見ることができます。

ポリシー パスワードポリシー

Available in the Policy Editor popup

Allows you to configure a detailed password policy.

The following configurations are available:

- **パスワードの最小文字数**
    - Use these settings to define minimum password length and required numerals, lowercase letters, uppercase letters and special characters. Please Note: For FIPS certified hardware, the recommended password length is at least 8 characters.

      最小パスワードの長さと必須の数字、小文字、大文字、特殊文字を定義するためにこれらの設定を使用してください。(注意:FIPS 認定ハードウェアの場合、。管理者がそれを 8 文字未満に設定するか否かに問わず、最小のパスワード長は 8 文字です。)

- **数字 (1,2,3…).** – checkbox
- **小文字・大文字 (a,b,c / A,B,C).** – checkbox
- **特殊文字 (#,!,?…).** – checkbox
- # 回目のログイン後のデバイスのパスワードの有効期限 – **数字入力**
- # 日目のログイン後のデバイスのパスワードの有効期限 – **数字入力**

Note that the NIST guideline preview recommends to no longer force password changes, as this might make users choose “easier” passwords.

NIST ガイドラインのプレビューでは、ユーザーは「簡単な」パスワードを選択できる可能性があるため、パスワードの変更を強制しないようにすることが推奨されています。

ポリシーユーザーインタラクション

Upon the first device setup or the next time the device is unlocked the password will be checked for compliance with the active policy. The policy will be displayed in the Welcome screen once connected to the server or in Change password screen that will be forced if the current password if found to be non-compliant with the active policy. The user cannot proceed without complying with the password policy.

最初のデバイスの設定時またはデバイスのロックが解除されたときに、パスワードはアクティブポリシーに準拠しているかどうかがチェックされます。このポリシーは、サーバーに接続すると、ウェルカム画面に表示されるか、現在のパスワードがアクティブなポリシーに準拠していない場合は強制的に変更されます。ユーザーは、パスワードポリシーに従わずに進むことはできません。

ポリシー　リモートパスワードリセット

Available in the Policy Editor popup

This policy allows SafeConsole staff to assist device users to recover from a forgotten password without losing any stored information. The technology is based on ciphers and does not weaken the security of the device as all attempts to reset the password are validated against device security controller.

このポリシーにより、SafeConsole のスタッフは、デバイスのユーザーが保存された情報を失うことなく、忘れたパスワードから回復できるように支援します。この技術は暗号に基づいており、パスワードをリセットしようとするすべての試みがデバイスセキュリティコントローラに対して検証されるため、デバイスのセキュリティが弱くなることはありません。

Once enabled the device must be unlocked one time with a connection to the server for the configuration to be applied. After this a remote password reset can be performed at any time. Remote password resets do not require an Internet connection. Please review the Actions sections on how to perform a remote password reset.

有効になると、構成を適用するために、サーバーに接続してデバイスのロックを解除する必要があります。この後、リモートパスワードのリセットはいつでも実行できます。リモートパスワードのリセットには、インターネット接続は必要ありません。リモートパスワードリセットの実行方法については、「アクション」のセクションを参照してください

It is not possible to activate the policy in hindsight to recover a now forgotten device password. It is therefore recommended to always have this policy enabled.

ポリシー適用前にパスワードを忘れてしまうとパスワードリセットができませんので常にこのポリシーを有効にすることをお勧めします。

The following configurations are available:

- **パスワードリセットを有効にする**
    - Select this checkbox to enable users to request remote password resets. You can also define the email address where password reset requests should be sent(typically a support email address), a phone number users may call(optional), and the subject line for password reset emails.

      ユーザがリモートパスワードリセットを要求できるようにするには、このチェックボックスを選択します。また、パスワードリセット要求を送信する e-mail アドレス（通常はサポート電子メールアドレス）、ユーザーが呼び出すことのできる電話番号（オプション）、およびパスワードリセット電子メールの件名を定義することもできます。

    - **サポート e-mail アドレス** – textbox to enter valid email address. The email is displayed in the device software to enable to user to contact support staff.

      有効な電子メールアドレスを入力するテキストボックス。電子メールはデバイスソフトウェアに表示され、ユーザーはサポートスタッフに連絡することができます。

    - **サポート電話番号** – entered numerically. This number is displayed in the device software to enable to user to contact support staff.

      数字で入力されています。この番号は、デバイスソフトウェアに表示され、ユーザーがサポートスタッフに連絡できるようにします。

    - **パスワードリセットメールの件名** – textbox to set the subject of the password reset email sent to user from the SafeConsole server by

the staff. Reset information is also available to be sent over any other online or offline communication channel.

SafeConsole サーバからユーザに送信されたパスワードリセットメールの件名をスタッフが設定するテキストボックス。リセット情報は、他のオンラインまたはオフライン通信チャネルを介して送信することもできます。

ポリシーデバイスのユーザーインタラクション

The user device is automatically enrolled in the remote password reset process the next time they have a SafeConsole connection and unlock the device. The user is not prompted but will now have the Actions menu option **Forgot password** available. Clicking this will bring forward the configured information and password ID required to perform the remote password reset. It is in this screen that user will enter the response code provide by the SafeConsole staff to initiate the password reset and get to choose a new compliant password.

ユーザーデバイスは、次に SafeConsole 接続が確立され、デバイスのロックが解除されたときに、リモートパスワードリセットプロセスに自動的に登録されます。ユーザーにはプロンプトは表示されませんが、オプションメニューに[パスワードを忘れた]が表示されます。これをクリックすると、リモートパスワードリセットを実行するために必要な設定済みの情報とパスワード ID が表示されます。この画面では、SafeConsole スタッフが提供するレスポンスコードを入力してパスワードリセットを開始し、新しいパスワードを選択することができます。

If you do not have a registered email address for the user in SafeConsole the device software will prompt the user to enter and confirm their email address, the message states that the address can be used for future password resets and that it only will be share with the staff of the private SafeConsole server.

SafeConsole に登録されているユーザーの電子メールアドレスが登録されていない場合、デバイスソフトウェアはユーザーに電子メールアドレスの入力と確認を促すメッセージを表示し、そのアドレスは今後パスワードのリセットに使用でき、プライベート SafeConsole サーバのスタッフに共有されます。

ポリシー 書き込み保護

Available in the Policy Editor popup

Enabling Write Protection is a powerful anti-malware measure as no files can be copied to the device when it is activated. This option is recommended to use when

unlocking devices on an unknown machine when there is no need to copy files to the device, for example during a presentation.

書き込み保護を有効にすることは、デバイスがアクティブになったときにデバイスにファイルをコピーすることができないため、マルウェア対策の強力な手段になります。このオプションは、プレゼンテーション中など、デバイスにファイルをコピーする必要がない場合および未知のマシン上でデバイスのロックを解除するときに使用することをお勧めします。

The following configurations are available:

- **書き込み保護を有効にする**
    - Select this checkbox to enforce write protection on all devices. This will allow users to read data on registered devices but will not allow them to update or delete data.

      このチェックボックスを選択すると、すべてのデバイスに書き込み保護が適用されます。これにより、ユーザーは登録済みのデバイスでデータを読み取ることができますが、データの更新や削除はできません。

    - **Write Protection Mode** selector. The modes that are available are either **User Configurable** (allows the end user to select to unlock the device as read-only) or **Activated when outside your Trusted Zone**.

      書き込み保護モード選択。利用可能なモードは、エンドユーザがデバイスを読み取り専用としてロック解除することを選択できるようにする「ユーザ設定可能」、または「信頼ゾーン」外で有効にするモードです。

    - Trusted Zone – section header
        - Configured through Trusted Network policy
        - Configured through Trusted Certificates policy

This policy can, for example, be useful for a group of users who you want to allow to do presentations outside of the network but not enable them to bring files back to the network on their devices.

たとえば、このポリシーは、ネットワーク外でのプレゼンテーションを許可したいが、デバイス上のネットワークにファイルを戻すことを許可しないユーザーのグループに役立ちます。

ポリシーデバイスのユーザーインタラクション

The users are not alerted that the policy is activated.

ユーザーにはポリシーが設定されたことは通知されません。

If the policy is set to be **User Configurable** a checkbox will become visible under the Enter password input in the main screen with the text *Unlock in read-only mode*. If checked the device will unlock as write protected in read-only mode, a balloon time will notify the user that the *[device_brand] has been unlocked in read-only mode*.

ポリシーがユーザ設定可能に設定されている場合、チェックボックスは、メイン画面の[パスワードを入力してください]の下に表示され、[読み取り専用モードでロック解除]というテキストが表示されます。オンにすると、デバイスは読み取り専用モードで書き込み保護された状態でロック解除されます。吹き出しは[device_brand]が読み取り専用モードでロック解除されたことをユーザーに通知します。

If the **Activated when outside your Trusted Network** is configured the device will be forced into the mode, a balloon time will notify the user that the *[device_brand] has been unlocked in read-only mode since you are outside the trusted network*.

信頼されたネットワークの外にあるときに有効にすると、デバイスは強制的に保護モードに入りますが、あなたが信頼できるネットワークの外にいるため、[デバイスブランド]が読み取り専用モードでロックされていることを吹き出しで通知します。

ポリシー ファイル制限

Available in the Policy Editor popup

You can either create a whitelist or a blacklist storage of files with different file extensions that apply to the secure storage partition of the devices. This option can be used to enable a malware protection as many organizations do not allow executable file formats on removable media. The feature only filters on the file extension, but this means that the files won't be able to run on the host machine – thus there is no need to analyze the file header.

デバイスのセキュアなストレージパーティションに適用される異なるファイル拡張子を持つファイルのホワイトリストまたはブラックリストストレージを作成することができます。このオプションは、多くの組織がリムーバブルメディア上で実行可能ファイル形式を許可しないため、およびマルウェア対策のために使用できます。この機能はファイル拡張子のみをフィルタリングしますが、これはファイルがホストマシン上で実行できないことを意味し、ファイルヘッダを分析する必要はありません。

The following configurations are available:

- **ファイル制限を有効にする** – checkbox

- Select this checkbox to limit the types of files users may save to their device. You can also define file extensions to restrict or allow(for example .exe,.dll,etc) and the restriction mode, which allows you to Restrict(blacklist) or Allow(whitelist). If you select “Restrict”, users will not be able to save the file types you specified to their device. If you select “Allow”, users will be able to save only the file types you specified to their device.

  ユーザーがデバイスに保存できるファイルの種類を制限するには、このチェックボックスを選択します。（例：.exe、.dll など） また、制限モード（制限（ブラックリスト）または許可（ホワイトリスト））を定義することもできます。「制限する」を選択すると、ユーザーは指定したファイルタイプをデバイスに保存できなくなります。「許可する」を選択すると、指定したファイルタイプのみをデバイスに保存することができます。

- **ファイルタイプの拡張** – text input. Enter the filetypes that you would like to change permissions for here with file extensions comma separated as: exe,dll, com…

  テキスト入力。ここではファイル拡張子をカンマで区切って、アクセス権を変更したいファイルタイプを入力してください：exe、dll、com …

- **制限モード**
  - **選択したファイルを制限 (Blacklist)** – the device software will immediately delete any files that **DO MATCH** the file extension listed in the *File Type Extensions*.

    デバイスソフトウェアは、ファイルタイプ拡張子にリストされているファイル拡張子と一致するファイルを直ちに削除します。

  - **選択したファイルのみ許可 (Whitelist)** the device software will immediately delete any files that **DO NOT MATCH** the file extension listed in the *File Type Extensions*.

    デバイスソフトウェアは、ファイルタイプ拡張子にリストされたファイル拡張子と一致しないファイルを直ちに削除します。

ファイルタイプ拡張機能の入力例

It is popular to **Restrict These Files (Blacklist)** executable file formats

これらのファイル（Blacklist）の実行可能ファイル形式を制限するのが一般的です

exe, dll, com, bat, js, jse, msi, msp, ocx, reg, sct, scr, sys, vb, vbe, vbs, wsc, wsf

ポリシーデバイスのユーザーインタラクション

The users are not alerted that the policy is activated. If a file is blocked from being stored on the secure storage partition the user will be notified in a custom balloon tip that *Some files have been blocked to protect you computer: [filepaths-listed]*. The file is deleted from the device secure storage. Note that you may have to update the file explorer to confirm that the deletion has taken place.

ポリシーがアクティブになったことをユーザーに警告しません。ファイルが保護されたストレージパーティションに格納されないようにブロックされている場合、カスタムバルーンヒントで通知されます。コンピュータを保護するためにいくつかのファイルがブロックされています：[filepaths-listed]。ファイルは、デバイスのセキュアストレージから削除されます。削除が行われたことを確認するには、ファイルエクスプローラを更新する必要があります。

ポリシー デバイス監査

Available in the Policy Editor popup

You can enable auditing on all device actions such as unlocks and also enable file auditing, which tracks file creations and deletions. It is also possible to limit your file audit to a set number of file extensions.

ロック解除などのすべてのデバイスアクションで監査を有効にすることができ、ファイルの作成と削除を追跡するファイル監査も有効にすることができます。また、ファイル監査を設定された数のファイル拡張子に制限することもできます。

A clear audit trail is often a requirement to achieve compliance with regulations and it is therefore recommended to enable these policies.

規制の遵守を達成するためには、監査証跡を明確にする必要があることが多いため、これらのポリシーを有効にすることを推奨します。

The logs are synchronized for a device session on the following device unlock (with a SafeConsole connection). Logs are uploaded encrypted from encrypted local buffer that resides in a hidden storage area partition of the device.

ログは、次のデバイスのロック解除（SafeConsole 接続の場合）のデバイスセッションに対して同期されます。ログは、デバイスの隠しストレージ領域パーティションに存在する暗号化されたローカルバッファから暗号化されてアップロードされます。

Logs can be searched under the main menu option Audit Logs > Device Audit Logs.

ログは、メインメニューオプション[監査ログ]> [デバイス監査ログ]で検索できます。

The following configurations are available:

- **すべてのデバイスの監査を有効にする** – checkbox
    - Select this checkbox to capture an audit log of all device activity(connections, failed log in attempts, password resets,etc.).

      すべてのデバイスアクティビティ（接続、失敗したログイン試行、パスワードリセットなど）の監査ログをキャプチャするには、このチェックボックスを選択します。

- **詳細なファイルの監査を有効にする.** – checkbox
    - Select this checkbox to capture an audit log of all files saved to or removed from devices. All file types are logged.

      デバイスに保存またはデバイスから削除されたすべてのファイルの監査ログをキャプチャするには、このチェックボックスを選択します。すべてのファイルタイプがログに記録されます。

        - **ファイルタイプ拡張** – text input. Input what filetypes you would like to audit as extensions, comma separated, for example: *pdf, docx, ppt*

          テキスト入力。拡張子として監査するファイルタイプをカンマ区切りで入力します（例：pdf、docx、ppt）。

ポリシーデバイスのユーザーインタラクション

The users are not alerted that the policy is activated and cannot affect the policy.

ユーザーは、ポリシーがアクティブになっていることを通知されず、ポリシーに影響を与えることもできません。

ポリシー カスタムメイドのデバイス情報

Available in the Policy Editor popup

This policy allows you to collect up to three text strings (tokens) of information from the device user during registration.

このポリシーを使用すると、登録時にデバイスユーザーから最大 3 つのテキスト文字列(トークン)を収集できます。

Each token has:

- A **Token Name** (the object name that can be used for scripting, ex: roomnumber) which is the identifier when being used in other policies, keep this small caps without special characters, examples:
- *roomnumber*, *fullname*

  他のポリシーで使用されているときの識別子であるトークン名(スクリプトに使用できるオブジェクト名、例:roomnumber)。特殊文字なしの小文字のままにします。例:roomnumber、fullname

- And a **Token Description** (the friendly display name, ex: Room Number) which is what will be displayed in the device software to allow the device user to understand what to enter into the field. Example: *Office Room Number*, *Full Name*

  また、デバイスのユーザーがフィールドに入るものを理解できるようにするために、デバイスソフトウェアに表示されるトークンの説明(簡単な表示名、例:Room Number)。例:オフィスルーム番号、氏名

The following configurations are available:

- **すべてのデバイスのユーザー情報を有効にする** – checkbox
  - The collected data will be displayed in the Devices section in SafeConsole and can be used for scripting in the Authorized Autorun policy.

    収集されたデータは SafeConsole の Devices セクションに表示され、Authorized Autorun ポリシーのスクリプト作成に使用できます。

  - Each **Token Name** should be provided with a **Token Description**.

    各トークン名は、トークン記述とともに提供されます。

  - **Token 1:** label, the first item of information to be collected, provided in two text input boxes.

トークン 1：ラベルは、収集される情報の最初の項目は 2 つのテキスト入力ボックスに表示されます。

- *Token Name*, text input トークン名：テキスト入力
- *Token Description*, text input トークン記述：テキスト入力

- **Token 2:** label, the second item of information to be collected, provided in two text input boxes.

  トークン 2：ラベルは、収集される 2 つの項目は 2 つのテキスト入力ボックスに表示されます。

  - *Token Name*, text input トークン名：テキスト入力
  - *Token Description*, text input トークン記述：テキスト入力
- **Token 3:** label, the third item of information to be collected, provided in two text input boxes.

  トークン 3：ラベルは、収集される 3 つの項目は 2 つのテキスト入力ボックスに表示されます。

-

  - *Token Name*, text input トークン名：テキスト入力
  - *Token Description*, text input トークン記述：テキスト入力

The custom information collected metadata is displayed as separate columns in the Devices section table located under Manage in the main menu. Make sure to enable the display of the columns in the top right option menu. Click away from the dropdown menu to close it. The data will be updated according to your selections.

収集されたカスタム情報は、メインメニューの[管理]にある[デバイス]セクションの表に別の列として表示されます。右上のオプションメニューの列の表示を有効にしてください。ドロップダウンメニューからクリックして閉じます。選択した内容に従ってデータが更新されます。

Once the data has been collected it can be updated on the server by a staff member by using the Edit Custom Data option.

データが収集されたら、Edit Data を使用して、スタッフがサーバー上で更新することができます。

ポリシーデバイスのユーザーインタラクション

The users will be prompted to enter the asked for information when the policy is activated. This will occur on their next unlock with a SafeConsole connection. A

separate screen with **Message to display** as the header and the configured text input boxes displayed and a next button to complete the collection.

ポリシーがアクティブになったときに、情報の入力を求めるメッセージが表示されます。これは、SafeConsole 接続を使用した次回のロック解除時に発生します。ヘッダーとして表示するメッセージと設定されたテキスト入力ボックスが表示された別の画面と、次のボタンでコレクションを完了します。

ポリシー ZoneBuilder

Available in the Policy editor popup

ZoneBuilder installs a local certificate, when enabled and invoked by policy (enforced or user configurable) and unlocked on a computer. The computer can be defined in the Trusted Network policy. The certificate is installed in the MY STORE certificate store of the user account that no one can export. The presence of this certificate will treat the device as being in the Trusted Zone. Between this certificate and the Trusted Network policy you can configure your Trusted Zone. ZoneBuilder utilizes this certificate to enable password features that either make the security of the solution more stringent or more convenient. Note that increased user convenience also may mean a better security posture as adoption rates and compliance to policies increase.

ZoneBuilder はポリシー（強制またはユーザ設定可能）で有効にすると、コンピュータ上でロック解除されたときにローカル証明書をインストールします。コンピュータは、トラステッドネットワークポリシーで定義できます。証明書は、誰もエクスポートできないユーザーアカウントの MY STORE 証明書にインストールされます。この証明書が存在すると、デバイスは信頼ゾーン内にあるものとして扱われます。この証明書とトラステッドネットワークポリシーの間で、トラステッドゾーンを設定できます。ZoneBuilder はこの証明書を使用して、ソリューションのセキュリティをより厳密に、またはより便利にするパスワード機能を有効にします。ユーザーの利便性が向上すると、採用率やポリシーへの準拠が向上するため、セキュリティの強化も期待できます。

Once turned on the feature cannot be fully deactivated as that would require a device reset to regenerate certificates.

一度オンにすると、証明書を再生成するためにデバイスをリセットする必要があるため、この機能を完全に無効にすることはできません。

ZoneBuilder can *enforce higher security* with **Restricted Device Access**:
ZoneBuilder は、制限付きデバイスアクセスを使用してより高度なセキュリティを強化できます。

1. Only allow automatic unlock when within the configured Trusted Zone as define by the installed Trusted Certificate or Trusted Network.

   インストールされた、信頼された証明書または信頼されたネットワークによって定義されるように、構成された信頼ゾーン内でのみ自動ロック解除を許可します。

2. Only allow devices to unlock that are currently inside the Trusted Network. This option means that the device cannot unlock at all outside the network and is a powerful way to allow data transport on or in between secured networks. This way the courier does not have to be trusted and cannot be forced to expose the stored data.

   トラステッドネットワーク内にあるデバイスのみをロック解除できるようにします。このオプションは、デバイスがネットワーク外でデバイスのロック解除ができないことを意味し、セキュリティで保護されたネットワーク間でデータ転送を行う強力な方法です。この方法では、デバイスは信頼される必要はなく、格納されたデータが勝手に公開されることはありません。

ZoneBuilder can as a *convenience* enable **Automatic Device Unlock**:

ZoneBuilder を使用すると、自動デバイスロックを有効にすることができます。

1. Allow automatic unlock of the devices on trusted machines. This setup makes the workday much more convenient for the end user and increases the adoption rate of the devices. As the users must authenticate towards their user account, the security remains high. The user uses their selected device password when unlocking on other machines.

   信頼できるマシン上のデバイスの自動ロック解除を許可します。この設定により、エンドユーザにとって作業がはるかに便利になり、デバイスの採用率が向上します。ユーザーが自分のユーザーアカウントに対して認証する必要があるため、セキュリティは高いままです。ユーザーは、他のマシンでロックを解除するときに、選択したデバイスパスワードを使用します。

2. Be employed as self-service password reset. If a user forgets their password they can bring back their device to their trusted user account and they will be prompted to reset their password. No data is lost.

   セルフサービスのパスワードリセットとして使用する。ユーザーがパスワードを忘れた場合、ユーザーは信頼できるユーザーアカウントにデバイスを戻すことができ、パスワードをリセットするよう求められます。データは失われません。

3. Be used to unlock on team members machines without sharing the device password. By allowing the user to trust their team members user accounts, the user only has to enter the device password once to enable the trust. They can do this themselves and do not need to expose their password. The trust can later be revoked from the device software Main Menu. This increases productivity and is ideal to share data quickly when WiFi is scarce, or the network is tightly locked down.

   デバイスパスワードを共有せずにチームメンバーのマシンのロックを解除するために使用されます。デバイスパスワードを 1 回入力するだけで、ユーザーがチームメンバーのユーザーアカウントを信頼できるようにすることができます。彼らはこれを自分で行うことができ、パスワードを公開する必要はありません。信頼は、後でデバイスソフトウェアのメインメニューから取り消すことができます。これにより生産性が向上し、WiFi が不足している場合やネットワークが緊密にロックされている場合にデータを迅速に共有するのに適しています。

The following configurations are available:

- **Enable ZoneBuilder** – checkbox

  ZoneBuilder を有効にする：チェックボックス

- ZoneBuilder can either be used to automatically unlock devices (mainly for ease of use) and/or to restrict which computer user accounts the device can be unlocked on (to limit usage of the device), based on client certificates. All allowed trusted computer users will become part of the Trusted Certificates.

  ZoneBuilder を使用すると、デバイスの自動ロック解除（主に使いやすさ）、またはクライアント証明書に基づいてデバイスのロックを解除できるコンピュータのユーザーアカウントを制限することができます。（デバイスの使用を制限する）許可されたすべてのトラステッドコンピュータユーザーは、信頼できる証明書の一部になります。

- **Restrict trusted computers to CA signed client certificates** – selector

  信頼済みコンピュータを CA 署名付きクライアント証明書に制限する：選択肢

  - **No** – Allow device software to generate certificates. Leave as ‘No’ to allow users to easily link a device with computers of their choice.

デバイスソフトウェアが証明書を生成できるようにする。「いいえ」のままにしておくと、ユーザーは選択したコンピュータと簡単にデバイスをリンクできます。

- **[A selected CA cert]** this will require that a client certificate of the configured CA is available on the host computer to use ZoneBuilder.

  [選択された CA 証明書]を使用するには、設定した CA のクライアント証明書を ZoneBuilder を使用するためにホストコンピュータで使用できるようにする必要があります。

- **Certificates**, wrench-menu, when click it displays currently available certificates (which can be deleted by clicking the trash can icon next to the name), there is also a **Add New** button available. The button will bring up an **Add New Certificate** popup where you can **Select a certificate** in a file browser and **Enter password (only required for PKCS12 files):** in text input box. The certificate must be either a PKCS12 file or an X509 certificate. An X509 certificate must be either DER or Base64 encoded.

  証明書、レンチメニュー、クリックすると現在使用可能な証明書が表示されます(名前の横にあるゴミ箱アイコンをクリックすると削除できます)。また、[新規追加]ボタンも利用できます。ボタンをクリックすると新しいファイルの追加ポップアップが表示され、ファイルブラウザで証明書を選択し、パスワードを入力できます(PKCS12 ファイルのみ必要):テキスト入力ボックスに入力します。証明書は、PKCS12 ファイルまたは X509 証明書のいずれかでなければなりません。X509 証明書は、DER または Base64 でエンコードされたものでなければなりません。

- There is also a link available in the interface on How to generate certificates with OpenSSL.

  OpenSSL で証明書を生成する方法のインタフェースには、リンクもあります。

- **Restricted Device Access** - section header デバイスアクセスの制限:セクションヘッダー
  - **Only allow device usage on computers linked within your Trusted Network** - checkbox.

    [信頼されたネットワーク] - チェックボックスにリンクされているコンピュータでのみ、デバイスの使用を許可します。:チェックボックス

The device will be linked to user's computers after the first successful unlock. The device may then be used outside the Trusted Network or while offline, but only on linked computers.

デバイスは、最初のロック解除の成功後にユーザーのコンピュータにリンクされます。デバイスは、リンクされたコンピュータでのみ信頼されたネットワークの外、またはオフラインで使用できます。

- **Require trusted computer users to have a connection to SafeConsole.** – checkbox. Device access will be denied while offline and when outside the Trusted Network.

  信頼できるコンピュータユーザーに SafeConsole への接続を要求する。– チェックボックス。デバイスへのアクセスは、オフラインおよびトラステッドネットワークの外部では拒否されます。

- **Automatic Device Unlock** – section header デバイスの自動ロック解除
  - **Automatically unlock devices on trusted computer users** – checkbox. Allow automatic device unlock (no password required) on the user's computer after it has been linked and trusted.

    信頼できるコンピュータユーザーのデバイスを自動的にロック解除する – チェックボックス。ユーザーのコンピュータがリンクされ、信頼された後、自動的にデバイスのロックを解除する(パスワード不要)を許可します。

    - **Require trusted computer users to have a connection to SafeConsole.** – checkbox. Devices will not automatic unlock while offline and when outside the Trusted Network.

      信頼できるコンピュータユーザーに SafeConsole への接続を要求する。– チェックボックス。オフライン中やトラステッドネットワーク外では、デバイスは自動的にロック解除されません。

- **Trusted Network** – section header 信頼されたネットワーク:セクションヘッダー
  - **Configured through Trusted Network policy Trusted Network ポリシーで設定可能**

ポリシーデバイスのユーザーインタラクション

Depending on setup different interactions will and can take place. セットアップに応じて、さまざまなやりとりが行われます。

- **Restrict trusted computers to CA signed client certificates** set to **No** and **Automatically unlock devices on trusted computer users** activated.

  信頼されたコンピュータを CA 署名付きクライアント証明書に限定して、[いいえ]に設定し、信頼できるコンピュータユーザーのデバイスを自動的にロック解除します。

  - The user will not be alerted that the policy is activated, but the ZoneBuilder section is displayed when the Settings button under the Main Menu window is clicked. The *ZoneBuilder settings* header is followed by a a **Trust this account** checkbox. The user is informed with a text that: *When you use[device-name] on trusted accounts, you will not have to enter your password to unlock.* It is also possible to click a **Show trusted accounts** button that will bring up a overview of **Trusted accounts**, in this view the user can confirm and revoke trust by clicking the minus-user-icon on each entry.

    ポリシーがアクティブになったことをユーザーに警告することはありませんが、Main Menu ウィンドウの下の Settings ボタンをクリックすると、ZoneBuilder セクションが表示されます。ZoneBuilder の設定ヘッダーの後には、このアカウントを信頼するチェックボックスが表示されます。信頼できるアカウントで[デバイス名]を使用すると、ロックを解除するためにパスワードを入力する必要はありません。信頼できるアカウントの概要を表示する[信頼できるアカウントを表示]ボタンをクリックすることもできます。このビューでは、各エントリのマイナスユーザーアイコンをクリックして信頼を確認し取り消すことができます。

- **Restrict trusted computers to CA signed client certificates** set to **[A selected CA cert]** and **Automatically unlock devices on trusted computer users** activated.

  [選択された CA 証明書]に設定された CA 署名付きクライアント証明書に信頼できるコンピュータを制限し、信頼できるコンピュータユーザーのデバイスを自動的にロック解除する。

  - The users will be prompted to *Trust* the user account to enable *Auto-unlock* upon unlock. Once the trust is established the device will be unlocked on any machines that have the same certificate installed. The *ZoneBuilder settings* are available under Main Menu, settings.

    ユーザーは、ロック解除時に自動ロックを有効にするためにユーザーアカウントを信頼するように求められます。信頼が確立されると、同じ

証明書がインストールされているマシンでデバイスのロックが解除されます。ZoneBuilder 設定はメインメニューの設定で使用できます。

ポリシー パブリッシャー

Available in the Policy Editor popup

This feature will let administrators deploy/push portable applications and file content to the secure storage volume of user's devices. Content and applications will be accessible to the end users through shortcuts in the login application interface once the device is unlocked.

この機能により、管理者はポータブルアプリケーションとファイルコンテンツをユーザーのデバイスの安全なストレージボリュームに展開/プッシュできます。デバイスがロック解除されると、ログインアプリケーションインタフェースのショートカットを介してエンドユーザがコンテンツおよびアプリケーションにアクセスできるようになります。

The process of setting up a network share on Windows is available on this Microsoft resource.

Windows 上でネットワーク共有を設定するプロセスは、この Microsoft リソースで利用できます。

To share an entire network share use the following form:

ネットワーク共有全体を共有するには、次の形式を使用します。

¥¥server-name¥network_share¥

To share a folder in a network share use the following form:

ネットワーク共有内のフォルダを共有するには、次の形式を使用します。

¥¥server-name¥network_share¥Published Folder

Note the trailing backslash is needed for the network share and not the folder.

バックスラッシュは、フォルダではなくネットワーク共有に必要です。

The following configurations are available:

- **Enable Publisher – Content Distribution** – checkbox Publisher を有効にする – コンテンツの配布]チェックボックス

    - Publisher lets you deliver content to devices.

      Publisher を使用すると、デバイスにコンテンツを配信できます。

- UNC path to the Publisher root folder – textbox

  Publisher ルートフォルダへの UNC パス – テキストボックス

- **Require a live connection to SafeConsole or be within the Trusted Device Network.**

  SafeConsole へのライブ接続を必要とするか、または信頼できるデバイスネットワーク内にあることが求められます。

    - Devices will not sync files while offline and when outside the Trusted Network when enabled.

      オフライン中および信頼済みネットワークの外部にあるときはデバイスはファイルを同期しません。

ポリシーデバイスのユーザーインタラクション

The device software will add one button in the device UI for each subdirectory of the published folder, during the initial download there is a progress bar displayed in the Main Menu:

デバイスソフトウェアは、公開されたフォルダの各サブディレクトリのデバイス UI に 1 つのボタンを追加します。最初のダウンロード時には、メインメニューにプログレスバーが表示されます。

- If a file called `safestick.ini` is found it will be used to configure the button. See below for syntax.

  safestick.ini というファイルが見つかった場合は、ボタンの設定に使用されます。構文については以下を参照してください。

- If an executable with an embedded description is found, the description will be used as the button caption and pressing it will launch the application.

  説明が埋め込まれた実行可能ファイルが見つかった場合は、その説明がボタンのキャプションとして使用され、それを押すとアプリケーションが起動します。

- If the folder contains only one file, the folder name will be the button caption and pressing the button will invoke that file with the system default action.

  フォルダに 1 つのファイルのみが含まれている場合、フォルダ名はボタンのキャプションになります。ボタンを押すと、システムのデフォルト動作でそのファイルが呼び出されます。*This applies only to device software before 4.7.　これは 4.7 より前のデバイスソフトウェアにのみ適用されます。*

- Otherwise, the folder name will be the button caption and pressing the button will open the folder.

  そうでない場合、フォルダ名はボタンのキャプションになり、ボタンを押すとフォルダが開きます。

Syntax of safestick.ini

With the ini file, it is possible to specify parameters to the executable to run.

ini ファイルを使用すると、実行ファイルのパラメータを指定して実行することができます。

The parameters may contain the same tokens as specified in Custom Information, so you may launch applications or scripts that know from which volume or device they launched.

パラメータには、カスタム情報で指定されているのと同じトークンが含まれている可能性があるため、起動したボリュームまたはデバイスからわかっているアプリケーションまたはスクリプトを起動できます。

The format of the safestick.ini is as follows:

safestick.ini の形式は次のとおりです。

```
[starter]
command=<program name>
parameters=<parameters> ; optional
name=<shortcut name>
```

- *program name* is the full path to the program to launch.

  program name は、起動するプログラムへのフルパスです。

  To start a program from the device, enter it in the format

デバイスからプログラムを開始するには、フォーマットで入力します

{store-path}¥Applications¥Program Directory¥Program.exe.

- *parameters* is any parameters to pass to the program.

  parameters は、プログラムに渡すパラメータです。

  This value is optional. この値はオプションです。

- *shortcut name* is the name to display in the device software UI.

  ショートカット名は、デバイスソフトウェアの UI に表示する名前です。

- It is possible to hide the icon from the Main Menu by specifying hidden=yes on a separate line.

  別の行に hidden = yes を指定すると、メインメニューからアイコンを非表示にすることができます。

ポリシー ジオフェンス

Available in the Policy Editor popup

Geofence will enforce a deny access state on a device if the device software attempts to connect from a restricted IP. Once the device connects from a network that is not restricted it will automatically work again.

デバイスソフトウェアが制限された IP からの接続を試みる場合、ジオフェンスはデバイスのアクセスを拒否します。デバイスが制限されていないネットワークから接続すると、自動的に再び動作します。

For GeoFence to work a live connection to the SafeConsole server is required. To strictly enforce a GeoFence policy it is therefore recommended that devices are either forced to always require a server connection for device unlock using the Device State policy or only allow devices to unlock inside the Trusted Network using ZoneBuilder.

GeoFence を動作させるには、SafeConsole サーバーへのライブ接続が必要です。したがって、ジオフェンスポリシーを厳密に適用するには、デバイス状態ポリシーを使用してデバイスをロック解除するためのデバイス接続を常に要求するか、デバイスが ZoneBuilder を使用して信頼できるネットワーク内でロックを解除できるようにすることが推奨されます。

When the GeoFence become enabled it is possible to restrict usage to only named countries and/or IPs, You can also **Allow Only** named countries and/or IPs.

GeoFence が有効になると、指定された国や IP のみに制限することができます。指定した国や IP のみ許可することもできます。

The purpose of the feature is to achieve regulatory compliance where data is not allowed outside of specified countries or IPs.

この機能の目的は、指定された国や IP の外でデータが許可されていない場合の規制遵守を達成することです。

The following configurations are available:

- **Enable Geofencing on devices デバイスのジオフェンスを有効にする**
    - Prevent device access based on user computer IP Address through Geofence. Geolocation data such as Country and ISP of the IP Address can also be used to control device access.

      Geofence を介してユーザーのコンピュータ IP アドレスに基づいてデバイスへのアクセスを防止する。IP アドレスの国や ISP などのジオロケーションデータを使用して、デバイスアクセスを制御することもできます。

- **Geofence message to user** textbox ユーザーへの Geofence メッセージ：テキストボックス
    - Send a custom message to users when their device has been denied access through the Geofence policy.

      Geofence ポリシーによるデバイスのアクセスが拒否されたときに、ユーザーにカスタムメッセージを送信します。

- **IP addresses** textbox IP アドレスのテキストボックス – All IP Addresses Allowed as default

  デフォルトではすべての IP アドレスが許可されています。

    - Separate multiple IP Addresses with commas

      複数の IP アドレスを入力する際はカンマで区切ります。
      (198.51.100.1,198.51.100.2). Wildcard and CIRD addresses are supported ：

Wildcard と CIRD アドレスがサポートされています(198.51.100.* or 198.51.100.0/24)

- Restriction Mode – radio button

  制限モード:ラジオボタン

  - Allow Only These IPs (Whitelist), for a secure geofence, we recommend whitelisting approved IP Addresses.

    これらの IP のみを許可する(ホワイトリスト)、安全なジオフェンスのために、承認された IP アドレスをホワイトリストに登録することを推奨します。

  - Restrict These IPs (Blacklist)

    これらの IP を制限する(ブラックリスト)

- **Countries** textbox 国　テキストボックス– No Countries Blocked as default デフォルトでは国の制限はありません
  - Restriction Mode – radio button 制限モード:ラジオボタン
    - Allow Only These Countries (Whitelist)

      これらの国のみ許可する(ホワイトリスト)

    - Restrict These Countries (Blacklist)

      これらの国を制限する(ブラックリスト)

- **ISP** textboxISP　テキストボックス – No ISP Blocked as default

  デフォルトでは ISP の制限はありません。

  - Restriction Mode – radio button

    制限モード:ラジオボタン

    - Allow Only These ISPs (Whitelist)これらの ISP を許可する(ホワイトリスト)
    - Restrict These ISPs (Blacklist)これらの ISP を制限する(ブラックリスト)
    - To add ISPs, click Add ISP, enter a known IP associated with the ISP in the popup and perform the lookup by clicking the

search-symbol button, then click Add in the bottom of the screen. ISP を追加するには、[ISP を追加]をクリックし、ポップアップで ISP に関連付けられた既知の IP を入力し、検索記号ボタンをクリックして検索を実行し、画面の下部にある[追加]をクリックします。

ポリシーデバイスのユーザーインタラクション

The device software will display the configured message if the device is blocked and the device enters denied access mode and cannot be unlocked. Once the device connects from a allowed location the device can again be unlocked.

デバイスがブロックされ、デバイスが拒否アクセスモードに入ってロックを解除できない場合、デバイスソフトウェアは設定されたメッセージを表示します。デバイスが許可された場所から接続されると、デバイスは再びロック解除されます。

ポリシー 信頼されたデバイスゾーン

Available in the Policy Editor popup

The Trusted Network is created by providing a whitelist of IP addresses, Countries, or ISPs. Once configured a device will need to be connected to a computer that can reach the SafeConsole server through an IP address that is whitelisted to be considered inside the Trusted Network and thus the Trusted Zone. Another way to be inside the Trusted Zone is with ZoneBuilder Trusted Certificates.

信頼できるネットワークは、IP アドレス、国、または ISP のホワイトリストを提供することによって作成されます。設定が完了したら、デバイスは、信頼できるネットワークの内部とみなされるようにホワイトリストに登録されている IP アドレスを介して SafeConsole サーバーに接続できるコンピュータに接続する必要があります。信頼ゾーン内に入る別の方法は、ZoneBuilder 信頼証明書です。

- When used with the Write-Protection policy, you can ensure that devices only unlock in read-only mode if connecting from an untrusted network

  . 書き込み保護ポリシーを使用すると、信頼できないネットワークから接続する場合、デバイスは読み取り専用モードでのみロック解除されます。

- When used with the ZoneBuilder policy, you can block devices from auto-unlocking or prevent access if the device is connecting from an unknown network. Note that you may use ZoneBuilder certificates to securely trust computers that are outside your trusted network. ZoneBuilder ポリシーを使

用すると、デバイスが未知のネットワークから接続している場合、デバイスの自動ロック解除を禁止したり、アクセスを禁止したりすることができます。ZoneBuilder 証明書を使用して、信頼できるネットワークの外にあるコンピュータを安全に信頼できることに注意してください。

For Trusted Network to work a live connection to the SafeConsole server is required. To strictly enforce a trusted network it is therefore recommend that devices are either forced to always require a server connection for device unlock using the Device State policy or only allow devices to unlock inside the Trusted Network using ZoneBuilder.

信頼できるネットワークを動作させるには、SafeConsole サーバーへのライブ接続が必要です。したがって、信頼できるネットワークを厳格に実施するには、デバイス状態ポリシーを使用してデバイスをロック解除するためのデバイス接続を常に要求するか、デバイスが ZoneBuilder を使用して信頼できるネットワーク内でロックを解除できるようにすることが推奨されます。

The following configurations are available:

- **Enable Trusted Network Trusted Network を有効にする**
    - Trusted Network is a way for admins to create a Trusted Zone in which other policies can use to either restrict or provide extra convenience or features depending if a device is unlocked inside or outside the Trusted Zone. If the Trusted Network policy is not configured then all live connections to the SafeConsole Server are considered to be in the Trusted Network and thus the Trusted Zone.

      信頼できるネットワークは、管理者が信頼ゾーンを作成して、信頼ゾーンの内側または外側でデバイスがロック解除されているかどうかに応じて、他のポリシーで使用できる、さらなる利便性や機能を制限または提供できます。トラステッドネットワークポリシーが設定されていない場合、SafeConsole サーバーへのすべてのライブ接続はトラステッドネットワーク、つまりトラストゾーンにあるとみなされます。**To register a device, the user will need to make a connection to SafeConsole from inside the Trusted Network**

      デバイスを登録するには、ユーザーは、Trusted Network 内から SafeConsole に接続する必要があります

- **IP addresses** textbox IP アドレスのテキストボックス – All IP Addresses Allowed as default デフォルトではすべての IP アドレスが許可されています。

- Separate multiple IP Addresses with commas 複数の IP アドレスを入力する際はカンマで区切ります。(198.51.100.1,198.51.100.2). Wildcard and CIRD addresses are supported :Wildcard と CIRD アドレスがサポートされています(198.51.100.* or 198.51.100.0/24)
- Restriction Mode – radio button 制限モード:ラジオボタン
  - Allow Only These IPs (Whitelist), for a secure geofence, we recommend whitelisting approved IP Addresses.

    これらの IP のみを許可する(ホワイトリスト)、安全なジオフェンスのために、承認された IP アドレスをホワイトリストに登録することを推奨します。

  - Restrict These IPs (Blacklist) これらの IP を制限する(ブラックリスト)

- **Countries** textbox 国 テキストボックス– No Countries Blocked as default デフォルトでは国の制限はありません
  - Restriction Mode – radio button 制限モード:ラジオボタン
    - Allow Only These Countries (Whitelist) これらの国のみ許可する(ホワイトリスト)
    - Restrict These Countries (Blacklist)これらの国を制限する(ブラックリスト)
- **ISP** textboxISP テキストボックス – No ISP Blocked as default

  デフォルトでは ISP の制限はありません。

  - Restriction Mode – radio button 制限モード:ラジオボタン
    - Allow Only These ISPs (Whitelist)これらの ISP を許可する(ホワイトリスト)
    - Restrict These ISPs (Blacklist)これらの ISP を制限する(ブラックリスト)
    - To add ISPs, click Add ISP, enter a known IP associated with the ISP in the popup and perform the lookup by clicking the search-symbol button, then click Add in the bottom of the screen.

      ISP を追加するには、[ISP を追加]をクリックし、ポップアップで ISP に関連付けられた既知の IP を入力し、検索記号ボタンをクリックして検索を実行し、画面の下部にある[追加]をクリックします。

ポリシーデバイスのユーザーインタラクション

The user is alerted when trying to register a device when outside the Trusted Network. Other policies can also change how they interact with the user based on if the user is inside the Trusted Network. An example would be the Write Protection policy, which can be configured to disable writing to the device when outside the Trusted Zone. In this case the user will be notified they the drive is write protected when unlocked outside the Trusted Zone.

ユーザーは、信頼できるネットワークの外にあるときにデバイスを登録しようとすると警告されます。他のポリシーは、ユーザーが信頼できるネットワークの内部にいるかどうかに基づいて、ユーザーとのやりとりを変更することもできます。たとえば、信頼されたゾーンの外にあるときにデバイスへの書き込みを無効にするように設定できるWrite Protection ポリシーがあります。この場合、トラステッドゾーン外でロック解除されたときにドライブが書き込み保護されていることがユーザに通知されます。

サーバー設定 – デバイス登録とジオロケーション編集

The *Server Settings* are located in the main menu and handle server behavior. There are *More info* icons that will explain each setting when expanded.

サーバー設定はメインメニューにあり、サーバーの動作を処理します。展開時に各設定について説明する情報アイコンがあります。

These are the options that are available under Server Settings.

これらは、[サーバー設定]で使用できるオプションです。

デバイス登録設定

登録中のマシン所有権確認を無効にする

By default asks the device user during device registration to the server to verify their identity by authenticating to their computer user account, which is either local or a domain account. The purpose of the authentication is to ensure which user has which device. The authentication relies on NT User Authentication, and if this is not available, the feature can be disabled (requires device client version 4.8.19+).

既定では、ローカルユーザーアカウントまたはドメインアカウントのいずれかのコンピュータユーザーアカウントに認証することによって、サーバーへのデバイス登録中にデバイスユーザーに ID を確認するように要求します。認証の目的は、どのユーザーがどのデバイスを所有しているかを確認することです。認証は NT ユーザー認証に依存しており、これが利用できない場合、機能を無効にすることができます（デバイスクライアントのバージョン 4.8.19 以上が必要です）。

すべてのデバイス登録に一意のトークン

For all device registrations, the user will be required to enter a unique registration token that the server sends through email. (Requires device client version 4.8.25+) This unique token is sent along with the connection token and the quick connect guide when using the deployment wizard. Optionally the unique token can be shown by an admin by clicking the wrench next to the User's name. When devices are activated with the unique token the user's policy will be used for device registration instead of the default policy. The user's policy will need GeoFence and Trusted Network configured to allow access. If the user is outside the GeoFence or Trusted Network registration will be blocked.

すべてのデバイス登録では、サーバーが電子メールで送信する一意の登録トークンをユーザーが入力する必要があります。（デバイス・クライアント・バージョン 4.8.25 以上が必要）この一意のトークンは、デプロイメント・ウィザード使用時に接続トークンおよびクイック・コネクト・ガイドとともに送信されます。オプションで、ユーザー名の横にあるレンチをクリックすることで、管理者が一意のトークンを表示することができます。デバイスが一意のトークンでアクティブ化されると、デフォルトのポリシーではなく、デバイスの登録にユーザーのポリシーが使用されます。ユーザーのポリシーでは、アクセスを許可するように GeoFence と信頼できるネットワークが構成されている必要があります。ユーザーが GeoFence または Trusted Network の外部にいる場合、登録はブロックされます。

管理者からの登録承認

To avoid the risk of non-organization devices to register towards your SafeConsole server you can require the SafeConsole administrator's manual approval before a full device registration completes. The administrator can approve devices under Users or Devices in the Actions menu of the device. When enabled the option allows input of a message towards the end user that will display during the registration process. And example of a message is:

組織化されていないデバイスが SafeConsole サーバに登録されるリスクを避けるため、デバイスの完全な登録が完了する前に SafeConsole 管理者の手動承認を要求することができます。管理者は、デバイスの[操作]メニューの[ユーザー]または[デバ

イス]でデバイスを承認できます。このオプションを有効にすると、登録プロセス中に表示されるエンドユーザ向けのメッセージの入力が許可されます。メッセージの例は次のとおりです。*The server requires this device to be approved to complete the registration. Please contact your SafeConsole Administrator for more info. サーバーは、このデバイスを承認して登録を完了する必要があります。詳細については、SafeConsole 管理者にお問い合わせください。*

ジオロケーション編集

To allow usage of the maps when local IPs are being used it is now possible to edit the geolocations that are reported by the devices. This allow administrators to get a better overview of device usage in their organization.

ローカル IP を使用しているときにマップを使用できるようにするため、デバイスによって報告されたジオロケーションを編集できるようになりました。これにより、管理者は組織内でのデバイス使用状況の概要を把握することができます。

監査ログ – デバイスの使用と管理者アクション

Audit Logs are reached through the main menu. メインメニューから監査ログにアクセスします。

At the top right under each submenu option, you manage which columns to display and trigger Export of all registered data to CSV or XML. 各サブメニューオプションの右上に表示する列を管理し、登録されたすべてのデータを CSV または XML にエクスポートします。

デバイス監査ログ

SafeConsole stores all device usage actions. To record device audit logs the Device Audits policy must be active and applied to the device.

SafeConsole はすべてのデバイス使用状況を保存します。デバイス監査ログを記録するには、デバイス監査ポリシーがアクティブで、デバイスに適用されている必要があります。

Devices will buffer log data when they are offline and transmit the data encrypted once they can connect to the SafeConsole server. They do this on each unlock of the device.

デバイスは、オフラインのときにログデータをバッファし、SafeConsole サーバーに接続できるようになるとデータを暗号化して送信します。 彼らは、デバイスのロック解除ごとにこれを行います。

システムメッセージ

All SafeConsole staff actions logged under System Messages.

すべての SafeConsole スタッフのアクションは、システムメッセージのもとに記録されます。

SIEM およびその他の外部ログ収集

It is possible to send all log events to an external target as well. This allows integrating SafeConsole logs with your current solution for log analysis. Please open a support ticket for a guided setup.

すべてのログイベントを外部ターゲットに送信することも可能です。 これにより、現在のソリューションと SafeConsole ログを統合してログ分析を行うことができます。 ガイド付きセットアップのサポートチケットを開いてください。

SafeConsole の管理スタッフ設定

SafeConsole staff are managed under the main menu option *Staff Settings*. For SafeConsole On-Prem staff access is managed with AD Security Groups that are configured during the setup, this is covered in the SafeConsole On-Prem Installation Guide.

SafeConsole スタッフは、メインメニューの[スタッフ設定]オプションで管理します。 SafeConsole の場合 On-Prem スタッフアクセスは、セットアップ中に設定された AD セキュリティグループで管理されます。これについては、SafeConsole On-Prem インストールガイドで説明しています。

管理者アカウントのプロファイル設定

You manage your own profile setting in the topright dropdown menu with the small user icon. These are the options:

あなたは、小さなユーザーアイコンを持つ正面のドロップダウンメニューで独自のプロファイル設定を管理します。 以下のオプションがあります。

- Name: Edit your full name as it should appear on the SafeConsole Admins Page. SafeConsole の管理ページに表示されるフルネームを編集します。
- Email: Update your email address.メールアドレスを更新します。
- Login Username: Update your login username. (must be one word)ログインユーザーネームを更新します。(1 単語でなければならない)
- Mobile Number: Provide your mobile phone number.携帯電話番号を入力します。
- Language: Select your language, or leave the system default(English) 言語を選択するか、システムをデフォルトのままにします(英語)
- Theme: Select a color palette to align with your organization's brand standards. 組織のブランド基準に合わせてカラーパレットを選択します。
- Page Template: Select the position of the SafeConsole navigation menu: Side or Top SafeConsole のナビゲーションメニューの位置を選択します:サイドまたはトップ
- Idle Timeout: Enter the number of minutes of idle time before you are logged out of SafeConsole SafeConsole からログアウトするまでのアイドル時間を分単位で入力します。

管理者スタッフのアクセスレベル

Three levels of access rights are available SafeConsole admin staff: SafeConsole の管理スタッフは 3 つのレベルのアクセス権が利用可能です:

- **Administrator** *Can Purchase Licenses, add administrators, configure devices, monitor audit logs and perform device actions 管理者は、ライセンスの購入、管理者の追加、デバイスの設定、監査ログの監視、およびデバイスアクションの実行が可能です。*
- **Manager** *Can configure devices, monitor audit logs and perform device actions マネージャーはデバイスの設定、監査ログの監視、デバイスアクションの実行が可能*
- **Support Team** *Can perform a limited number of device actions, such as password resets. Cannot change device configurations サポートチームはパスワードリセットなど、限られた数のデバイスアクションを実行できます。デバイスの設定を変更できません*

新しい管理者スタッフの設定

To set up an admin in SafeConsole, follow these steps:

SafeConsole で管理者を設定するには、次の手順を実行します。

- Under Tools, click SafeConsole Admins in the navigation menu. [ツール]の下のナビゲーションメニューで[SafeConsole Admins]をクリックします。
- Click Add New: The admin setup window should open. [新規追加]をクリックします。管理者設定ウィンドウが開きます。
- Enter the admin's full name and email address. 管理者のフルネームと電子メールアドレスを入力します。
- Select the appropriate level of access: Administrator, Manager or Support Team. 適切なアクセスレベルを選択します：管理者、マネージャまたはサポートチーム。
- Click Add: The admin user is created and will receive a welcome email with instructions for logging in. [追加]をクリックします。管理ユーザーが作成され、ログインの手順が記載されたウェルカムメールが送信されます。

管理者スタッフの消去

To remove an admin from the SafeConsole Admins page, click Remove in the Action column. Then click OK to confirm the admin removal. The admin will no longer be able to log into SafeConsole.

SafeConsole Admins ページから管理者を削除するには、[Action]列の[Remove]をクリックします。次に、[OK]をクリックして管理者の削除を確認します。管理者は SafeConsole にログインできなくなります。

NOTE: If you only have one registered admin, that user cannot be removed.

登録済みの管理者が 1 人しかいない場合、そのユーザーは削除できません。

管理情報の表示をカスタマイズする

To change the display of admin information, follow these steps:

管理情報の表示を変更するには、次の手順を実行します。

- Click Columns on the SafeConsole Admins page. SafeConsole Admins ページのコラムをクリックします。
- In the dropdown menu, select the columns of data you want to display or remove. ドロップダウンメニューで、表示または削除するデータの列を選択します。
- Click away from the dropdown menu to close it. The data will update according to your selections. ドロップダウンメニューからクリックして閉じます。選択した内容に従ってデータが更新されます。

管理者スタッフの情報をエクスポートする

To export admin data out of SafeConsole, follow these steps:

SafeConsole から管理データをエクスポートするには、次の手順を実行します。

- Click Export on the SafeConsole Admins page. Select to export the data in XML or CSV format.

  SafeConsole Admins ページで Export をクリックします。XML または CSV 形式でデータをエクスポートする場合に選択します。

- Save the export file to your desired location

  エクスポートファイルを目的の場所に保存する

管理者スタッフの 2 段階認証を設定する

Two-step authentication adds an extra layer of security for your SafeConsole admin account. To set up two-step authentication, follow these steps:

2 段階認証では、SafeConsole 管理者アカウントのセキュリティが強化されます。2 段階認証を設定するには、次の手順を実行します。

- Click your username in the top-right corner and select Profile Settings in the dropdown.

  右上にあるユーザー名をクリックし、プルダウンで[プロフィールの設定]を選択します。

- Click the Two-Step Authentication tab.

  2 段階認証タブをクリックします。

- Click Next to begin the setup process.

  [次へ]をクリックして、セットアップ処理を開始します。

- Follow the onscreen prompts with your mobile device to complete the two-factor authentication setup.

  モバイルデバイスで画面の指示に従って、2 要素認証の設定を完了します。

You can use, for example, text messages, the Google Authenticator app or WinAuth for Windows to generate the Time-based One-time Passwords (TOTP).

たとえば、テキストメッセージ、Google Authenticator アプリまたは Windows 用 WinAuth を使用して、Time-based One-Time Passwords（TOTP）を生成することができます。

デバイスを SafeConsole に接続する

Devices become managed by SafeConsole when you register them to the server.

デバイスをサーバーに登録すると、デバイスは SafeConsole によって管理されます。

Users register their devices to SafeConsole either by the device software recognizing a deployed registry key with the SafeConsole URL – or – by the user entering a Connection Token in the device software that they can be emailed through SafeConsole together with a Quick Connect Guide.

ユーザーは、SafeConsole URL に展開されたレジストリキーを認識するデバイスソフトウェアによってデバイスを SafeConsole に登録します。または、ユーザーがデバイスソフトウェアに接続トークンを入力すると、SecureConsole 経由で Quick Connect Guide とともに電子メールで送信できます。

Once registered, the devices have the server information embedded and can be used on any computer – if allowed to do so.

登録されると、デバイスにはサーバー情報が埋め込まれ、許可されている場合は、どのコンピュータでも使用できます。

The process for device communication and setup is the same for SafeConsole Cloud and SafeConsole On-Prem.

デバイスの通信とセットアップのプロセスは、SafeConsole Cloud と SafeConsole On-Prem で同じです。

SafeConsole Cloud network schematic

デバイスを SafeConsole に素早く接続する

Under Help > Quick Connect Guide you find a step by step instruction on how to register you SafeConsole Ready device to you server.

[ヘルプ]> [クイック接続ガイド]で、SafeConsole Ready デバイスをサーバーに登録する方法の手順を確認できます。

組織のデバイスを SafeConsole に登録する

Once you have become familiar with SafeConsole, it is time to connect all your devices to SafeConsole.

SafeConsole に慣れたら、すべてのデバイスを SafeConsole に接続します。

Go to Tools > Deployment Wizard to enter the email addresses to send the Quick Connect Guide. Enter several email addresses either comma separated or with new lines.

[ツール]> [デプロイメントウィザード]の順に進み、クイック接続ガイドを送信するメールアドレスを入力します。複数の電子メールアドレスをコンマ区切りまたは改行で入力します。

Note that there is an option that allows you to deploy the Connection token, used for the device to find the server, using a registry that can be deployed with an ADM template in a Group Policy. Documentation for this is available under Help > Quick Connect Guide in the upper right option *Legacy Devices*.

グループポリシーで ADM テンプレートを使用して展開できるレジストリを使用して、デバイスがサーバーを見つけるために使用する Connection トークンを展開できるオプションがあります。。これに関するドキュメントは、右上のオプションであるレガシーデバイスの[ヘルプ]> [クイック接続ガイド]で利用できます。

New device registrations will use the GeoFence and Trusted Network configuration of the Default Policy unless Unique Token is enabled in server settings.

新しいデバイス登録では、サーバー設定で一意のトークンが有効になっていない限り、既定のポリシーの GeoFence および信頼されたネットワーク構成を使用します。

デバイス登録のトラブルシューティング

Ensure that:

- The device is an actual SafeConsole Ready, secure USB device. There are secure USB devices that cannot be managed by SafeConsole, and some vendors sell both types. The supported hardware for you license is displayed at Help > License in the Supported Hardware box.

  デバイスは実際の SafeConsole 対応の安全な USB デバイスです。SafeConsole で管理できないセキュア USB デバイスがあり、両方のタイプを販売するベンダーもあります。サポートされているハードウェアのライセンスは、[サポートされているハードウェア]ボックスの[ヘルプ]> [ライセンス]に表示されます。

- The license has been installed correctly and that you have a seat available to allow the device to connect.

  ライセンスが正しくインストールされており、デバイスの接続を許可する空きがあること。

- If you have the Server Setting device registrations approval activated you will need to approve actively the device under Device or Users once you have completed the device registration steps.

  サーバー設定のデバイス登録の承認が有効になっている場合は、デバイス登録手順を完了すると、デバイスまたはユーザーでデバイスを積極的に承認する必要があります。

- The device is not managed by another server, when re-installing servers this can happen. Each time the device is factory reset it can connect to a new server. This option can be removed from the device software under the policy User Defauls. Just make sure that you factory reset your device from the server and that action is applied before uninstalling SafeConsole as it will not be possible to break the connection to the uninstalled server once it has been deleted.

  デバイスが別のサーバによって管理されていない場合、サーバを再インストールすると、このようなことが起こります。デバイスが出荷時にリセットされるたびに、新しいサーバに接続できます。このオプションは、ユーザ Defauls ポリシーの下でデバイスソフトウェアから削除することができます。サーバからデバイスを工場出荷時にリセットし、SafeConsole をアンインストールする前にそのアクションが適用されていることを確認してください。一度削除されると、アンインストールされたサーバへの接続を切断することはできません。

- The device is reaching the server from inside the GeoFence and Trusted Network as defined in the default policy.

デバイスは、デフォルトポリシーで定義されているように、GeoFence およびトラステッドネットワーク内からサーバーに到達しています。

ライセンスのインストール

Under the page *Help > License* you can review and install your license. No devices can register to the SafeConsole without an activated license that has seats/slots available.

[ヘルプ]> [ライセンス]ページで、ライセンスを確認してインストールできます。使用可能なシート/スロットがない場合デバイスは SafeConsole に登録できません。

To install a new license click the green button *Install New*, enter your Product Key and click *Activate*. You may need to lock the blue *Refresh* button to ensure that the new license is active.

新しいライセンスをインストールするには、緑色の Install New をクリックし、プロダクトキーを入力して Activate をクリックします。新しいライセンスがアクティブであることを確認するには、青い更新ボタンをロックする必要があります。

SafeConsole On-Prem のライセンス

The licensing mechanism relies on calling back DataLocker's central management server over the Internet to activate, so ensure that this is allowed.

ライセンスメカニズムでは、DataLocker の中央管理サーバーをインターネット経由で呼び出してアクティブにするため、これが許可されていることを確認する必要があります。

サポート

Under Help > Support you will find links to:

[ヘルプ]> [サポート]の順にクリックすると、下記を確認することができます。

- Request customer support – through our online knowledge base.

  オンラインナレッジベースを通じて、顧客サポートを要求する。

- This manual アドミンマニュアル
- Release notes for SafeConsole リリースノート

- Download the latest device updates.

  最新デバイスアップデートをダウンロード

Please visit http://support.datalocker.com/ to find the most up to date resources.
最新のリソースについては、http://support.datalocker.com/をご覧ください。

トラブルシューティングのベストプラクティス

- Update your device and server (On-Prem only) to the latest version.

  デバイスとサーバー(Prem-On のみ)を最新バージョンに更新します。

- Ensure that you can reproduce the error

  エラーを再現できることを確認します。.

- Collect server logs containing the error (for SafeConsole On-Prem).

  エラーを含むサーバーログを収集します(SafeConsole On-Prem の場合)。

  - Located at . . /logs/safeconsole-*. log
- Collect a device log when applicable. This can be generated by pressing ctrl+alt+F6 with the device software running. You can also start the device software with more detailed logging by running windows key+r with the parameter -log-level 3, example: g:¥Sentry3. exe --log-level 3

  必要に応じてデバイスログを収集します。 これは、デバイスソフトウェアを実行して ctrl + alt + F6 を押すことで生成できます。 また、Windows のキー+ r をパラメータ-log-level 3 (例 : g : ¥ Sentry3. exe --log-level 3) で実行して、より詳細なログを使用してデバイスソフトウェアを起動することもできます

- Review the logs in a good text editor, these may be hard to digest at first glance, but sometimes this will tell you what is wrong once you locate the point of failure. If applicable check the corresponding time in the device or server log.

  良いテキストエディタでログを確認します。一見したところで消化するのは難しいかもしれませんが、失敗点を見つけたら何が間違っているかを教えてくれることがあります。該当する場合は、デバイスまたはサーバーのログで対応する時刻を確認します。

- Search http://support.datalocker.com/ to see if you can find a solution.
  http://support.datalocker.com/を検索し、ソリューションを見つけることができるかどうかを確認してください。
- Screenshots or recordings of the error often lead to much quicker resolution times.

  スクリーンショットやエラーの録音により、解決時間が大幅に短縮されることがあります。

- If you are to post a support ticket with DataLocker the first contact is with your valued added reseller as they will probably be able to assist you the quickest.

  DataLocker でサポートチケットを投稿する場合、最初の連絡先は代理店です。これはおそらくあなたを最も迅速に支援することができるからです。

May, 2017, version 5.2.0