AppTec360 Enterprise Mobile Manager & ContentBox

管理マニュアル | バージョン5.0 (202110)

目次

- SecurePIMセキュリティ
- SecurePIMブラウザ
- 交換

コネクション管理

- Wi-Fi
  - プロキシの設定
  - セキュリティ・タイプ
- かそうへいいきもう
  - VPNタイプ
    - かそうへいいきもう
    - アプリごとのVPN
  - プロキシの設定
- APN
- セルラー
- HTTPプロキシ
- エアプリント
- エアプレイ

PIM管理

- Exchangeアクティブ同期
- 電子メール
  - 受信メール
  - 送信メール
- カルダヴ
- 購読カレンダー
- ライトウェイトディレクトリアクセスプロトコル

ウェブ管理

- ウェブクリップ
- ウェブコンテンツフィルター

アプリ管理

- エンタープライズアプリマネージャー
  - インストール済みアプリ (デバイスレベルのみ)
  - 必須アプリ
    - インストール・オプション
  - ウェブアプリ

- 制限と設定
  - ブラックリスト/ホワイトリストのアプリ
  - システアプリの制限
  - アプリ-VPN
  - アプリの設定
- エンタープライズ・アプリケーション・ストア
  - iTunesアプリ
  - インハウス
- キオスク・モード
  - アプリケーション・タイプ
    - パッケージ
    - URL
  - キオスクモードの設定

Android Enterprise – フルマネージド・デバイス構成

一般

- グループプロフィールの概要 (グループレベルのみ)
- デバイスの概要 (デバイスレベルのみ)
- コンフィグ改訂 (デバイスレベルのみ)
- デバイスログ (デバイスレベルのみ)
  - コマンドログ
  - 可能なコマンドステータス
- デバイス設定
  - クライアント設定
  - 壁紙

資産管理 (デバイスレベルのみ)

- デバイス情報
  - Wi-Fi
- セルラー
- ブルートゥース

セキュリティ管理

- 盗難防止 (デバイスレベルのみ)
  - GPS情報 (デバイスレベルのみ)
  - ワイプ＆ロック (デバイスレベルのみ)
  - メッセージ (デバイスレベルのみ)

- 壁紙

資産管理 (デバイスレベルのみ)

- デバイス情報
  - Wi-Fi
- セルラー
- ブルートゥース

セキュリティ管理

- 盗難防止 (デバイスレベルのみ)
  - GPS情報 (デバイスレベルのみ)
  - ワイプ＆ロック (デバイスレベルのみ)
  - メッセージ (デバイスレベルのみ)
- セキュリティ設定
  - デバイスのパスコード
  - コンテナ・パスコード
  - アンチウイルス
- エンド・オブ・ライフ (デバイス・レベルのみ)
  - ワイプ (デバイスレベルのみ)
- 制限の設定
  - 制限事項
- 証明書管理

コネクション管理

- 無線LAN
  - セキュリティ・タイプ
    - ウェップ
    - WPA/WPA2
    - 802.1x EAP
- かそうへいいきもう
  - VPNタイプ
    - かそうへいいきもう
    - アプリごとのVPN
- 制限事項

PIM管理

- Gmailエクスチェンジ

アプリ管理

- エンタープライズアプリマネージャー

- メッセージ (デバイスレベルのみ)
- セキュリティ設定
  - パスコード
  - 暗号化
  - アンチウイルス
- エンド・オブ・ライフ (デバイス・レベルのみ)
  - ワイプ (デバイスレベルのみ)
- 制限の設定
  - 制限事項
  - AEデバイス所有者

BYODコンテナ

- アンドロイド・エンタープライズ
  - アンドロイド・エンタープライズ
  - Gmailエクスチェンジ
  - AEシステムアプリ
  - コンテナ・パスコード
- サムスンKNOX
  - アクティベーション
  - ノックスのパスコード
  - ノックス・セキュリティ
  - ノックス・エクスチェンジ
  - ノックスeメール
  - ノックスアプリ

コネクション管理

- 無線LAN
  - セキュリティ・タイプ
    - ウェップ
    - WPA/WPA2
    - 802.1x EAP
- かそうへいいきもう
- 制限事項
- APN
- ブルートゥース

PIM管理

- 交換

- デバイスログ (デバイスレベルのみ)
  - コマンドログ
  - 可能なコマンドステータス
- 資産管理 (デバイスレベルのみ)
  - デバイス情報
  - セルラー
  - 同期情報
- セキュリティ管理
  - 盗難防止 (デバイスレベルのみ)
    - GPS情報 (デバイスレベルのみ)
    - GPS設定
  - セキュリティ設定
    - パスコード
    - アンチウイルス
    - セキュリティセンター
    - ファイアウォールの設定
    - ファイアウォールルール
  - 制限の設定
    - デバイスの機能
  - ビットロッカー
    - ビットロッカーの設定
    - ビットロッカーの状態
  - 証明書管理
    - 証明書リスト
    - 証明書の構成
    - SCEP
- コネクション管理
  - 無線LAN
    - セキュリティ・タイプ
    - プロキシサーバーの使用
  - Wifiの制限
  - かそうへいいきもう
    - 接続タイプ
    - 一般的なVPN構成
  - VPNの制限
  - ブルートゥース
- PIM管理

- Exchangeアクティブ同期
- 電子メール
- アプリ管理
  - エンタープライズアプリマネージャー
    - インストール済みアプリ
    - 必須アプリ
    - シスアプリの制限
    - ブラックリストとホワイトリスト

MacOSの設定

一般

- グループプロフィールの概要 (グループレベルのみ)
- デバイスの概要 (デバイスレベルのみ)
- コンフィグ改訂 (デバイスレベルのみ)
- デバイスログ (デバイスレベルのみ)
  - コマンドログ
  - 可能なコマンドステータス

資産管理 (デバイスレベルのみ)

- デバイス情報
- WiFi
- セルラー
- ブルートゥース

アップデート管理 (デバイスレベルのみ)

- 更新情報

セキュリティ管理

- 盗難防止
  - ワイプ＆ロック
- セキュリティ設定
  - パスコード
  - 証明書
- 制限の設定
  - デバイスの機能
  - iCloud
  - メディア・マネジメント

コネクション管理

概要

AppTec360の紹介

AppTecのEnterprise-Mobile-Management-Solutionは、直感的な管理コンソールですべてのモバイルデバイスを管理・設定するオプションを提供します。 このシナリオでは、EMMサーバーはお客様の周囲で実行することも、当社のクラウドベースのソリューションを利用することもできます。

スマートフォンに企業アプリケーションを集中インストールするという話題でも、あなたは正しい場所に来た。 Enterprise Mobile Managerを使用すると、企業のアプリケーションやドキュメントを数秒以内にデバイスに配布したり、ホワイトリスト/ブラックリストを使用して望ましくないアプリケーションをブロックしたりできます。

企業における私物端末の利用は、スマートフォンやタブレット端末のセキュリティ確保に新たな課題を突きつけている。 従業員がますますスマートフォンを使いたがるようになっているため、IT管理者は数多くの種類のデバイスを保護しなければならない。 私たちは、すべてのデバイスとデバイスに保存されている機密データを保護し、直感的なコンソールから管理するお手伝いをします。

対応デバイスOS

AppTec360はiOS、Android、Windowsデバイスをサポートしています。 なお、上記プラットフォームの機能容量は、OSごとに異なる場合があります。

- Apple iOS 11.0以上
- Apple macOS 10.11以上
- Google Android 4.4以上**のクラウド版
- Google Android 4.1以上**のオンプレミス版
- MS Windows 10以上*** (デスクトップパソコン、 ノートパソコン、タブレット)

iOS10以前の端末は、 アップル社による登録プロセスの大幅な変更により、登録できませんのでご注意ください。

**メーカーのサポートが終了したバージョンを使用しているデバイスであっても、接続およびコンフィギュレーションは可能です。 特定のAndroidバージョンを必要とする機能があることにご注意ください。 サポートの場合は、メーカーの公式サポートに従う。 メーカーのサポートが終了した古いバージョンに起因する問題やバグが発生した場合、弊社は限定的なサポートのみを提供する権利を留保します。*

***HomeバージョンのWindowsは、OSの制限によりサポートされていません。 メーカーがまだサポートしているOSバージョンを使用することを強くお勧めします。 互換性だけでなく、セキュリティ上の理由もある。 そのため、iOS 12以上、Android 9以上を推奨する。*

対応LDAPディレクトリ

- マイクロソフト・アクティブ・ディレクトリ
- LDAPを開く

サポートされるデバイス・オペレーティング・システム」および「サポートされるLDAPディレクトリ」に関する最新情報は、こちらをご覧ください：

https://www.apptec360.com/products/systemrequirements/

アップル製デバイスにおける「監視モード」の説明

Supervised-Modeは、iOSデバイス用の拡張インターフェイスです。

それぞれ設定された装置において、エンドユーザー装置の機能に関連する追加制限を適用することができる。 これらは管理ハンドブックにも記載されており、バナーで示されている。

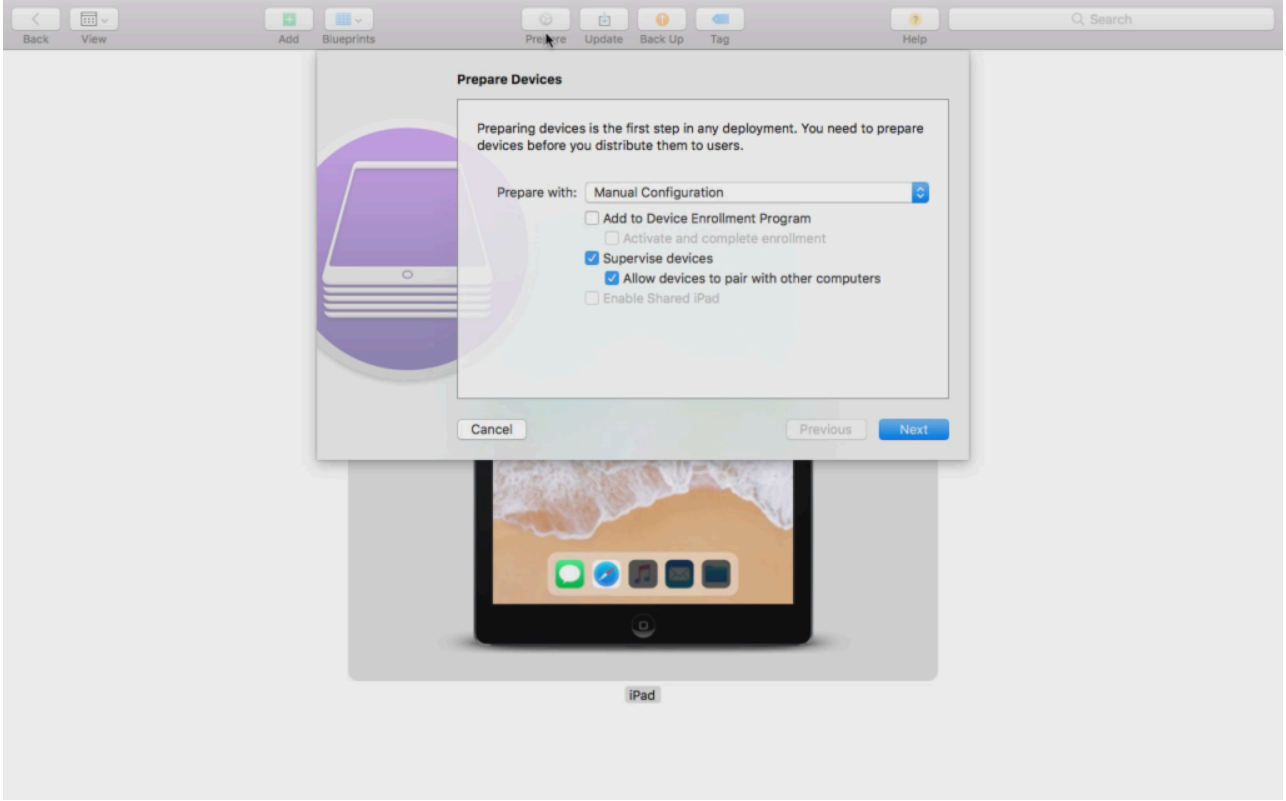
監視付きモードで使用可能

Supervised-Mode "は "Apple Configurator "プログラムで有効にすることができます。 Apple Configuratorは、コンフィギュレーションツールとして新しいiOSデバイスのデフォルト設定を行うことができます（USBインターフェース経由）。

このツールは構成プロファイルだけでなく、アプリもインストールできる。 無料だが、マック・コンピューターが必要。

監視モードを起動する

1. Apple Configuratorを開く



2. デバイスをクリックし、"Prepare "を選択する。
3. 手動設定 "と "デバイスの監視 "を選択する。
4. 次へ」をクリック
5. (オプション）これで、デバイスを登録するMDMサーバーを追加できます。 このリンクは、"一般設定 - iOS設定 - 設定とURL "で見つけることができます。
6. 組織を選択するか、新しい組織を作成する
7. 初期セットアップでどのステップをスキップするかを選択し、「次へ」をクリックします。

これであなたのデバイスは監視モードになります。 これには数分かかる。 完了後、デバイスが再起動します。

これであなたのデバイスは監視される！

DEPにデバイスを追加する

また、iOS 11以上のデバイスであれば、Apple Configuratorを使用してDEP（Device Enrollment Programm）にデバイスを追加することもできます。

DEPに関する詳細情報: https://www.apple.com/business/dep/

デバイスを監督するのと同じ手順で、さらに「Add to Device Enrollment Programm」にチェックを入れます。Apple ConfiguratorでDEPにログインしたことがない場合は、DEPログインデータの入力を求められます。

プロセスが完了すると、デバイスは DEP サーバー「Apple Configurator 2 によって追加されたデバイス」に表示されます。このサーバーを使用し、管理コンソールに接続するか、すでに存在するサーバーにデバイスを転送することができます。

これでDEPへのデバイス追加が完了しました！

アンドロイド・エンタープライズの説明

Android Enterpriseとは？

Android Enterpriseは、MDMで管理されている業務用デバイスをより適切に管理します。これにより、管理者はアンドロイドデバイスを完全に管理することも、コンテナデバイス上のプライベートなデータから会社のデータを分離することもできます。さらに、Android Enterpriseでは、デバイスの登録が簡単になり、アプリの配布も簡単になります。

Android Enterpriseを使用するための条件は何ですか？

Android Enterprise は誰でも無料で使用できます。Android Enterprise のすべての機能を有効にするには、MDM に google アカウントを接続するだけです。詳しくはAndroid Enterpriseのセクションをご覧ください。

Android Enterpriseは、Enhanced Work Profile（下記参照）を除き、Android 5.1以上の端末でご利用いただけます。利用可能なすべての機能を利用するには、より簡単に登録するために少なくともAndroid 7以上、またはAndroid 11をお勧めします。

Android Enterpriseで利用可能なモードは何ですか？

Android Enterpriseを使用する際には、3つの異なるモードがあります。

AEフルマネージドデバイス（ワークマネージド）：業務にのみ使用されるフルマネージド・デバイス。管理者がデバイスを完全に管理できる。デバイスの私的利用は許可されません。このモードでデバイスを登録するには、デバイスをリセットして QR コードで登録するか（「AE 登録」を参照）、Knox 登録または Zero Touch で登録する必要があります。

AE BYODコンテナ：BYOD (Bring Your Own Device)コンテナでは、ユーザーはプライベートな携帯電話で会社のデータにアクセスすることができます。このモードでは、プライベート・アプリは会社のデータやアプリを見ることができず、その逆も同様です。このモードでデバイスを登録するには、AppTecアプリをダウンロードし、QRコードをスキャンする必要があります。コンソールでデバイスを作成し、デバイス・タイプとして「AE Container (BYOD & Enahnced Work Profile)」を選択する。新しく生成されたデバイスの QR コードをクリックして QR コードを取得し、最初のスイッチを「Legacy & BYOD」に設定します。

AE Enhanced Work Profile: (Android 11 以上が必要) 上記の BYOD Container がプライベート・デバイスに会社のデータを持ち込むのに対して、Enhanced Work Profile は同じことを会社所有のデバイスに対して行います。同じコンテナを作成しますが、管理者がデバイスをもう少しコントロールできるため、ユーザーはデバイスから MDM を削除することはできません。コンソールでデバイスを作成し、デバイス・タイプとして「AE コンテナ（BYOD & Enahnced Work Profile）」を選択します。新しく作成したデバイスの QR コードをクリックして QR コードを取得し、最初のスイッチを

「Enhanced Work Profile」に設定します。この QR コードは、AE 登録の方法 1 で説明したように、デバイスをリセットして画面を 6 回タップした後にスキャンできます。

Android Enterpriseデバイスにアプリを割り当てる方法を教えてください。

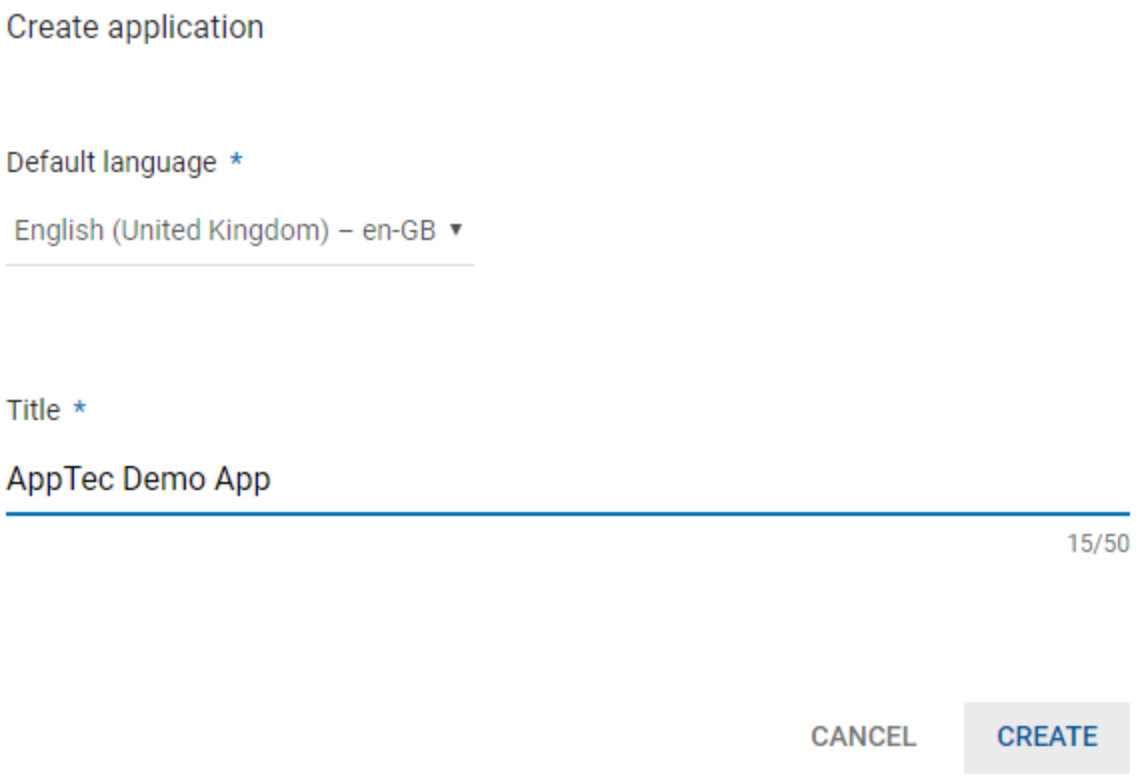
まず、「一般設定」→「アプリ管理」→「AE Playストア」→「Playストアアプリ」で使用するアプリを承認する必要があります。アプリを承認した後、「+」をクリックし、「AE Play Store」タブからアプリを選択することで、プロフィールの必須アプリリスト→にアプリを割り当てることができます。自動的にアプリがダウンロードされ、インストールされます。端末のgoogleアカウントは不要で、ユーザーは確認や許可する必要はありません。

Google Playストアに自分のアプリをアップロードする

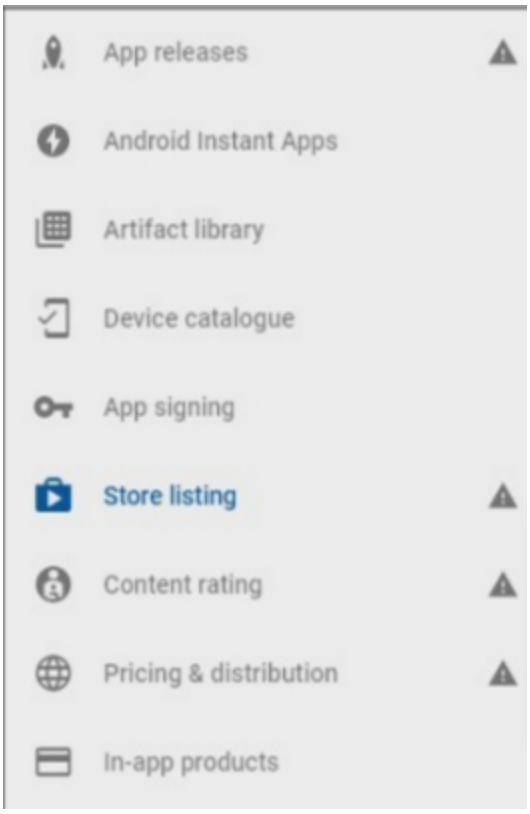
自社アプリをGoogle Playストアにアップロードすることが可能です。こうすることで、Playストアのアップデートメカニズムなど、さまざまなメリットを享受することができます。

そのためには、Googleデベロッパーアカウントが必要です。Google Play Console(https://play.google.com/apps/publish) からログインします。

アプリケーションの作成」をクリックします。デフォルトの言語とアプリのタイトルを選択します。



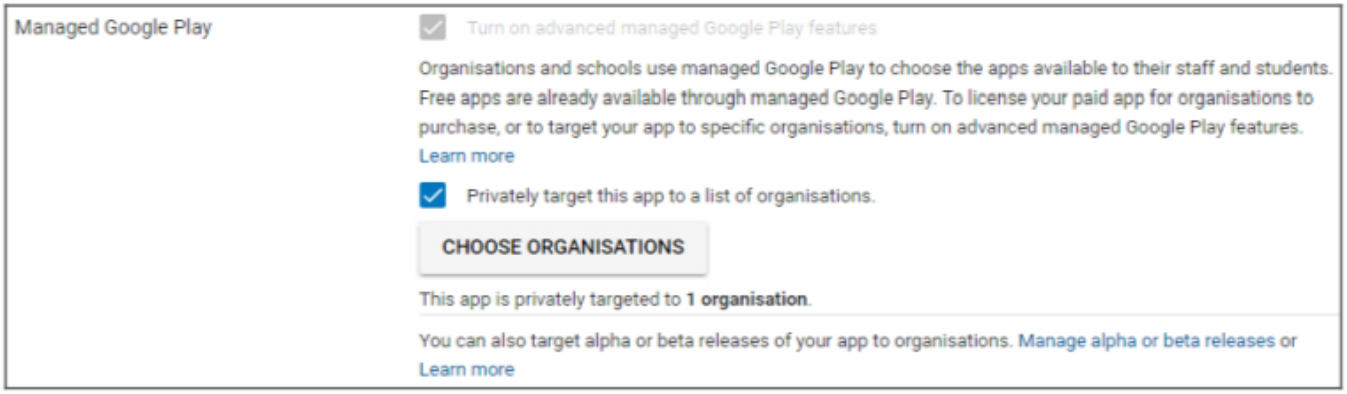
次のページでは、アプリに関するさまざまな詳細を入力するよう求められます。



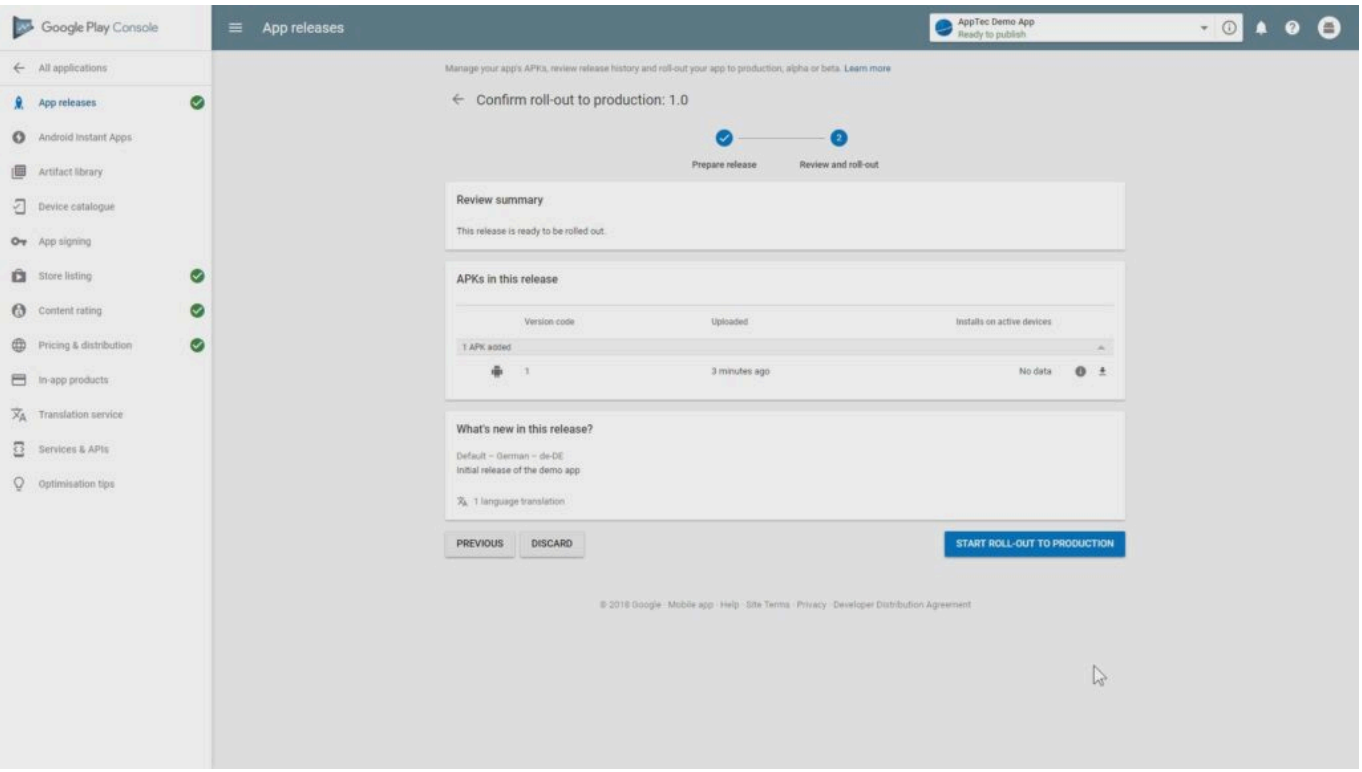
すべての詳細を入力した後、左側にさまざまなヒントマークが表示されます。

カーソルを合わせると残りのステップが表示されるので、好きな順番でステップを踏んでいく。

注意：「価格と配信」の「Google Playを管理する」の2つのチェックボックスを必ずチェックしてください。そうしないと、アプリは公開され、誰でもアクセスできるようになります。また、配信する国を必ず選択してください。



すべてのステップが完了したら、"App releases "に進みます。レビュー "をクリックし、"本番環境へのロールアウトを開始 "をクリックすると、ドラフトが完成し、アプリが公開されます。



アプリがPlayストアで利用可能になるまで、しばらく時間がかかります。プロセスが終了したら、Play for Work ストアでアプリを検索し、承認することができます。その後、他のアプリと同じようにEMMコンソールを使ってアプリをデバイスに割り当てることができます。

必要条件とインストール

必要条件

システム要件

仮想アプライアンスは、Open Virtualization Format（VMWare、VirtualBox、Citrix Xen Server）および圧縮された.vhdx（Hyper-V）ファイル*で提供されます。

*注：Hyper-Vを使用する場合、マシンはジェネレーション1で作成する必要があります。

仮想ディスクの目標サイズは20GBで、マシンには4GBのRAMが必要です。

アプライアンスはDebian 9 64bitをベースにしています。

インポートしたマシンを最新の互換性（VMWareなど）にアップグレードし、ハイパーバイザーでマシンのOSタイプが正しく設定されていることを確認する。

ライセンスキー

サーバーのアクティベーションとインストールを成功させるには、有効なライセンスファイルが必要です。AppTec360から直接、または各販売店から入手できます。

IPアドレスとDNSの解決

AppTec360 アプライアンスは、ライセンスが発行されたホスト名を使用するデバイスから到達可能でなければなりません。

Windows 10デバイスを登録するには、アプライアンスを指す "enterpriseenrollment. "という形で追加のサブドメインを設定する必要もある。

SSL証明書

デバイスとのすべての接続はSSLを使用して保護する必要があるため、デバイスから信頼されている認証局から発行されたホスト名の有効な証明書が必要です。証明書の秘密鍵は、パスワード保護なしでアップロードする必要があります。ほとんどの場合、デバイスがサーバー証明書を認識するためには、認証局の中間証明書が必要です。

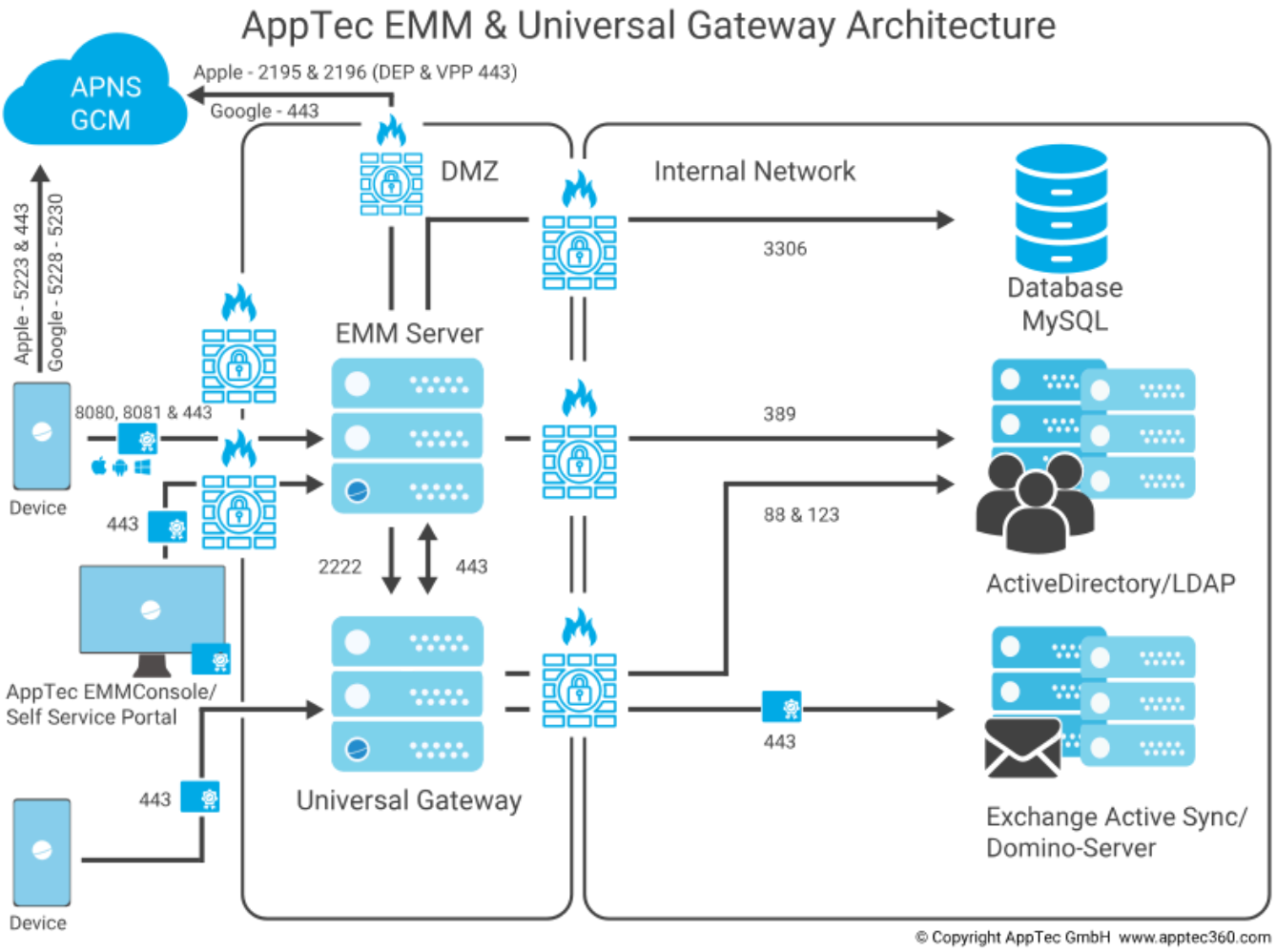
Windows 10デバイスには、enterpriseenrollmentサブドメイン用の特定の証明書が必要です。

アプライアンスのバージョン 202104 からは、自動的に生成される Let's Encrypt 証明書も使用できます (ステップ 2 - SSL 証明書で説明) 。

SMTPサーバー

AppTec360 EMM が電子メールを送信するためには、電子メールサーバーおよび/または電子メールリレーが必要です (デバイス登録やアカウント認証など) 。

ファイアウォールルール



この図は、利用したいサービスによってどの接続が必要かを示しています。

より詳細な説明は次ページの表を参照。

任意（外部/デバイス）	→	**AppTec360 アプライアンス / emmconsole.com**
港湾	443	管理、エンタープライズAppStore & Windows Phoneコミュニケーション
	8080	Android & iOS コミュニケーション
	80	Let´s Encryptの初回セットアップ。その後443を使用。
すべて（デバイス）	→	**任意（外部）**
港湾	5223, 443	Apple Push Service、プロキシなしで到達可能でなければならない、フォールバックとして443、https://support.apple.com/en-us/HT203609を参照。
	5228-5230	Android Push Service (FCM)は、プロキシなしで到達可能でなければならない。
AppTec360 アプライアンス	→	**ドメインコントローラ**
港湾	389、（LDAP636）	LDAPによるユーザー同期
AppTec360 アプライアンス	→	**どんなものでも**
ポート	443	Androidプッシュサービス（GCM）に使用されます。 AppStore / Playストア検索
AppTec360 アプライアンス	→	**エムエムコンソールドットコム**
港湾	443	AppTec360アプライアンスのアップデート、APNS証明書の生成
AppTec360 アプライアンス	→	**アップルネットワーク（17.0.0.0/8）**
港湾	2195, 2196	Appleプッシュサービス＆フィードバックサービス
	443	DEP & VPP

セキュリティ・アップデート

Debian オペレーティングシステムは、最新のセキュリティフィックスを得るために 定期的にアップデートされるべきです。しかし、手動で Debian の新しいメジャーバージョンにアップグレードしないように注意してください。AppTec360 EMM が新しいメジャーバージョンと互換性がある場合、アプライアンスのアップデートでアップグレードする方法を追加します。

仮想アプライアンスのデフォルトパスワード

ログインユーザー (Rootログインは無効。管理作業には "sudo "を使用)

アプリテック

ログインパスワード

アプリテック

MySQLルートユーザー

ルート

MySQLルートパスワード

アプリテック

MySQL デフォルトユーザ

アプテック

MySQLデフォルトユーザーパスワード

アプテック

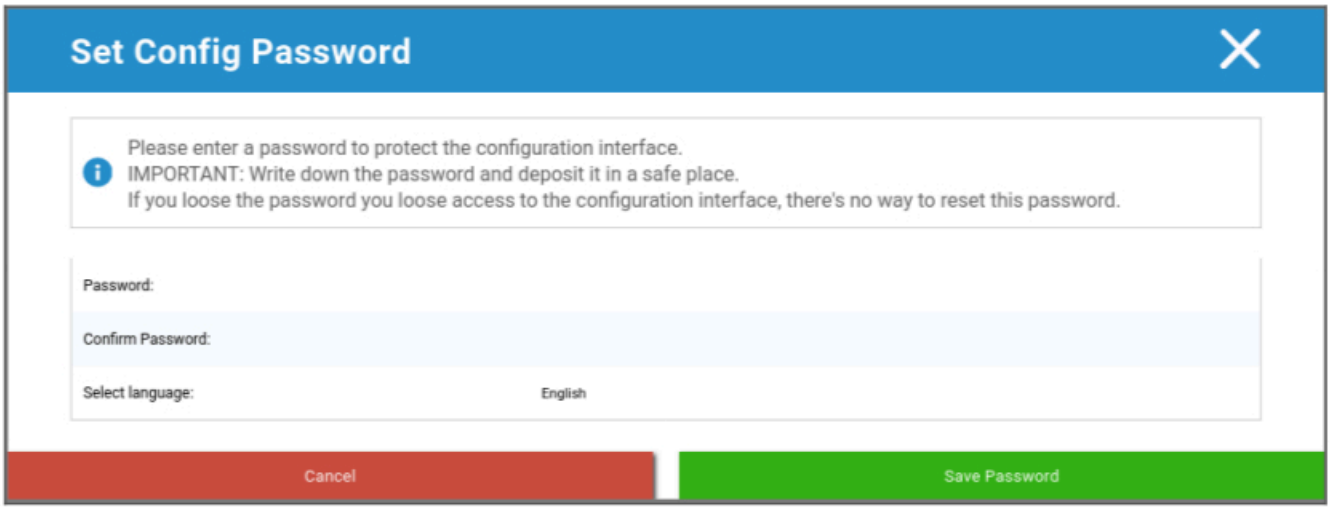
仮想アプライアンスの構成

重要:仮想アプライアンスの構成を開始する前に、ディスプレイ解像度を 1280 x 800ピクセル以上に設定してください。

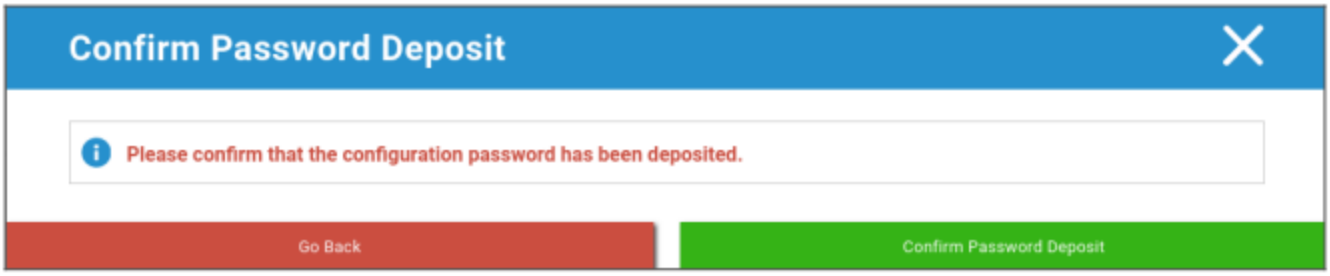
アプライアンスにロングインすると、Firefoxが自動的に起動し、構成インターフェイスが表示されます。

準備

最初に、コンフィギュレーション・インターフェースのパスワードを入力する必要があります。このパスワードは、コンフィギュレーション・インターフェイスに入力されたすべての情報とファイルを暗号化するために使用されます。ここでインターフェイスの表示言語を設定することもできます（後で変更可能）。

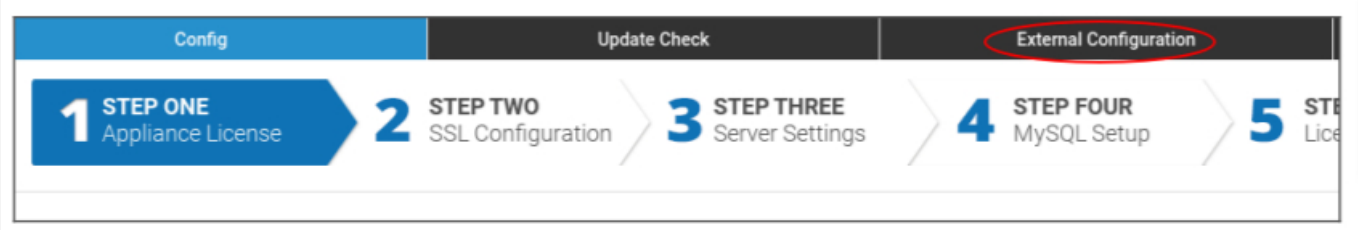


パスワードはAppTec360サポートによってのみリセットできますので、安全な場所に預け、今後のポップアップを確認してください。



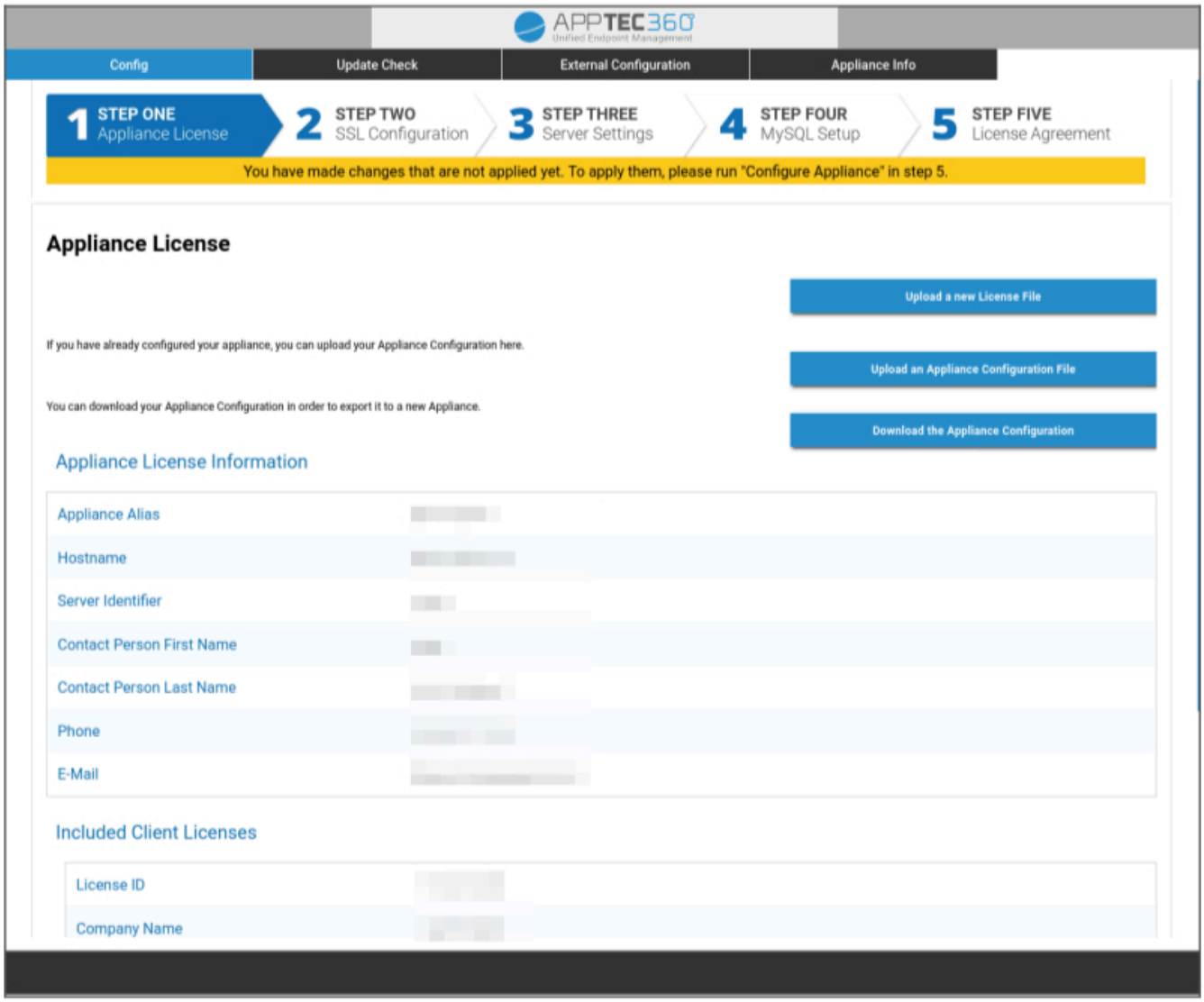
外部ホストからの設定

設定プロセスを簡単にするために、リモートから設定ページにアクセスできるようにすることができます。そのためには、「外部ホストから設定する」の手順に従ってください。



ステップ1 – アプライアンス・ライセンス

1. AppTecから受け取ったライセンスファイルをアップロードしてください。
2. ライセンスファイルが正常にアップロードされると、以下のスクリーンショットのようにアプライアンスのライセンス情報が表示されます。



ステップ2 – SSL証明書

Let's Encryptを使用した証明書の自動セットアップを使用するか、証明書を自分で用意することができます（詳細はSSL-Certificateを参照）。

自動

証明書はLet's Encryptサービスを使用して自動的に生成されます。

AppTec360 EMM は、ドメインの検証のためにHTTP-01 チャレンジを使用します。これは、証明書の最初の要求のために HTTP ポートがインターネットから開いている必要があることを意味します。その後の更新リクエストは HTTPS 経由で検証できる。

ラジオボタンを「自動（Let's Encrypt）」に切り替え、「SAVE VALUES」を押します。ステップ5「ライセンス契約」で設定を適用する際に、証明書が自動的に要求されます。証明書は必要に応じて自動的に更新され、証明書の有効期限が切れるとEメールが届きます（更新に失敗したことを意味します）。

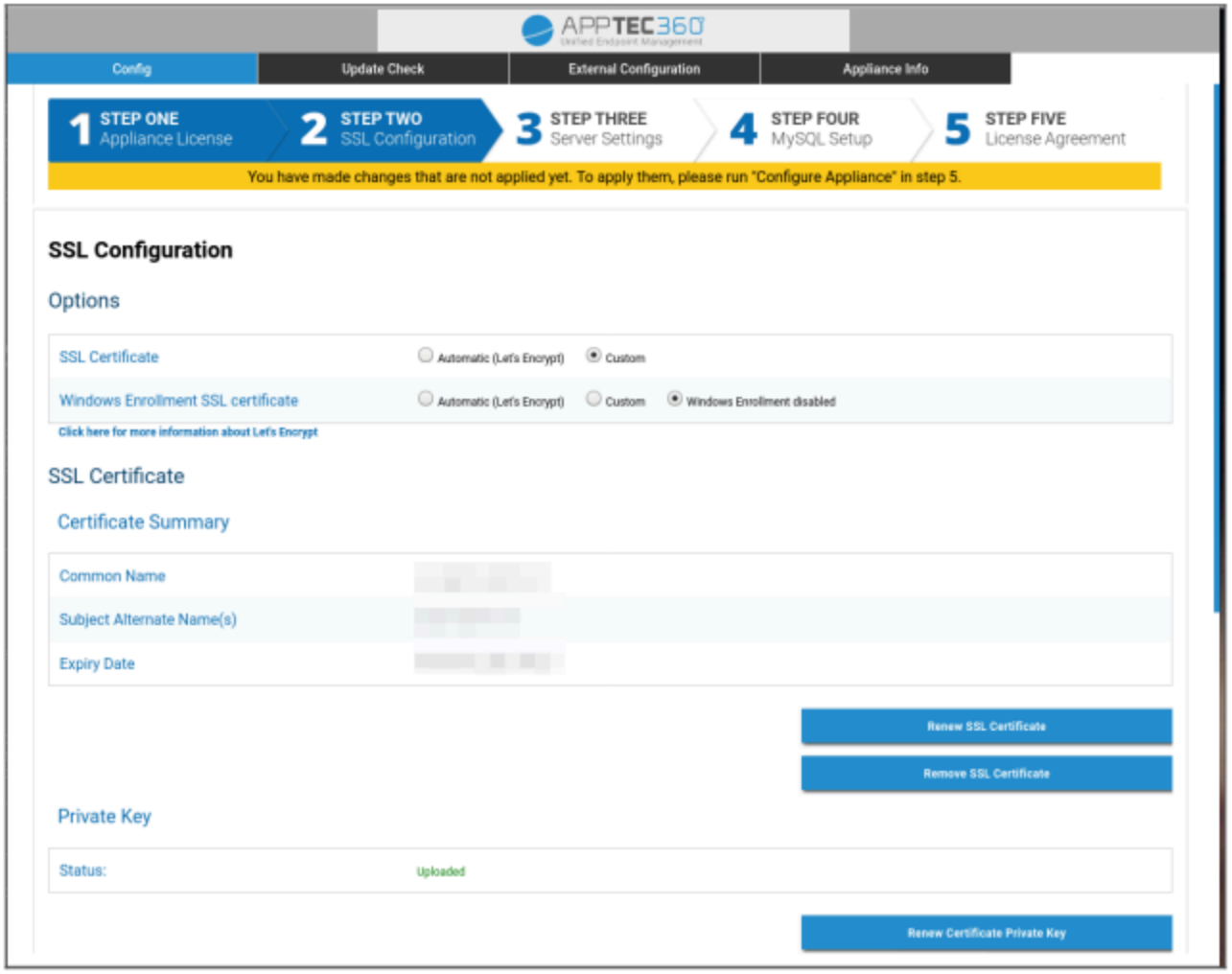
カスタム

1.ライセンスを受けたホスト名のSSL証明書をアップロードします。ホスト名はステップ1 - アプライアンスライセンスで確認できます。

2.証明書の秘密鍵と、必要に応じて中間証明書もアップロードしてください。

重要：キーにはパスワードをかけてはいけません。パスワードがかかっている場合は、アップロードする前にパスワードを解除してください。

ヒント：Windows 10デバイスも使用したい場合は、"Windows Enrollment SSL certificate "を有効にし、サブドメインの証明書、秘密鍵、中間証明書をアップロードする必要があります（ページ下部のIPアドレスとDNS解決に記載）。



ステップ3 – サーバー設定

1. グローバルサポートメールアドレスを入力してください。このアドレスはユーザーへのEメールに使用され、デバイスに関して何か問題が発生した場合の連絡先を知ることができます。
2. システムが電子メールを送信するために使用する電子メール設定を提供します。この設定は、ユーザーにEメールを送信するために使用されます。また、バグレポートや機能要求を"support@apptec360.com "に送信するためにも使用されます。Eメール設定を保存した後、"Test E-Mail Configuration "をクリックし、指示に従って設定を確認する必要があります。

ステップ4 – MySQLのセットアップ

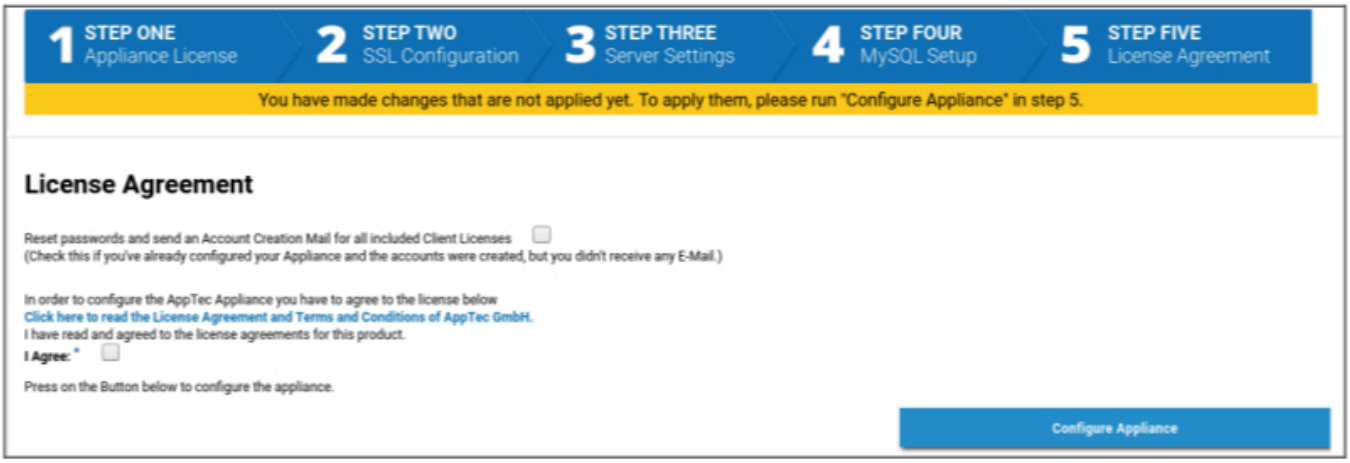
1. 内部データベースを使用する場合は、この手順を省略できます。そうでない場合は、外部データベースサーバーの接続情報を入力します。


1 STEP ONE Appliance License
2 STEP TWO SSL Configuration
3 STEP THREE Server Settings
4 STEP FOUR MySQL Setup
5 STEP FIVE License Agreement
You have made changes that are not applied yet. To apply them, please run "Configure Appliance" in step 5.
MySQL Setup
The MySQL connection has been successfully tested at April 7, 2021, 8:45 am.
If you change the settings after the initial configuration, you have to reconfigure your appliance by clicking on "Configure now" in step 5.
IP Address or Hostname
127.0.0.1
(Default: 127.0.0.1)
Username
AppTec
(Default: AppTec)
Password
(Default: AppTec)
Port
3306
(Default: 3306)

ステップ5 – ライセンス契約

1. 使用許諾契約書を必ずお読みください。
2. I Agree "をチェックし、"Configure Appliance "ボタンを押して設定を適用します。

ヒント：設定を適用するには、5つのステップで設定を変更するたびに「アプライア ンスの構成」を実行する必要があります。



おめでとう！

これで仮想アプライアンスの設定は完了です。

パスワードを含む電子メールが、ライセンス用に提供したアドレス（ステップ1 - アプライアンスライセンスの「含まれるクライアントライセンス」で確認できます）に送信されます。

これで、このパスワードと受け取ったEメールアドレスを使用してコンソールにログインできるようになります。

コンソールにログインするには、ブラウザのアドレスバーにコンソールのホスト名を入力してください。

アプライアンスのホスト名は、ステップ1 - アプライアンスライセンスで確認できます。

トラブルシューティング

1.ステップ 5 - ライセンス契約」でアプライアンスを構成する際に、電子メールを受信しませんでした：

ステップ3「サーバー設定」の電子メール設定が正しいことを確認してください。パスワードを再送信するには、[アプライアンスの設定]を再度実行する前に、ステッ プ5 - ライセンス契約の[パスワードをリセットし、含まれるすべてのクライアントライセン スにアカウント作成メールを送信する]をチェックしてください。

2.ステップ5「ライセンス契約」の設定中に、Let's Encryptに関してエラーが発生しました：

アプライアンスがポート80のドメイン名で到達可能であることを確認する。Let's encryptは「/var/log/letsencrypt」にログも書き込むので、さらなるトラブルシューティングに役立つかもしれない。

セキュリティに関する推奨事項

AppTec360 アプライアンスを保護するために、以下の手順を実行することを推奨します。

これは指示の完全なセットではなく、基本的な構成の推奨に過ぎない。

- AppTec360ユーザーのパスワードを変更する
- MySQLユーザー "root "と "AppTec "のパスワードを変更し、ステップ4 - MySQL Setupを更新する。
- デフォルトのSSHサーバー・ポートを変更する
- コンソールで80番ポートをブロックし、HTTPトラフィックの着信を拒否し、HTTPSのみを使用する。一度設定すれば、HTTPS経由での外部設定も可能です。
- ステップ3「サーバー設定」の下部で、管理インターフェイスへのアクセスを特定のIPSのみに制限する。
- ファイアウォールの設定

一般設定

アカウント概要

口座情報

概要

ここでは、AppTec360アカウントの概要を見ることができます。

会社名	貴社名
作成日	アカウントの作成日
ライセンスの種類	有料 = 有料ライセンス フリー = 無償ライセンス 注：オンプレミス・アプライアンス上のアカウントは、技術的な理由により常に支払済みとして表示されます。
クライアント識別子	アカウントの識別子（これは顧客番号ではありません）
ライセンス有効期限	AppTec360ライセンスの有効期限
ContentBoxライセンス	無料 = 25台分の無料ライセンス 有料 = x台分の有料ライセンス
ランチャー	Androidのカスタムランチャーを使用できるかどうかを表示します。
デバイス	現在使用中のライセンス数 / 総ライセンス数
担当者	提供された連絡先
電話	提供電話番号
電子メール	提供メールアドレス
ルートユーザー	ログイン可能なルートユーザー
ソフトウェア版	現在のソフトウェア・バージョン

**注: ここに表示されるEメールアドレスは、アカウント登録時に入力したものです。これに基づいて、ユーザ/デバイスツリーにユーザが作成され、変更することができます。このユーザーを編集すると、ログインに使用するメールアドレスは変更されますが、アカウント概要の情報は変更されません。 .*

バグレポート

バグレポートは、問題やバグを報告するためにサポートに直接送信することができ、あなたのアカウントとセットアップに関する情報とログが含まれています。

テーマ	バグレポートの件名。既存のサポートチケットに追加する場合は、チケット番号を入力してください。
期待される行動	何をしたのか、何が起こると予想したのかを詳しく説明すること。
実際の行動	具体的に何が起こったのか、詳しく説明してください。エラーメッセージを正確に引用してください。また、スクリーンショットを添付していただけると助かります。
どのような時に問題が発生しましたか？	具体的なエラーメッセージや問題が発生した正確な時刻を教えてください。 最良の場合、秒数も含める（例：18:55:27
その問題は再現できますか？もし可能なら、どのように（詳細に）再現できますか？	問題の再現方法を詳しく説明してください。
この機能は以前、期待通りに機能しましたか？もしそうなら、いつまでですか？	わからない場合は空欄にしてください。
この問題が発生する前に、システムに特定の変更が加えられましたか？ある場合、どのような変更（詳細）がありましたか？	たとえそれが関係ないと思っても、その問題が現れる前にあなたが最後に行った変更や行動について、常に言及すること。
該当する場合影響を受けるデバイスのモデルとOSのバージョンは？	OSのバージョンを必ず正確に指定してください（例：iOS 14.7.1、Android 11）
該当する場合デバイスのパブリックIPアドレスまたはシリアル番号を教えてください。	すべてのデバイスが影響を受けている場合でも、少なくとも1つの名前を挙げてください。
ログファイルを含む	バグレポートと一緒にログファイルを送信するには、これをチェックしてください。これは推奨されます。
Appleから現在のVPPの状態を取得し、バグレポートに含める。	VPPライセンスの割り当てに関する情報が含まれています。サポートから要求された場合、または問題がVPPに関するものである場合のみ、これを有効にしてください。

アタッチメント	役に立ちそうなファイルがあれば添付してください (エラーメッセージのスクリーンショットなど) 。

機能リクエスト

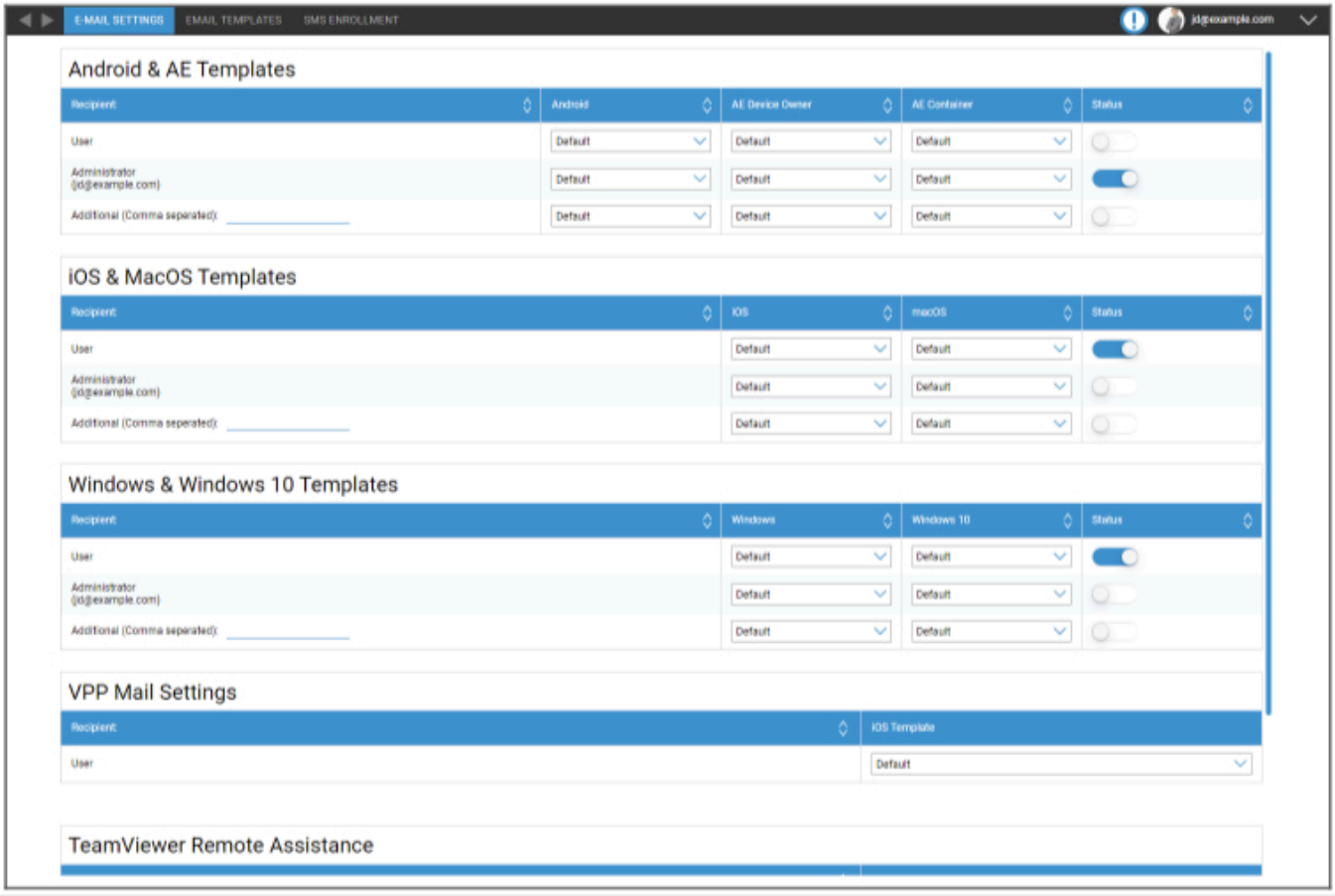
機能リクエストはサポートに直接送ることができます。このリクエストには、特定の機能に対するリクエストや、次のような改善点が含まれます。

概要	問題の簡単な概要
説明	問題の詳細、できるだけ具体的にご記入ください。
アタッチメント	バグレポートにファイルを添付する

グローバル設定

電子メール設定

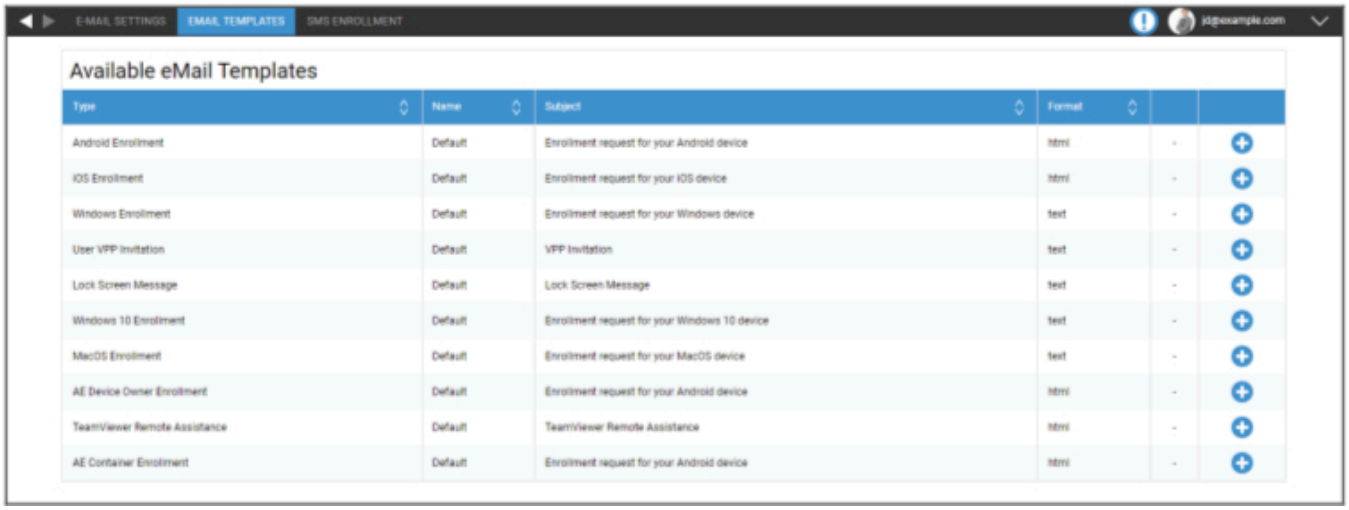
ここでは、登録リクエストが生成されたときにメールを受け取る人、およびそのメールに使用されるテキストテンプレートを定義できます。



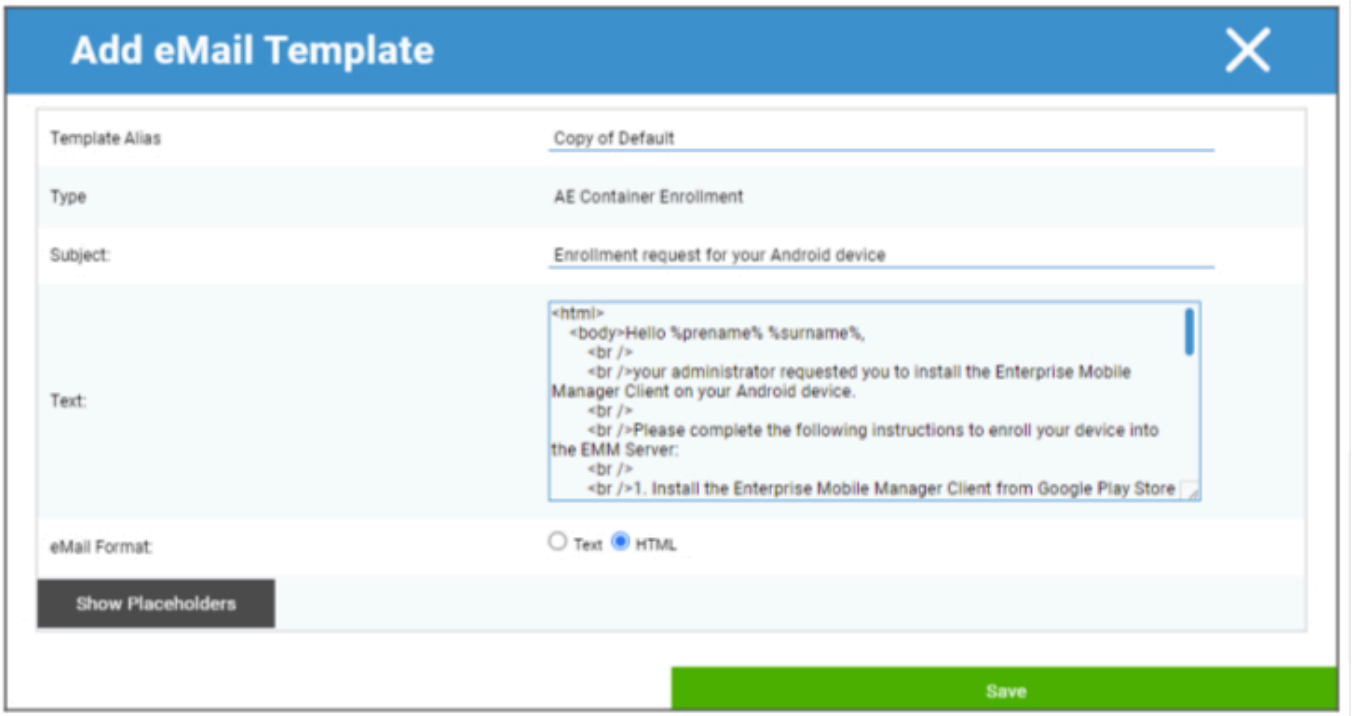
電子メールテンプレート

ここでは、様々なシナリオに対応したテンプレートを作成・編集することができます。テンプレートは通常のテキスト形式でも、HTML形式でも可能です。HTMLでは、テキストの書式をよりよく制御することができます。

デフォルトのテンプレートを編集したり、消去したりすることはできません。



自動的に置換されるプレースホルダを変数として使用することもできます。編集中に「プレースホルダーを表示」をクリックすると、利用可能なプレースホルダーが表示されます。カテゴリーによってプレースホルダーは異なります。



SMS登録

ここで、SMS登録の手続きを行うことができます。

(デフォルト：無効)

SMSクレジットの残数が表示されます。

SMSクレジットは別途購入する必要があります。

プライバシー

GPSアクセス

ここでは、1つまたは2つのパスワード（4つの目の原則）で各デバイスのGPSビューを保護することができます。デバイスの位置情報にアクセスしようとするたびに、パスワードの入力を求められます。

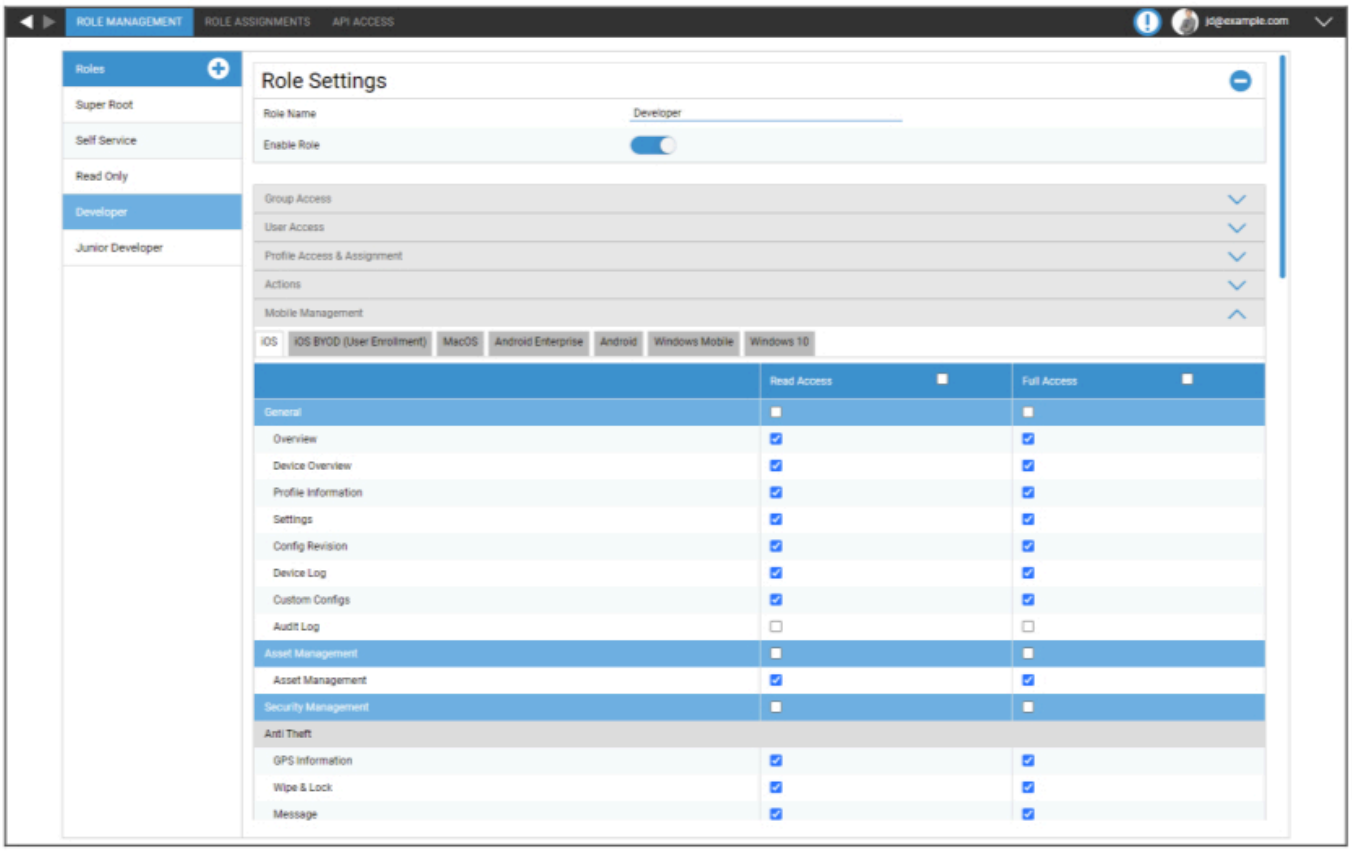
GPS設定へのアクセスを制限する	オフ = 機能がオフになり、ローカライズにパスワードは必要ありません。
	オン = 機能がオンになり、ローカライズにパスワードが必要になる。
保護方法	1つのパスワードを使う = ローカライズに1つのパスワードを使う
	2つのパスワードを使う = ローカライズに2つのパスワードを使う
パスワードを入力 (1)	選択したパスワードを入力
リピートパスワード (1)	選択したパスワードを再入力する
オプションパスワード2を入力	2番目に選んだパスワードを入力
オプションパスワード2を繰り返す	2番目に選んだパスワードを再入力する

注：パスコードを設定した後、パスコードが完全に有効になるまで、もう一度パスコードを入力する必要があります。

役割ベースのアクセス

役割管理

ロールは、ユーザーが管理コンソールにログインしたときに表示され、実行できることを定義します。これにより、ログインはできるが機能が制限されたユーザーを作成することができます。



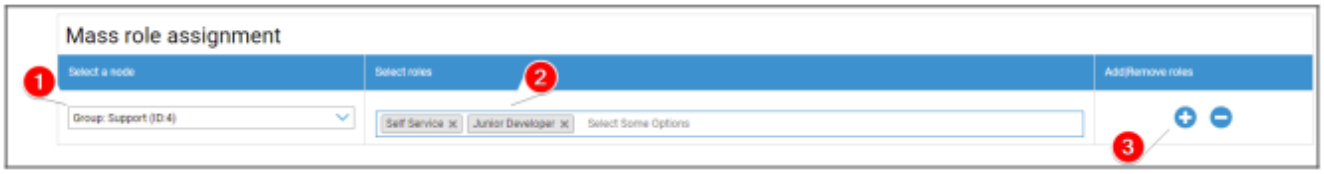
スーパールート役割はデフォルトの役割で、常にすべてを見たり変更したりすることができます。変更や削除はできません。セルフサービスロールは自分のユーザとデバイスしか見ることができません。セルフサービスとカスタムロールを組み合わせることで、例えば、ユーザが自分のユーザに対してのみ、ログインやデバイスの登録を行うことができます。

カスタムロールは手動で有効または無効にできます。新しいロールはデフォルトで無効になっています。無効化されたロールを持つユーザは、そのロールを持っていないかのように動作します。これにより、例えばあるロールのアクションを一時的に制限することができます。

すべてのパーミッションは、"Read Access" と "Full Access" に分かれています。RoleにRead Accessを与えると、コンソールの特定の部分を見ることができます。フルアクセスを与えることで、Roleはコンソールの特定の部分を見たり変更したりすることができます。

役割分担

ここでは、ロールを持つ全ユーザーの概要が表示され、どのロールを持つかを確認することができます。また、ユーザーやグループ全体にロールを割り当てることもできます：

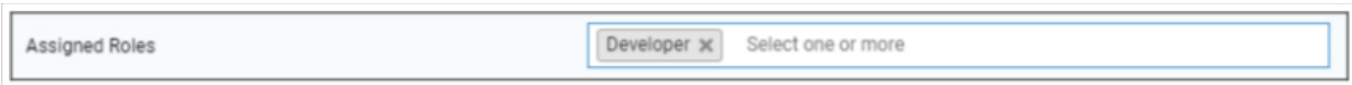


1. ロールを追加または削除するグループまたはユーザを選択します。単一のユーザを選択することも、グループを選択することもできます。グループを選択した場合、変更はそのグループ内のすべてのユーザーと、選択したグループ内のサブグループのすべてのユーザーに影響します。
2. 追加または削除するロールを選択します。1つまたは複数のロールを選択できます。
3. . Select what operation you want to perform. Clicking the “+” adds the selected roles if the user(s) did not have them already. Clicking the “-” removes the selected roles from the user(s). If you add roles to a user which did not yet have any role, it will automatically enable “Can Login” for the user.
4. 保存して処理を終了します。以前はロールがなく、「ログインできる」が無効になっていたユーザーには、パスワードを設定するためのリンクが記載されたメールが自動的に送信されます。

ロールの一括割り当ての下には、割り当てられたロールの概要が表示されます。また、特定のユーザのロールを手動で変更することもできます。

役割の割り当て

ユーザーにロールを割り当てるには、グループ、ユーザー、デバイスのツリーがある「モバイル管理」に移動する必要があります。ユーザーを編集してロールを割り当てます。また、単一のユーザーのみに上記の方法を使用することもできます。



APIアクセス

AppTec360 REST APIにアクセスする

AppTec360 REST APIには認証トークン（APIキー）とプライベートキーが必要で、これらはマネージメントコンソールで生成する必要があります。

これを行うには、AppTec360 EMMにログインし、次の場所に移動します。

General Settings → Role Based Access → API Access と進み、新しいキーを追加する。

APIキーに権限を適用するユーザーを選択する必要があります。

秘密鍵は一度しかダウンロードできません。ダウンロード開始後、鍵は削除され、「ダウンロード」ボタンは消えます。

秘密鍵を紛失した場合は、新しいAPIキーを生成する必要があります。

一般規定

- REST APIはベースURLの下にある：

/public/external/api

- すべてのリクエストはPOSTで送信されなければならない。
- REST APIはHTTPS経由のリクエストのみをサポートしています。
- リクエストには以下のヘッダーが含まれていなければならない：

ヘッダー名	ヘッダー値	説明
コンテンツタイプ	application/json	固定
オーサー	123...xyz	APIアクセス」タブのAPIキー
署名	Base64エンコードされた署名	で生成されたペイロードの署名。 APIアクセス」タブのプライベート・キー

- リクエスト・ボディは、以下の値を含むjsonエンコードされたオブジェクトでなければならない：

フィールド	フィールド例 値	説明
アプリ	v2/device/listdevices	API名
時間	1529662725	クライアントマシンのUnixタイムスタンプ (UTC) 。 最大許容時間差 クライアントとサーバー間は30 分。

- 成功すると、APIは要求されたデータ (下記のクエリーを参照) とHTTPステータスコード200を返す。
- エラーが発生した場合、HTTPステータスコードはエラーに応じて4xxから5xxの間となり、レスポンスオブジェクトは、人間が読めるエラーメッセージのリストを含むキー "errors "を持つ配列を含む。
- デバイスにマッチするデータがない場合は、空の配列が返される。
- デバイスIDが存在しない場合、返されるデータはNULLとなる。

リクエスト例

POST /public/external/api HTTP/1.1
Host: myapptecemm.com
Accept: /
Content-Type: application/jsonauth: 1234567890abcdefghijklmnopqrstuvwxyz
signature: a/bnOV466a0SiyVfsbpspZ+NxiTpmeF18NkfnOIq+OrEZDu9+VW7ESKziPXvw
kTM5B9j/t1WGN1mRcIKe80m8fDKPj+lr3BqoMJe7wGXift+uy6iS7Chpdz2iZA4KPxxU9Z
GU2cdQ/SQceX57pi+ch7ApxBeVX2+lJapTwA6CfB0mJFaf4MPcg/
7LZWkzKxKF7LNzNJHiy/vSpZcqjbXjpC4HWrX6j2uZG5eSP8kYcTR
9VQfGtkX9pcyaNAwguR7zOOwMu/8L0oKq21/19rkabE4ZgUjtKS2+
+q+rh6mrP1g4BCZ7Xq/wvgZkaP
b0CStBdMRvj46i3enxCXcLQQ==
Content-Length: 74
{"api":"v2/device/listposition","time":1529665112,"params":{"ids": [10]}}

クエリ

すべてのデバイスをリストアップ

機能：デバイスID、IMEI、シリアルを含む全デバイスのリストを返す
API URI: v2/device/listdevices
必須パラメータ: なし
任意パラメータ: なし

リクエスト・ボディの例

{
"api": "v2/device/listdevices",
"time": 1529662725
}

レスポンス・ボディの例

{
"errors": [],
"list":[
{ "id":"10","serial":"987612345","imei":"899938455454"},
{ "id":"11","serial":"619723118","imei":"713032378599"}
]
}

(GPS)位置のリストを取得

機能：
API URI: v2/device/listposition
必須パラメータ："ids" - デバイスIDの配列
オプションパラメータ：なし

リクエスト・ボディの例

{
"api": "device/listposition",
"params": {
"ids": [10, 11]
},
"time": 1529662725
}

レスポンス・ボディの例

{
"errors": [],
"list":[
"10":[
{"time":"1529632725","pos":"47.5572,7.5967"},
{"time":"1529642725","pos":"47.5572,7.5968"},
{"time":"1529652725","pos":"47.5573,7.5969"},
],
"88":[],
]
}

アセットマップ取得

機能：
Get any asset dataを使用してリクエストする、保存されている可能性のあるすべてのアセットのリストを返します。
データをリクエストするには、人間が読めるフォームまたはアセットタグのどちらかを使用できます。
API URI: v2/device/getassetmap
必須パラメータ：なし
オプションパラメータ：なし

リクエスト・ボディの例

{
"api": "v2/device/getassetmap",
"time": 1529662725
}

レスポンス・ボディの例

この回答は読みやすくするために短くした。

{
"AssetKeys": {
"UDID": "AT001",
"Device Alias": "AT002",
"OS Version WinMobile iOS MacOS": "AT003",
"Model Name": "AT004",
"Serial Number": "AT005",
"Total Storage": "AT006",
"Free Storage": "AT007",
"IMEI": "AT008",
…
"apptecID": "APPTECID"
},
"errors": []
}

あらゆる資産データを取得する

機能：
API URI: v2/device/getassetdata
必須パラメータ："ids" - デバイスIDの配列
オプションパラメータ：
"assetkeys" - 返すアセットデータキー。指定しない場合は、利用可能なすべての資産データが返される
。資産キーのリストは Get asset map で取得できます。

リクエスト・ボディの例

{
"api": "v2/device/getassetdata",
"time": 1529662725,
"params": {
"ids": [
26
],
"assetkeys": [
"imei"
]
}
}

レスポンス・ボディの例

{
"result": {
"26": {
"imei": "349157642516427”
}
},
"errors": []
}

Python3でのコード例

```
! /usr/bin/python
import base64
from Crypto.Hash import SHA512
from Crypto.Signature import PKCS1_v1_5
from Crypto.PublicKey import RSA
import os
import time
import json
import urllib.request
import urllib.parse
import urllib.error
import http.client
applianceDomain = "YOURAPPLIANCE.COM"
apiURL = "https://"+applianceDomain+"/public/external/api"
privateKeyPath = "/path/to/PrivateKey-XXXXXXXXXXX.pem"
apptecAPIAuthToken = "7eXXXXXXXXXXXXXXXXXXXXXXXXXXX20"
currentTimestamp = int(time.time())
# Get Devices
#requestData = {"api": "v2/device/listdevices", "time": currentTimestamp}
# Get Positions
#requestData = {"api": "v2/device/listposition", "time": currentTimestamp,
"params":{"ids":[26]}}
# Get AssetData
requestData = {"api": "v2/device/getassetdata", "time": currentTimestamp,
"params":{"ids":[26], "assetkeys": ["imei"]}}
# encode the request data to json
print(json.dumps(requestData, indent=1))
jsonEncodedRequestData = json.dumps(requestData)
# Sign the request data json with the API private key
message = jsonEncodedRequestData.encode('utf-8')
print("Body:", message)
digest = SHA512.new()
digest.update(message)
```

```
# Read private key from file
with open(privateKeyPath, "r") as myKeyFile:
private_key = RSA.importKey(myKeyFile.read())
```

```
# Load private key and sign message
signer = PKCS1_v1_5.new(private_key)
signatureOfRequestData = signer.sign(digest)
Base64EncodedSignature = base64.b64encode(
signatureOfRequestData).decode("utf-8")

headers = {"Content-type": "application/json",
"auth": apptecAPIAuthToken, "signature": Base64EncodedSignature}
print("Headers:", headers, "\n")

# Send request to Server
httpsClient = http.client.HTTPSConnection(applianceDomain, 443, timeout=10)
httpsClient.request("POST", apiURL, jsonEncodedRequestData, headers)

# Get answer
response = httpsClient.getresponse()
status = response.status
data = response.read()

if data == False:
print("Invalid answer from the server")
else:
print("Answer:")
print(json.dumps(json.loads(data), indent=1))
if status != 200:
print("http error: lastReceivedHttpCode")
print(status)
```

アップルの設定

APNS認定証

ここでAPNS証明書をアップロードできます。これはiOSとMacOSデバイスを管理するために必要です。

注意：APNS証明書の有効期限は1年間です。有効期限が切れる前に更新する必要があります。更新プロセスは、作成（下記参照）と同じであり、数分しかかかりません。

更新を忘れた場合、登録済みのデバイスの変更はできません。 **すべてのデバイスを再度登録する必要があります。**.

ステップ1

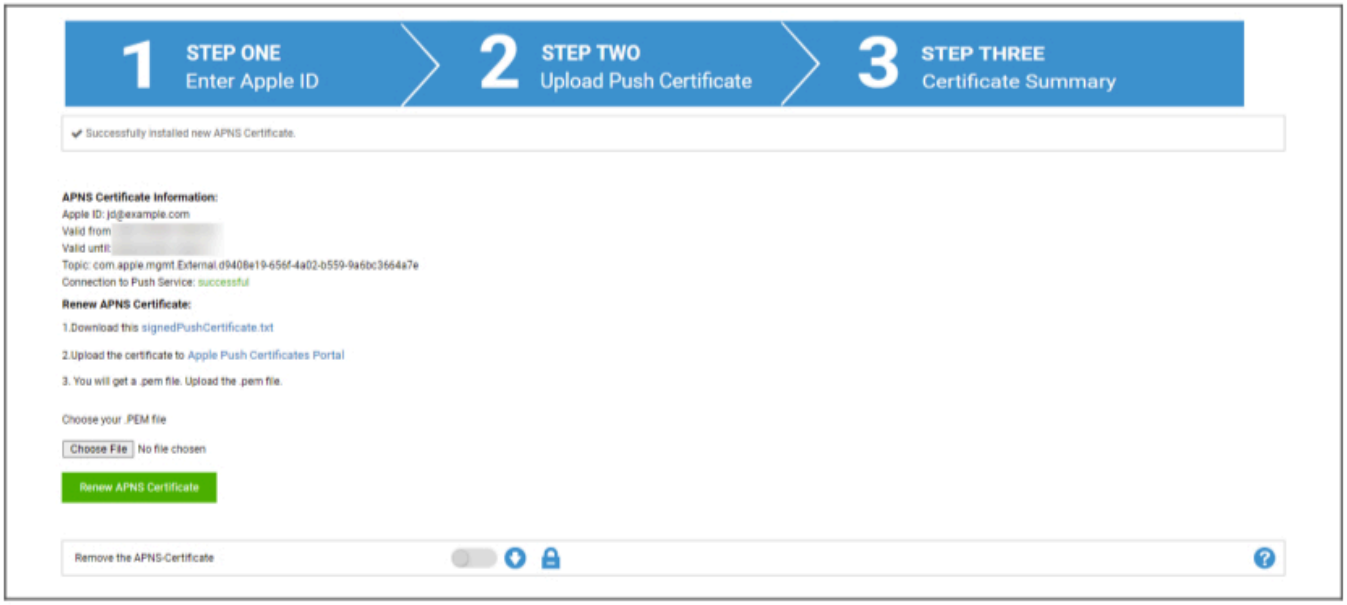
- まず、APNS証明書を作成するために使用するApple IDを入力します。

注意： このApple IDはAPNS証明書の作成にのみ使用されます。このApple IDはデバイスとは無関係であり、デバイスがこのApple IDを知ることはありません。さらに、APNS証明書を更新する際にも、このApple IDにアクセスする必要があります。したがって、汎用的なApple IDを使用し、ログインデータを文書化することを推奨する。APNS証明書の有効期限が切れる前に、Apple IDのメールアドレスにリマインダーが送信されます。

- Next Step "をクリックして次に進む。
- (オプション) 誤ってAPNS証明書を削除してしまった場合は、削除したAPNS証明書を復元することもできます。

ステップ2

- signedPushCertificate.txtのダウンロード
- https://identity.apple.com/pushcert/、ステップ1のApple IDでログインします。
- 証明書の作成」をクリック
- (オプション) ノートを入力します。複数のテナントを管理する場合、テナントを簡単に特定するのに役立ちます。
- Choose File "をクリックして、事前にダウンロードしたsignedPushCertificate.txtを選択する。
- アップロード」をクリックする。
- APNS証明書を作成したことが確認できます。
- ダウンロード」をクリックし、保存する。
- 管理コンソールに戻る。
- Choose File」をクリックし、アップロードしたいAPNS証明書を選択します。
- "アップロード "をクリック



ステップ3

これでAPNS証明書のセットアップが完了し、iOSとMacOSデバイスを管理できるようになりました。

ステップ3では、現在使用しているAPNS証明書の概要が表示されます。

また、画面に表示される手順に従って、APNS証明書を更新するオプションもあります。有効期限が切れる前に更新してください。

APNS証明書を更新する際は、ステップ3で表示されるApple IDでログインすることと、以前に使用した証明書を更新し、新しい証明書を作成しないことに注意してください。ステップ3およびApple Push Certificate Portalの「i」をクリックすると、APNS証明書の「トピック」が表示されます。これは証明書を識別する固有のIDです。これにより、正しい証明書を識別し、正しい証明書を更新することができます。

更新中に「Error：更新中に「Error: The Push Certificate has a different topic!

以前使用していた Apple ID にアクセスできなくなった場合など、新しい証明書をアップロードする場合は、まず現在アップロードされている証明書を削除する必要があります。

いずれにせよ、APNS証明書を削除すると、現在登録されているデバイスは、再度登録するまで変更できなくなる。そのため、この事態に備え、他に方法がない場合にのみ証明書を削除するようにしてください。

マネージド・アクセス

ここでは、iOSデバイスのユーザー登録とiOSデバイスの共有iPadを有効にすることができます。

ユーザー登録

ユーザー登録」は、BYODデバイスのための特別なモードを有効にします。

各ユーザーには、Apple Business Portalで管理されたApple-IDを作成する必要があります。

登録の過程で、ユーザーはApple-IDの認証情報の入力を求められます。

ユーザー登録」は、MDMによって構成される設定と制限の限られたセットのみを許可するため、ユーザーの最大限の安全性を保証する。

管理ドメイン：

ユーザーのメールアドレスを管理するApple-IDにマッピングするために使用するドメイン（'@appleid.company.com'の形式でなければなりません）。例えば、john.doe@example.com は、john.doe@appleid.company.com にマッピングされます。

Apple Business Managerでマネージドドメインをご確認ください。

共有iPad

共有iPadは、特別なDEPプロファイルで設定されたDEPデバイスです。

これにより、管理されているApple-IDを使って複数のユーザーがデバイスにログインできる。

管理するApple-IDは、Apple Business PortalまたはApple School Managerで作成する必要があります。

共有iPadにログインするユーザーは、管理されているApple-ID認証情報の入力を求められる。

管理ドメイン：

ユーザーのメールアドレスを管理するApple-IDにマッピングするために使用するドメイン（'@appleid.company.com'の形式でなければなりません）。例えば、john.doe@example.com は、john.doe@appleid.company.com にマッピングされます。

Apple Business Managerでマネージドドメインをご確認ください。

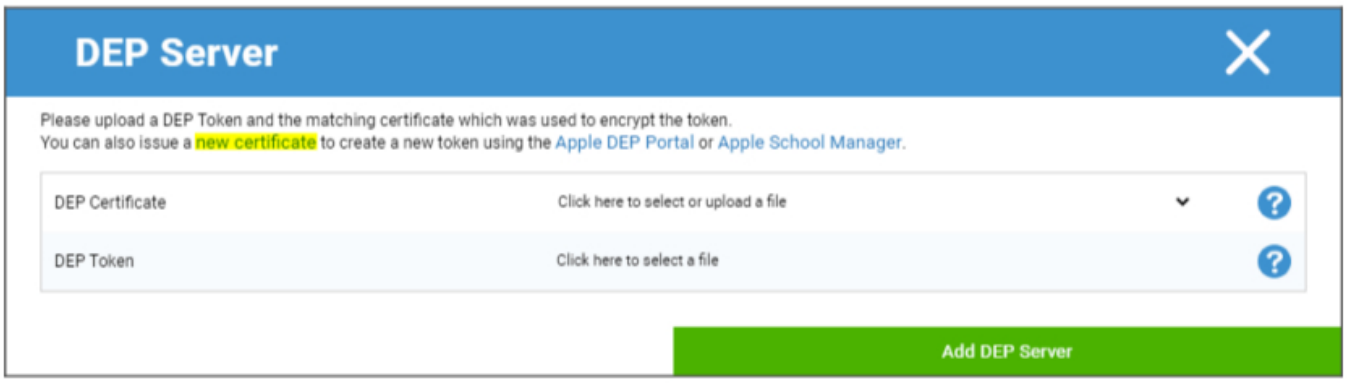
デップ

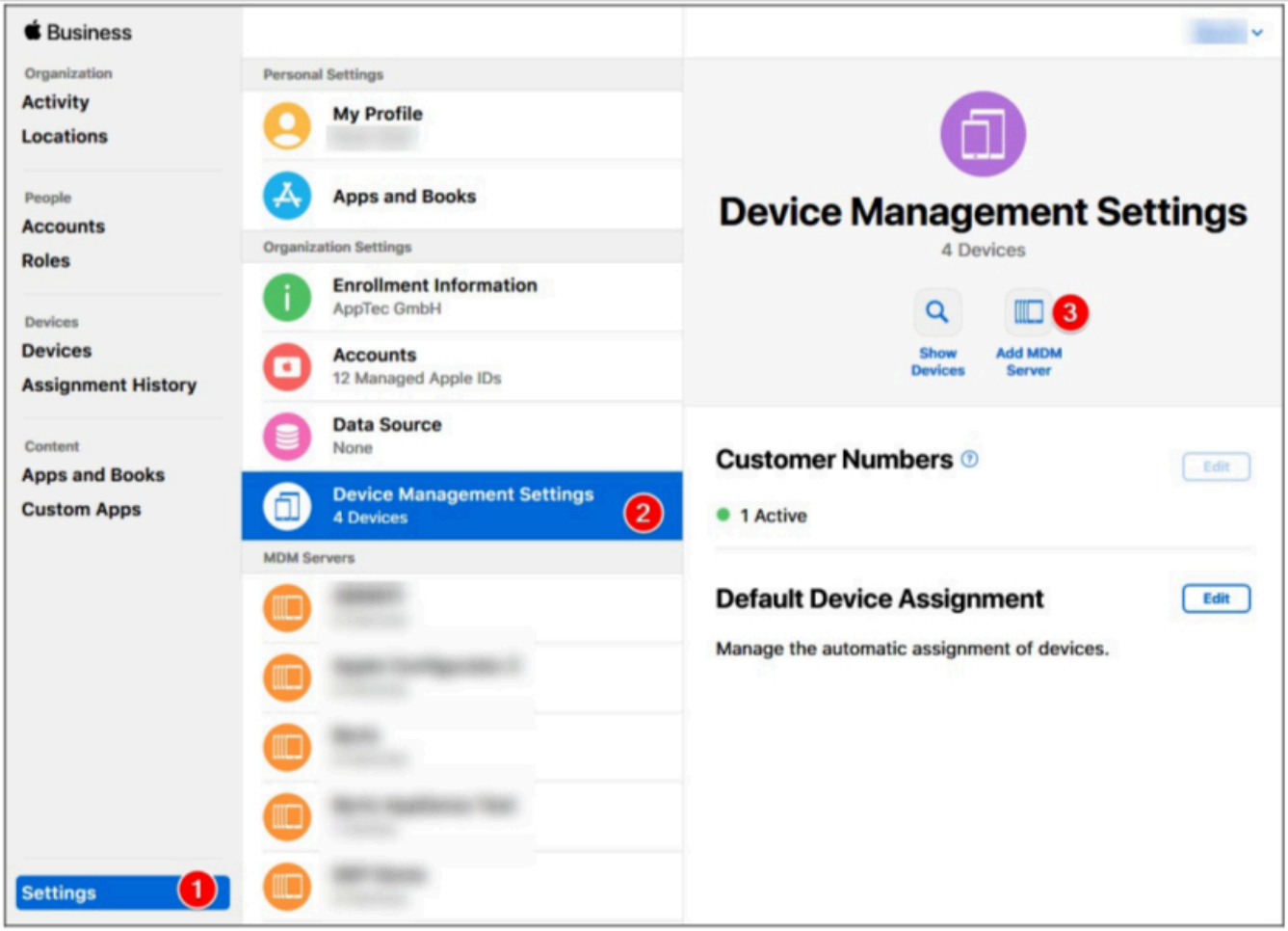
DEP（Device Enrollment Program）を使用すると、デバイスを MDM に簡単に登録できます。DEPを使用すると、デバイスのセットアップ時に自動的にMDMに接続される。また、iOSでは通常必須となるセットアップ手順のほとんどすべてを省略することができる。

DEPをサポートしている販売店からデバイスを購入する必要があることに留意してください。詳しくは、販売店またはAppleにお問い合わせください。

DEPに関する詳細情報: https://www.apple.com/business/dep/

をクリックして DEP トークンを追加する。ポップアップで、テキスト内の「新しい証明書」をクリックします（下の画像では黄色でマークされています）。これでDEP証明書が生成され、ダウンロードされます。その後、Apple Business Manager(https://business.apple.com/)またはApple School Manager(https://school.apple.com/)にアクセスしてください。

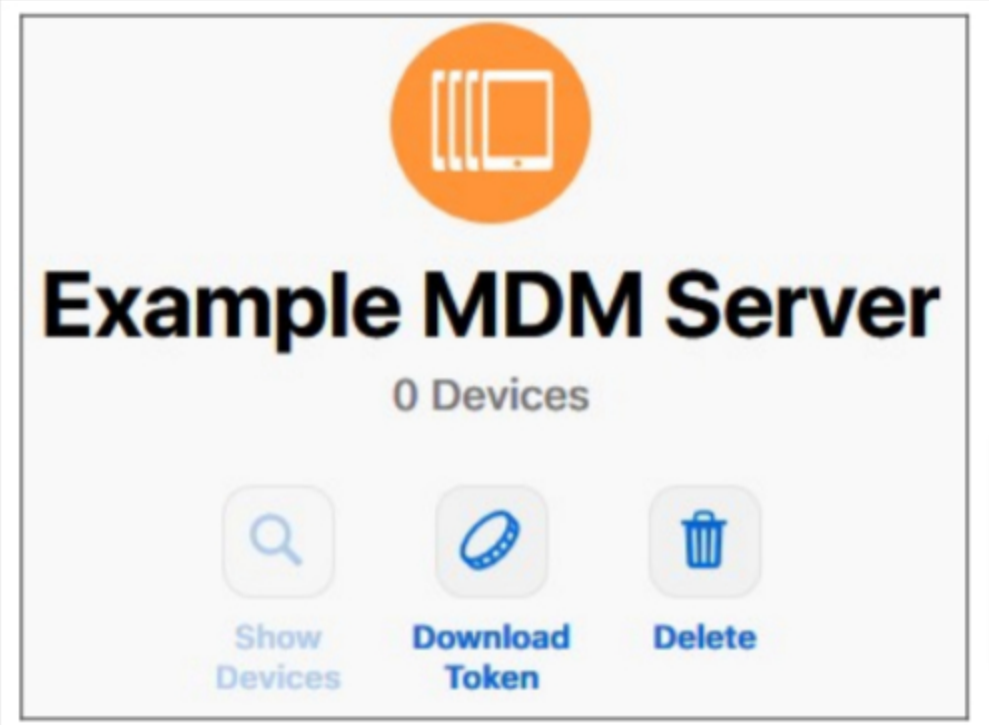




Apple Business Managerで、上の画像に示す手順に従ってください。設定 → デバイス管理設定 → MDMサーバーを追加。

サーバーに任意の名前を付け、MDMサーバー設定→公開鍵のアップロードで先にダウンロードしたDEP証明書をアップロードし、「保存」をクリックします。

トークンをダウンロード」というオプションが表示されます。これをクリックして保存してください。トークンの有効期限は1年間です。トークンの更新はとても簡単です。



DEP 証明書をダウンロードした MDM に戻ることができます。タブを閉じていない場合は、DEP サーバを追加するポップアップが開き、DEP 証明書が選択されているはずです。DEP Token」フィールドにトークンをアップロードし、「DEP Server」をクリックします。

デバイス」の列には、このDEPサーバーに割り当てられているデバイスの数が表示されます。このDEPサーバーに追加されたデバイスは、モバイル管理のDEPプールに自動的に作成されます。

この番号をクリックすると、すべてのDEPデバイスとそのステータスの概要が表示されます。

注: ワークフローまたは Business Manager の設定によっては、これらのデバイスを手動で DEP サーバーに割り当てる必要がある場合があります。Apple Business Managerで、新しいデバイスのデフォルトDEPサーバーを設定することもできます。

Profiles"の列には、あなたが持っているDEP Profilesの量が表示されます。この数字をクリックすると、DEPプロファイルの詳細を見ることができます。現在のところ、これらを変更することはできません。変更したい場合は、新規に作成する必要があります。

最終同期」列では、手動でDEPサーバーを同期し（例えば、DEPに新しいデバイスを追加した場合）、最後に同期に成功した日付を確認できます。

Auto Profile"列では、DEPプロファイルを自動デフォルトとして設定できます。このプロファイルは新しいデバイスに自動的に割り当てられます。自動プロファイルを設定しない場合、新しいデバイス

には毎回手動でプロファイルを割り当てる必要があります。

Add Profile（プロファイルの追加）」欄で、新しいDEPプロファイルを追加できます。デバイスは、デバイスセットアップの最初にこれを受け取ります。DEPプロファイルは、デバイスがどのようにセットアップされ、どのセットアップステップがスキップされるかを定義します。

注意：デバイスを登録した後、これらの設定を変更するには、ファクトリーリセットを実行し、新しいプロファイルでデバイスを登録する必要があります。これは特に「**リムーバブル**」と「**ペアリングを許可**」に関連します。**ペアリングを許可**」の場合、MDMの制限によって無効にすることができるため、これをオンにすることをお勧めします。

Edit"欄では、トークンの更新時などに新しいトークンをアップロードすることができます。

コンフィギュレーターとURL

プール登録URL

ここでは、登録URLと登録QRコードを作成することができます。これにより、1つのリンクまたはQRコードで複数のデバイスを登録することができます。

このURLまたはQRコードで登録されたデバイスは、モバイル管理のプールに登録され、その後、手動でグループまたはユーザーに割り当てる必要があります。

注意：これは手動登録の場合のみです。Apple Configurator経由でデバイスを登録する場合は、このURLを使用しないでください。

MDMプロファイル – Apple Configurator

Apple Configuratorでデバイスを登録する際に必要なURLを取得できます。Apple Configuratorでデバイスを準備している間、同じプロセスでデバイスをMDMに追加できます。Apple Configuratorはこのためにこのを必要とします。

Apple Configurator経由で追加されたデバイスは、モバイル管理内のプールに表示され、その後、手動でグループまたはユーザーに割り当てる必要があります。

また、Apple Configurator経由でデバイスを登録するための.mobileconfigファイルもここにあります。いずれにせよ、URLを使用することをお勧めします。

アンドロイドの設定

アンドロイドの設定

プロテクションのアンインストール	この機能が有効になっている場合、ユーザーは、MDM 管理者によって設定されたパスワードを入力しなければ、デバイス管理者を非アクティブにすることはできません。パスワードは登録時に設定されるため、パスワードを更新するにはデバイスを再登録する必要があります。 デバイス管理者の削除には2つのオプションがあります： 1. デバイス上で手動 ◦ デバイスでEMMアプリを開く ◦ ステータスタブに切り替える ◦ 保護のアンインストール」をタップする ◦ パスワードの入力 コンソールの「パスワード履歴」から正しいパスワードを取得するには、リビジョンを使用します。 ◦ 下にスクロールし、新しく追加されたポイント「Tap to uninstall AppTec360 MDM App」をタップします。 ◦ "Uninstall AppTec360 MDM App "のダイアログを "ok "で確認する。これでコンソールからデバイスの登録が解除されます。 ◦ デバイスからアプリを削除するには、"AppTec360 MDM will be uninstalled "のダイアログを "UNINSTALL "で確認します。 2. オートマチック（コンソール） ◦ コンソールでデバイスを選択 ◦ 青い歯車のアイコンをクリックし、"Enterprise Wipe "を選択します。 注：Android 4.x以下のバージョン、またはKNOX APIを搭載したデバイス（サムスン製デバイス）のみで利用可能です。
パスワードのアンインストール (リビジョン x)	ユーザーがデバイス管理者を削除するためのパスワード。 デバイスが AppTec360 サーバーと通信しておらず、最新のパスワードがまだ送信されていない可能性があるためです。

パスワード履歴	青いボタン ("Show History") をクリックすると、過去に設定したパスワードを見ることができます。
拡張アンインストール保護	このオプションは、非 SAFE デバイスに対する保護を提供します。 この設定が有効になっている限り、デバイス管理者を簡単に解除することはできない。
ブロックされたアプリのアンインストールを促す？	可能であれば、ブロックされたアプリはブロックされるだけでなく、自動的にアンインストールされます。自動アンインストールが不可能な場合は、ブロックされたアプリをアンインストールするよう促されます。
インテリジェント・システム・アプリ・ブロック	ホワイトリストが有効な場合、Android MDM Clientは、ユーザーがインストールしたすべてのアプリをブロックします。ホワイトリスティングモードで起動可能なすべてのシステムアプリをブロックするには、この設定を有効にします。

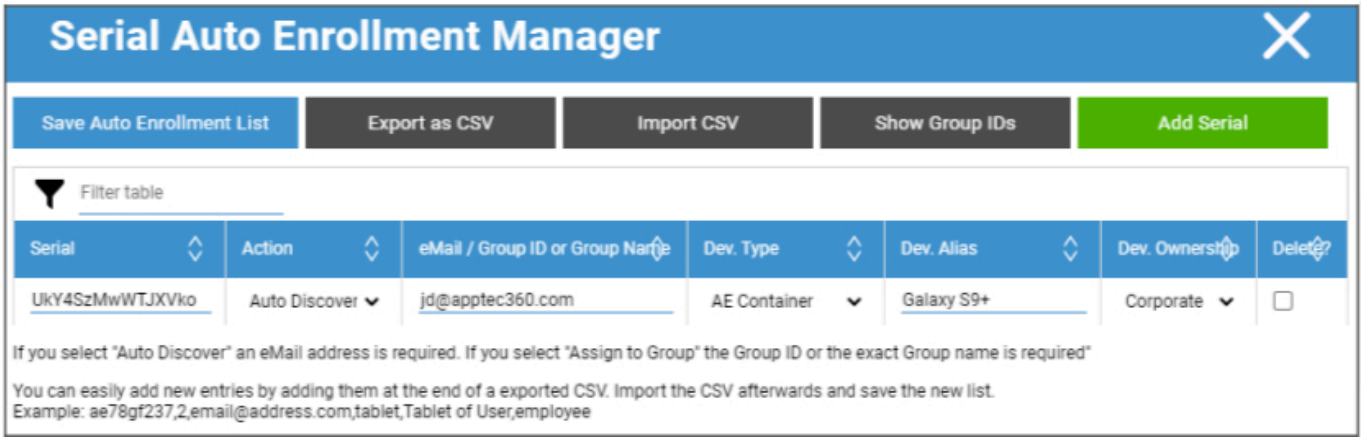
自動登録

ここでは、AppTec360 MDM Clientがデバイス上で開かれたときに自動的にデバイスを登録するために、自動登録機能を有効にすることができます。

重要：この登録方法は非推奨であり、Android 10以降では機能しなくなりました。Android 7以降を使用する場合は、Android Enterpriseフルマネージドとしてデバイスを登録する必要があります。Android Enterprise BYODコンテナを使用し、Android 10以降を使用している場合は、認証情報、QRコード、またはSMSを介してデバイスを手動で登録する必要があります。自動登録リストは、AE 登録、Knox 登録などの登録プロセスを自動化するために使用されます。

いずれにせよ、自動登録リストは、AE登録やノックス登録などの登録プロセスを自動化するために使用される。

Serial Manager "または "IMEI Manager "をクリックすると、デバイスのシリアルまたはIMEIをそれぞれ追加できます。両方行う必要はなく、片方だけで十分です。



Actionは、デバイスをプール、ユーザー、グループのいずれに登録するかを定義する。

また、.csvファイルのエクスポートやインポート、キーワードによるエントリーのフィルタリングも可能です。

アンドロイド・エンタープライズ

ここで Android Enterprise をセットアップします。これは、Android Enterpriseのすべての機能を使用するために必要です。

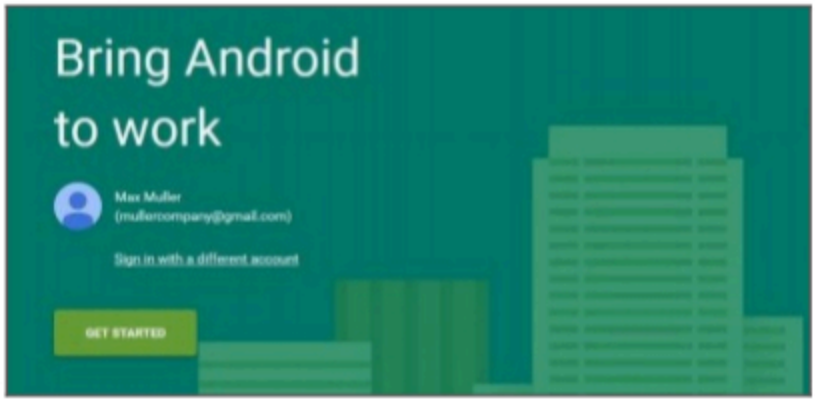
最初の方法Androidエンタープライズアカウント（Googleアカウント）

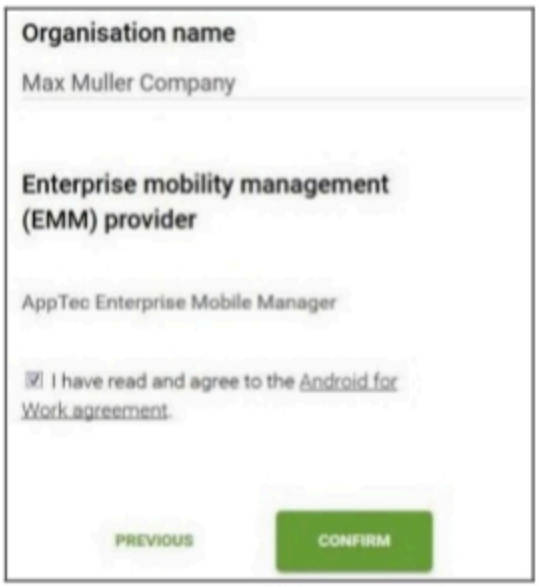
まず "Prepare Setup"（セットアップ準備）を押し、しばらくすると "Start Setup"（セットアップ開始）のボタンがあるはずです。

GoogleのAndroid Enterprise Setupページが表示されます。

まだログインしていない場合は、使用するGoogleアカウントでログインし、「開始」を押します。

会社名を入力します。入力後、チェックボックスにチェックを入れ、"確認 "を押してください。





最後のステップで登録を完了し、コンソールに戻ります。すべてがうまくいけば、このように表示されるはずです：

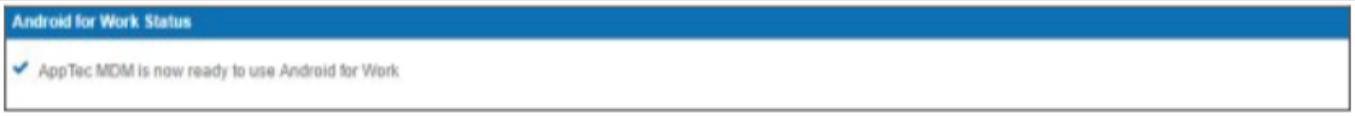
これで Android Enterprise Container の設定を開始できます。

第二の方法G-Suiteアカウント

G-Suiteを使用する」を押し、Google管理者アカウントにログインします。そこで、"Security" -> "Show more" -> "Manage EMM provider for Android" と進み、Token を生成する。注意: G-SuiteアカウントにAndroid Enterprise Settingsが表示されていない場合は、"Get more apps and services "からAndroidデバイス管理を追加する必要があります。コンソールにトークンとプライマリドメインを入力し、"Save Changes "をクリックします。完了したら、"Use Android Enterprise Account "をクリックしてください。

サービスアカウントの作成」ボタンが表示されます。それをクリックしてください。このプロセスには少し時間がかかります。

すべてがうまくいけば、このようになるはずだ：



これで Android Enterprise Container の設定を開始できます。

ファクトリー・リセット・プロテクション

ファクトリー・リセット・プロテクションを使用すると、デバイスをお好みのgoogleアカウントにバインドすることができ、既存のgoogleアカウントへのバインドも上書きされます。ファクトリー・リセット・プロテクションを使用するには、まずここで設定し、その後プロファイルで有効にする必要があります。

ファクトリー・リセット・プロテクションを設定するには、「FRPセットアップ」をクリックし、画面の指示に従ってください。

注意：手順をよく読んで実行してください。間違ったGoogleアカウントに自動的にログインしてしまうのを防ぐため、新しいシークレットブラウザウィンドウで行うことをお勧めします。万が一、間違ったIDを入力したり、使用中のGoogleアカウントにアクセスできなくなったりした場合は、デバイスから完全にロックアウトすることができます！

AE入学

ここで Android Enterprise Ernollment を有効にします。この方法を使用すると、デバイスがAndroid Enterpriseデバイスオーナーモードに登録されます。このモードでは、デバイスを完全に制御できます。

AE登録の有効化	AE Enrollment を有効にします：AE Enrollmentを無効にすると、既存のQRコードや設定済みのNFCプログラマーデバイスは動作しなくなります。AE Enrollmentを再度有効にすると、NFCプッシュ設定を再送信したり、新しいQRコードを生成する必要があります。
自動検出を有効にする	デバイスが「AE登録」によって登録されると、システムはシリアル/IMEIホワイトリスト（「一般設定」>「Android設定」>「自動登録」）で設定された情報に基づいて、そのデバイスをユーザーに割り当てようとします。
不明なデバイスをブロック	シリアル/IMEIホワイトリスト（"一般設定" > "Android Configuration" > "Auto Enrollment"）でホワイトリストに登録されたデバイスのみが登録できます。

方法1と2に関する注意：「ようこそ画面」とは、ファクトリーリセット後に最初に表示される画面のことです。これは、お使いのアンドロイドのバージョンや機種によって異なる場合があります。

方法1：QRコードによる登録

(アンドロイド7.0以上が必要です) アンドロイド7以上をお使いの方は、必ずこの方法を使うことをお勧めします。

1. ファクトリーリセット
2. 以下の2つの方法のいずれかを使用して、エンロールメントのQRコードを生成します：
   - 一般設定 -> Android設定 -> AE登録」の「QRコードの生成」をクリックする。ストレージの暗号化をスキップするか、すべてのシステムアプリを削除するかを選択します。
   - (または) 既存のデバイスを選択します。デバイスの概要」で表示されるQRコードをクリックします。ストレージの暗号化をスキップするか、すべてのシステムアプリを削除するかを選択します。
3. デバイスのようこそ画面を6回タップします。QR登録モードが開始されます。
4. ワイヤレスネットワークに接続し、QRコードリーダーがインストールされるまでしばらくお待ちください。
5. QRコードをスキャンする
6. これで完了です。これであなたのデバイスはAndroid Enterprise Device Modeに登録されました。

- a.一般設定」でQRコードを使用した場合は、「プール -> AEデバイス所有者デバイス」でデバイスを見つけることができます。(ヒント：サイトをリロードしないとデバイスが表示されない可能性があります) 。自動検出を有効にする」にチェックを入れている場合は、自動検出ユーザー内で見つけることができます。
- 既存のデバイスプロファイルのQRコードを使用した場合、デバイスはこのプロファイルに登録されます。

方法2：NFC登録

(NFCとAndroid 6.0以上が必要です)

準備一般設定→Android設定→AE登録→NFCプロビジョニング用データ」にWiFi情報を入力する。次に、「NFC Device」でプログラマーとなるデバイスを検索する。このデバイスは、NFC経由で他のデバイスに登録情報を送信するために使用されます。

1. デバイスを工場出荷時にリセットする
2. プログラマでAppTec360のNFCペアリングアプリを開く
3. ストレージの暗号化をスキップするか、すべてのシステムアプリを削除するかを選択します。
4. 両方のデバイスを背中合わせに持つ
5. アンドロイド・エンタープライズ・エンロールメントは、次のようになるはずです。
6. コンソールにデバイスが表示されます。
    - a.プールで、自動検出を設定していない場合
    - b.ユーザー内で、自動検出のために設定した
    - c.ヒント：デバイスを表示するには、サイトをリロードする必要がある可能性があります。

方法3：Googleアカウント

(アンドロイド5.1以上が必要)

(注意：この方法を使用する場合、デバイスは自動的に登録されません。代わりに手動で登録するか、自動登録を使用してプロセスを自動化する必要があります)。

1. デバイスを工場出荷時にリセットする
2. googleアカウントでログインできるようになるまで、セットアップ手順を実行します。
3. ユーザー名/メールに "afw#apptec "を入力してください。
4. 次へ」をタップ
5. お使いのデバイスがAndroid Enterprise Deviceになりました

ノックス入学

ここでは、KNOX Enrollmentを有効化し、KNOX導入ポータルでKNOX Enrollmentプロファイルを作成するために必要な情報を確認できます。設定と使用には、KNOX導入ポータルのアカウントが必要です。

(https://www.samsungknox.com/en/knox-deployment-program)

KNOX登録の有効化	KNOX Enrollmentを有効にします。 注意KNOX Enrollmentを無効にすると、既存のMDMプロファイルは機能しなくなります。KNOX Enrollmentを再度有効にする場合は、MDMプロファイルの「カスタムJSONデータ」フィールドを更新する必要があります。
自動検出を有効にする	デバイスが「KNOX登録」経由で登録されると、システムはシリアル/IMEIホワイトリスト（「一般設定」>「Android設定」>「自動登録」）で設定された情報に基づいて、そのデバイスをユーザーに割り当てようとします。

1. Samsung KNOX Mobile Enrollment Portalhttps://eukme.samsungknox.com/itadminにログインします。
2. "MDMプロファイル "に進む
3. "追加 "をクリック
4. Server URI not required for my MDM "を選択し、"Next "をクリックする。
5. 次に、管理コンソールに表示されている情報でプロファイルを作成します。

サムスンから直接デバイスを入手した場合、このKNOX登録プロファイルはサムスンから直接デバイスにインストールできます。

または、KNOX Deploymentアプリをダウンロードし、KNOX Deploymentアカウントでログインして、NFC経由でKNOX Enrollment Profileを他のデバイスに送信することもできます。

デバイスにKNOX Enrollment Profileがインストールされている場合、デバイスがインターネットに接続していれば、アプリがダウンロードされ、デバイスが登録されます。

KNOX登録によるデバイスの登録は、「プール -> KNOX登録」、または自動検出で指定したユーザー内で行うことができます。

ゼロタッチ

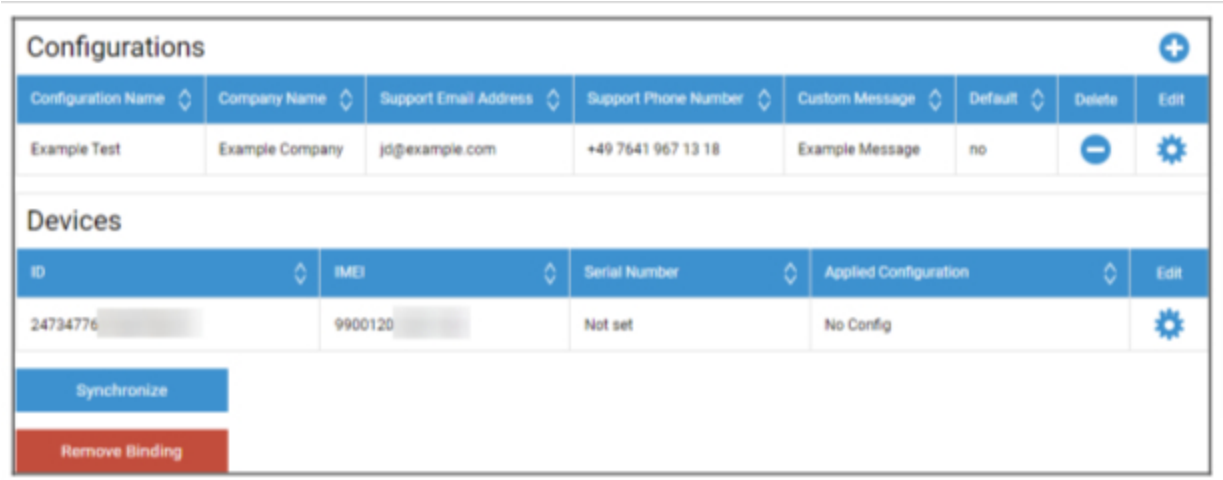
Zero-Touchでは、デバイスに触れたり、デバイス自体で何かを設定したりすることなく、簡単にデバイスを登録することができます。電源を入れ、通常通り設定を進めるだけで、デバイスはMDMのセットアップと接続方法に関するすべての情報を完全に自動的に受け取ります。

ゼロタッチを使用するには、ゼロタッチをサポートするリセラーからデバイスを購入する必要があります。同じリセラーがゼロタッチポータルでお客様のアカウントも作成します。手続きについての詳細や、ゼロタッチ・ポータルへのアクセス時に問題がある場合は、リセラーにお問い合わせください。

セットアップ開始」をクリックしてセットアップを開始します。ログインページにリダイレクトされますので、ゼロタッチポータルにアクセスできるGoogleアカウントを選択してください。

注意：どのアカウントでも選択可能です。そのため、このステップでは正しいアカウントを選択してください。デバイスや設定が表示されない場合は、間違ったアカウントを使用している可能性が高いです。

ログインが完了すると、このように表示されます：



をクリックしてコンフィグレーションを追加し、画面に表示されるフィールドに必要事項を入力します。コンフィグレーションをデフォルトコンフィグレーションとして有効にすると、新しいデバイスに自動的に割り当てられます。デフォルト設定を作成または設定しても、すでに存在するデバイスには割り当てられません。

デバイスにコンフィギュレーションが割り当てられていない場合、通常のデバイスとしてセットアップされ、MDMに接続されません。そのため、デバイスにConfigurationが割り当てられていることを確認してください。

アカウントに接続し、デバイスが表示され、デバイスに設定が割り当てられたら、デバイスの設定を開始できます。

デバイスを自動登録リストに追加すると、指定したグループまたはユーザーに自動的に登録されます。自動登録リストで何も設定しなかった場合、デバイスはプールに登録されます。

Windowsの構成

Windowsの構成

ここでは、Windows 10 PCで以下の設定を有効にするオプションがあります：

インスタントDMコネクション	
初回リトライ時間	デバイスへの最初の接続を確立し、この値は指数関数的に増加する。
接続の再試行	接続エラー時に、DM-クライアントが何回接続を試みるかを示す。
最大睡眠時間	接続エラー後の最大スリープ時間を示す。
最初の同期再試行	最初の接続の後、デバイスがサーバーと通信する間隔。
最初の再試行間隔	最初の同期再試行」に関する記事情報 ここでは分単位で時間が表示されている 例えば、"First Sync Retries "の下に "2 "という値があり、"First Retry Interval "の下に "4 Minutes "という値があります。
2回目の同期リトライ	最初の同期再試行 "が完了した後、デバイスがサーバーと通信する間隔。
秒リトライ間隔	1回目の再試行間隔」と同じ原理で、ここでは「2回目の同期再試行」に適用される。
通常の同期再試行	今後、デバイスがサーバーと通信する頻度の間隔。 デフォルト：「無限 10 "を入力した場合、デバイスはサーバーと10倍通信し、その後停止するため、AppTec360サーバーとの通信は切断されます！
通常の再試行間隔	1回目/2回目の再試行間隔」と同じ原理で、ここでは将来の設定を適用するだけです。
通常の再試行間隔	1回目/2回目の再試行間隔」と同じ原理で、ここでは将来の設定を適用するだけです。

コンテンツボックス

構成

ここで ContentBox を設定できます。デバイス上の ContentBox App でアクセスできる ContentBox にグループ用のファイルを配置できます。

コンテンツボックスを有効にする	ContentBoxを有効にします。ContentBoxを使用しない場合は、これを無効にすると、オンプレミスのマシンのリソースを節約できます。
外部ContentBoxインストールを使用する	ContentBoxは独自のNextcloudで操作することもできます。
URL	Nextcloudエンティティの完全なURL
ルートユーザー	Nextcloudアカウントのルートユーザー
ルートパスワード	Nextcloudアカウントのルートパスワード
デフォルトのグループフォルダ権限	デフォルトのグループフォルダ権限、グループごとに個別に変更可能（モバイル管理にて）
グループフォルダをサブグループで共有	アクティブな場合、各サブグループはメイングループのすべてのフォルダを読むことができます。
サブグループの権限	サブグループの権限 グループごとに個別に設定可能（モバイル管理）
共有を許可する	各グループごとに個別に設定可能。
最大ファイルアップロードサイズ（MB	ファイルの最大サイズ 標準：512MB 最大構成：2048
WebDAV認証情報	
WebDAV URL	WebDAVでContentBoxを開くこともできます。 以下のフォルダは、いかなる場合でも削除しないでください：/apptecgroups /apptecgroups/AppTecGroup-X
ルートユーザー	ルートユーザー名
パスワード	ルートユーザーのパスワード

ContentBoxとの同期は自動的に行われます。ただし、"ContentBoxを同期 "で手動同期を実行することもできます。

さらに、ここで各デバイスのContentBoxを有効/無効にすることができます。

これは、ContentBoxのライセンスを追加取得していない場合にのみ関係するもので、ContentBoxをテストできる25台のデバイスにアクセスできます。

LDAPの設定

LDAPの概要

ここでは、LDAP経由でActive Directoryへの接続を確立し、ユーザーとグループを大量にインポートすることができます。同期は手動で行う必要があります。複数のLDAP接続を異なるシステムや異なる設定/フィルタで構成することができます。

サーバー名	サーバーの表示名
タイプ	現在、LDAPをサポートするActive Directoryのみがサポートされています。
LDAPドメイン	プライマリLDAPドメイン（example.comなど）
LDAPホスト	LDAPホストが指定されたLDAPドメインに到達できない場合にのみ必要です。
ポート	標準ポート（SSLでは389または636）を使用する場合は空のままにします。
ユーザー名	例：CN=John,OU=Users,DC=EXAMPLE,DC=COM 注：ほとんどのシステムはこの形式のユーザー名を必要とし、"John "をユーザー名として受け付けません。
パスワード	
パスワードの確認	
コネクション・セキュリティー	注：SSLまたはTLSを使用する場合、Active Directoryの証明書がチェックされます。これが自己署名の場合、ルートCAをオンプレミスマシンのトラストストレージに追加する必要があります。クラウド上の場合、Active Directoryは信頼できる証明書を提供する必要があります。
自動シンク。	LDAP一般設定で指定された時間間隔で、LDAPディレクトリの自動同期を有効にします。
ベースDN	例えば、OU=AndroidUsers,OU=Users,DC=EXAMPLE,DC=COM。
メンバー	インポートされたすべてのユーザーは、選択したグループに追加されます。
アクティベートされたユーザーだけか？	有効にすると、userAccountControl属性が考慮され、その属性を持たないユーザーはインポートされません。
LDAPフィルター	LDAP フィルタを使用して、インポートするユーザをフィルタリングできます。

正規表現フィルター	正規表現フィルタを使用して、インポートするユーザーをフィルタリングできます。
テスト接続	設定の保存時に接続をテストする
同期時にディレクトリ構造をリセットしますか？	trueの場合、すべてのLDAPエントリはLDAPツリー内の元の位置に戻される。有効にすることを推奨します。
削除したユーザーとグループを再インポートしますか？	有効にすると、削除されたユーザーとグループが再作成されます。有効にすることをお勧めします。
同期削除？	有効にすると、LDAPサーバー上でグループとユーザーが削除されると、そのグループとユーザーも削除されます。また、削除されたユーザーのデバイスも削除されます。

LDAP 設定のリストの下に、システムが自動的に同期する期間を定義できます。自動同期には、該当するオプションが有効になっている LDAP 設定のみを使用します。

アプリ管理

社内アプリDB

アンドロイド

ここでは、貴社が開発したAndroidアプリをアップロードし、後でモバイル管理でデバイスまたはグループプロファイルに配布することができます。

GooglePlayストアで入手できないアプリのみ、この方法で配布することをお勧めします。

をクリックして、アップロードしたいアプリのAPKをアップロードしてください。現在はAPK形式のみ対応しています。

オンプレミスアプライアンスのアップロード制限は、アプライアンス設定のステップ3で増やすことができます。クラウドのアップロード制限を増やしたい場合は、サポートにお問い合わせください。

通常、APKはそのコンテンツよりも少し小さいことに注意してください。アップロードの過程でAPKが解凍されるため、これが原因でアップロードに失敗する可能性があります。例えば、100MBのアップロード制限で95MBのAPKが失敗する可能性があります。この場合、上記のようにアップロード制限を増やしてください。

また、まず手動でAPKを1つのテストデバイスに移動し（USB経由など）、デバイスのFilesアプリを使って手動でインストールしてみることをお勧めします。これが何らかの理由でうまくいかない場合、MDM経由でも失敗します。

更新目標

アップデート対象」機能では、インストールするアプリのバージョンを選択したり、アプリの「最新状態を保つ」を有効にしているアプリをどのバージョンにアップデートするかを選択することができます。

アップデート対象を選択していない場合は、最も高いバージョンが使用されます。

Androidではアプリのダウングレードはできないことを覚えておいてください。また、バージョンが高いか低いか、あるいは同じかどうかは、「バージョンコード」によって決まります。そのため、アップデートをビルドする際には、アプリ内でこのバージョンを正しく増やすようにしてください。

iOS

ここで開発したiOSアプリをアップロードし、後でデバイスまたはグループプロファイルのモバイル管理で配布することができます。

をクリックして、アップロードしたいアプリのIPAをアップロードしてください。現在のところIPA形式のみ対応しています。

オンプレミスアプライアンスのアップロード制限は、アプライアンス設定のステップ3で増やすことができます。クラウドのアップロード制限を増やしたい場合は、サポートにお問い合わせください。

更新目標

アップデート対象」機能では、インストールするアプリのバージョンを選択したり、アプリの「最新の状態に保つ」を有効にしているアプリをどのバージョンにアップデートするかを選択することができます。

更新対象を選択していない場合は、最も高いバージョンが使用されます。

マックオス

ここでは、開発したMacOSアプリをアップロードし、後でデバイスまたはグループプロファイルのモバイル管理で配布することができます。

をクリックして、アップロードしたいアプリのPKGをアップロードしてください。現在はPKG形式のみ対応しています。

オンプレミスアプライアンスのアップロード制限は、アプライアンス設定のステップ3で増やすことができます。クラウドのアップロード制限を増やしたい場合は、サポートにお問い合わせください。

更新目標

アップデート対象」機能では、インストールするアプリのバージョンを選択したり、アプリの「最新状態に保つ」を有効にしているアプリをどのバージョンにアップデートするかを選択することができます。

アップデート対象を選択していない場合は、最も高いバージョンが使用されます。

ウィンドウズ10

ここでWindows 10アプリをアップロードし、後でデバイスまたはグループプロファイルのモバイル管理で配布することができます。

をクリックして、アップロードしたいアプリのAPPX、APPXBUNDLE、またはMSIをアップロードします。現在のところ、APPX、APPXBUNDLE、またはMSI形式のみがサポートされています。

また、アプリの依存関係をアップロードして定義することもできます。

オンプレミスアプライアンスのアップロード制限は、アプライアンス設定のステップ3で増やすことができます。クラウドのアップロード制限を増やしたい場合は、サポートにお問い合わせください。

更新目標

アップデート対象」機能では、インストールするアプリのバージョンを選択したり、アプリの「最新状態に保つ」を有効にしているアプリをどのバージョンにアップデートするかを選択することができます。

更新対象を選択していない場合は、最も高いバージョンが使用されます。

Win32パッケージ (.exe)

.exeファイル/インストーラーをデバイスに配布することもできます。

パッケージ名	MDMに表示される名前
説明	MDMに表示される説明
パッケージファイル	.zipファイルのみ使用可能です。配備したいファイルをこのzipファイルに入れてください。
展開コンテキスト	**システム**：システム: インストールコマンドは、「ユーザー」よりも高いシステム特権で実行されま す。また、"System" を使用している場合、プロセスは UI を持たないため、無音となり、 ユーザプロファイル (%AppDat% などの環境変数) にアクセスできません。**User**: インストールコマンドはユーザプロファイルにアクセスでき、必 要なら UI を表示できます。注意: プロセスによっては、1 つのコンテキストでのみ動作する場合がありま す。例: AppData にインストールするソフトウェアは、"User" を選択したときのみ動作します。
インストールコマンド	プログラムのインストールに使用するコマンド。例えば、ルートに "setup.exe "を含むzipファイルのインストールコマンドは "setup.exe /s "となります。ソフトウェアによってパラメータが異なる場合があるので注意してください。
アンインストールコマンド	MDM経由でソフトウェアをアンインストールするために実行するコマンド。通常はアンインストーラを指す。例えば "C:◆Program Files◆ExampleSoftware◆uninstall.exe"。
必要条件	
注意：ソフトウェアをインストールするには、設定されたすべての要件を満たす必要があります。そうでない場合はインストールされません。一部のフ ィ ール ド は必須です。要件に値が設定されていない場合、その要件は無視されます。	
OSアーキテクチャ	OSアーキテクチャ
最小OSバージョン	最小OSバージョン
最小ディスク空き容量 (MB)	最小ディスク空き容量 (MB)
最小物理メモリ (MB)	最小物理メモリ (MB)

最小論理プロセッサ数	最小論理プロセッサ数
最小CPU速度（MHz）	最小CPU速度（MHz）
追加要件	また、手動でルールを定義したり、スクリプトをここにアップロードして、追加の要件チェックを実行することもできます。
検出ルール	
検出方法	ここでは、アプリがデバイスにインストールされているかどうかを検出する方法を定義できます。インストールコマンドは、これらのルールがアプリがインストールされていないことを検出した場合にのみ実行されます。アンインストールコマンドは、これらのルールがアプリがインストールされていないことを検出した場合にのみ実行されます。**手動でルールを定義**します：例えば、特定のファイル、フォルダ、MSI、またはレジストリキーが存在するかどうかをチェックするために、1つまたは複数のルールを手動で定義できます。指定された検出ルールがすべて真である場合、アプリは存在すると見なされます。**スクリプトを使用します**：独自のチェックで独自のスクリプトをアップロードします。スクリプトが"$TRUE "を返した場合、アプリは存在するとみなされます。
検出ルール	

アプリの設定

iOSアプリの設定

ここでは、必須アプリまたはエンタープライズアプリストアにアプリを追加するためのデフォルト設定を定義できます。

注:これは、アプリの追加時にデフォルトで選択されているもののみを設定します。これは、必須アプリまたはエンタープライズアプリストアに既に追加されているアプリの既存の設定を変更するものではありません。

最新情報	自動的にアプリを最新の状態に保ちます。アップデートがリリースされてからアプリが更新されるまで、最大7日間かかることがありますので、ご了承ください。
管理されていないときに追い越す	アプリがすでに（ユーザーによって）非管理対象としてインストールされている場合、そのアプリはMDMによって引き継がれ、管理される。
MDMプロファイルの削除時にアプリを削除する	MDMの削除時にアプリをアンインストールします。
アプリデータのバックアップを防止	アプリデータのバックアップを防ぎます。

Androidアプリの設定

ここでは、必須アプリまたはエンタープライズアプリストアにアプリを追加するためのデフォルト設定を定義できます。

注：これは、追加時にデフォルトで選択されているもののみを設定します。必須アプリまたはエンタープライズアプリストアにすでに追加されているアプリの設定は変更されません。

最新情報	自動的にアプリを最新の状態に保ちます。InHouse Appsでのみ利用可能です。
制御されたAppTec360 EMMクライアントのアップデート	有効にすると、管理者はAppTec360 EMM Clientのアップデートターゲットを指定できる。AppTec360 EMM Clientのすべての利用可能なバージョンのリストは、"General Settings" → "App Management" → "In-House App DB" → "Android "に表示されます。

サードパーティアプリ

アンドロイド

ここでIkarusのアクティベーションコードを設定できます。

アクティベーションコードを使用する」に設定し、アクティベーションコードを入力してください。

注意：コードを入力して保存した後、コードはまだデバイスに送信されるプロファイルに追加されていません。コードをプロファイルに追加するには、プロファイルに変更を加える必要があります。
例：プロファイルのスイッチをオフ→オン→オフ→保存→今すぐ割り当てる。

iOS

ここで、SecurePIM ライセンスを入力できます。ライセンスの入力後、「変更を保存」を押すと、SecurePIM のオプションを使用できるようになります。

VPP / KNOX プレミアム

Apples Volume Purchase Program (VPP)を使えば、有料・無料のAppを簡単にデバイスに配布することができます。デバイスにApple IDが必要なく、ユーザーはインストールを確認する必要がなく（監視付き）、ユーザーはApple IDのパスワードを入力する必要がありません。

VPPを利用するには、Apple Business Managerに登録する必要があります。

VPPライセンス

ここでは、VPPアプリケーションの概要、使用されているライセンス数、および使用可能なライセンス数を確認できます。

ホイールをクリックすると、どのデバイスにライセンスが割り当てられているか、またその割り当てのステータスが表示されます。

をクリックすると、VPPキャッシュが更新され、MDMで割り当てられたライセンスとApple側で割り当てられたライセンスが比較されます。これにより、ライセンスの問題が解決される場合があります。

VPPトークン

ここでVPP Tokenをアップロードできます。VPP TokenはApple Business Managerの「設定」→「Apps & Books」で確認できます。複数のVPPトークンをアップロードすることができます。

Apple Business Managerで新しいTokenをダウンロードし、「編集」ホイールをクリックして新しいTokenをアップロードするだけで、Tokenを更新することができます。

VPPモード "は、ライセンス割り当ての処理方法を決定します。シナリオに応じて、異なるモードを使用する必要があります：

「デバイスベース」は、QRコード、リンク、Apple Configurator、またはDEP経由でデバイスを登録する場合に使用する必要があります。

デバイスがユーザー登録または共有iPadとして登録されている場合は、「ユーザーベース」が必要です。

自動ライセンス管理」を有効にすると、あるグループから別のグループに移動したユーザーには、移動先のグループプロファイルに基づいてApple VPPライセンスが自動的に割り当てられます。

移籍元グループの既存のApple VPPライセンスは失効しません。

グループに追加された新規ユーザーには、それぞれのグループプロファイルに基づいて自動的にApple VPPライセンスが割り当てられます。

KNOXプレミアムキー

ここで、サムスンKNOXコンテナを使用するためのKNOXプレミアムキーを入力できます。

これはAndroid 10以降サポートされなくなりましたのでご注意ください。代わりにAndroid Enterprise Containerをご利用ください。

App Storeの設定

地域と言語

ここでは、App ManagementのApp Searchのデフォルトの Language（言語）とRegion（地域）を設定できます。

iTunesの設定は、システムが特定のアプリに関する情報を取得する方法も定義していることにご注意ください。リストに表示されるAppが変な場合（アイコンがないなど）、特定のAppが利用できない地域を設定している可能性があります。

AE Playストア

ここでは、アプリの承認、Playストアへのアプリのアップロード、または独自のWebアプリを作成するためのAndroidエンタープライズデバイス用のPlayストアのすべてのオプションを見つけることができます。

承認されたアプリ

ここでは、承認したすべてのアプリの概要を見ることができます。

Playストアアプリ

Playストアを表示するiFrameがロードされます。好きなアプリを検索し、クリックして承認します。アプリを承認している間、必要なパーミッションが変更された場合、承認が取り消されるように定義することもできます。アプリを承認する際は、これらの設定をデフォルトのままにしておくことをお勧めします。

アプリが承認されると、自分のプロフィールに追加できます。

承認」ボタンは承認後に「承認を取り消す」に変わるので、不要になったアプリはいつでも削除できます。

プライベートアプリ

ここでは、Google Playストアに自分のアプリをプライベートアプリとしてアップロードすることができます。これにより、Googleのサービスを通じてアプリを配布し、アップデートすることができま

す。また、通常必要なユーザー確認なしに、自分のアプリをインストールできるというメリットもあります。

ウェブアプリ

ここでは、アプリのように割り当てることができる特定のWebページへのリンクであるWebアプリを作成することができます。

また、このアイコンにカスタムアイコンを設定し、表示方法を定義することもできます。

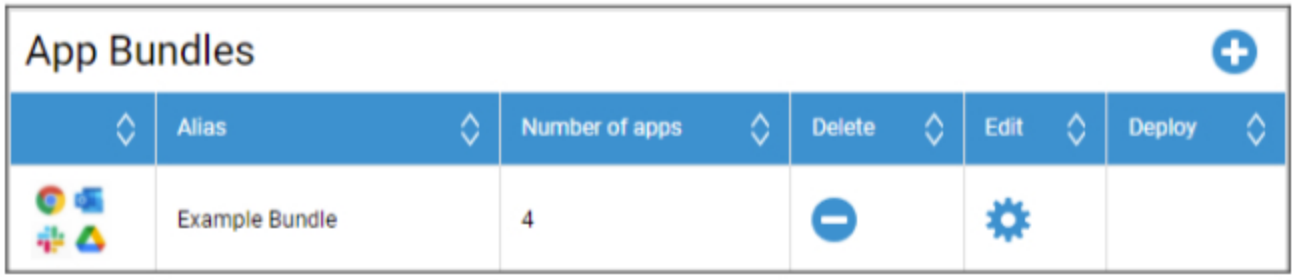
店舗レイアウト

ストアレイアウトは、PlayストアでのAppの表示方法、または表示されるかどうかを定義します。

ユーザーが手動でインストールできるようにPlayストアのアプリを表示したい場合は、レイアウトのここに追加する必要があります。 とに追加する必要があります。どちらか一方だけにアプリを追加した場合、そのアプリは表示されません。

アプリバンドル

App Bundlesを使用すると、ワンクリックでデバイスまたはグループプロファイルに割り当てることができるアプリのグループを定義できます。



をクリックして新しいApp Bundleを作成します。App Bundleを作成したら、「Edit（編集）」をクリックして、様々なソースからのアプリをBundleに追加することができます。

バンドルは他のアプリと同じようにプロファイルに追加できます。アプリを追加する際、"App Bundles "というタブが追加されます。

App Bundleに変更を加えると、"Deploy "列のボタンが表示されます。これにより、このBundleを含むすべてのプロファイルに変更をプッシュできます。そのため、バンドル内のアプリを追加または削除した後は、手動でこの操作を行う必要があることを覚えておいてください。

リモコン

チームビューアー

TeamViewer コネクタ

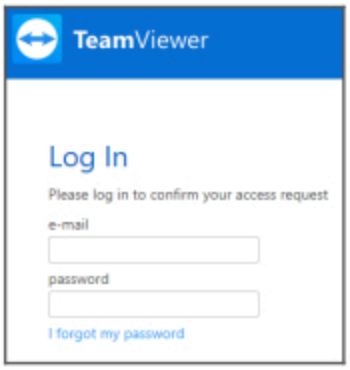
注: クラウド版の無料トライアルでは、TeamViewerアカウントを接続することはできません。代わりに、無料のデモアカウントが自動的にリンクされます。

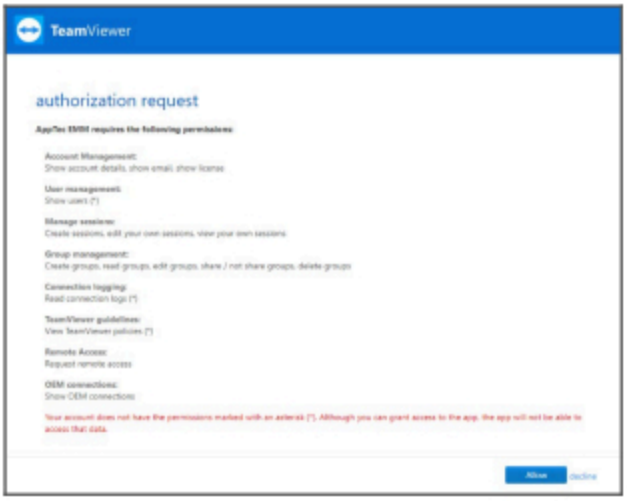
一般設定]->[リモートコントロール]->[TeamViewer]に進みます。ここで、TeamViewerアカウントとコンソールをリンクしたり、現在接続しているアカウントの情報を確認したりできます。また、[アクティブセッション]に移動すると、現在アクティブなすべてのセッションを表示できます。

アカウントをリンクするには、「セットアップ開始」をクリックしてください。

TeamViewerアカウントでログインする必要があります。

ログイン後、AppTec360 MDM がこのアカウントを使用することを承認する必要がある。確認後、数秒待つとアカウントが接続される。


TeamViewer
Log In
Please log in to confirm your access request
e-mail
password
I forgot my password


TeamViewer
authorization request

TeamViewer QuickSupportのインストール

アプリ "TeamViewer QuickSupport "をデバイスプロファイルまたはグループプロファ イルの必須アプリに追加し、[Assign Now]をクリックします。アプリがデバイスにインストールされるまで待ちます。

アプリがインストールされていないデバイスにアクセスしようとすると、デバイスの設定に応じて、アプリがインストールされるか、インストールするように求められます。

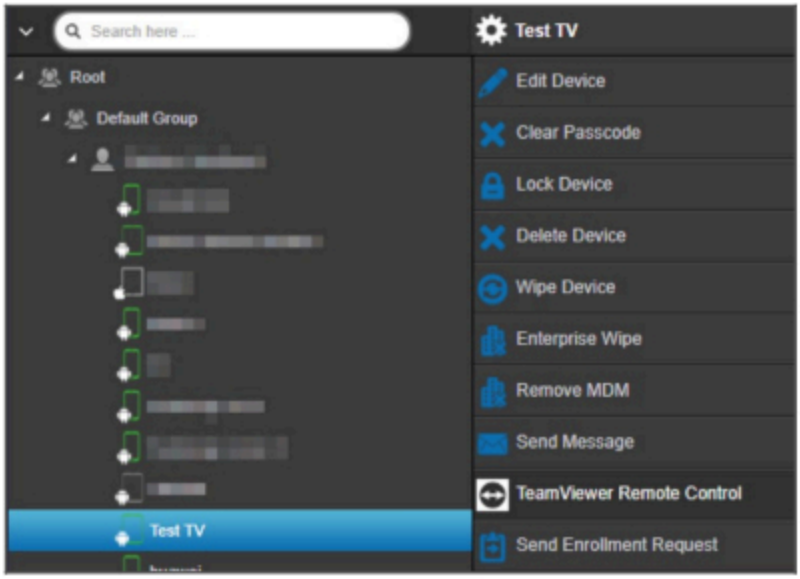
リモートコントロール

デバイスをリモートコントロールするには、デバイスを選択してホイールをクリックし、"TeamViewer Remote Control "を選択します。

すでにアクティブなセッションがある場合は、古いセッションを使用するか、新しいセッションを作成することができます。

新しいTeamViewerセッションを作成することを確認します。

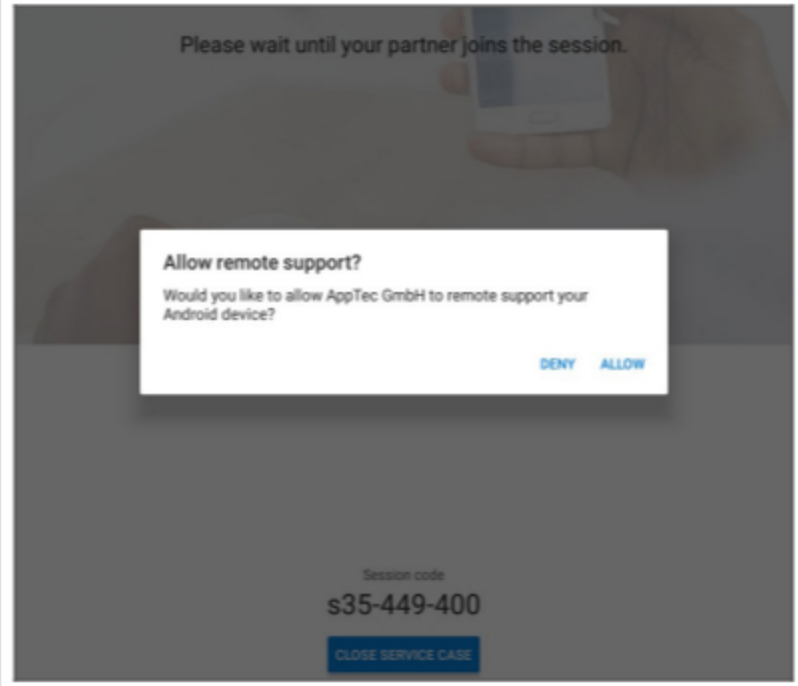
数秒後、TeamViewer セッションのリンクが表示されます。開始]をクリックして、このリンクを新しいウィンドウで開くことができます。


Search here ...
Root
Default Group
Test TV
Test TV
Edit Device
Clear Passcode
Lock Device
Delete Device
Wipe Device
Enterprise Wipe
Remove MDM
Send Message
TeamViewer Remote Control
Send Enrollment Request


Remote Control
Supporter URL: https://get.teamviewer.com/v13/
Click on "Start" to open the TeamViewer Remote Control in a new window.
Cancel
Start

このリンクをクリックすると、インストール済みのTeamViewerが開き、デバイスに接続されます。

リモートコントロールを行うには、デバイス自体で接続を確認する必要がある。

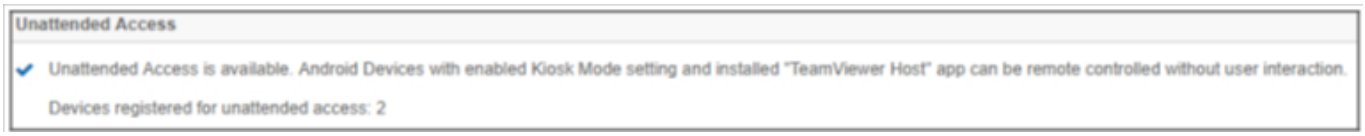


iOSを使用している場合、AppTec360 MDM Clientにメッセージが表示されます。そのリンクにより、デバイスはリモートセッションに参加します。デバイスの通知設定によっては、通知を受け取らず、AppTec360 MDM Clientを手動で開く必要があります。

一部のAndroidデバイス(Samsungなど)では、アドオンとして追加のアプリをインストールする必要があります。ご使用のデバイスでこれが必要な場合は、デバイス上のTeamViewerアプリがそのことを通知します。

無人アクセス

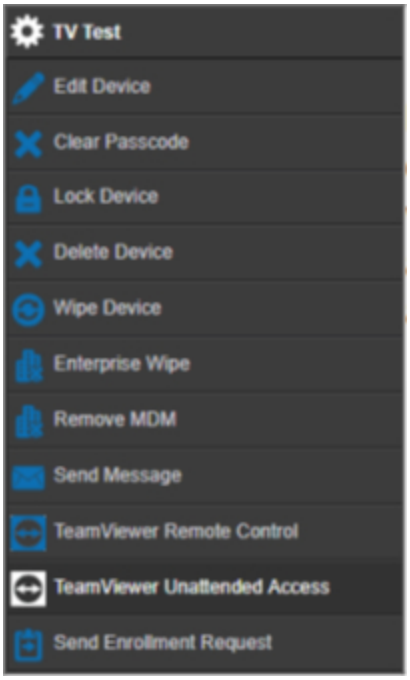
注：無人アクセスはアンドロイド端末でのみ可能です。



TeamViewerアカウントが「Tensor」または「Corporate」ライセンスを使用している 場合のみ、デバイス上で接続を受け入れずに、デバイスに接続できます。

アカウントをリンクした後、"一般設定 "で確認できます。

無人アクセスを使用するには、アプリ "TeamViewer Host "をインストールし、プロフィールの[Kiosk Mode & Launcher]で[無人アクセスを有効にする]を有効にする必要があります。これは、キオスクモードを使用している場合にのみ可能です。



デバイスを選択してホイールをクリックすると、無人アクセスが選択できるようになります。これにより、デバイス上で確認することなく、デバイスに接続することができます。デバイスにアクセスするためのリンクが表示されるまで、しばらく時間がかかります。

スプラッシュトップ

Splashtop オプションを有効にすると、プロファイルに Splashtop 設定オプションが表示されます。

Splashtopを使用するには、Splashtop Streamer (com.splashtop.streamer.csrs)を必須アプリとしてプロファイルに設定する必要があります。その後、プロファイルの「リモートコントロール」でSplashtopの設定を有効にします。これを有効にすると、Splashtop Streamerアプリが設定されます。Splashtop Streamer を使用しているが MDM と組み合わせていない場合は、この設定をオフにしてください。

プロフィールの「リモートコントロール」で、デプロイコードも設定する必要があります。https://my.splashtop.com にアクセスし、Splashtopアカウントにログインします。コンピュータの追加」をクリックし、表示されたページから12桁のデプロイコードをコピーします。

Deploy Codeがないとリモートコントロールはできません。

その後、デバイスを右クリックし、"Splashtop Remote Control "をクリックしてリモートセッションを開始できます。

シムカード管理

CSV一括インポート

これは、割り当てられたシムカードとそれらに関するすべての情報の概要を表示します。これにより、デバイスだけでなくシムカードに関するすべての情報を1つのシステムで管理することができます。

注意これは手動による管理/文書化です。オペレーティングシステムのプライバシー/セキュリティ・メカニズムにより、デバイスからこのデータを自動的に取得することはできません。

また、このリストをCSVでインポートすることもできます。

キャリアと料金表

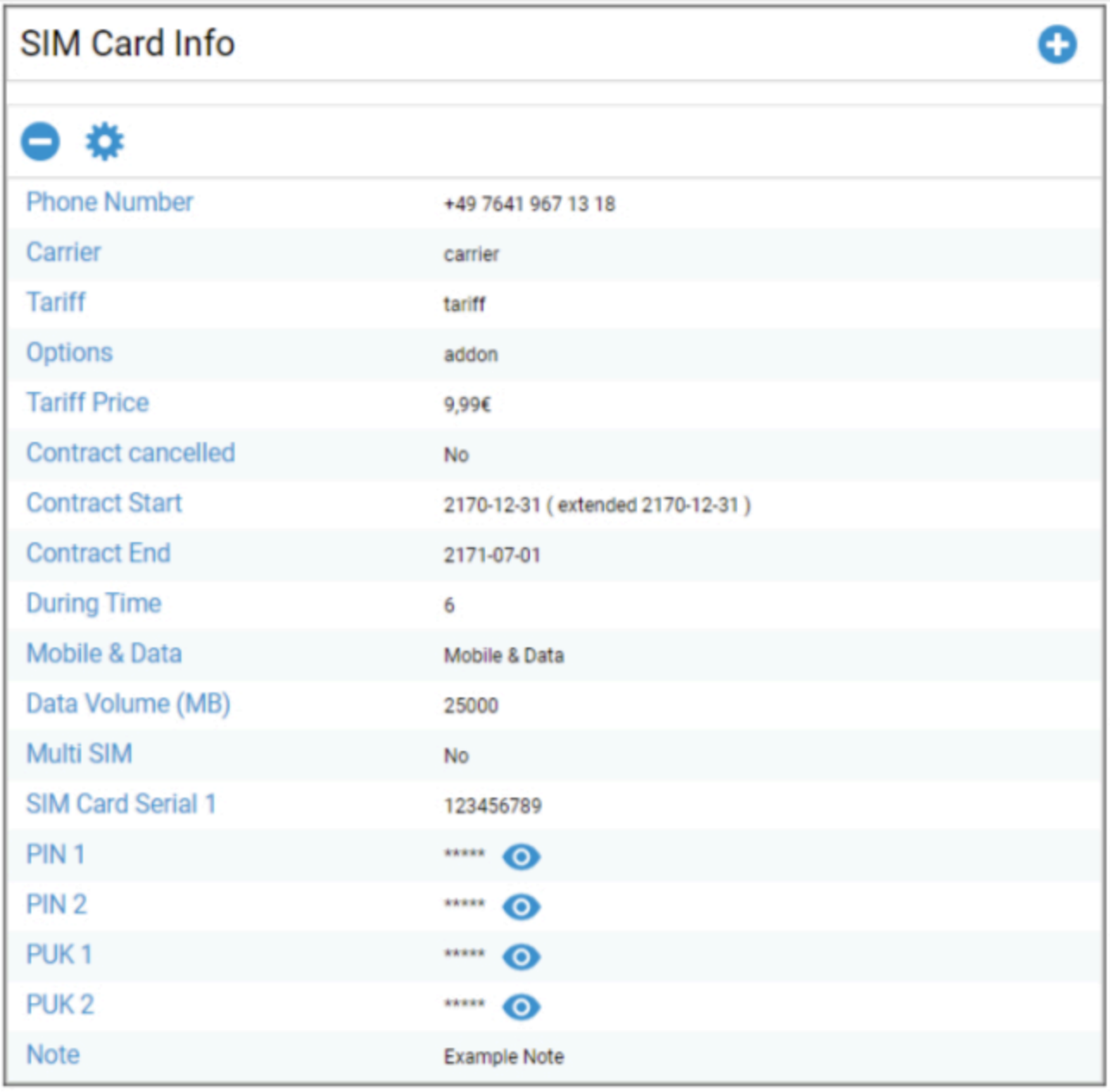
Simカードを追加するには、まず1つまたは複数のキャリアを追加するボタンをクリックします。

その後、「料金表情報」の「+」をクリックし、キャリアに料金表を追加します。

このようなものがあれば、オプションでアドオンを追加することができます。

これは、実際のシムカードを追加するために必要なすべてを準備します。シムカードは現在ユーザーに割り当てられています。そのため、モバイル管理からユーザーを選択し、「Simカード概要」に進みます。

このユーザーのシムカードが表示されます。もしあれば、編集または削除することができます。ユーザーは複数のシムカードを持つことができます。

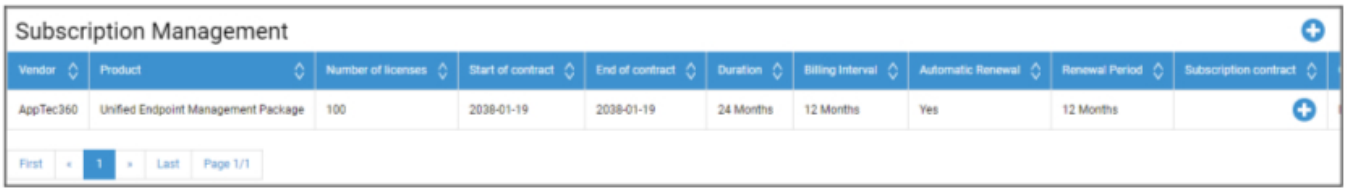


をクリックしてシムカードを追加し、必要な情報をすべて追加します。これらのシムカードは、一般設定 → シムカード管理のすべてのシムカードのリストにも表示されます。

サブスクリプション管理

サブスクリプション管理

ここでは、実行中のサブスクリプションやその詳細を文書化したり、署名済みの契約書、解約通知書などのさまざまなファイルを保存することができます。また、購読終了前にメールでお知らせするリマインダーを設定することもできます。



購読を追加するには、上部の「+」をクリックしてください。お好きなだけ購読を追加できます。

このサブスクリプションに関するファイルをアップロードするには、各フィールドの「+」をクリックしてください。技術的にはどのようなファイルタイプでもアップロードできますが、どのようなファイルタイプでもブラウザでプレビューできるわけではありませんのでご注意ください。

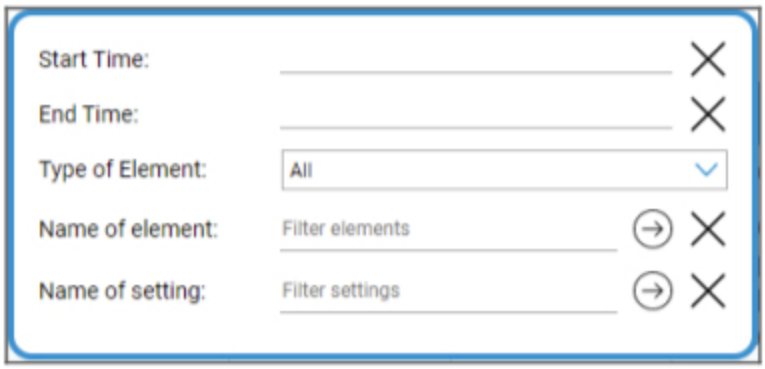
一般監査ログ

監査ログ

ここには、すべての変更を表示する一般的な監査ログがあります。ユーザーまたはグループの監査ログでは、そのユーザーまたはグループによる変更のみが表示されますが、ここでは、コンソール内のあらゆる場所で行われたすべての変更が表示されます。

いつ、誰が、どこで、何を変更したかを確認することができます。場合によっては、エントリーを拡張してさらに詳細を見ることもできます。

ユーザーをクリックするか、"Path / Type "のエントリーをクリックすることで、変更が行われた場所に移動することができる。



右上では、フィルタを定義することもでき、多くの変化が起きている環境で特定の変化を見つけるのに役立つ。

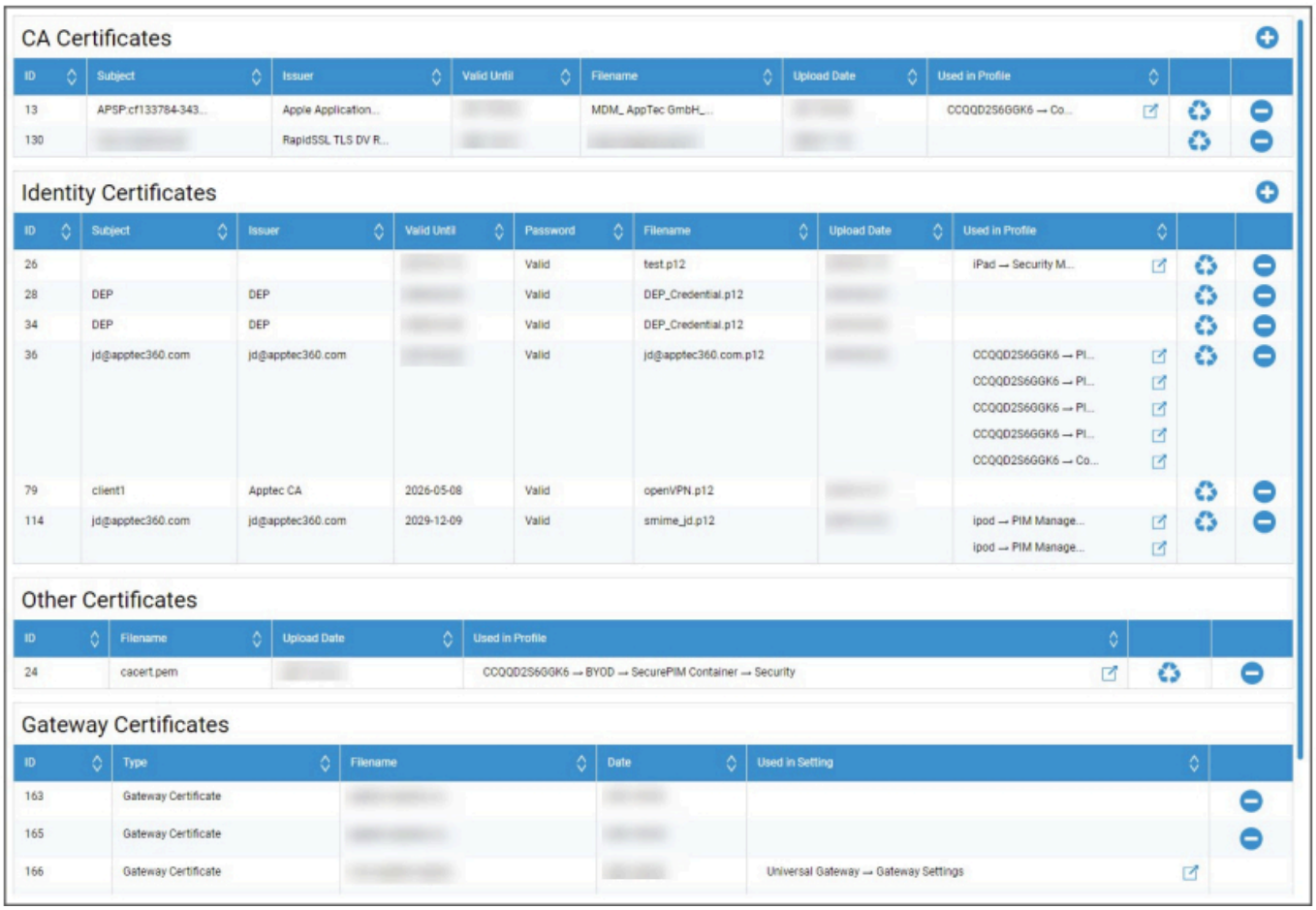
監査ログの設定

「監査ログの保存期間」は、削除するまでの監査ログの保存期間を定義します。

証明書管理

ここでは、アップロードされ、コンソールで使用されているすべての証明書の概要が表示されます。これはあくまで概要です。Wi-Fi証明書などの実際の設定は、対応する場所のプロファイルで行います。

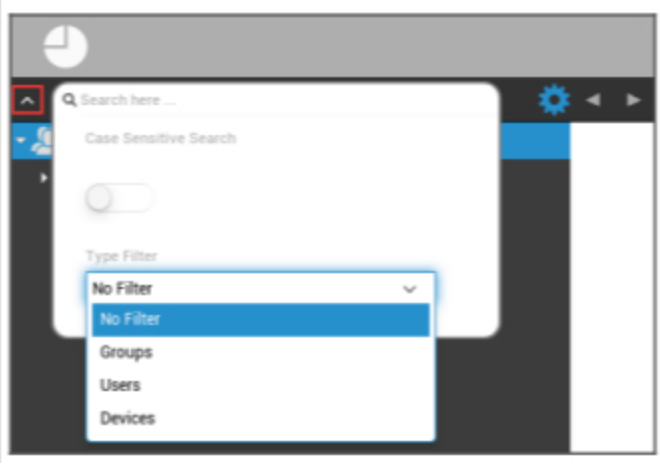
ここで証明書を削除または更新することもでき、影響を受けるプロファイルに自動的に反映されます。Used in Profile "の情報をクリックすると、まだ証明書が割り当てられている場所を確認できます。



モバイル管理

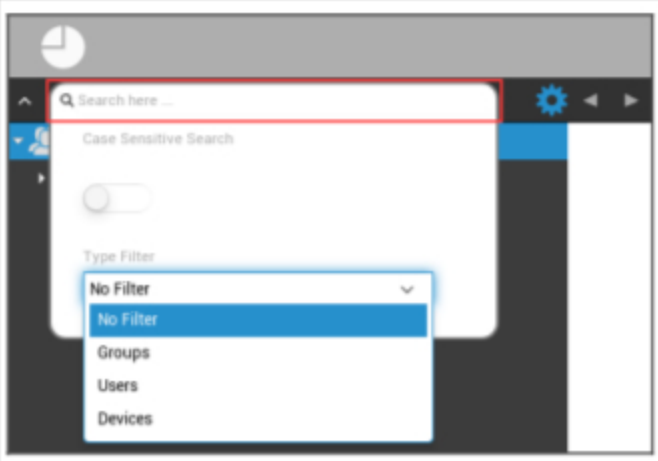
モバイル管理画面

デバイスフィルター



画面の左上隅をクリックすると、デバイスを表示するためのさまざまなフィルターを見つけることができます。

検索窓



検索ウィンドウでは、特定のキーワードですべてのデバイスやユーザーを検索できます。

オプションギア

それぞれのシンボルをクリックすると、利用可能なオプションのリストが表示されます。

これらは現在のウィンドウごとに変わり、それぞれの章で説明されている。

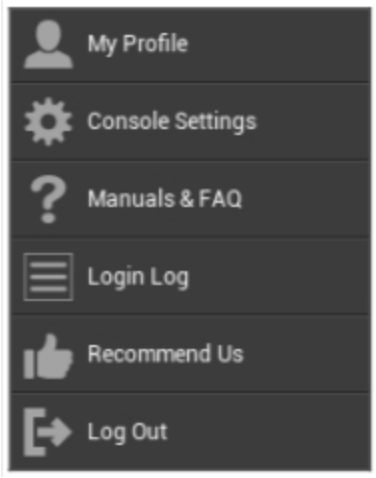
ナビゲーション矢印

左の矢印をクリックすると、前のページに移動します。

その後、右の矢印をクリックすると、先ほどのページに移動します。

管理アカウント設定

上記のようにメールアドレスをクリックすると、以下のメニューが表示されます：



プロフィール	管理者アカウントの詳細を編集する
コンソール設定	管理者アカウントのコンソール設定
マニュアル＆FAQ	"一般設定 "の "マニュアル＆FAQ "ページを見る
ログインログ	ログインログ」にアクセスする
私たちを推薦	一般設定 "の "おすすめ "ページを見る
ログアウト	MDMコンソールからログアウトする

ユーザー情報

ここでは、現在ログインしている管理者のアカウント詳細を編集することができます。

ユーザー名	アカウントのユーザー名および/またはメールアドレス
名称	管理者名
ラストネーム	管理者の姓
ログイン名	管理者ログイン名
電子メールアドレス	管理者メールアドレス
代替メールアドレス	管理者の代替メールアドレス
写真	プロフィール写真
電話番号	管理者の電話番号
携帯電話番号	管理者の携帯電話番号
内線電話	内線電話
所在地	所在地
ポジション	会社での地位
ユーザーグループ	管理者アカウントをどのユーザーグループに割り当てるかを選択します。
コメント	コメントを入力
新しいパスワードを入力	パスワード変更用のパスワードを入力
新しいパスワードを繰り返す	新しいパスワードを繰り返して確認する

管理者アクセスは、階層構造の中でローカルユーザーアカウントとしてファイルすることもできることに注意してください。追加の管理者を設定しない限り、このアカウントは削除しないでください！

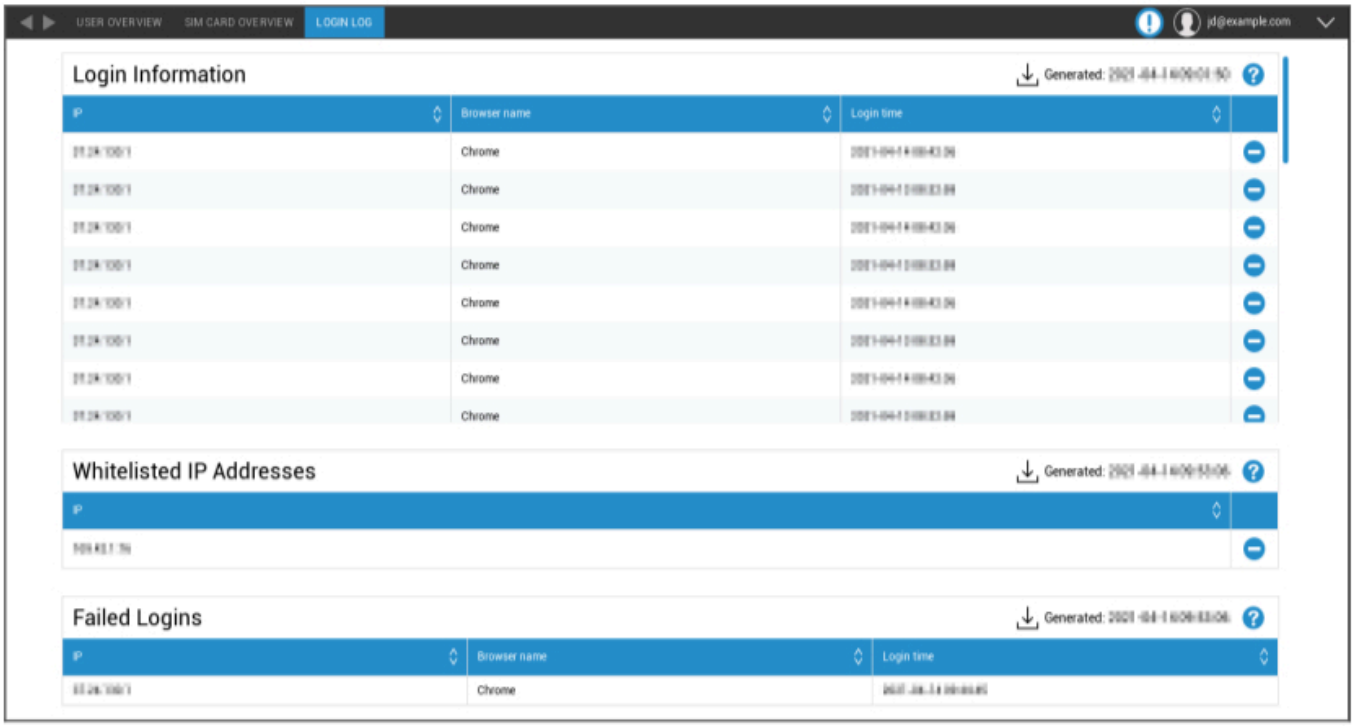
コンソール設定

ここでは、Adminsアカウントの以下のコンソール設定を行うことができます：

ディレクトリユーザー表示オプション	ツリー内でユーザーをどのようにラベル付けするかを定義する。
ディレクトリデバイス表示オプション	ツリー内でのデバイスのラベルの付け方を定義する。
セッションタイムアウト	指定された時間内にユーザーが何もしなければ、ログアウトされます。デフォルト値は60分です。設定変更後は一旦ログアウトし、再度ログオンしてください。
タイムゾーン	使用するタイムゾーンを選択する
時間形式	タイムスタンプの表示方法を選択する
コンソール言語	コンソールを表示する言語を選択します。英語とドイツ語があります。
メインカラー	コンソールの配色のベースとなる色を設定できます。 カラーピッカーを使うか、HTMLのHEX記法で色を入力することができます。 ピンク」や「イエロー」のようなRGBフォーマーも機能する。
セーブコマンド	保存 "ボタンを押さずに保存をトリガーするキーの組み合わせ。
二要素認証を使用する	ログイン時に2要素認証を使用できるようにする。 ログイン時にEメールが送信されますので、コードを入力してログインしてください。
二要素認証タイムアウト	認証に成功した後、2要素認証を要求されない期間を設定します。
認証コードを送信する	選択したオプションに認証コードが送信されます。デバイスメッセージは、AppTec360 MDMアプリで、あなたが所有するすべてのAndroidとiOSデバイスに表示されます。
ログイン後にログインメッセージを送信する	有効にすると、ホワイトリストに登録されていないIPアドレスからログインするたびにメールが送信されます。 メールにはログインに関する情報（IP、ブラウザなど）が含まれています。

ログインログ

ここでは、現在ログインしている管理者アカウントのログインに関する情報を見ることができます。



ログイン情報	コンソールによって記録された、現在ログインしている管理者アカウントのログインを含むリスト。 このリストには、過去30日間に成功したログインがすべて表示されます。
ホワイトリストIPアドレス	これは、ホワイトリストに登録されているすべてのIPアドレスのリストです。 ここに記載されているIPからログインした場合、ログインメッセージは表示されません。 このリストにIPアドレスを追加するには、上記の「ログイン情報」リストのエントリの横にあるボタンをクリックします。 このリストまたは上記の「ログイン情報」リストのエントリの横にあるボタンをクリックすると、このリストからIPアドレスを削除できます。
ログイン失敗	これは、過去30日間にログインに失敗したすべてのリストです。 20分間に3回以上正しいパスワードを入力できなかった場合、このリストに項目が表示されます。 また、ログインに失敗した場合は、電子メールで通知されます。

モバイル管理における企業管理（ルートノード

Root-Node（最初のグループ）に到達すると、モバイル管理に関する様々な設定を行うことができます。

サブグループの作成	サブグループを作る
ルートノードの名前を変更する	ルート・ノード名の変更（例：会社名）
大量登録	複数のデバイス/ユーザーを同時に登録する
大量割り当て	各グループにプロファイルを割り当てる。
クイックアプリ管理	アプリケーションの（アン）インストール要求を各グループ機器に送信する。
CSVユーザーインポート	CSVから各グループにユーザーをインポート

サブグループの作成

サブグループの作成」では、さらにサブグループを作成することができます。

サブグループをどのグループに割り当てるかを設定できる。

(デフォルトでは、ルート・ノードのサブグループとして割り当てられた新しいグループが作成されます。)

ルートノードの名前を変更する

ここでルートネームの名前を変更することができます。この場合、会社名が使われるのが一般的です。

大量登録

一括登録」では、複数のデバイスやユーザーを登録することができます。

ユーザーがどのような方法で登録情報を受け取るかを直接選択できます（eメール、代替eメール、SMS）。

ユーザーが受け取るデバイス（iOS、Android、Windows Phone）に応じて、ここで直接マークすることができます。

スマートフォンかタブレットかの区別もここで設定でき、チェックマークで正しく選択する必要がある。

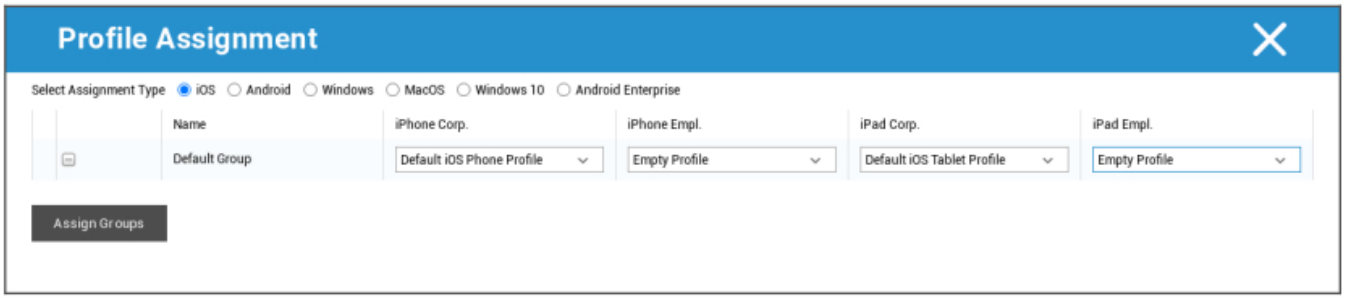
最後のステップとして、それぞれのデバイスが企業用か私用（BYOD）かを確定することができる。

CSVエクスポート」で、情報をCSVデータファイルとしてエクスポートできます。その代わり、「CSVインポート」でCSVファイルをインポートすることもできます：

Philipp Reiss; philipp.reis@apptec360.com; pr@apptec360.com; +41 61 511 3210 ;

大量割り当て

Mass Assignmentでは、すべてのグループにプロファイルを割り当てることができます。

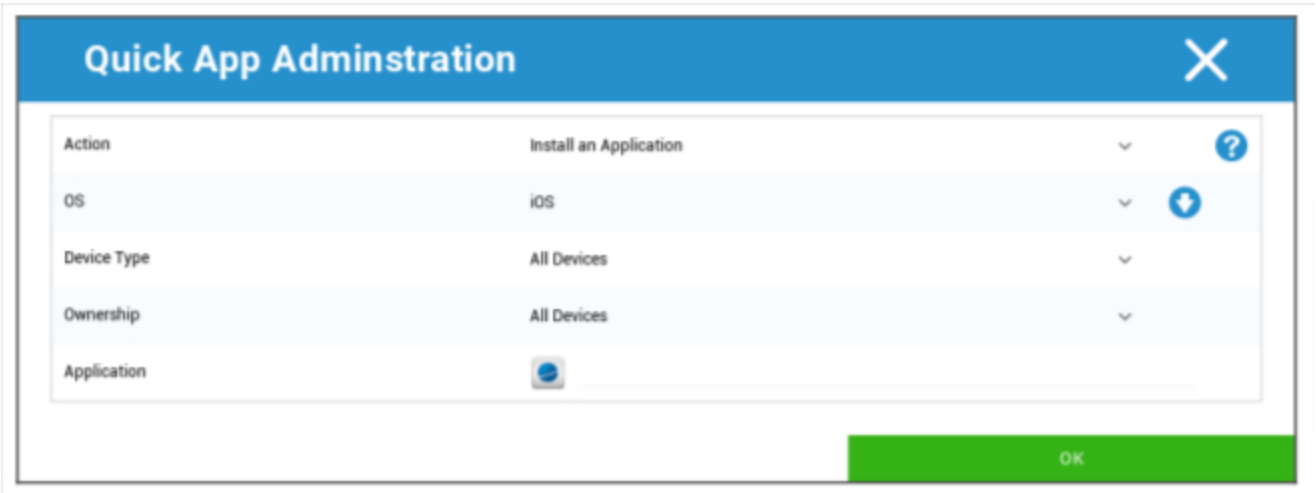


Windows - MacOS - Windows 10 - Android Enterprise

クイックアプリ管理

クイックアプリ管理]では、指定したアプリケーションのインストールまたはアンインストール要求を任意のOSに送信できます。

また、選択したOSの全デバイスタイプにリクエストを送るか、特定のデバイスタイプにのみリクエストを送るかを定義することもできる。



CSVユーザーインポート

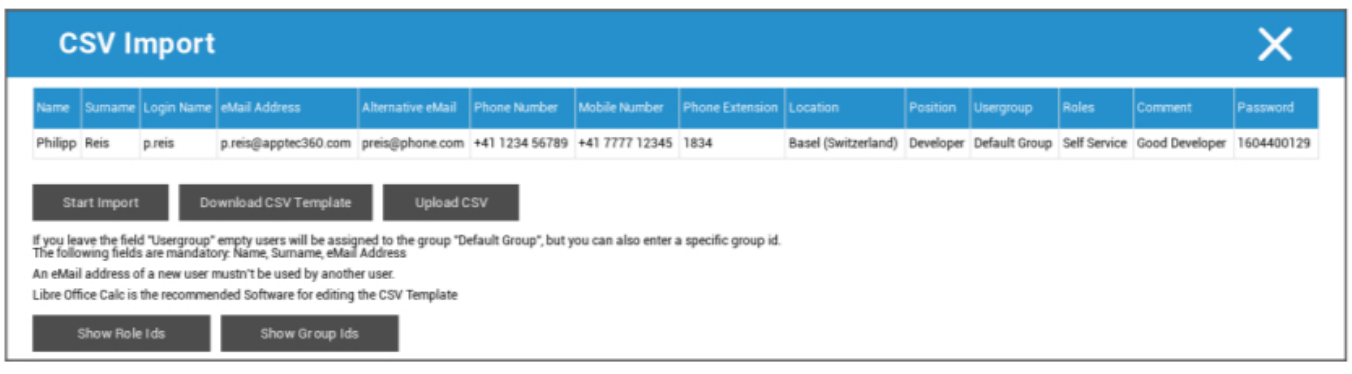
CSVから各グループにユーザーをインポートします。

CSVテンプレートダウンロード」では、CSVテンプレートファイルをエクスポートすることができます。

また、「役割のIDを表示する」と「グループのIDを表示する」オプションを使用して、独自のCSVファイルを作成することもできます。

CSVファイルは「Upload CSV」でMDMにアップロードできる。

最後のステップとして、"Start Import "をクリックしてインポートを開始することができます。



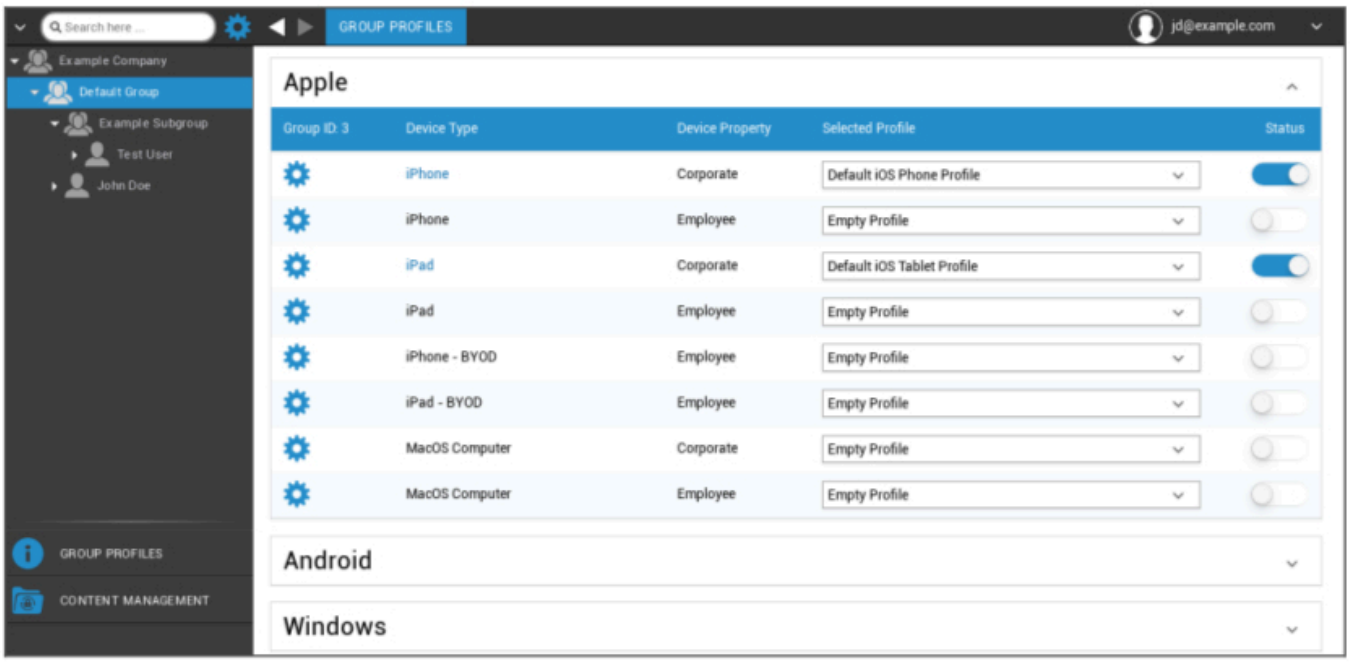
モバイル管理におけるグループ管理

概要をクリックすると、各プラットフォームのさまざまな構成プロファイルが表示されます。

1つのプロファイルには、AppTec360でエンドユーザーデバイスに事前に設定できるすべての設定オプションが含まれています。各プラットフォームでは、企業デバイス（Corporate）または持ち込みデバイス（Employee）用のプロファイルを作成できます。

例えば、場所や機能に基づいてデバイスグループの設定を区別するために、いくつかのサブグループを作成することをお勧めします。

モバイル管理のプロファイル管理に注意してください



ギアメニューでは、それぞれの（サブ）グループに対して様々な設定を行います。

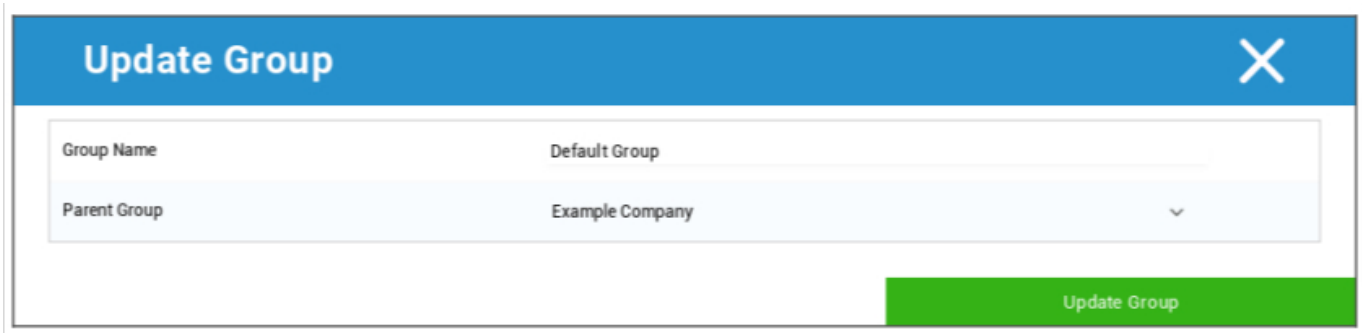
サブグループの作成	それぞれの（サブ）グループにサブグループを作成する
選択したグループの編集	選択したグループの編集
選択したグループの削除	選択したグループを削除する
大量登録	選択したプロファイルに一度に多くのデバイス/ユーザーを登録する
大量割り当て	現在選択されているグループにプロファイルを割り当てる
サブグループの作成	それぞれの（サブ）グループにサブグループを作成する
ユーザーの作成	それぞれの（サブ）グループのユーザーを作成する。

サブグループの作成

サブグループの作成」では、さらにサブグループを作成することができます。

サブグループをどのグループに割り当てるかを設定できます（デフォルトでは、サブグループは現在選択されているグループに割り当てられます）。

選択したグループの編集



ここでプロフィールを編集することができます - ここでは以下の設定が可能です：

- グループ名の変更が可能
- 親グループは変更可能

選択したグループの削除

選択したグループを削除 "の下に、それぞれのグループに属するすべてのユーザーとデバイスが表示されます。ここで、それらを削除するオプションがあります。

1人のユーザーに対して、以下の削除コマンドを実行できる：

ユーザー削除	ユーザーが削除される
ユーザーをグループに移動します：	ユーザーを別のグループ（次の列、例：「Admins」）に移動させることができます。

つのデバイスに対して、以下の削除コマンドを実行できます：

ワイプ＆削除	デバイスのワイプと削除
システムから削除	AppTecからデバイスのみを削除

リファレンス大量登録

参考質量割り当て

ユーザーの作成

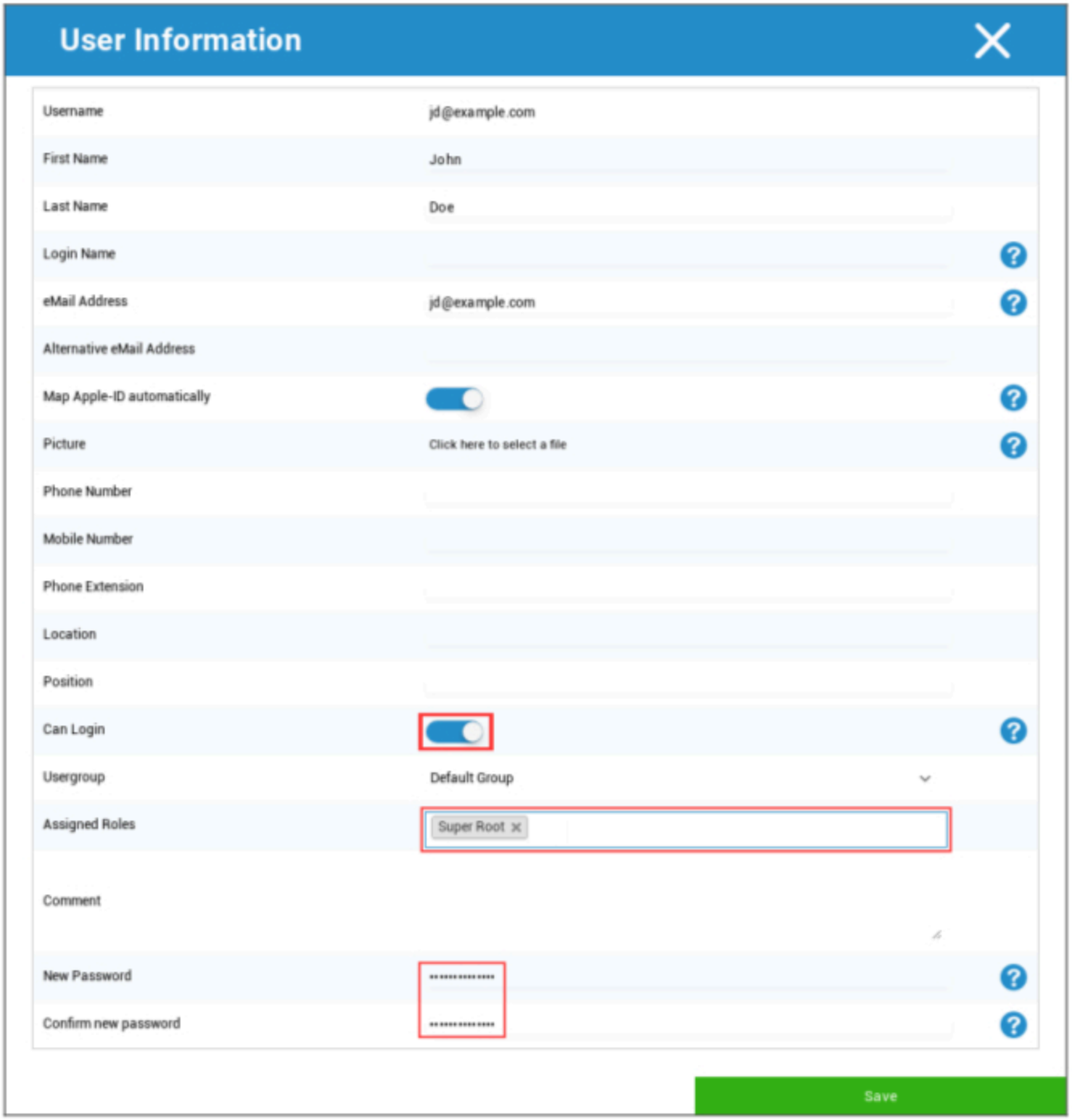
Create a User "では、新しいユーザーを追加することができます。

新しい管理者ユーザーを作成する

ユーザーを Admin-User に設定することができます。そうすることで、コンソールにログインし、ユーザー/グループ/デバイスを変更する権限が与えられます。

通常のユーザーを作成するか、既存のユーザーを使用します。管理者権限を与えたいユーザーを選択し、ホイールをクリックして "Edit User "を選択してください：

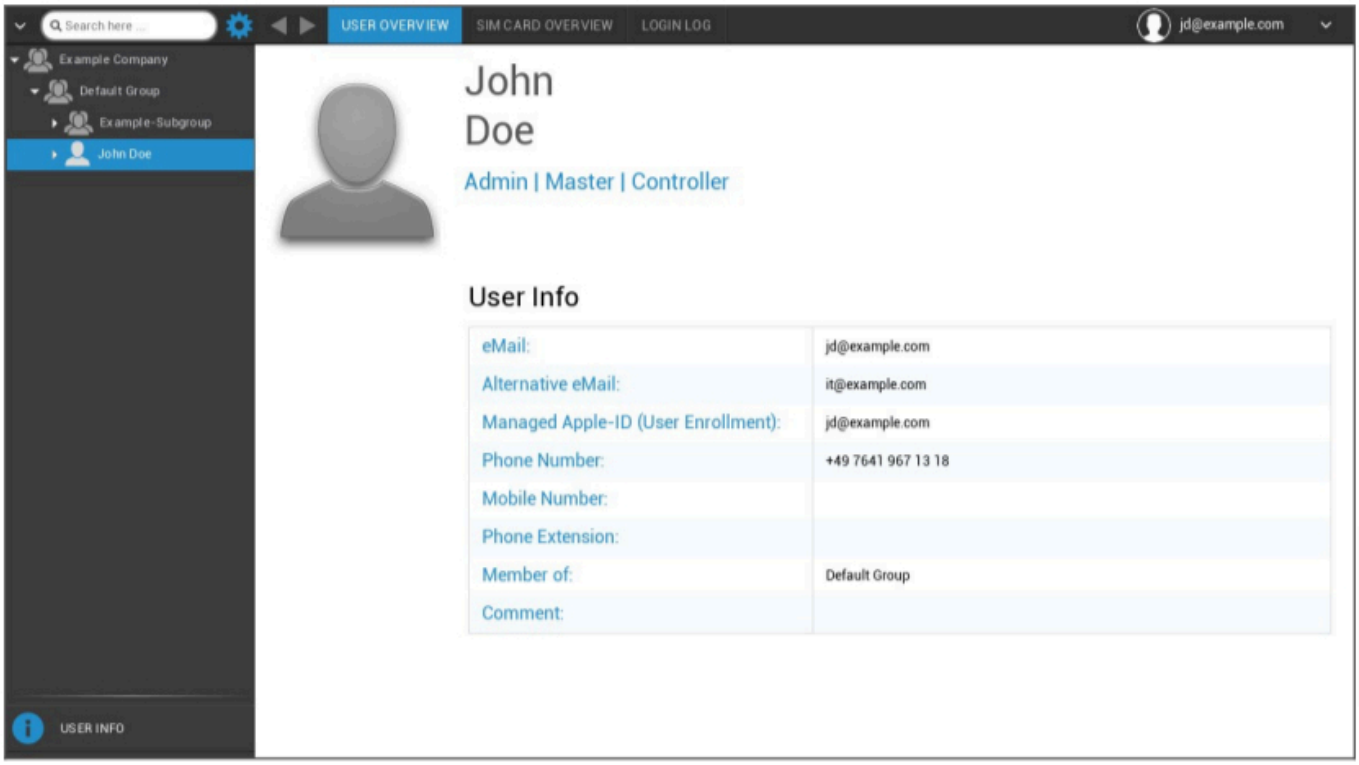
Can Login "スイッチを有効にし、ユーザーに "Super-Root "ロールを割り当て、パスワードを設定する。



これを保存すると、ユーザーはユーザー名とパスワードでログインできるようになります。

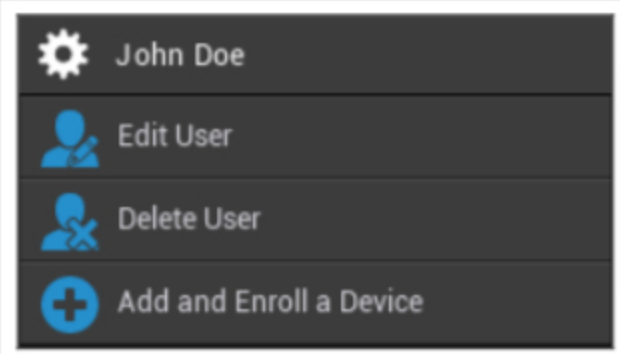
モバイル管理におけるユーザー管理

特定のユーザーを選択すると、次のような概要が表示されます：



ユーザーの作成」で入力したすべての情報の概要が表示されます。

上部に取り付けられているギアで、以下のコンフィギュレーションを行うことができる：



ユーザー名	選択したユーザーのユーザー名
編集ユーザー	ユーザー情報の編集
ユーザー削除	ユーザー削除 • システムから削除 = デバイスはAppTecから削除されます。

	• ワイプ＆削除 = デバイスは工場出荷時の設定に復元され、AppTecから削除されます。
デバイスの追加と登録	選択したユーザーのデバイスを登録する

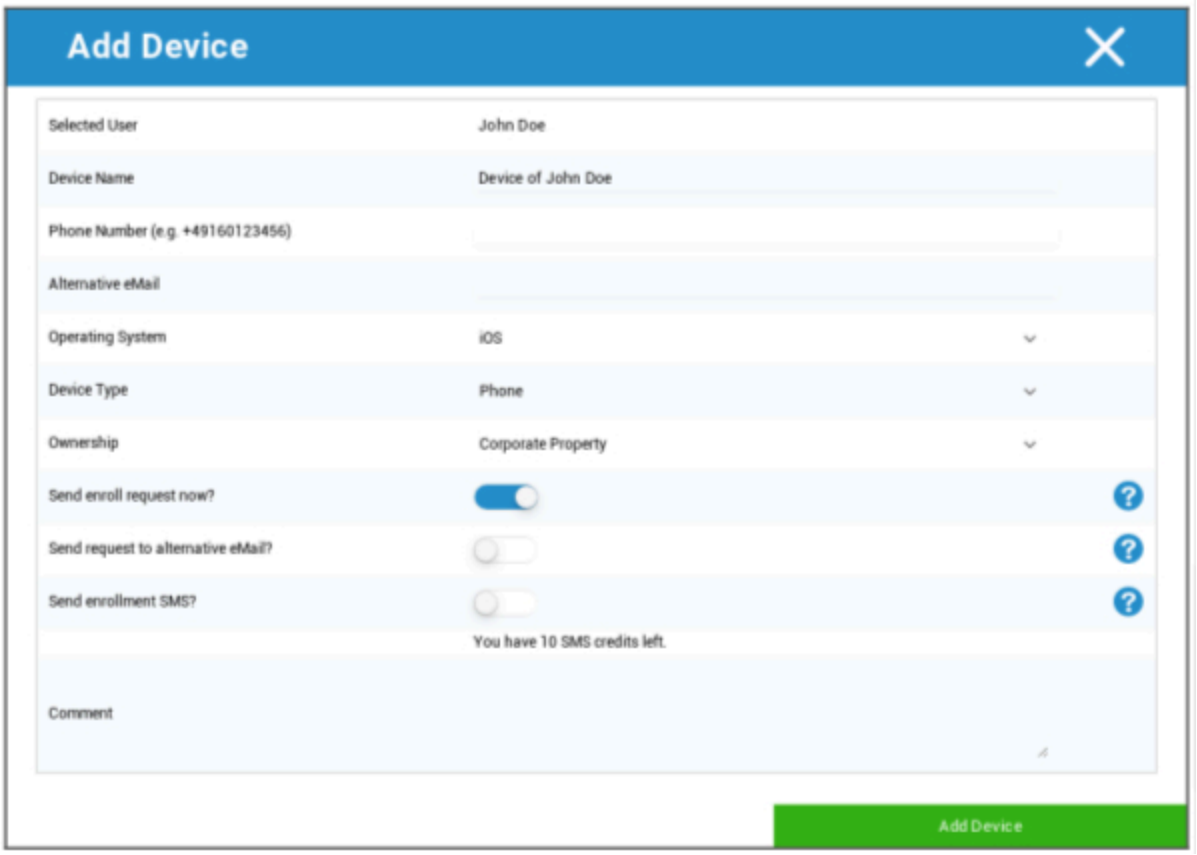
管理者アクセスは、階層構造の中でローカルユーザーアカウントとしてファイルすることもできることに注意してください。追加の管理者を設定しない限り、このアカウントは削除しないでください！

デバイスの追加と登録

ここで、選択した用途のデバイスを選択することができます。

または、デバイスを直接グループに登録することもできます。その場合は、グループをクリックし、ホイールをクリックして「Add and enroll a Device（デバイスの追加と登録）」を選択します。

以下のような概要が表示されるはずだ：



登録したいデバイスの種類に応じて、以下の設定を行う必要があります：

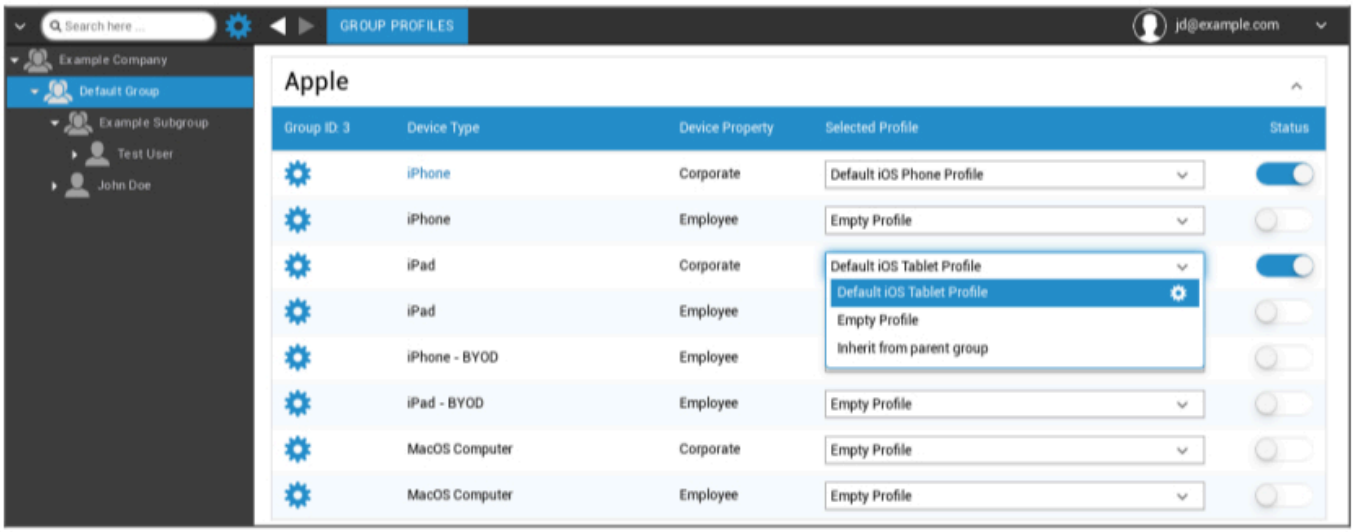
選択されたユーザー	選択されたユーザー（自動的に入力されます）
デバイス名	自動的に入力されます（"ユーザー名 "用のデバイス）-ただし変更可能
電話番号	電話番号は、（ユーザーによって提供された限り）自動的に入力されます。
代替Eメール	代替Eメールは、（ユーザーによって提供された限り）自動的に入力されます。
デバイス所有者	コーポレート・プロパティ = 企業用デバイス 従業員の所有物 = BYODデバイス
操作システムの選択	ここでは、以下のオペレーティングシステムから選択できる： • iOS • iOS BYOD（ユーザー登録） • マックオス • アンドロイド・エンタープライズ • アンドロイド • ウィンドウズ・モバイル • ウィンドウズ10
入会リクエストを送信しますか？	メールはメインメールアドレスに即座に送信され、ユーザーはデバイスを接続するよう促される。
別の電子メールにリクエストを送信しますか？	追加的または排他的に（「登録リクエストを送信しますか」が無効になっている場合）、代替メールアドレス（「通常の」登録リクエストメールとは異なるメールアドレス）にメールを送信する。
入会SMSを送る？	SMSで入会リクエストを送信する（「電話番号」を入力する必要があります）

Enrollment Requestが送信されると、すぐにデバイスが表示されます（赤いマーク）。

デバイスが正常に接続されると、その後すぐにデバイスが緑色にマークされ、制限やアプリなどを受信する準備が整います。

モバイル管理におけるプロファイル管理

グループをクリックすると、設定するすべてのデバイスプラットフォームと、それぞれ割り当てられたプロファイルの概要が表示されます。



	選択したプロファイルのコンフィギュレーションを実行する
デバイス・タイプ	デバイスのタイプおよび/またはモデル
デバイス特性	デバイスの所有者（Corporate = 企業の所有物、Employee = 従業員の私有デバイス）
プロフィール	選択したプロファイル（歯車はプロファイルの設定ダイアログを開きます）
ステータス	オン/オフ（プロファイルの有効化/無効化）

ギアを選択すると、以下のオプションが表示されます：

プロフィールの作成

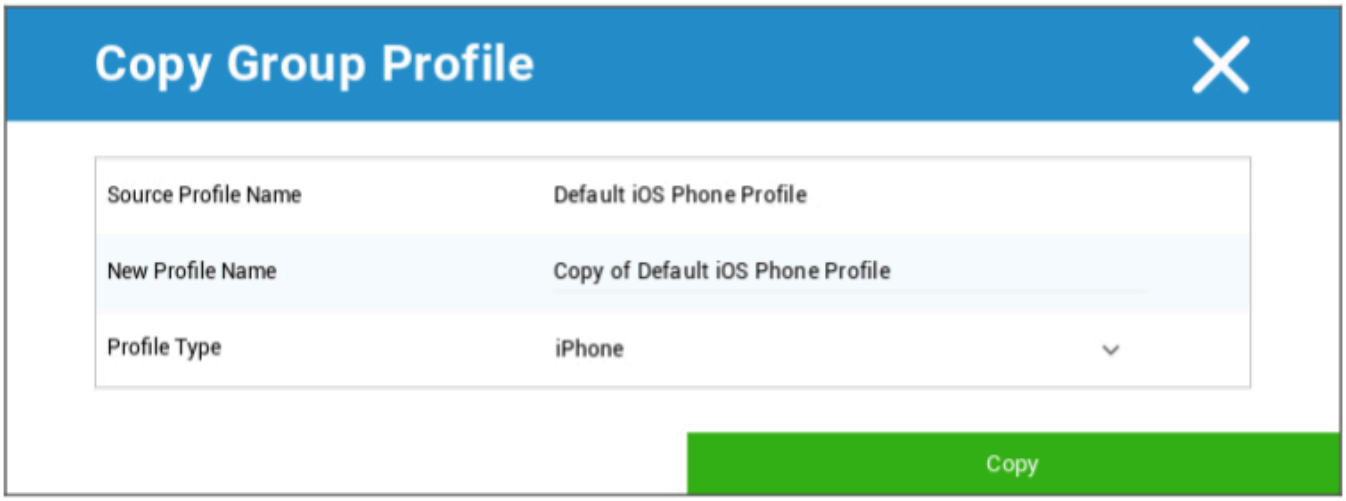
各エントリーおよび/またはプラットフォームごとに新しいプロファイルを作成し、設定することができます。このサブポイントをクリックすると、すぐにプロファイルが作成され、iOS、Android、Windows Phoneの設定をすぐに始めることができます。

プロフィール編集

Edit Profile "をクリックすると、各プロファイルの設定画面が表示され、設定を行うことができます。

コピープロフィール

プロファイルのコピー」機能を使用すると、既存のプロファイルからセットアップ/設定をコピーして、新しいプロファイルに追加することができます。

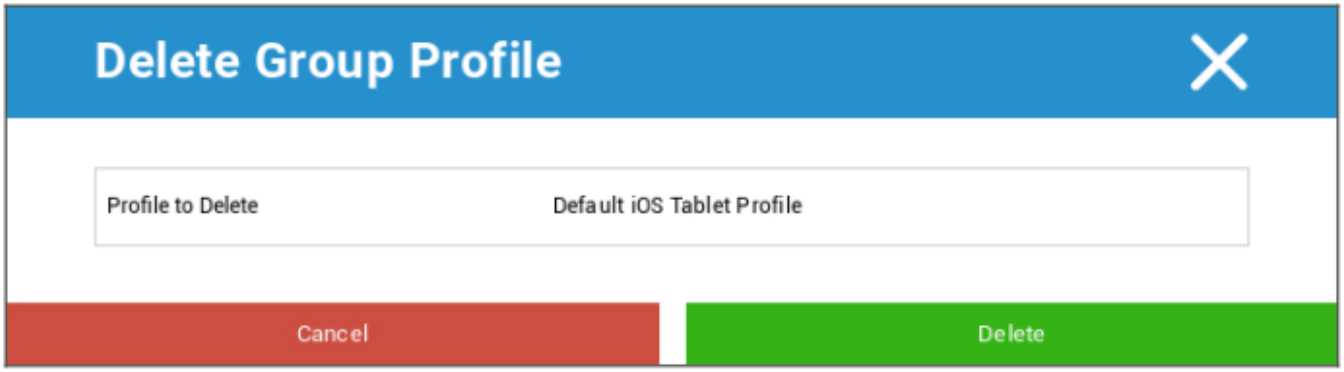


ソース・プロフィール名	コピーするプロファイルの名前
新しいプロフィール名	新しいプロファイルの名前
プロフィール・タイプ	プロファイルタイプ (電話/タブレット)

コピー」をクリックすると、プロフィールが作成され、グループに割り当てることができます。

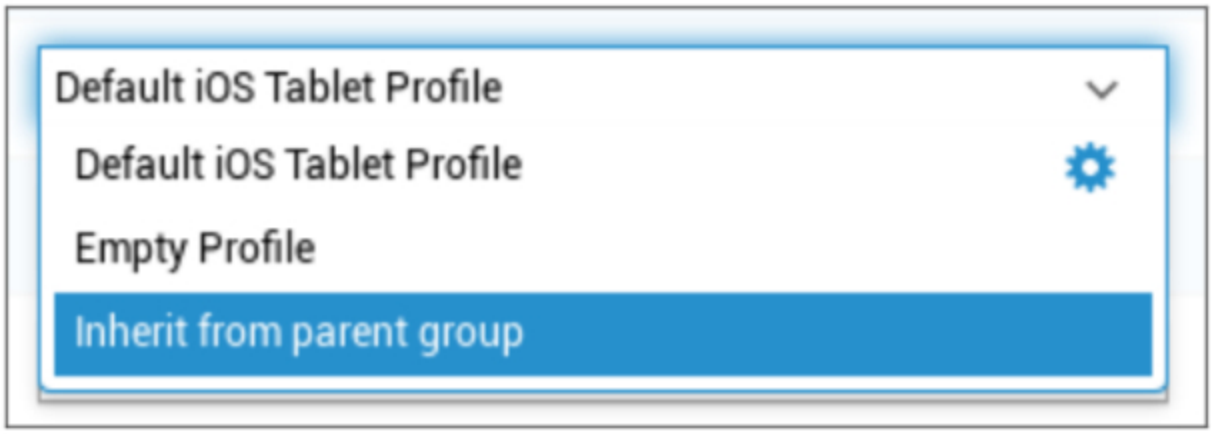
プロフィール削除

ここでプロファイルを完全に削除できます。プロファイルの削除処理中および次の「今すぐ割り当て」処理中は、影響を受けるグループの各デバイスで設定が消え、復元できないことに注意してください！


Delete Group Profile
Profile to Delete
Default iOS Tablet Profile
Cancel
Delete

プロファイルの継承

プロファイルを選択する際、「親グループから継承する」というオプションが利用できます。



プロファイルが有効になると、親グループのプロファイルが、それぞれ選択されたデバイス（およびそれぞれのデバイスタイプ）に使用されます。また、このプロファイルを変更すると、多数のグループに影響する可能性があることにご注意ください。

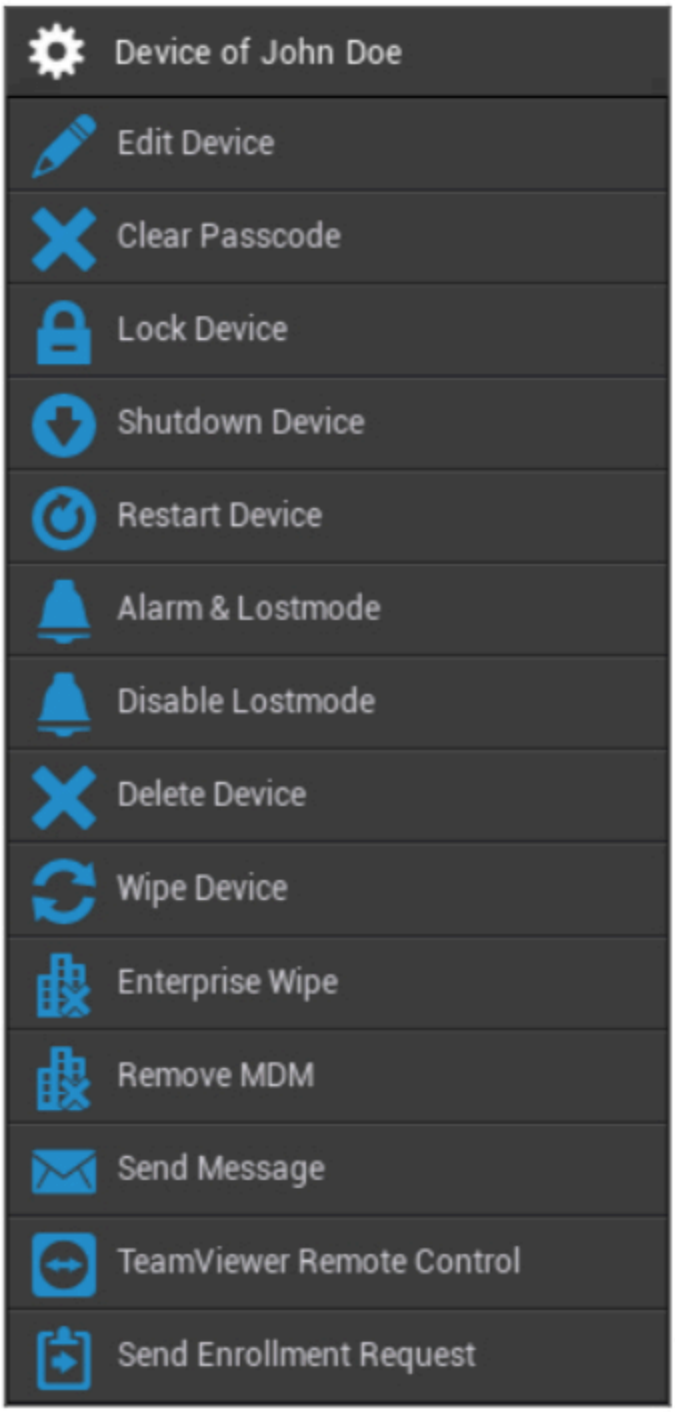
このコンフィギュレーションは、新しいサブグループの作成時にデフォルト値として設定される。

これは空のプロファイルに相当し、最終的にエンドユーザーデバイス上で新しいコンフィギュレーションが実行されないことを意味します。

モバイル管理におけるデバイス管理

デバイスを選択すると、"歯車 "を介して様々なタスクを実行することができます。これらはOSプラットフォーム（iOS、Android Enterprise、Android、Windows Mobile、Windows 10）によって異なる。

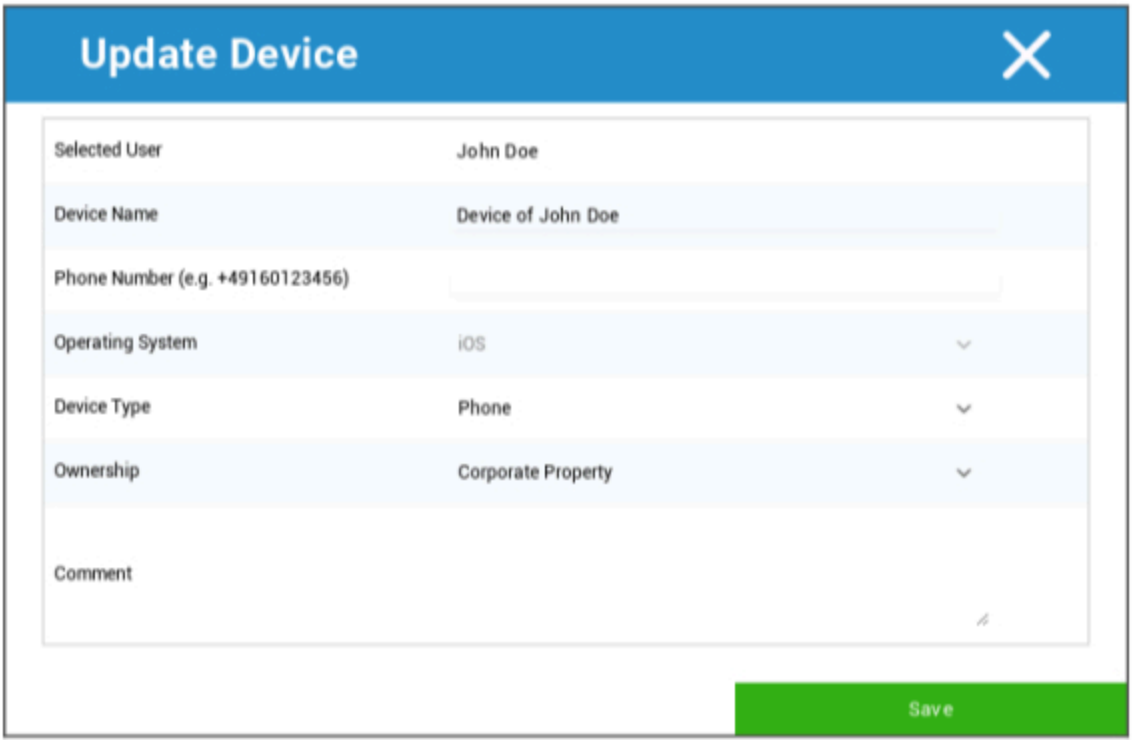
IOS



デバイスの編集	デバイスの編集
パスコードクリア	デバイスのパスコードが消去される
ロック装置	デバイスをロックする (ロック画面)
シャットダウン装置	シャットダウン装置

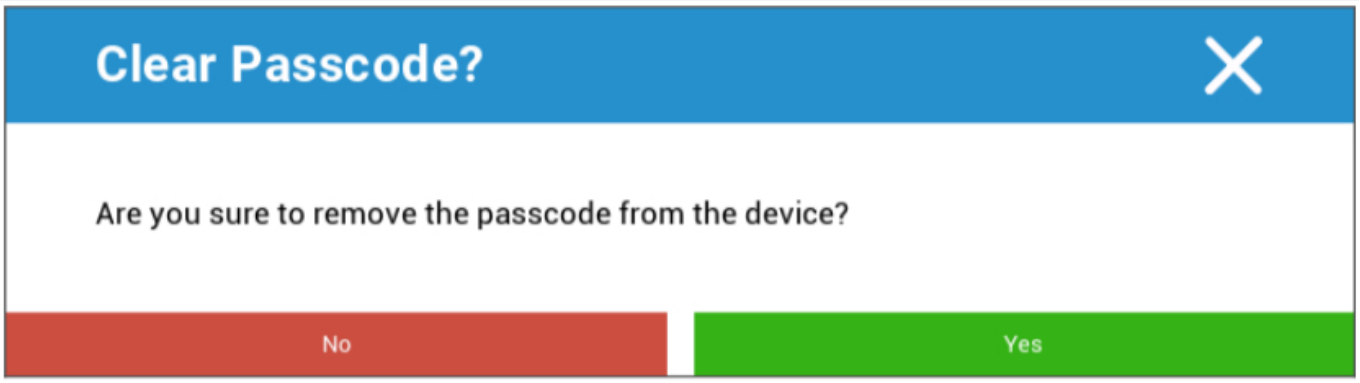
デバイスの再起動	デバイスの再起動
アラーム＆ロストモード	スタートアラーム＆ロストモード
ロストモードを無効にする	ロストモードを無効にする
デバイスの削除	AppTecからデバイスを削除する
ワイプ装置	デバイスを工場出荷時の設定に戻す
エンタープライズ・ワイプ	AppTec360が提供した情報、アプリ、プロファイルが削除される（デバイスがMDMから切り離される）
MDMの削除	
メッセージを送る	プッシュ通知をデバイスに送信 メッセージはAppTec360アプリ（メッセージタブ）に表示されます。
TeamViewerリモートコントロール	TeamViewerを使用したリモートコントロールセッションの開始
入会リクエストを送信	送信 (繰り返し) 入会リクエスト

デバイスの編集



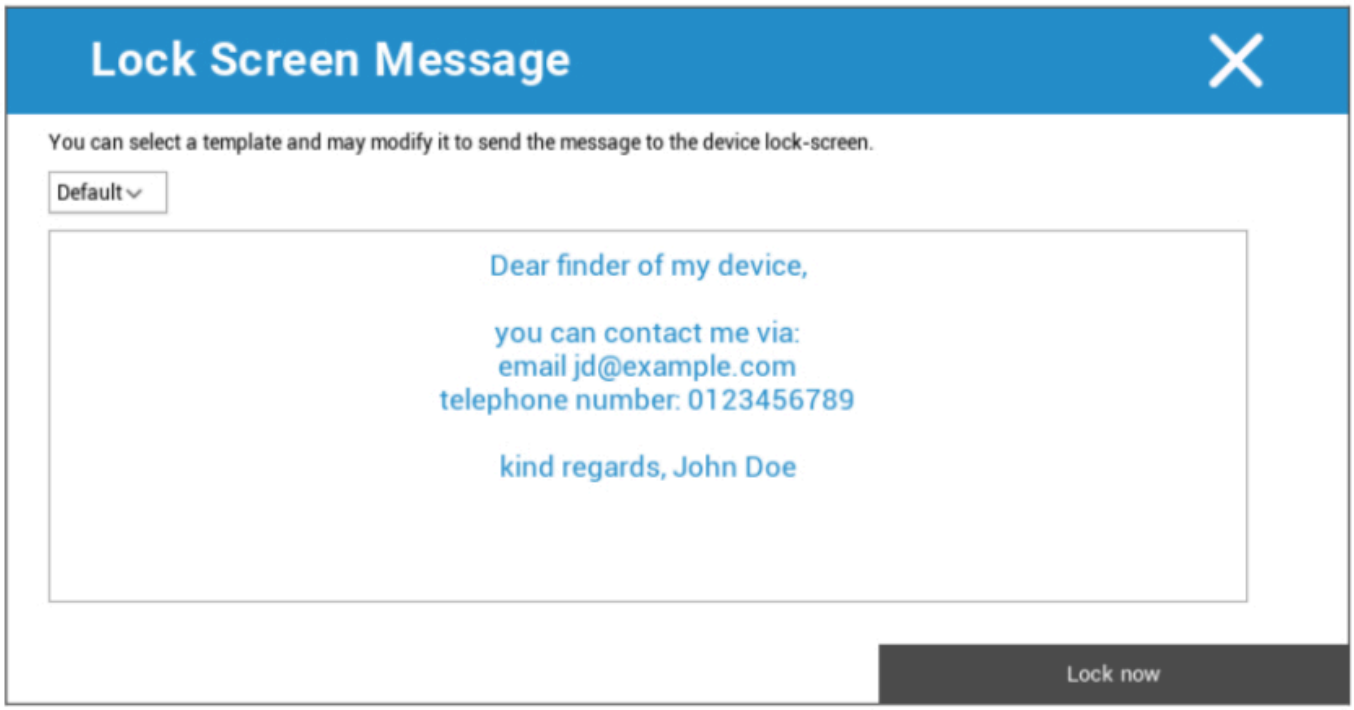
ここでは、デバイスの様々な情報を更新することができます。

パスコードクリア



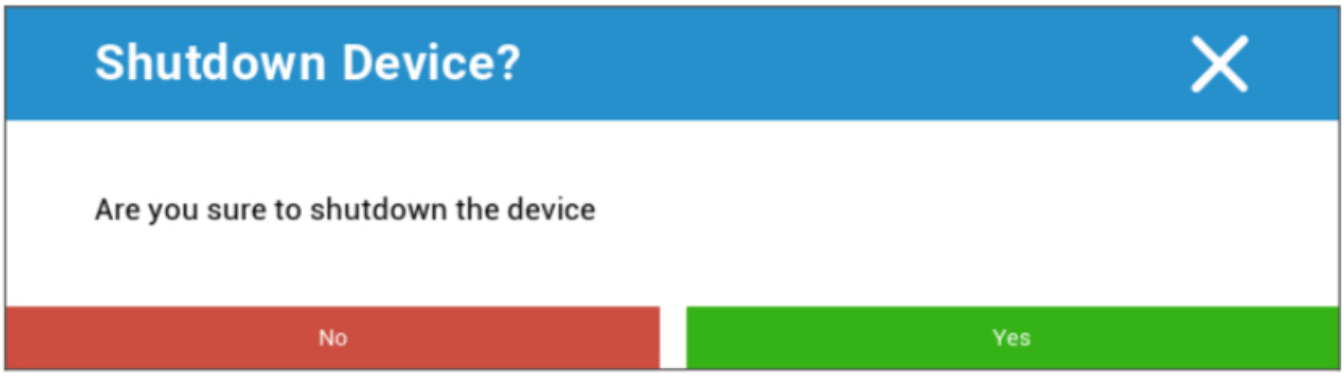
Clear Passcode "の下で、リモートでデバイスからパスコードを削除することができます。その後、ユーザーは新しいパスワードを発行するよう促されます (パスコードのガイドラインによる) 。

ロック装置



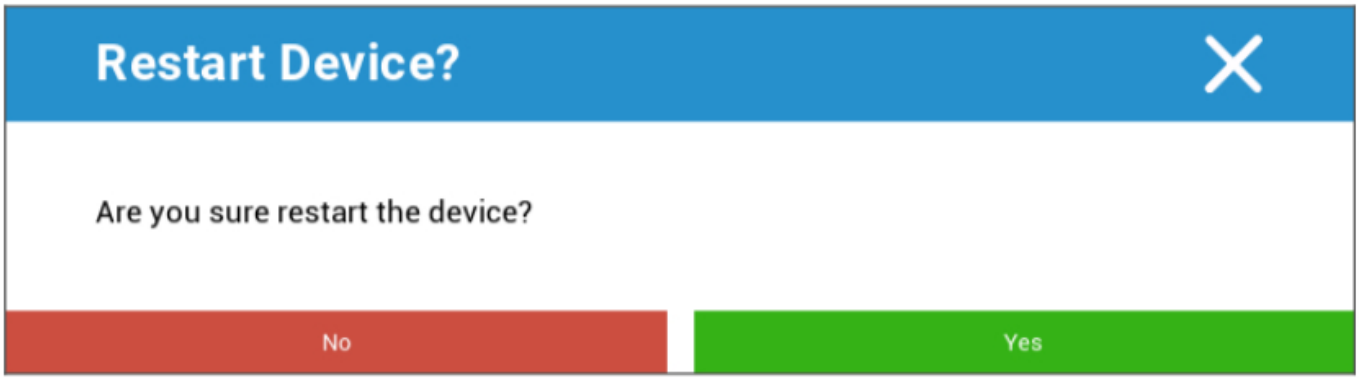
ここでは、ロック・コマンドがエンドユーザー・デバイス（ロック画面）に送信される。

シャットダウン装置



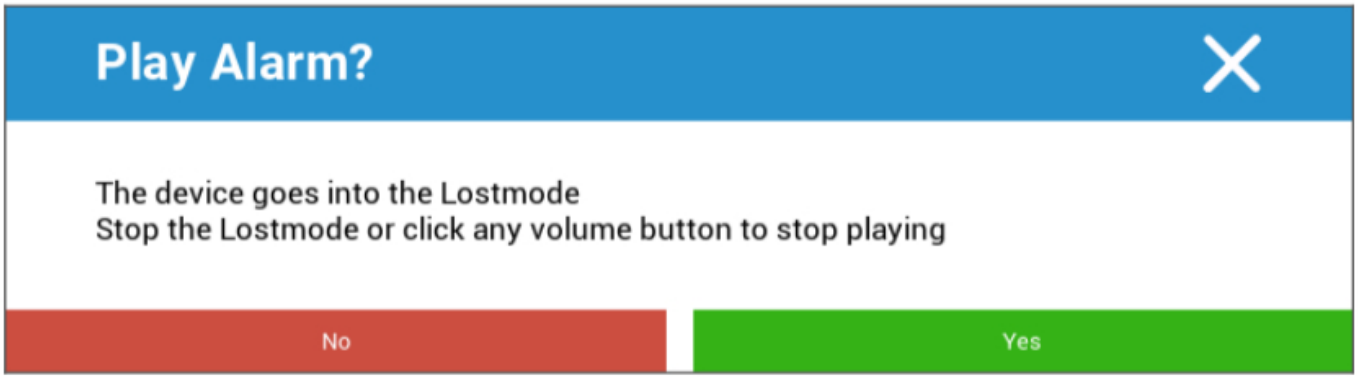
ここで、シャットダウンコマンドがエンドユーザーデバイスに送信される。

デバイスの再起動

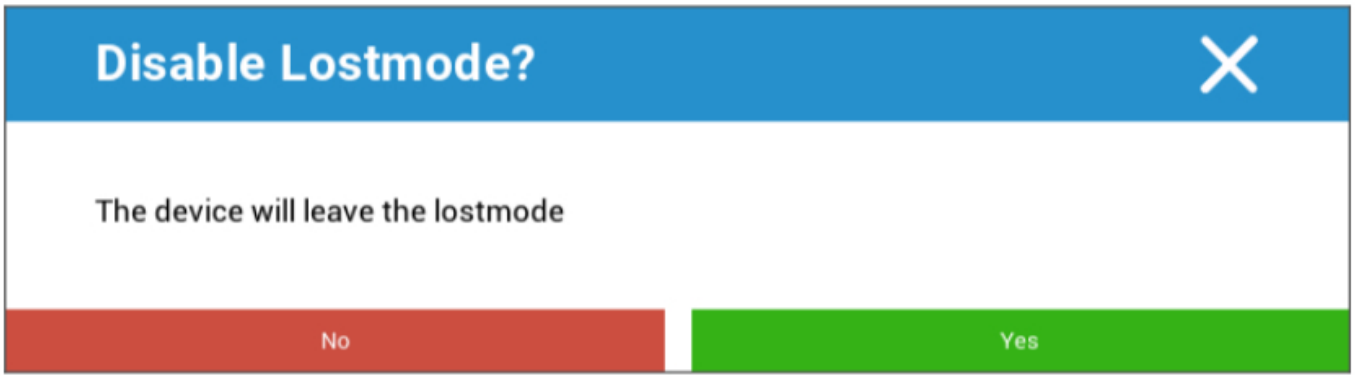


ここでリスタート・コマンドがエンドユーザー・デバイスに送られる。

アラームとロストモード | ロストモードを無効にする



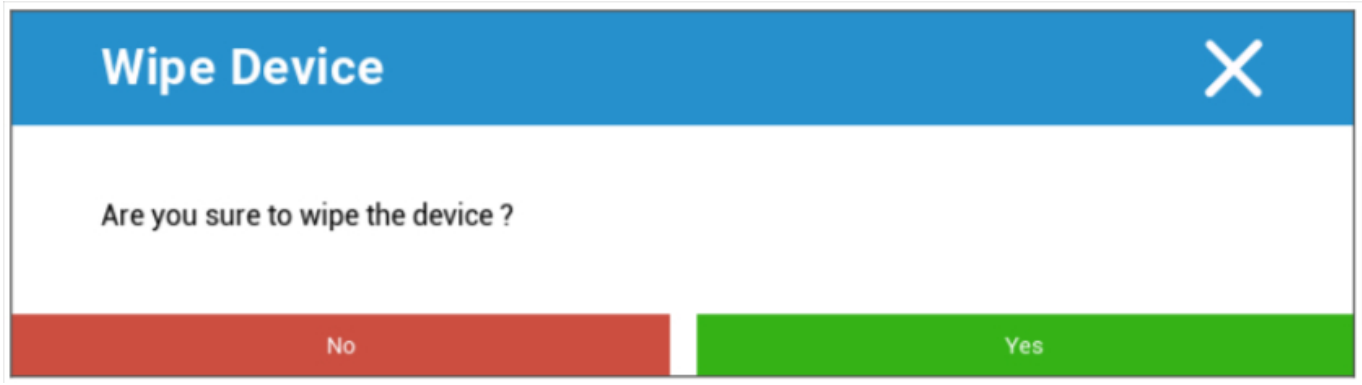
ここでデバイスをロストモードに設定することができ、常にアラーム音を再生するように設定します。ロストモードは、デバイスのボリュームボタンを押すか、リモートで「ロストモードを解除」をクリックすることで停止できます：



デバイスの削除

ここで削除コマンドを実行できる。デバイスをAppTec360からのみ削除する（「システムから削除」）か、AppTec360から削除し、工場出荷時の設定に戻す（「ワイプ＆削除」）かを再度決定できます。

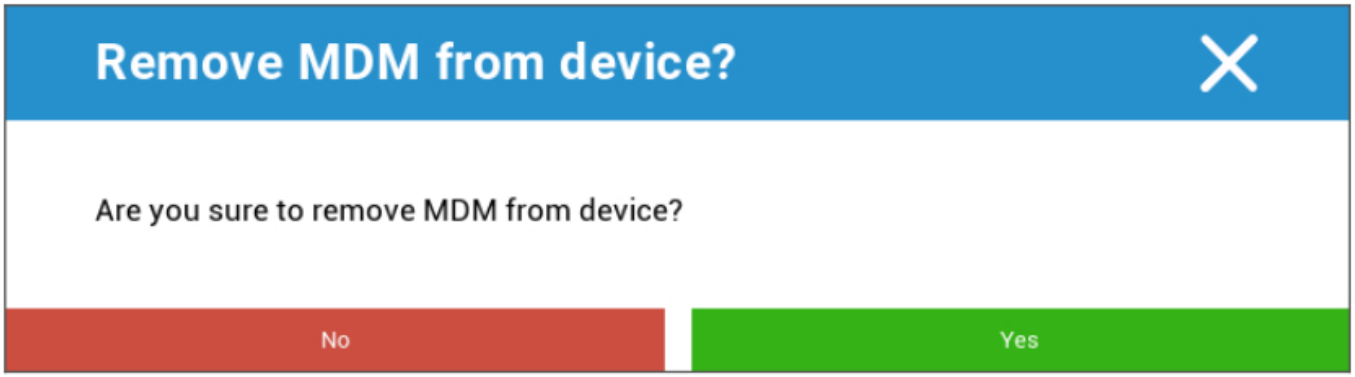
ワイプ装置



デバイスのワイプ」では、デバイスの完全なワイプを実行できます。デバイスは工場出荷時の設定に復元されます。

エンタープライズ・ワイプ｜MDMの削除

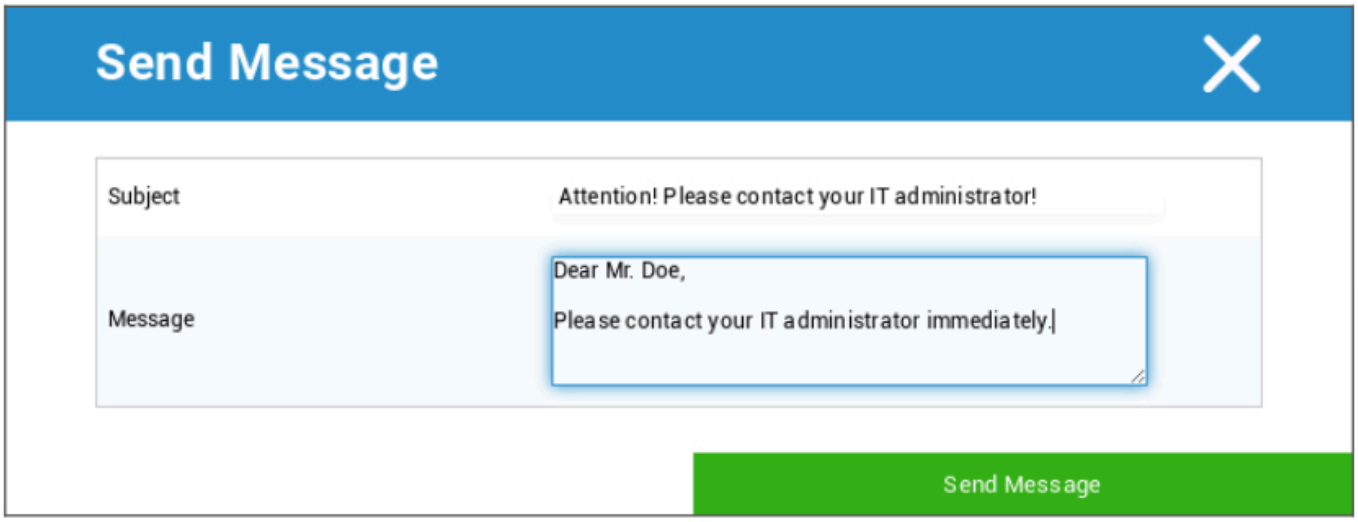
AppTec360によって提供された情報、アプリ、プロファイルのみが削除されます。こうすることで、企業データはエンドユーザーデバイス上で利用できなくなります。プライベートエリアは影響を受けず、エンドユーザーデバイスに残り続けます。



RemoveMDM」で、エンドユーザーデバイスのMDMプロファイルと、AppTecが提供する他のすべてのアイテムを削除できます。

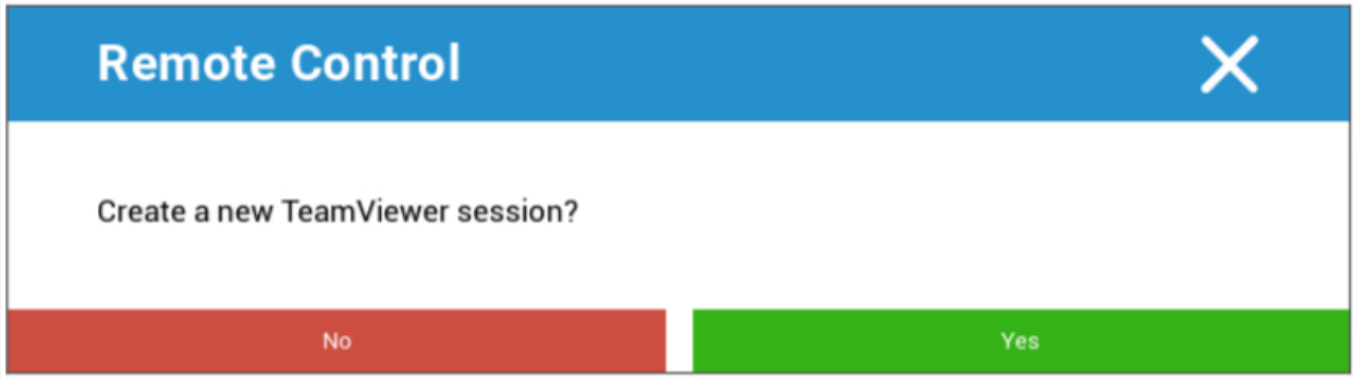
このコマンドは "Enterprise Wipe "と同じ動作を実行する。

メッセージを送る



ここで、それぞれのデバイスにプッシュ通知を送信できます。

TeamViewerリモートコントロール



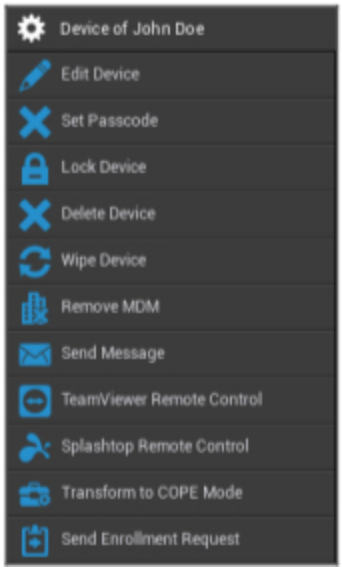
ここで、Teamviewer リモートコントロールセッションを開始できます。

入会リクエストを送信

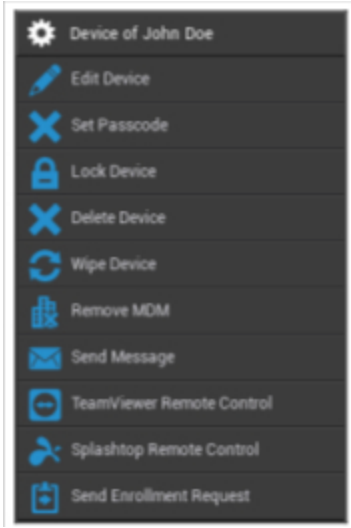
Send Enrollment Request"（登録リクエストの送信）により、それぞれのユーザーに登録リクエストを（再度）送信することができます。

アンドロイド

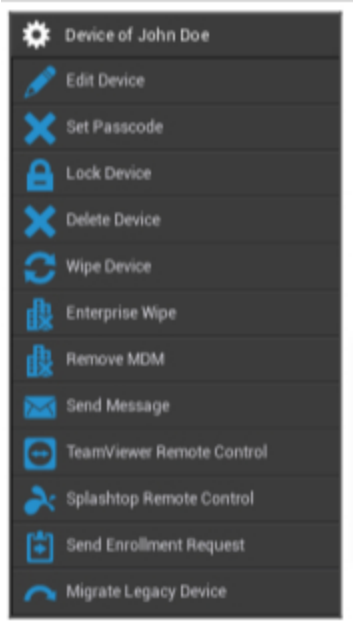
AEフルマネージド・デバイス (ワークマネージド)



AEワークプロフィール (コンテナ)



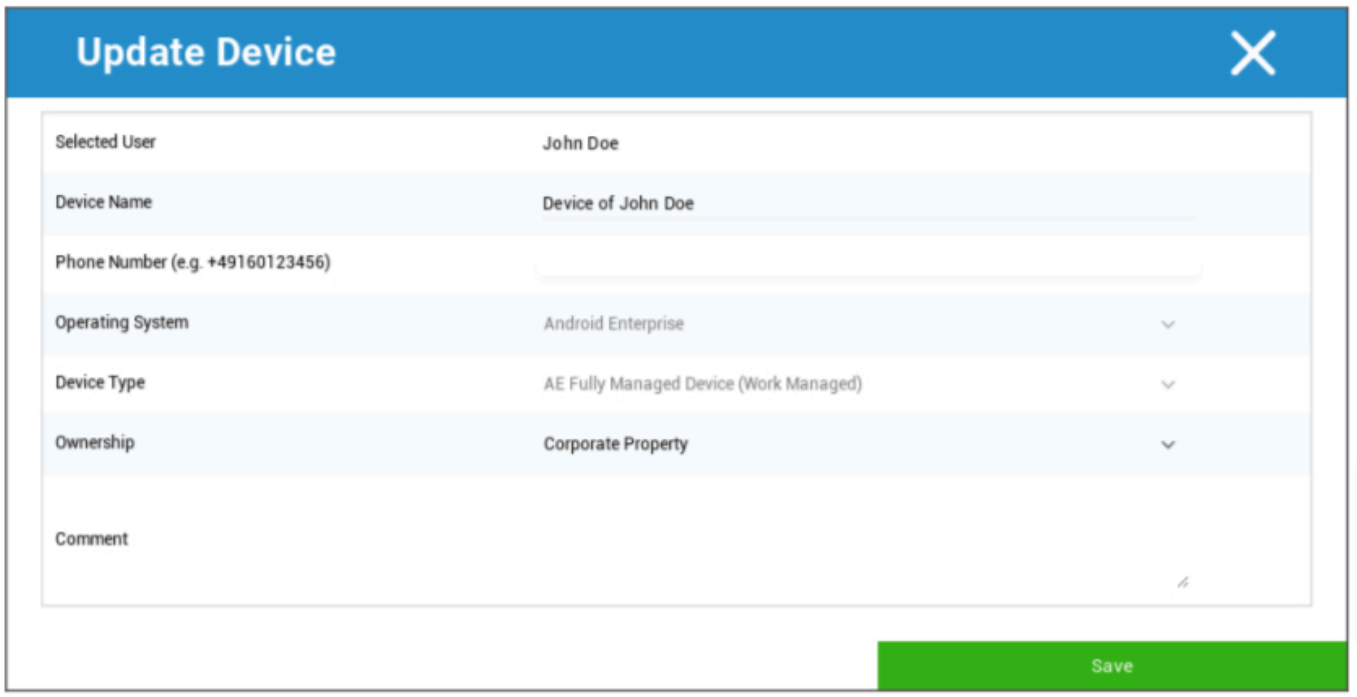
アンドロイド・フォン | タブレット



デバイスの編集	デバイス情報の編集
パスコードの設定	デバイスのパスコードを設定する
ロック装置	デバイスをロックする（ロック画面）
デバイスの削除	AppTecからデバイスを削除する
ワイプ装置	デバイスを工場出荷時の設定に戻す
エンタープライズ・ワイプ	AppTec360が提供する情報、アプリ、プロファイルは削除される（デバイスはMDMから切り離される）
MDMの削除	
メッセージを送る	プッシュ通知をデバイスに送信 メッセージはAppTec360アプリ（メッセージタブ）に表示されます。
TeamViewerリモートコントロール	TeamViewerを使用して、このデバイスのリモートコントロールセッションを開始します。
スプラッシュトップ・リモコン	Splashtop を使用して、このデバイスのリモートコントロールセッションを開始します。
COPEモードへの変換（AEフルマネージドデバイス（ワークマネージド）のみ）	このAEフルマネージド（ワークマネージド）デバイスにワークプロファイルを作成する
入会リクエストを送信	入団要請の送信（繰り返し
レガシーデバイスの移行（デバイスオーナーモードプロビジョニングを使用して登録されたAndroid携帯電話/タブレットのみ）	Android Phone / TabletプロファイルをAEフルマネージドデバイス（ワークマネージド）プロファイルに移行する

デバイスの編集

ここで様々なデバイス情報を更新することができます。



選択されたユーザー	デバイスユーザー
デバイス名	デバイス名
電話番号	デバイスの電話番号
オペレーティングシステム	アンドロイド・エンタープライズ アンドロイド
デバイス・タイプ	アンドロイド・エンタープライズ • AEフルマネージド・デバイス (ワークマネージド) • AEワークプロファイルモード (コンテナのみ) • ワークプロファイル (COPE) 付きAEフルマネージド・デバイス アンドロイドだ : • 電話 • タブレット
所有権	コーポレート = 企業財産

	従業員 = 従業員プロパティ
コメント	デバイスに関する補足説明

パスコードクリア

ここでは、選択したデバイスのパスコードを削除することができます。Androidのデフォルトでは、パスコードは "123456 "に設定されています。

ロック装置

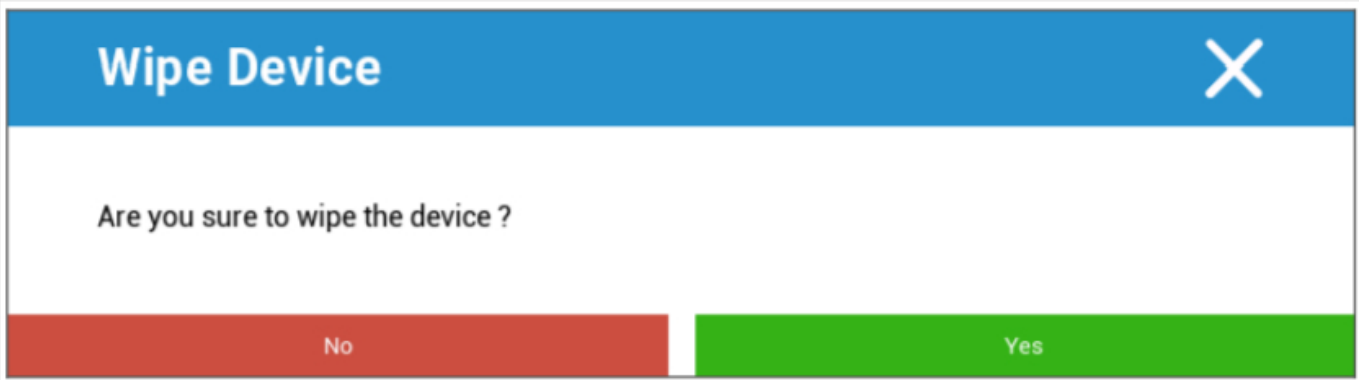
ここで、デバイスをロックするコマンドがデバイス (ロック画面) に送信されます。

デバイスの削除

ここで削除コマンドを実行できます。デバイスをAppTec360からのみ削除するか (「システムから削除」)、デバイスをAppTec360から削除し、さらに工場出荷時の設定に戻すか (「ワイプ＆削除」) を再度決定できます。

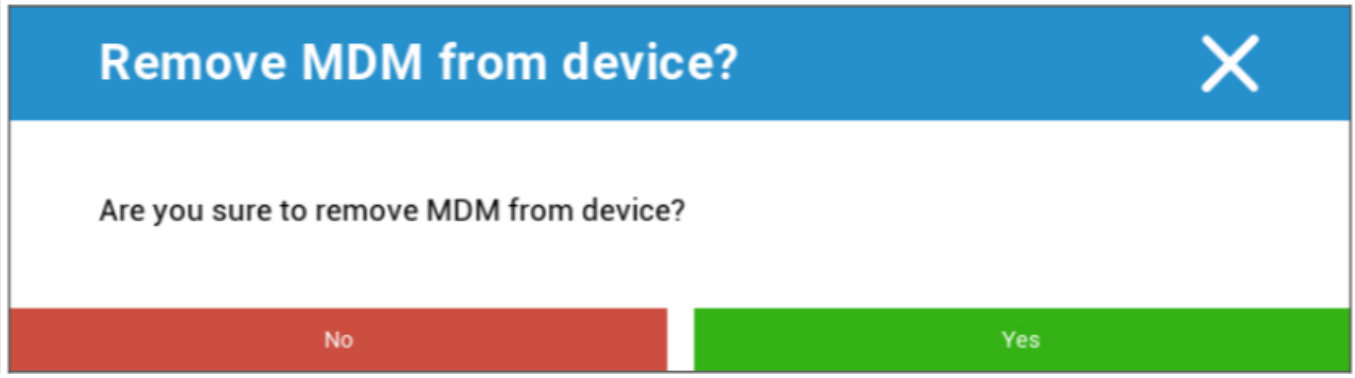
ワイプ装置

デバイスのワイプ」では、デバイスの完全なワイプを実行できます。その後、デバイスは工場出荷時の設定に復元されます。



さらに、デバイスにSDカードが含まれている場合は、SDカードを消去することができます。SDカードも消去しますか？"を "オン "に設定することで実現できます。

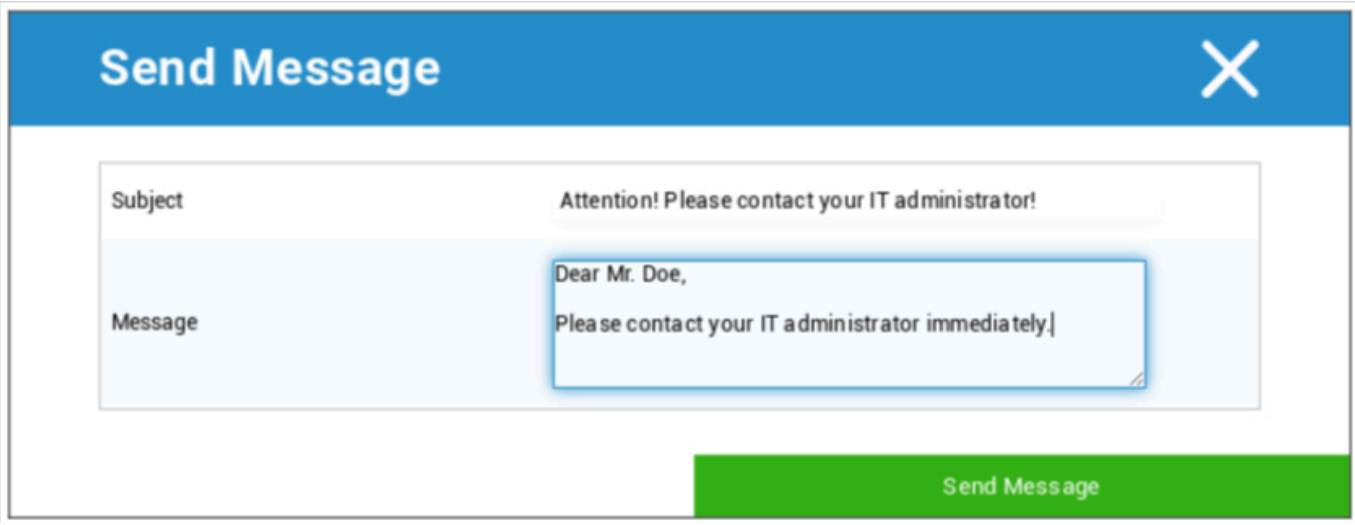
MDMの削除



これは、MDMから分離するために推奨される方法である。

AppTec360 によって提供された情報、アプリ、プロファイルのみが削除され、すべての企業データはエンドユーザー・デバイス上で利用できなくなる。しかし、プライベートな領域は影響を受けず、エンドユーザーのデバイスに残り続けます。

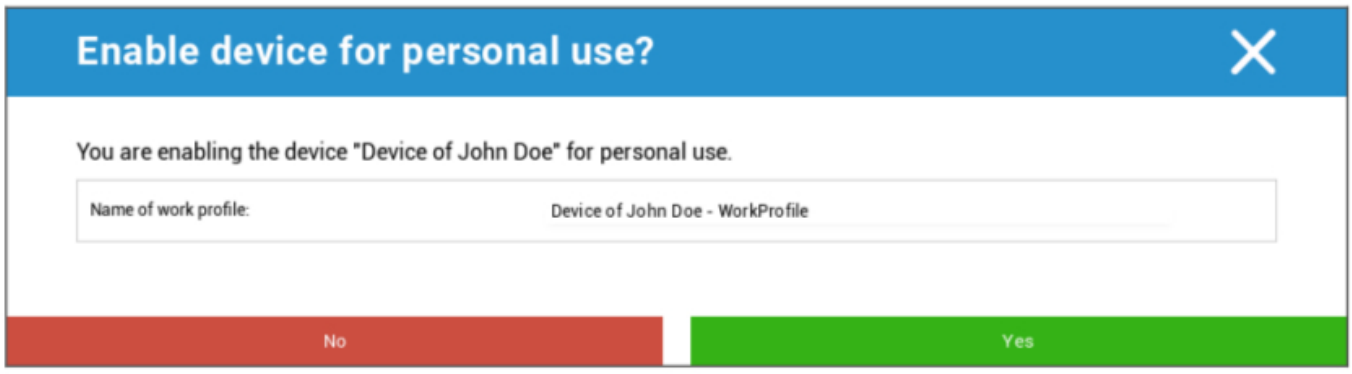
メッセージを送る



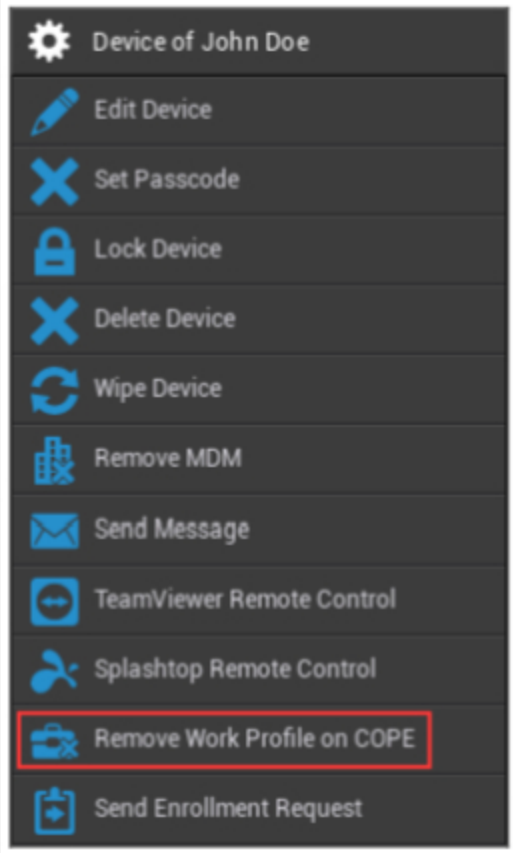
ここで、それぞれのエンドユーザーデバイスにプッシュ通知を送信することができます。

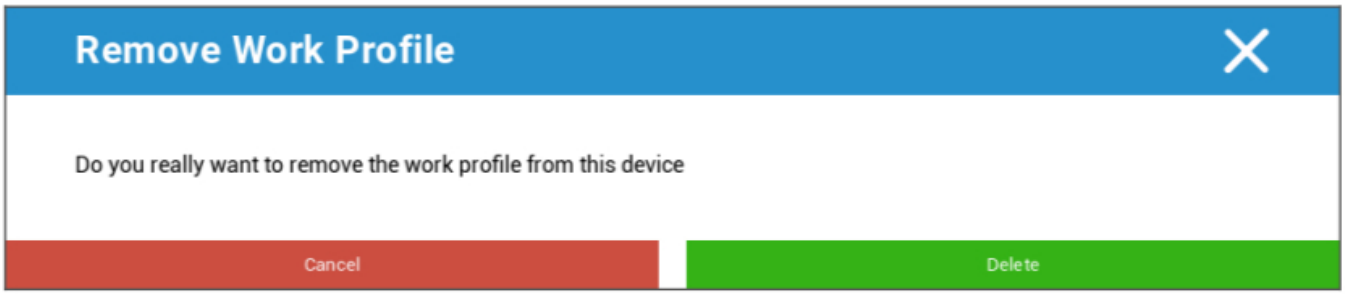
COPEモードに変換

このAEフルマネージド（ワークマネージド）デバイスにワークプロファイルを作成する



デバイスをCOPEモードに変換した後、歯車のオプション「**COPEのワークプロファイルを削除**」をクリックして、ワークプロファイルを削除することができます：




Remove Work Profile
Do you really want to remove the work profile from this device
Cancel
Delete

入会リクエストを送信

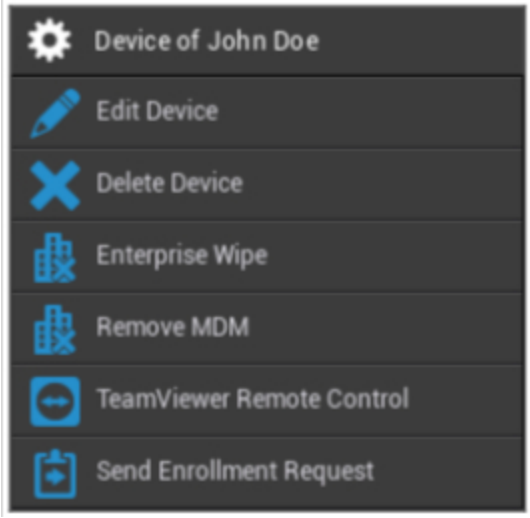
Send Enrollment Request" (登録リクエストの送信) により、それぞれのユーザーに登録リクエストを (再度) 送信することができます。

最新のEnrollment - Requestのみが有効であることにご注意ください。

レガシーデバイスの移行

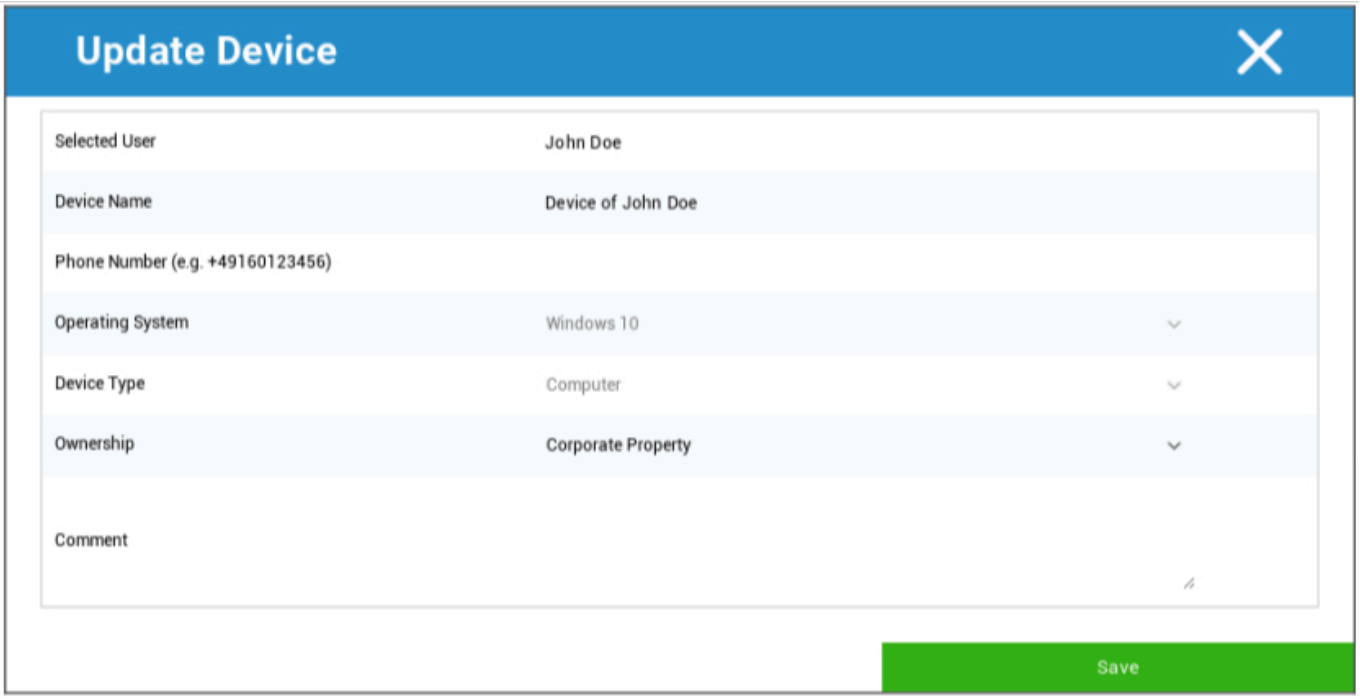
Android Phone / TabletプロファイルをAEフルマネージドデバイス (ワークマネージド) プロファイルに移行する

ウィンドウズ



デバイス名	選択したデバイスの名前
デバイスの編集	デバイスの編集
デバイスの削除	AppTecからデバイスを削除する
エンタープライズ・ワイプ	AppTec360が提供した情報、アプリ、プロフィールは削除されます。
MDMの削除	
TeamViewerリモートコントロール	TeamViewerでデバイスをリモートコントロール
入会リクエストを送信	入会リクエストを送信する（再度）

デバイスの編集

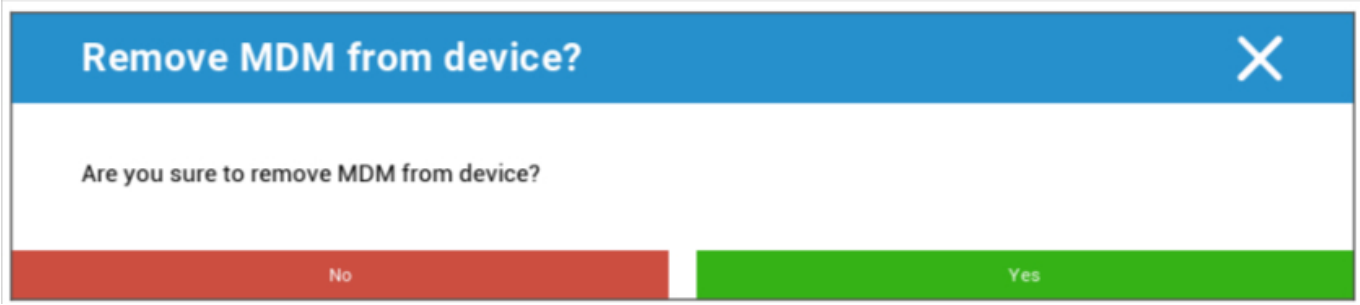


ここでは、デバイスの様々な情報を更新することができます。

デバイスの削除

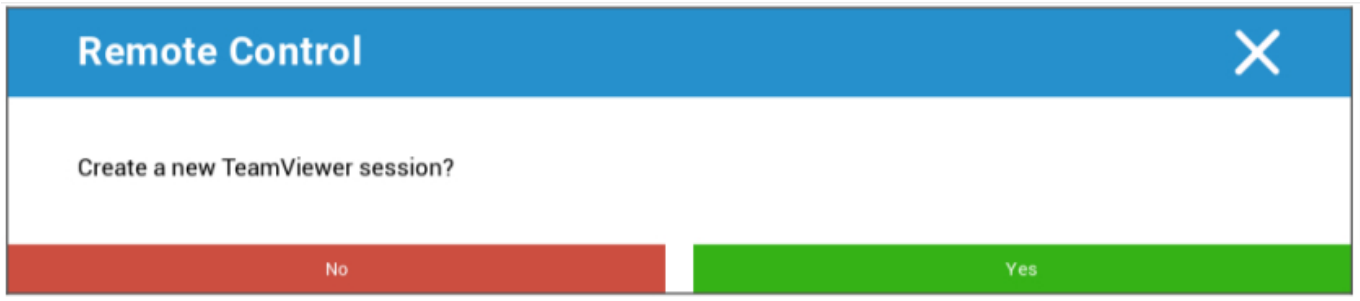
ここでは、AppTec360からデバイスのみを削除するdeleteコマンドを実行できる。

エンタープライズ・ワイプ | MDMの削除



AppTec360によって提供された情報、アプリ、プロファイルのみが削除されます。こうすることで、企業データはエンドユーザーデバイス上で利用できなくなります。プライベートエリアは影響を受けず、エンドユーザーデバイスに残り続けます。

TeamViewerリモートコントロール



このデバイスのTeamViewerリモートコントロールセッションを開始できます。

入会リクエストを送信

Send Enrollment Request"（登録リクエストの送信）により、それぞれのユーザーに登録リクエストを（再度）送信することができます。

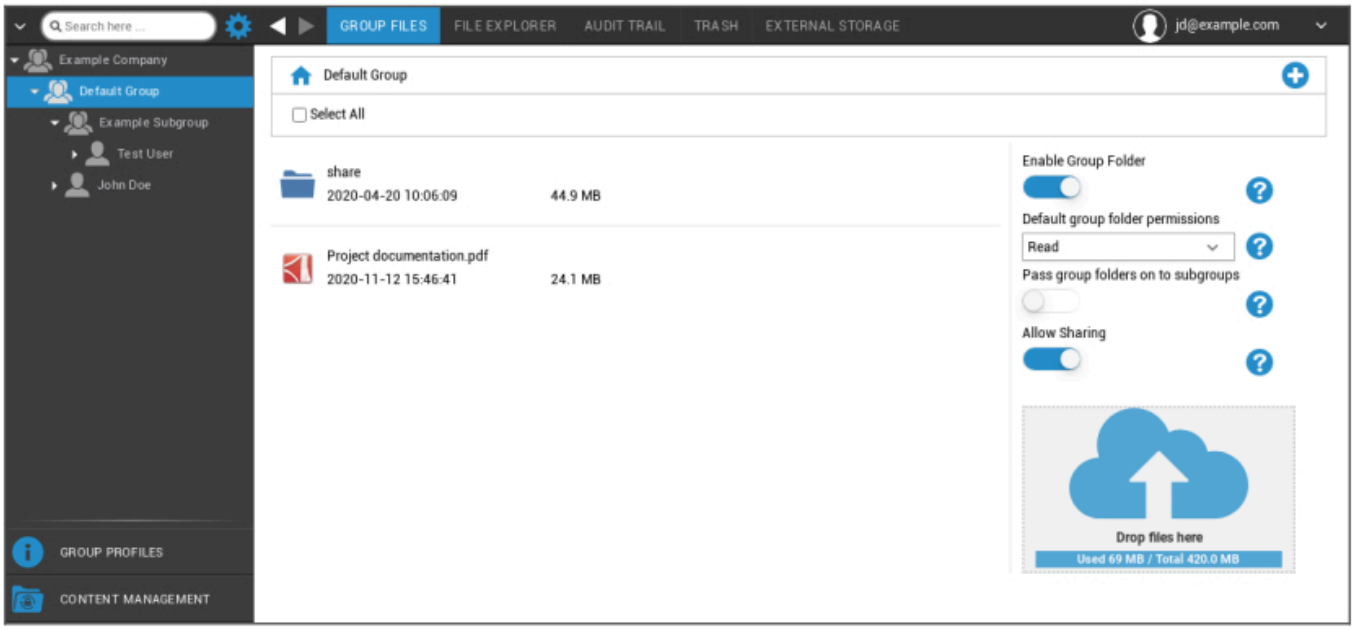
コンテンツ管理

グループ内では「コンテンツ管理」でAppTecのContentBoxを管理できます。

コンテンツボックスを使用すれば、ドキュメントやその他の企業データをエンドユーザーのデバイスに安全に配布することができます。

グループファイル

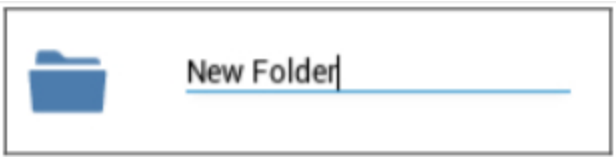
「グループファイル "はContentBoxの基本部分です。ここでは、設定、ドキュメントのアップロード、新しいフォルダの作成などを行います。



右上隅のシンボルで、"Add Folder "でそれぞれのグループに指定された新しいフォルダを作成することができます。

右上隅のシンボルで、"Add Folder"（フォルダーの追加）から新しいフォルダーを作成し、それぞれのグループに割り当てることができます。

フォルダ名は何でもいい。



Upload Files "からデータをアップロードできます。ここでStandard-Explorerが開きます。もちろん、この2つの操作はすべての（サブ）フォルダで実行できます。

左上のマークでメインメニューに戻ることができます。

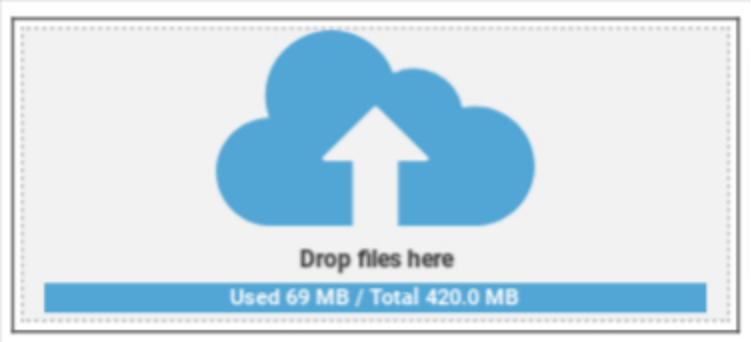
複数のフォルダやファイルを選択して「Download」でダウンロードしたり、「Delete」で消去することができる。

また、すべてのファイルとフォルダを選択して、「ダウンロード」と「削除」コマンドを実行することもできます。

フォルダやファイルの上にマウスを移動すると、次のような概要が表示されます：

- Rename "で、フォルダやファイルの名前を変更することができます。
- ダウンロード」で、フォルダ/ファイルをダウンロードすることができます。
- Delete "で、フォルダ/ファイルを削除できます。

グループフォルダーを有効にする	アクティブにすると、グループのメンバー全員がそれぞれのフォルダにアクセスできるようになります。
デフォルトのグループフォルダ権限	選択したグループのユーザーの権限： Read = 読み取りのみ許可 更新 = 更新許可 作成 = 作成許可 Delete = 削除許可
グループフォルダをサブグループに渡す	有効にすると、各サブグループは親データ・ファイルにアクセスできるようになる。
サブグループの権限	選択したサブグループのユーザーの権限： Read = 読み取りのみ許可 更新 = 更新許可 作成 = 作成許可 Delete = 削除許可
共有を許可する	有効にすると、ユーザーはリンク経由でファイルを共有できます。



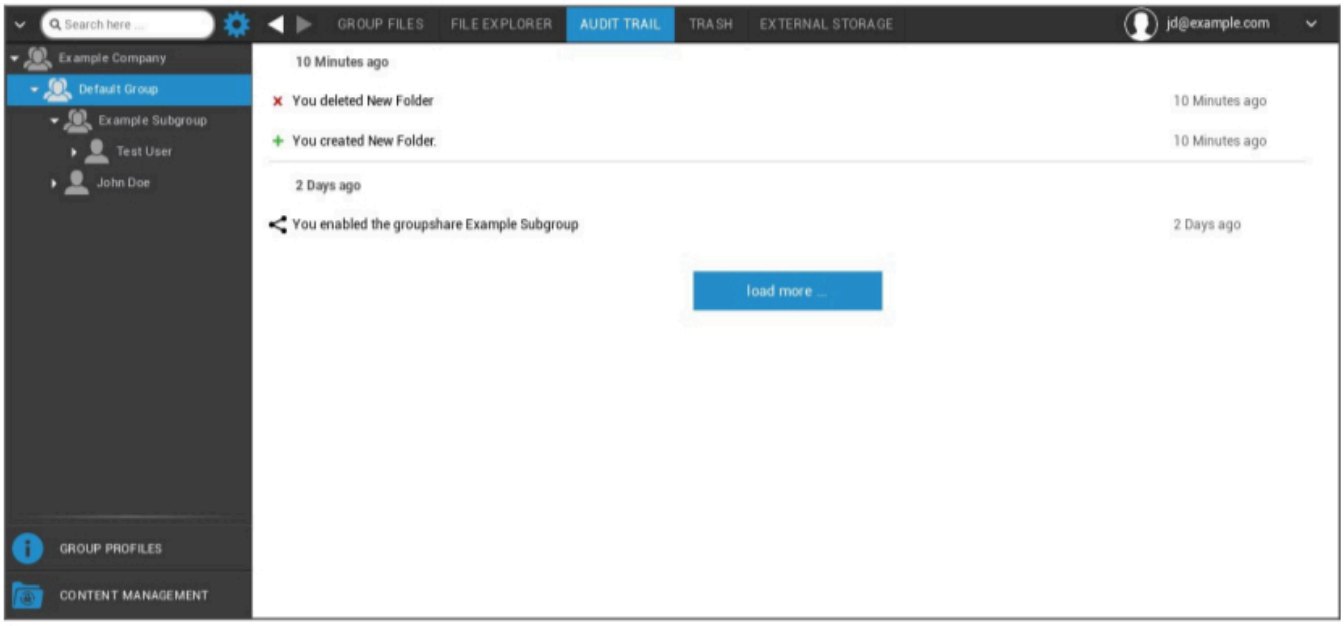
ファイルをアップロードするには、このフィールドを使用します。また、インターネットエクスプローラの助けを借りてファイルを選択してアップロードするために、このフィールドをクリックすることもできます。

ファイルエクスプローラー

ファイルエクスプローラー」を使えば、フォルダやファイルが保存されているグループに関係なく、すべてのフォルダやファイルを管理することができます。

グループファイル」で学んだ設定やボタンもあります。

監査証跡



監査証跡」では、どのユーザーが何を作成、削除、共有したかを履歴から確認することができます。これにより、企業データで何が行われたかをいつでも確認することができます。

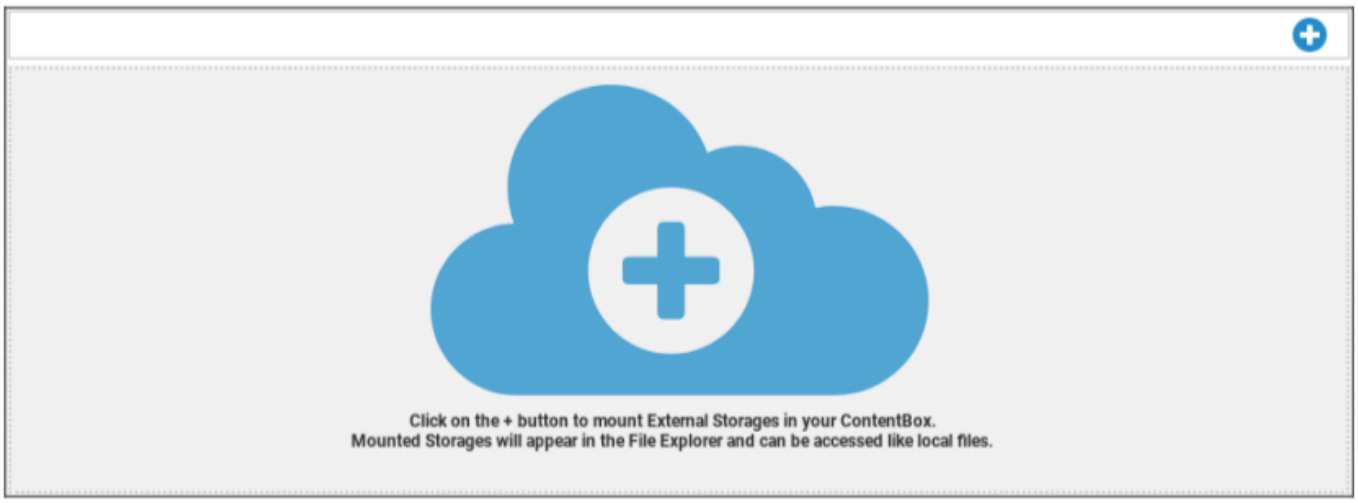
ゴミ

誤って）何かを削除してしまった場合、「ゴミ箱」の下にあるフォルダやファイルを確認し、希望に応じて復元することができます。

- Undelete" で、データ/フォルダを復元することができます。
- Delete "を使えば、データやフォルダを完全に削除することができます。

ゴミ箱で使用されているストレージ容量は、使用可能な "合計スペース "を減少させることに注意してください - これはownCloudの要件です。

外部ストレージ



外部ストレージ」では、外部ストレージを接続することができます。

このシンボルによって、（追加の）ストレージを追加することができる。

タイプ	Amazon S3、FTP、SFTP、ownCloud、WebDAV、Windows Share、SharePoint

アマゾンS3	
表示名	表示名
アクセスキー	アクセスキー
シークレット・キー	セキュリティ・キー
バケット	あなたに割り当てられたサブフォルダーの明確なID
ホスト名（オプション）	ホスト名（オプション）
ポート（オプション）	ポート（オプション）
地域	地域（オプション）
SSLを有効にする	SSLを有効にする
パススタイルを有効にする	あなたに割り当てられたクリアパスアドレス

ファイル転送プロトコル	
表示名	表示名
ホスト	ホストアドレス
ユーザー名	ユーザー名
パスワード	パスワード
ルート	メインメニュー
セキュア ftps://	

SFTP	
表示名	表示名
ホスト	ホストアドレス
ユーザー名	ユーザー名
パスワード	パスワード
ルート	メインメニュー

独自クラウド	
表示名	表示名
URL	ownCloudのURL
ユーザー名	ユーザー名
パスワード	パスワード
リモートサブフォルダ	標準フォルダ
セキュア https://	

ウェブダブリュー	
表示名	表示名
URL	WebDAV URL
ユーザー名	ユーザー名
パスワード	パスワード
ルート	メインメニュー
セキュア https://	
ウィンドウズ・シェア	Windows Shareは近日中に対応予定
シェアポイント	Microsoft SharePointのサポートは近日中に提供される予定です。

監査ログ

ここには、MDMコンソールで実行されたアクションに関する情報を記録するログがあります。

フィルターアイコンを使用すると、表示されたリストにフィルターを適用できます。

ドロップダウンメニュー「**Items per page（1ページあたりのアイテム数）**」で、リストの1ページに表示するアイテムの数を選択できます。

実施された措置 / 設定変更	行われた処置 / 変更された設定
価値	実行されたアクション/変更された設定の値
ユーザー	アクションを実行した/設定を変更したユーザー名
日付	このアクションが実行された/この設定が変更されたタイムスタンプ
パス / タイプ	このアクションが実行された/この設定が変更された場所へのパス

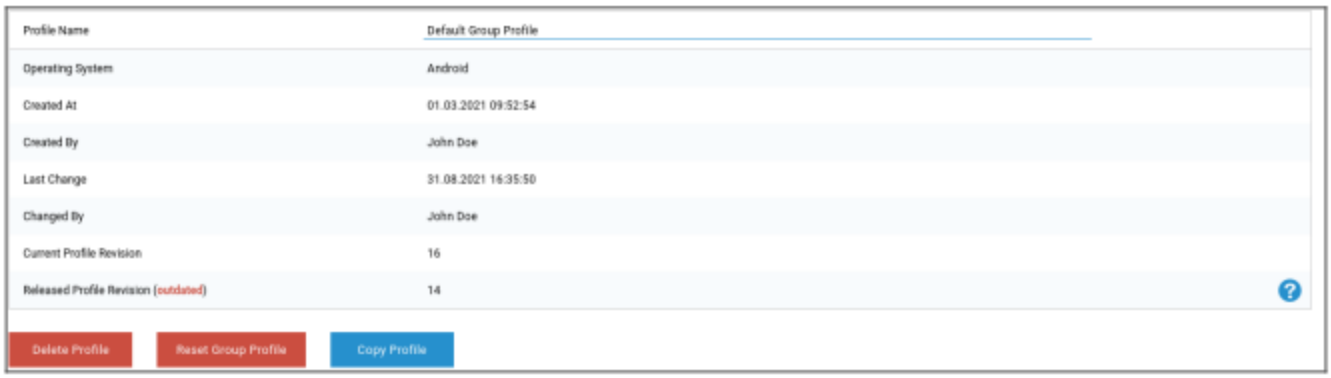
iOSの設定

一般

現在選択しているのがグループなのかデバイスなのかによって、表示とそのサブポイントが異なります！

グループプロフィールの概要（グループレベルのみ）

グループプロフィールを開くと、プロフィールの概要が表示されます。



プロフィール名	プロフィールの名前（ここで変更可能）
オペレーティングシステム	対象OS
作成日時	創造の時
作成者	プロフィールの作成者
最後の変更	プロフィールの最終変更時刻
変更履歴	最後の変更を行ったアカウント
現在のプロフィール改訂	保存されたプロファイル状態の修正
プロフィール改訂版をリリース	割り当てられたプロファイルのリビジョン（"Assign now"）。ラベルのテキストの後ろに"(outdated) "と表示されている場合は、プロファイルを保存したものの、まだ割り当てていないことを意味します。

一般情報

デバイスに直接アクセスすると、選択したデバイスの簡単な概要が表示されます。

デバイス名	デバイス名
電話番号	デバイスの電話番号
モデル	モデル番号
オペレーティングシステム	OS
シリアル番号	デバイスのシリアル番号
デバイスの所有権	企業用または個人用デバイス コーポレート = 企業用デバイス 従業員 = プライベート・デバイス
デバイス・タイプ	デバイスの種類 (タブレットまたは電話)
脱獄	デバイスにJailbreakがある場合
監督	このデバイスが監視対象かどうかを示す
準拠	ガイドラインに違反した場合
ラストシーン	デバイスが最後にAppTec360 Serverと通信したときのステータス

設定

これらの設定には、デバイス名と定義済みの背景が含まれます。

デバイス名をシステム名に	AppTec360 Console（左の階層構造）で発行される名前は、それぞれのエンドユーザーデバイスと同じになります（デバイスの設定で確認できます）。
カスタム壁紙を使用する（管理下のデバイスのみ）	ここでは、エンドユーザーデバイスに表示される背景を事前に定義することができます。 監視モードでのみ使用可能！
OSの自動アップデート	利用可能であれば、OSのアップデートを強制する。監視モードのDEPデバイスのみ。
カスタムフォント	ここでカスタムフォントを追加できます。
名称	オプション。ユーザーから見えるフォントの名前。このフィールドは、インストール後に実際のフォント名に置き換えられます。
フォント	フォントファイル（.otfまたは.ttf）をアップロードします。

コンフィグ改訂

ここで、どのグループプロファイルがデバイスに指定されているかの概要が表示されます。

グループプロフィールをクリックすると、そのプロフィールに直接アクセスし、設定を行うことができます。

このマークがあれば、割り当てられたアプリをグループプロファイルの設定に戻すことができます。

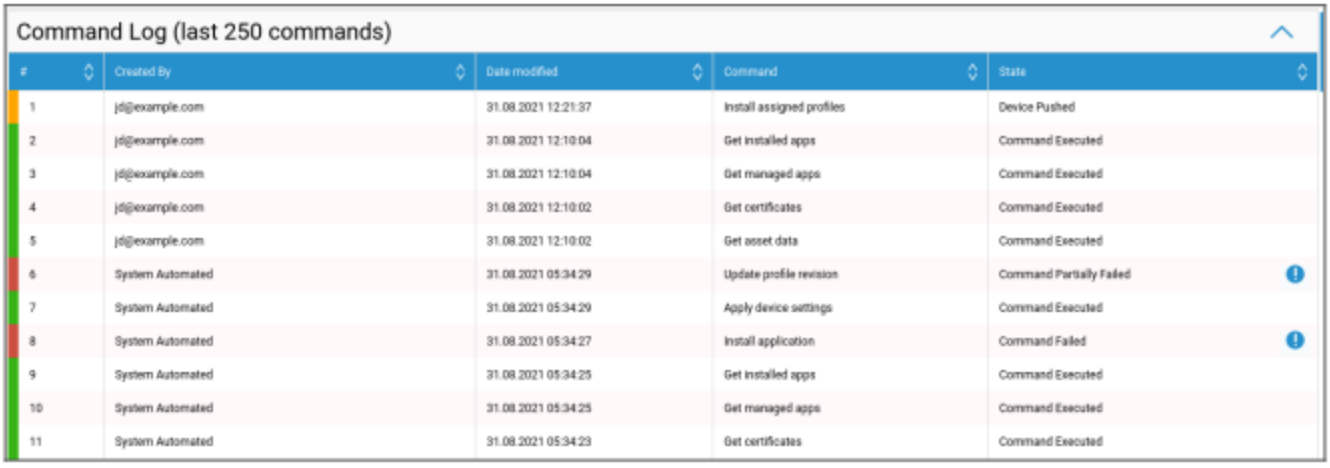
この記号を使えば、デバイスのプロファイルをリセットして、設定を一切なしにすることができる。

"Newer Revision available "は、グループプロファイルが変更され保存されたが、割り当てられていないことを示します。グループプロファイルの変更をデバイスに適用するには、グループレベルで "Assign now "を使用してグループプロファイルを割り当てる必要があります。

デバイスログ（デバイスレベルのみ）

コマンドログ

ここでは、デバイスに対して発行されたコマンドとそのステータスを確認することができます。



System Automated」によって作成されたコマンドは、システムによって自動的に作成される。

可能なコマンドステータス

デバイスが押される	プッシュリクエストは、EMM サーバーに接続するようデバイスに指示するため、プッシュサービス (APNS など) に送信されました。
コマンド作成	コマンドがシステム内に作成された。
コマンド送信	コマンドは、サーバーに接続された後、デバイスに送信された。
コマンド実行	コマンドは正常に実行された。
コマンド失敗	コマンドが失敗しました。*
コマンド一部失敗	デバイスのOSによっては、いくつかのコマンドがグループ化されることがある。 このコマンドグループの一部は失敗した。*
コマンドは実行されたが、最終的に失敗	コマンドは実行されたが、もしかしたら実行されていなかったかもしれない。
コマンド・リパッシュ	コマンドはユーザーによってリプッシュされた。
廃棄	コマンドが破棄された。例えば、他のコマンドに取って代わられたとか、デバイスが再登録されて古いコマンドが削除されたとか。

メッセージの後ろにエクスクラメーションマークが表示されている場合は、カーソルをアイコンの上に置くと詳細情報を得ることができます。

資産管理 (デバイスレベルのみ)

資産管理 (デバイスレベルのみ)

デバイス情報

モデル	機器の型番
オペレーティングシステム	OS
OSバージョン	OSバージョン
シリアル番号	シリアル番号
ユーディーアイディー	デバイスUDID
デバイス名	デバイス名
監督	デバイスが監視されているかどうかを表示します。
バッテリーの状態	バッテリーの状態

Wi-Fi

IPアドレス	デバイスIPアドレス
WiFi MAC	WiFiのMACアドレス

セルラー

ステータス	ステータス（SIMカードあり）
電話番号	電話番号
ローミング状況	現在のローミング状況
ローミング（音声/データ）	音声/データのローミング状況
IPアドレス	IPアドレス
IMEI	IMEI番号
オペレーター/キャリア	携帯電話サービスプロバイダー
SIMキャリアネットワーク	SIMキャリアのネットワーク
キャリア版	キャリア版
モデム・ファームウェア	モデムファームウェア
現在のMCC/MNC	SIM MCC/MNC」を参照。
SIM MCC/MNC	モバイル国コードは、E.212標準に従ってITUによって確立された国識別であり、モバイルネットワークコード（MNC）と組み合わせて、携帯電話ネットワーク（=国コード）を識別するために使用されます。 そのため、別の携帯電話ネットワークに入った場合、「現在のMCC/MNC」と「SIM MCC/MNC」は異なります。

ブルートゥース

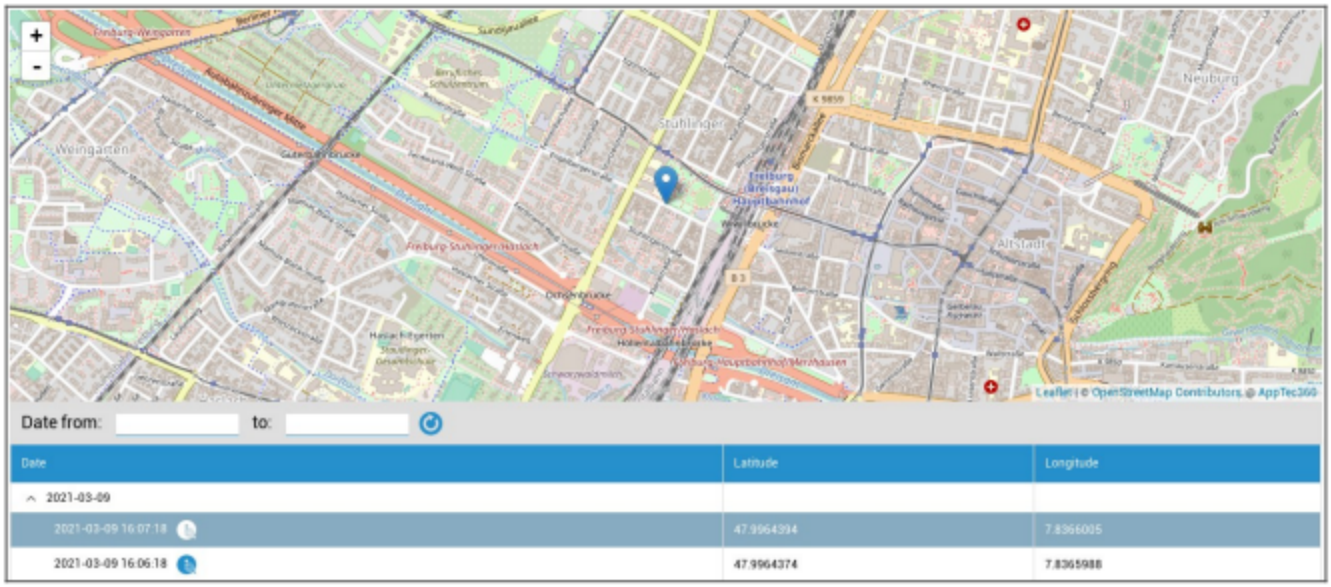
ブルートゥースMAC	ブルートゥースMACアドレス

セキュリティ管理

盗難防止（デバイスレベルのみ）

GPS情報（デバイスレベルのみ）

ここでは、デバイスの現在/最終位置を評価することができます。ローカライズは1つまたは2つのパスワードで保護することができます：一般設定 - プライバシー - GPSアクセス



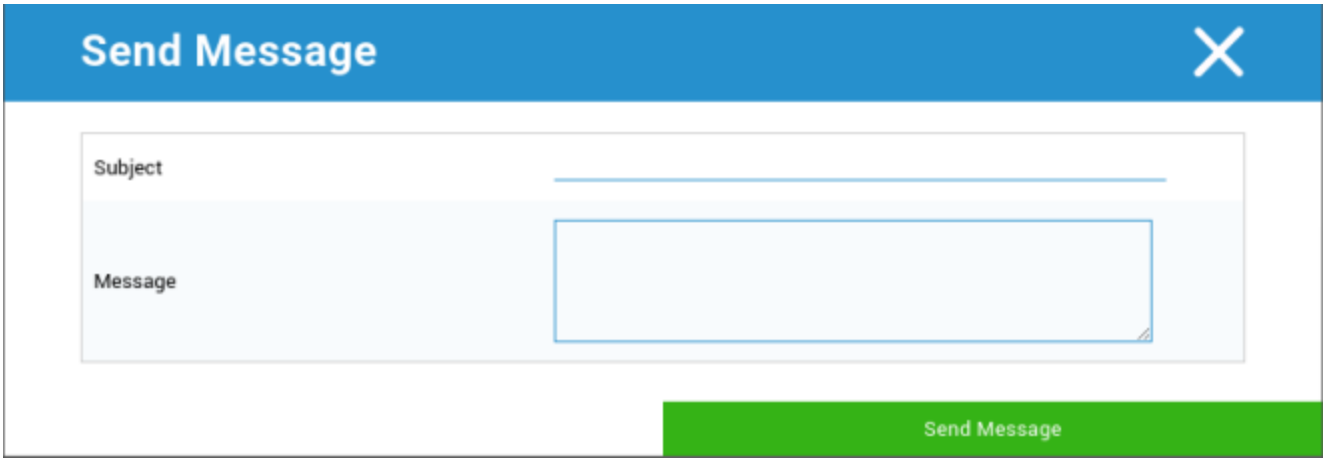
ワイプ＆ロック（デバイスレベルのみ）

ワイプ＆ロック」では、以下の3つのアクションを実行できます：

フルワイプ	デバイスを工場出荷時の設定に戻す（企業および個人データは削除される）
エンタープライズ・ワイプ	エンドユーザーデバイスから企業データのみを削除（AppTecが提供したすべてのアプリ、データなど）
ロック画面	スクリーンロックが有効になっている場合、デバイスパスワード/PINでデバイスのロックを解除すれば十分です。
フォレンジック・ロックダウン（監視下デバイスのみ）	この機能を  のシンボルで有効にすると、デバイスがロックされ、閉じることができないメッセージが表示されます。従業員はデバイスのロックを解除することもできません。 管理者だけが、コンソールでロック解除マーク（  ）を使ってデバイスのロックを解除できます。
アクティベーションロックの許可（監視下デバイスのみ）	この機能が有効になっている場合、iCloudの設定で「iPhoneを探す」が有効になると同時に、デバイスはロックされます。

メッセージ (デバイスレベルのみ)

次のウィンドウで、件名とメッセージを入力し、エンドユーザーデバイスに送信することができます：



セキュリティ設定

パスコード

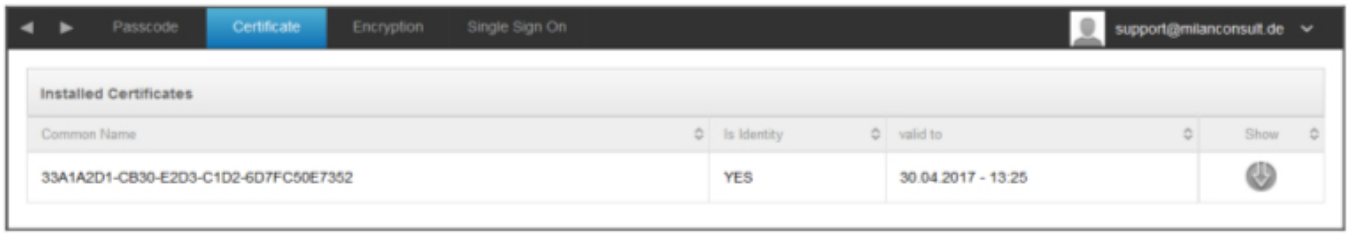
ここでは、デバイスのパスワードの設定を行います。

コードの無効化が許可される	この設定を有効にすると、パスワード入力のプロンプトは表示されません。 パスワードが確立されると、それを無効にすることはできない。
シンプルな値	ユーザーが同じ、エスカレーション、縮小番号文字列（例：1234、1111）を使用できるようにする。
英数字が必要	パスワードには少なくとも1文字が含まれていなければならない
最小パスコード長	パスワードの最小長
複雑な文字の最小数	パスワードに含まれる英数字記号の最小数
最大パスコード年齢	パスワードを変更しなければならない日数
最大オートロック	デバイスがロックされる最大時間
デバイス・ロックの最大猶予期間	その後、デバイスはロックされたスタンバイ状態に入ります。
最大失敗回数	デバイスの完全消去が実行されるまでに、パスワードが誤って入力される頻度を設定します。
最大パスコード日数（1～730日）	最大パスワード年齢
パスコード履歴（1～50個）	この番号以降、古いパスワードの使用が許可されます。

ゴミ箱をクリックすると、パスワードリセットダイアログが開き、忘れたデバイスのパスワードを消去することができます。

証明書（デバイスレベルのみ）

デバイスで利用可能な証明書を表示します。


Passcode
Certificate
Encryption
Single Sign On
support@mlianconsult.de
Installed Certificates
Common Name
Is Identity
valid to
Show
33A1A2D1-CB30-E2D3-C1D2-6D7FC50E7352
YES
30.04.2017 - 13:25

暗号化

ストレージの暗号化が必要	インストールされたデバイスの暗号化機能を有効にする

シングルサインオン

シングルサインオン」では、Kerberos認証を設定することができます。

ここでは、Kerberosトークンの使用を許可するアクセス認証情報とそれぞれのURL/アプリを設定します。

監視付きモードで使用可能	
口座名	口座名
代表者名	Kerberosチケットの配布先となる一意のID
領域	使用するKerberosレルム（例：ドメイン）

シンボルを使えば、さらにURLを追加することができる。

このアカウントを制限するために使用されるURLパターン	Kerberosチケットの配布先URLは未定です。

シンボルを使えば、追加のアプリを立ち上げることができる。

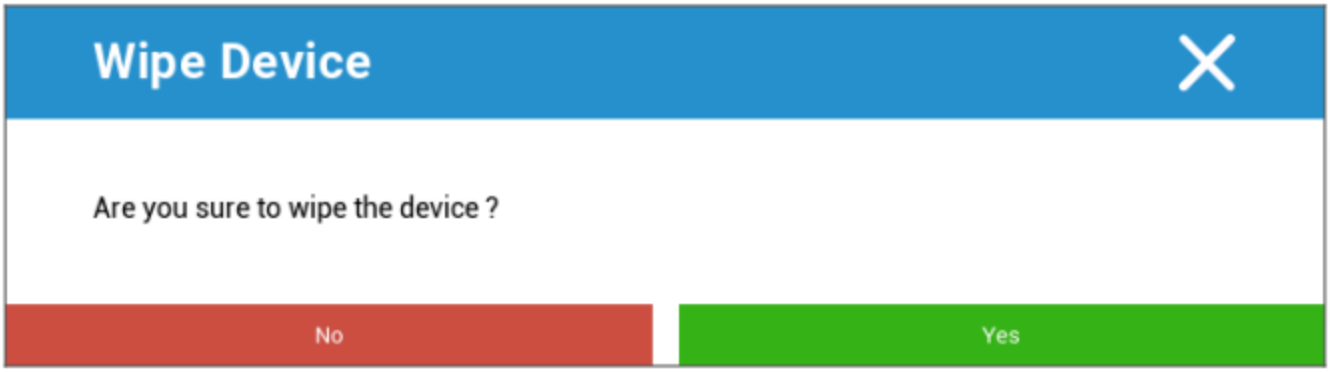
このアカウントを制限するアプリ	未定 Kerberosチケットの配布先となるアプリ

エンド・オブ・ライフ (デバイス・レベルのみ)

ワイプ (デバイスレベルのみ)

ワイプ」では、デバイスを工場出荷時の設定に戻すことができる。ここで、企業や個人データはエンドユーザーのデバイスから削除されます。

マイナス記号」をクリックすると、次のようなメッセージが表示されます。



はい」でワイプを実行できる。

Wipe Report "の下に以下の項目が表示される。

で拭いた。	誰がワイプを行ったかの履歴
日付	日付
ステータス	ステータス (ワイプが正常に実行された場合など)

制限の設定

デバイスの機能

ここでは、個々のエンドユーザーデバイスの機能をブロックすることができます。

アプリのインストールを許可する	アプリのインストールを許可する
カメラを許可する	カメラの使用を許可する
FaceTimeを許可する	FaceTimeを許可する
スクリーンキャプチャを許可する	スクリーンキャプチャを許可する
ローミング中の自動同期を許可する	ローミング中の自動同期を許可する
Siriを許可する	Siriを許可する
音声ダイヤルを許可する	音声ダイヤルを許可する
アプリ内課金を許可する	アプリ内課金を許可する
すべての購入にiTunes Storeのパスワードが必要	すべての購入にiTunes Storeのパスワードが必要
マルチプレイヤーゲームの許可	マルチプレイヤーゲームの許可
Game Centerフレンドの追加を許可する	Game Centerフレンドの追加を許可する
マネージドからアンマネージドへのオープンを許可	非管理アプリで管理アプリのコンテンツを開けるようにする
アンマネージドからマネージドへのオープンを許可	非管理アプリのコンテンツを管理アプリで開けるようにする
ロック画面で今日の表示を許可する	この設定が有効な場合、ロック画面の通知センターに「Today」ビューが表示されます。
ロック画面でコントロールセンターを許可する	ロック画面でコントロールセンターを許可する
TouchIDを許可する	TouchIDを許可する
PKI の無線アップデートを許可する	PKI の無線アップデートを許可する

ロック中の通帳を許可する	デバイスがロックされている間、通帳を許可する
広告のトラッキングを制限する	これらの機能は、広告トラッキングを無効にします（例：広告主は、パーソナライズされた広告を配信するために広告トラッキングを使用できません）。
ハンドオフを許可する	ハンドオフを許可する
インターネットの結果をスポットライトで表示	スポットライトにインターネットの結果を表示する（例：BingやWikipedia）
最初のAirPlayペアリングでパスコードを要求する	最初のAirPlayペアリングでパスコードを要求する
フォース・ウォッチ・リスト・プロテクション	有効にすると、Apple Watchは強制的に「リストプロテクション」（手首認識）を使用するようになる
iCloudフォトライブラリを許可する	iCloudフォトライブラリを許可します。許可しない場合、iCloudから完全にダウンロードされなかったすべての写真は、ローカルストレージ上で消去されます。
監視付きモードで使用可能	
アカウントの変更を許可する	メール、連絡先、カレンダー」の変更を許可する
AirDropを許可する	AirDropを許可する
アプリの携帯電話の変更を許可する	この設定は、モバイルデータの使用を許可するアプリの設定をブロックします。 この設定は、例えば、エンドユーザーデバイス上で手動で設定することができ、その後、この制限を有効にすることができます。
Siriがウェブからユーザーが作成したコンテンツを照会できるようにする	特定のウェブサイトでのウェブ検索がブロックされている（例：ウィキペディア）。
Siriの冒涜フィルタを有効にする	Siriに向けられた冒涜的な言葉は検閲される
iBook Storeを許可する	iBook Storeを許可する
iBook Storeエロティカを許可する	iBook Storeエロティカを許可する
友達を探す」設定の変更を許可する	友達を探す」設定の変更を許可する
ゲームセンターを許可する	ゲームセンターを許可する
ホストのペアリングを許可する	コントロールコンピューターのペアリング

構成プロファイルのインストールを許可する	構成プロファイルのインストールを許可する
アプリの削除を許可する	コントロールアプリの削除
iMessageを許可する	iMessageを許可する
すべてのコンテンツと設定の消去を許可する	すべてのコンテンツと設定の消去を許可する
制限の設定を許可する	制限の設定を許可する
ポッドキャストを許可する	ポッドキャストを許可する
定義検索を許可する	定義検索を許可する
予測キーボードを許可する	予測キーボードを許可する
自動補正を許可する	自動修正を許可する
UIアプリのインストールを許可する	非アクティブにすると、AppStoreからアプリをインストールできなくなります（アイコンが表示されなくなります）。ただし、iTunesやConfigurator経由でアプリをインストールすることは可能です。
キーボードショートカットを許可する	物理的なキーボードにデバイスが接続されている場合、キーボードショートカットを許可する。
Apple Watchのペアリングを許可する	デバイスとApple Watchのペアリングを禁止し、既存の接続は終了します。
パスコードの変更を許可する	許可されていない場合、デバイスパスワードの追加、変更、削除はできません。
デバイス名の変更を許可する	デバイス名を変更できるかどうかのガイドライン
壁紙の変更を許可する	壁紙の変更が可能かどうかの判断基準
アプリの自動ダウンロードを許可する	無効化すると、購入したアプリは他のデバイスに自動的にインストールされません。既存アプリのアップデートには適用されません。
ニュース	iOSデバイスでニュースを許可する
エンタープライズアプリの信頼を許可する	Falseに設定すると、企業アプリを信頼できなくなる。

iCloud

iCloudペアリング中に特定の機能をブロックする

バックアップを許可する	バックアップを許可する
ドキュメントの同期を許可する	ドキュメントの同期を許可する
フォトストリームを許可する	フォトストリームを許可する
共有フォトストリームを許可する	共有フォトストリームを許可する
クラウド・キーチェーンの同期を許可する	クラウド・キーチェーンの同期を許可する
管理対象アプリにデータ保存を許可する	管理対象アプリにデータ保存を許可する
エンタープライズ・ブックでノートとハイライトの同期を許可する	エンタープライズブックでノートとハイライトの同期を許可する
企業ブックのバックアップを許可する	企業ブックのバックアップを許可する

セキュリティとプライバシー

診断データに関連するこれらの機能をブロックする

診断データをアップルに送信できるようにする	診断データをアップルに送信できるようにする
信頼できないTLS証明書の受け入れを許可する	信頼できないTLS証明書を受け入れることをユーザーに許可する。
強制暗号化バックアップ	強制暗号化バックアップ

BYOD

ビルトインiOSセキュリティ（コンテナ）

iOSは常に、マネージド（ビジネス）とアンマネージド（プライベート）を区別することができた。MDMシステムから来たものはすべてマネージドとして扱われる。例えば、MDM経由でアプリをインストールしたり、Exchangeアカウントを設定したりすると、iOSはこれを管理対象として扱う。

デバイスに手動で設定/インストールされたものは全て非管理対象として扱われます。例えば、ユーザーが独自に WhatsApp をインストールした場合や、Exchange アカウントを追加した場合などです。しかしこの分離が連絡先に影響を与えることはありませんでした。しかしiOS 11.3以降、連絡先にも適用されるようになりました。

これはオペレーティング・システムの基本機能なので、何かをインストールしたり、特別なコンテナをセットアップしたりする必要はない。

プライベートとビジネスのアプリ/情報/ファイルを分離する内蔵機能を有効にします。この設定により、他の機能も無効になり、誤ってこの分離の一部をオフにする可能性があります。

アクティベーション

AppTec360がサポートするコンテナソリューションを有効にする

グーグル・ディバイド・コンテナを有効にする	グーグル・ディバイド・コンテナを有効にする
SecurePIMコンテナを有効にする	SecurePIMコンテナを有効にする

SecurePIM コンテナをアクティベートしている場合は、「アクティベート」の下に以下のポイントも表示されます。さらに、以下の4つのタブがすぐに開きます。

サポートメールアドレス	ユーザーが問題を解決するためのサポートメールアドレス

SecurePIM パスワード

SecurePIM パスワード」では、パスワードのセキュリティ強度のガイドラインを設定できます。

セッションタイムアウト	ここで、SecurePIM がバックグラウンドで実行された後、何分後に新しいパスワードを再入力しなければならないかを設定できます。
パスワードの長さ	SecurePIM コンテナにアクセスするためのパスワードの長さ
大文字	最小の大文字
小文字	最小の小文字
特殊文字	最小限の特殊文字
数字	最小桁数
拭き取りアプリケーション	SecurePIM コンテンツが削除されるまでにパスワードを誤って入力できる回数 (ただし、アプリはエンドユーザーのデバイスに残ります。)

SecurePIMセキュリティ

SecurePIMセキュリティ」では、さまざまなセキュリティ設定を行うことができます。

ジェイルブレイクしたデバイスを検出する	この設定を有効にすると、デバイスがジェイルブレイクされていると検出された時点で、SecurePIM コンテナへのアクセスがブロックされます。
安全なテキストフィールド	投稿欄の内容は暗号化され、OS (iOS) には情報が届かない 注：この設定が有効である限り、オートコレクトは使用できません。
連絡先データをデバイスにエクスポート	この設定を有効にすると、ユーザーは Exchange 連絡先をローカルデバイスにエクスポートできます。 注：名前と電話番号のみがエクスポートされます。
イベント会場	この設定を有効にすると、通知バーに今後のイベントの場所が表示されます。
イベントタイトルを表示	この設定を有効にすると、通知バーに近日開催予定のイベントのタイトルが表示されます。

SecurePIMブラウザ

ここでは、SecurePIM のブラウザを設定できます。

このシンボルを使えば、新しいURLを定義することができる。

このシンボルを使えば、定義したURLを再び削除することができる。

「ホワイトリストのURL」とは、読み込むことができるURLのこと。

「ブラックリストに掲載されたURL」とは、読み込むことができず、ブロックされたURLのことである。

ホワイトリストのエントリーはブラックリストのエントリーより優先順位が高いことに注意してください。ブックマークタイトル」では、タイトルを発行することができます。ブックマークURL」では、ブックマークタイトルにURLアドレスを関連付けることができます。

交換

Exchange」では、Exchange アカウントを設定することができます。

ActiveSyncメールアドレス	交換用メールアドレス（「プレースホルダー」に注意）
ActiveSync Exchangeログイン	ユーザー名を交換する（「プレースホルダー」に注意）
Exchangeサーバー	Exchangeサーバーのアドレス（FQDN）
ActiveSync Exchangeドメイン	Exchange ドメインアドレス
ユーザー証明書	ユーザー証明書
証明書ベースの認証	利用者が証明書を用いて自分自身を認証する
S/MIME暗号化を許可する	ユーザーがメールを暗号化できるようにする
S/MIME署名を許可する	ユーザーが自分のメールに署名できるようにする
CRLチェック	アクティブな場合、プライベート証明書はCRL（証明書失効リスト）と比較される。

コネクション管理

Wi-Fi

サービスセット識別子（SSID）	接続するネットワークのSSID
オートジョイン	ネットワーク参加時に自動参加を有効にする
隠しネットワーク	APがSSIDをブロードキャストしない場合は、アクティブにする。

プロキシの設定

アクセスポイントごとのプロキシ設定

なし	代理人を立てない
マニュアル	手動プロキシの確立
プロキシサーバーURL	プロキシ設定にアクセスするためのアドレス
ポート	プロキシのポートを設定する
認証	プロキシで認証するためのユーザ名
パスワード	プロキシ認証用パスワード
自動	自動的にプロキシを確立する
プロキシサーバーURL	プロキシ設定にアクセスするためのURL

セキュリティ・タイプ

APのセキュリティ・タイプを確立する

ウェップ	
パスワード	APのパスワード

WPA/WPA2	
パスワード	APのパスワード

WEPエンタープライズ - WPA / WPA2エンタープライズ - エニーエンタープライズ		
プロトコル		
TLS	アクティブ/非アクティブ	
TTLS	アクティブ/非アクティブ	
リープ	アクティブ/非アクティブ	
ピーエーピー	アクティブ/非アクティブ	
EAP-FAST	アクティブ/非アクティブ	
EAP-SIM	アクティブ/非アクティブ	
PAC使用		PAC（保護されたアクセス制御）の使用
提供PAC	提供PACの構成	
匿名でのPAC提供	PACの匿名提供	
内部認証	使用すべき認証プロトコル： PAP、CHAP、MSCHAP、 MSCHAPv2	
ユーザー名	認証ユーザー名	
接続ごとのパスワードを使用しない	接続ごとのパスワードを使用しない	
身分証明書	認証証明書のアップロード/選択	
アウター・アイデンティティー	外から見えるアイデンティティ	
信頼		
信頼できる証明書 1	最初の信頼できる証明書をアップロードする	
信頼できる証明書 2	2つ目の信頼できる証明書をアップロードする	
信頼できる証明書 3	信頼できる第3の証明書をアップロードする	
信頼できるサーバー証明書の名前	想定されるサーバー証明書の名前(カンマ区切りリスト)	

なし	セキュリティを確立しない

かそうへいいきもう

接続名	VPNプロファイル名

VPNタイプ

かそうへいいきもう

デバイスのネットワーク・トラフィックはすべて、VPN接続を介してルーティングされる。

接続タイプ	VPN接続タイプを確立する
IPsec（シスコ）	シスコのIPsecプロトコル
PPTP	PPTPプロトコル
L2TP	L2TPプロトコル
Cisco AnyConnect	AnyConnect プロトコル
ジュニパーSSL	ジュニパーSSLプロトコル
F5 SSL	F5 SSLプロトコル
ソニックウォール mConnect	SonicWall モバイルコネクト
アルバ VIA	Aruba VIAプロトコル
カスタムSSL	カスタムSSLによる接続
オープンVPN	OpenVPNプロトコル

アプリごとのVPN

特定のアプリを開くと、VPN接続が確立されます。

アプリごとのVPN接続を自動的に開始	アプリごとのVPN接続を自動的に開始
接続タイプ	VPN接続タイプを確立する
Cisco AnyConnect	AnyConnect プロトコル
ジュニパーSSL	ジュニパーSSLプロトコル
F5 SSL	F5 SSLプロトコル
ソニックウォール mConnect	SonicWall モバイルコネクト
アルバ VIA	Aruba VIAプロトコル
カスタムSSL	カスタムSSLによる接続
オープンVPN	OpenVPNプロトコル

プロキシの設定

VPN接続用プロキシの設定

なし	代理人を立てない
マニュアル	手動でプロキシを確立する
プロキシサーバーURL	プロキシ設定へのアクセス用アドレス
ポート	プロキシのポートを設定する
認証	プロキシで認証するためのユーザ名
パスワード	プロキシ認証用パスワード
自動	自動的にプロキシを確立する
プロキシサーバーURL	プロキシ設定にアクセスするためのURL

プレースホルダーを表示する	AppTec360 が使用できるすべてのユーザー変数を表示します。

APN

アクセスポイント名	アクセスポイント名
アクセスポイントのユーザー名	アクセスポイントのユーザー名
アクセスポイントのパスワード	アクセスポイントのパスワード
プロキシサーバー	プロキシサーバーのアドレス
ポート	それぞれのプロキシポート

セルラー

データローミングを有効にする	データローミングを有効にする
音声ローミングを有効にする	音声ローミングを有効にする
ホットスポットを有効にする	ホットスポットを有効にする

HTTPプロキシ

プロキシ・タイプ	
マニュアル	手動でプロキシを確立する
プロキシサーバーURL	プロキシ設定にアクセスするためのアドレス
ポート	プロキシポートの確立
認証	プロキシで認証するためのユーザ名
パスワード	プロキシ認証用パスワード
自動	自動的にプロキシを確立する
プロキシPAC URL	プロキシPAC URL
PACにアクセスできない場合、直接接続を許可する。	PACに到達できない場合、（VPNを介さずに）直接接続を許可する。
プロキシをバイパスしてキャプティブ・ネットワークにアクセスできるようにする。	プロキシをバイパスしてキャプティブな内部ネットワークにアクセスできるようにする。

エアプリント

IPアドレス	プリンタIPアドレス
リソースパス	AirPrintデバイスへの明確なパス

エアプレイ

デバイス名	デバイス名
パスワード	ペアリング・パスワード
ホワイトリスト	デバイスが排他的にペアリングできるデバイスのリストを定義します。

PIM管理

Exchangeアクティブ同期

口座名	メールアカウント名
Exchange ActiveSyncホスト	サーバーのアドレス/FQDN
移動を許可する	電子メールの移動を許可する
メールでのみ使用	インタラクションは、ネイティブのメールアプリ上でのみ発生します。
SSLの使用	SSL暗号化を使用する
ドメイン	サーバードメイン
ユーザー	ユーザー名
電子メールアドレス	メールアドレス（デバイスレベルのみ）
パスワード（デバイスレベルのみ）	ユーザーパスワード
身分証明書	サーバーでの認証に使用する証明書を選択します。
過去の同期メール	メールが同期されるまでの日数。 ノーリミット = 無制限
S/MIMEを有効にする	S/MIME暗号化を有効にする
署名証明書	それぞれの署名証明書をアップロードする
暗号化証明書	それぞれの暗号化証明書をアップロードする。

電子メール

エンドユーザーデバイスへのPOP3/IMAPアカウントのセットアップ

口座詳細	電子メールアカウント名		
口座種別	アイマップ	パスのプレフィックス	特殊フォルダのパスプレフィックス
	ポップ		
ユーザー表示名	ユーザー表示名		
メールアドレス	ユーザーメールアドレス		
移動を許可する	電子メールの移動を許可する		
S/MIMEを有効にする	S/MIME暗号化を有効にする		
署名証明書	それぞれの署名証明書をアップロードする		
暗号化証明書	それぞれの暗号化証明書をアップロードする。		

受信メール

受信サーバーの設定

メールサーバーアドレス	メールサーバーアドレス
メールサーバーポート	メールサーバーポート
ユーザー名	それぞれのユーザー名
認証タイプ	認証タイプ
なし	認証タイプなし
パスワード (デバイスレベルのみ)	パスワードプロンプト
MDM チャレンジ・レスポンス	
エヌティーエルエム	NTLM認証
HTTP MD5 ダイジェスト	
SSLの使用	必要に応じてSSLを使用する

送信メール

送信サーバーの設定

メールサーバーアドレス	メールサーバーアドレス
メールサーバーポート	メールサーバーポート
ユーザー名	それぞれのユーザー名
認証タイプ	
なし	認証方法なし
パスワード (デバイスレベルのみ)	パスワードプロンプト
MDM チャレンジ・レスポンス	
エヌティーエルエム	NTLM認証
HTTP MD5 ダイジェスト	
SSLの使用	必要に応じてSSLを使用する
送信パスワードは受信パスワードと同じ	送信パスワードは受信パスワードと同じ
郵便でのみ使用	すべての送信メールをMail-App経由で送信する場合、有効にする。

カルダヴ

CalDavアカウントのセットアップと配布の設定

口座詳細	アカウントの表示名
ホスト名	ホスト名および/またはIPアドレス
ポート	CalDavアカウントのポート
主なURL	口座の主なURL
ユーザー名	それぞれのCalDavユーザー名
パスワード (デバイスレベルのみ)	それぞれのCalDavパスワード
SSLの使用	必要に応じてSSLを使用する

購読カレンダー

購読カレンダーの設定と配布

説明	アカウントの表示名
URL	カレンダーデータベースのURL
ユーザー名	カレンダー購読のユーザー名
パスワード (デバイスレベルのみ)	カレンダー購読のパスワード
SSLの使用	必要に応じてSSLを使用する

ライトウェイトディレクトリアクセスプロトコル

このエリアでは、エンドユーザーデバイスとActive Directoryの間で動的な証明書交換を可能にするために、LDAP接続を設定します。

選択されたユーザーには、それぞれの読み取り権限が必要であることに注意してください。

口座詳細	口座詳細
アカウントユーザー名	LDAPアクセス用ユーザー
アカウントパスワード	LDAPアクセス用パスワード
アカウントホスト名	LDAPサーバーのホスト名/IPアドレス
SSLの使用	必要に応じてSSLを使用する

第2部では、LDAPレジストリを検索するための個々のフィルターを定義することができる。

説明	スコープ	検索ベース
フィルターの説明	LDAPレジストリの検索レベル	個々のフィルターを定義する

ウェブ管理

ウェブクリップ

この場所で、ウェブページやイントラネット・ポータルなどへのリンクを含むブックマークを定義し、エンドユーザー・デバイス上のアプリケーションとして表示する。

ラベル	エンドユーザーデバイス上の接続名
URL	各ウェブサイトへのリンク
取り外し可能	アクティブにすると、ユーザーはウェブクリップを削除できます。
アイコン	このダイアログから、接続用のロゴをアップロードしてください：寸法180x180、png形式
合成済みアイコン	有効にすると、アイコンに追加効果（影、反射）は表示されません。
フルスクリーン	ウェブクリップを開く際、ブラウザがフルスクリーンモードで開く

ウェブコンテンツフィルター

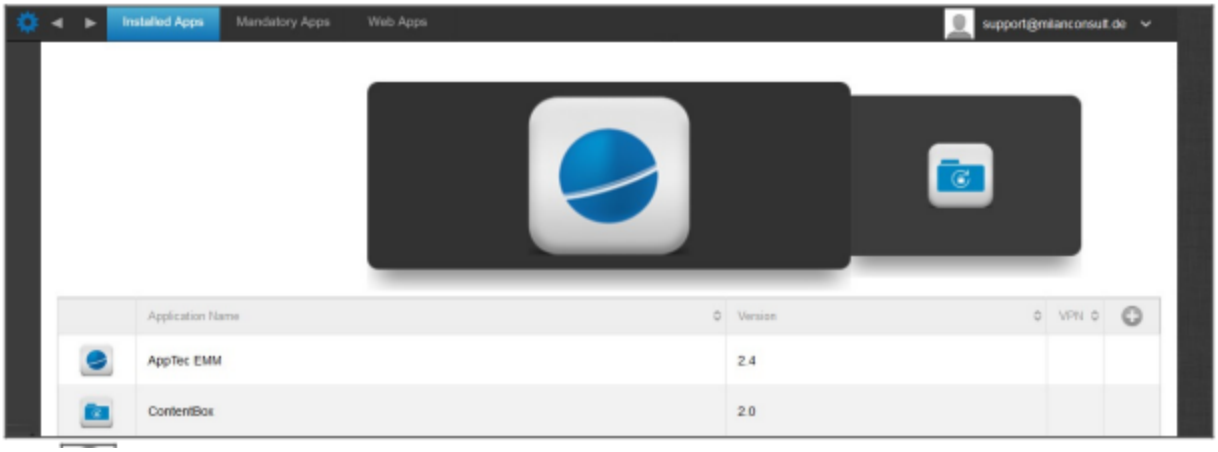
ウェブコンテンツフィルターは、特定のインターネットページへのアクセスを制限することができます。

許可されたウェブサイト	
アダルトコンテンツの制限	アダルトコンテンツには自動的にWebフィルタが適用される
許可されたURL	記号で許可されたページを追加
ブラックリストに掲載されたURL	記号でブロックされたページを追加する
特定のウェブサイトのみ	特定のコンテンツのみを表示することができ、+記号で追加することができます。

アプリ管理

エンタープライズアプリマネージャー

インストール済みアプリ（デバイスレベルのみ）



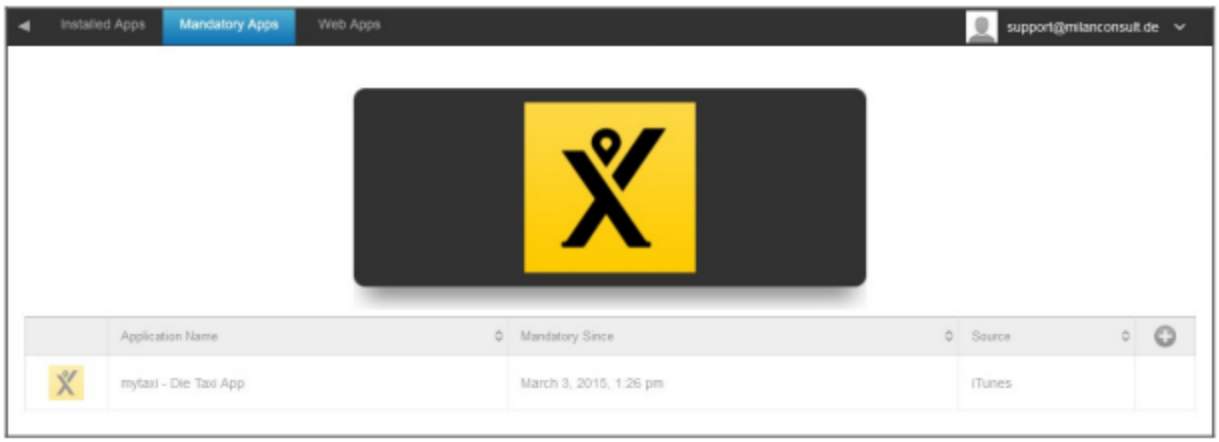
ここでは、現在デバイスにインストールされているアプリを見ることができます。

必須アプリ

必須アプリ（Mandatory Apps）」では、必要なアプリを指定することができます。

ユーザーは、このアプリをインストールするよう継続的に促される。

を介して、義務付けられたアプリを定義することができる。



これはApple App Storeアプリでも、社内アプリでも可能です。

管理されたデバイスを使用する場合は、アプリが自動的にインストールされます。

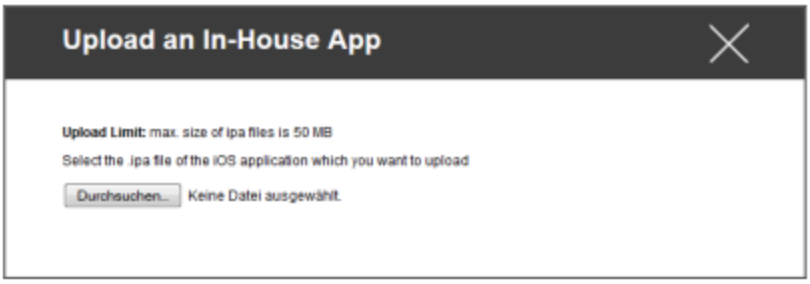
Apple AppStore "アプリを一般のAppStoreからデバイスにプッシュすることができます。

または、"iOS In-House Apps "カテゴリーから、一般設定の下にアップロードしたIn-House Appを選択することもできます。

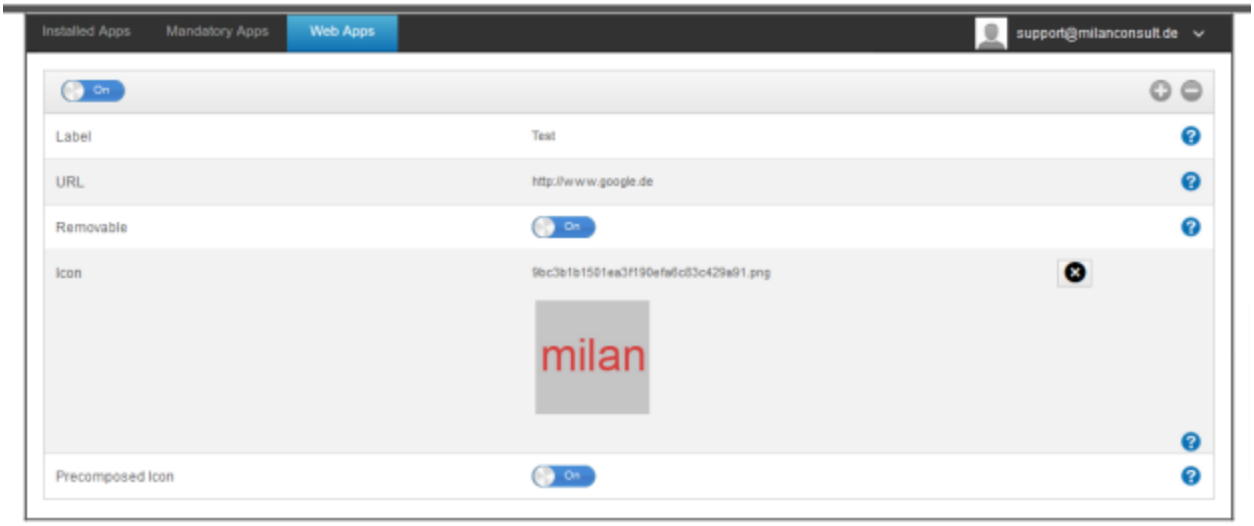
インストール・オプション

最新の状態に保つ（デバイスごとのVPPにのみ対応）	週に一度、アプリのアップデートがあるかどうかが判断されます。はい」の場合、アップデートがインストールされます。 社内アプリの場合、一般設定で設定した更新ターゲットが更新処理に使用されます。
管理されていないときに追い越す	アプリがすでにインストールされている場合は、MDMがアプリを引き継いで管理する
MDMプロファイルの削除時にアプリを削除する	デバイス管理の削除の場合、アプリはアンインストールされます。
アプリデータのバックアップを防止	アプリ固有のデータのバックアップは作成されません。
アプリ設定	アプリの設定」では、アプリに特定の値をフォアグラウンドに割り当てることができます（アプリがサポートしている限り、必要であればアプリの開発者に問い合わせてください）。

Upload In-House App "から直接ipaファイルを選択してアップロードすることもできます。



ウェブアプリ



Web Apps "では、"Web Clips "と同様に、インターネットページやイントラネットのポータルをアプリケーションとしてエンドユーザー端末にプッシュすることができます。デフォルトでは、Web Appsはフルスクリーンモードで表示されます。

ラベル	エンドユーザーデバイス上の接続名
URL	各ウェブサイトへのリンク
取り外し可能	アクティブにすると、ユーザーはウェブクリップを削除できます。
アイコン	このダイアログから、接続用のロゴをアップロードしてください：寸法180x180、png形式
合成済みアイコン	有効にすると、アイコンに追加効果（影、反射）は表示されません。

制限と設定

ブラックリスト/ホワイトリストのアプリ

ここでは、「一般設定」の設定に応じて、ブロックする（または許可する）アプリを設定できます。をクリックすると、既知のアプリ検索が表示されます。そこで追加したいアプリを検索できます。

この機能を使用するには、監視付きデバイスが必要です。

シスアプリの制限

デバイスの特定のアプリや機能をブロックする

YouTubeの使用を許可する	YouTubeの使用を許可する
iTunes Storeの使用を許可する	iTunes Storeの使用を許可する
サファリの使用を許可する	サファリの使用を許可する
オートフィルを有効にする	オートフィルを許可する
強制詐欺の警告	詐欺警告を強制する
JavScriptを有効にする	JavaScriptの使用を可能にする
ポップアップをブロックする	あらゆるパップアップをブロック
クッキーを許可する	SafariがCookieを受け入れるタイミングを選択する

アプリ-VPN

このシンボルにより、起動時に選択したVPN接続を自動的に起動するアプリケーションを定義できます。

アプリの設定

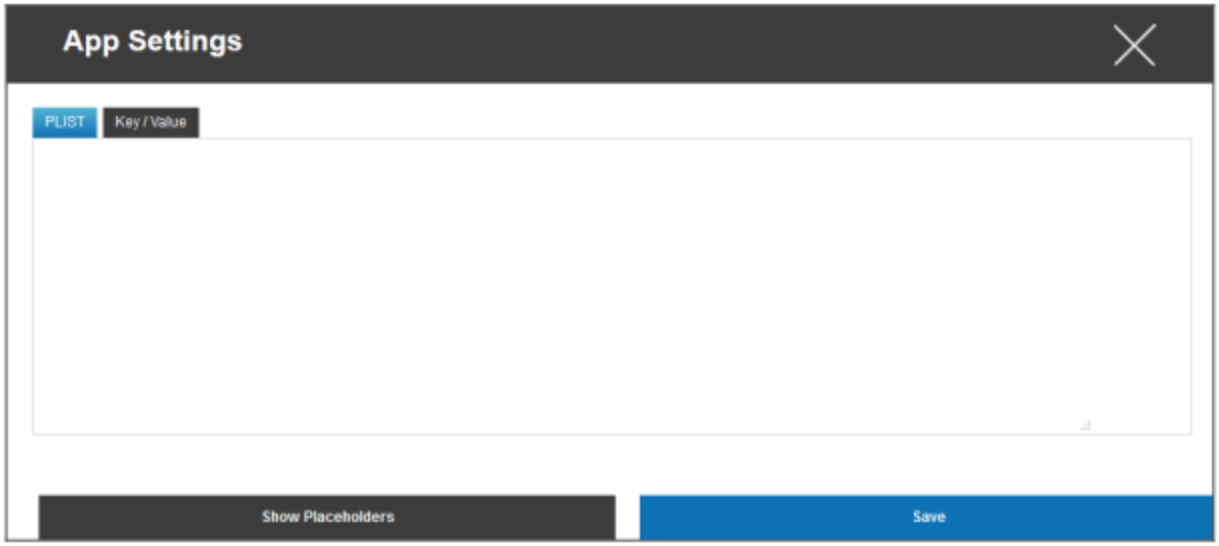
アプリの設定」では、アプリに特定の値をフォアグラウンドに割り当てることができます（アプリがサポートしている限り、必要であればアプリの開発者に問い合わせてください）。

シンボルを使って、アプリを追加します。AppTec360でお馴染みのApp-Importが表示されます。

ここで設定したいアプリを検索し、選択します。設定は管理アプリにのみ適用されます。

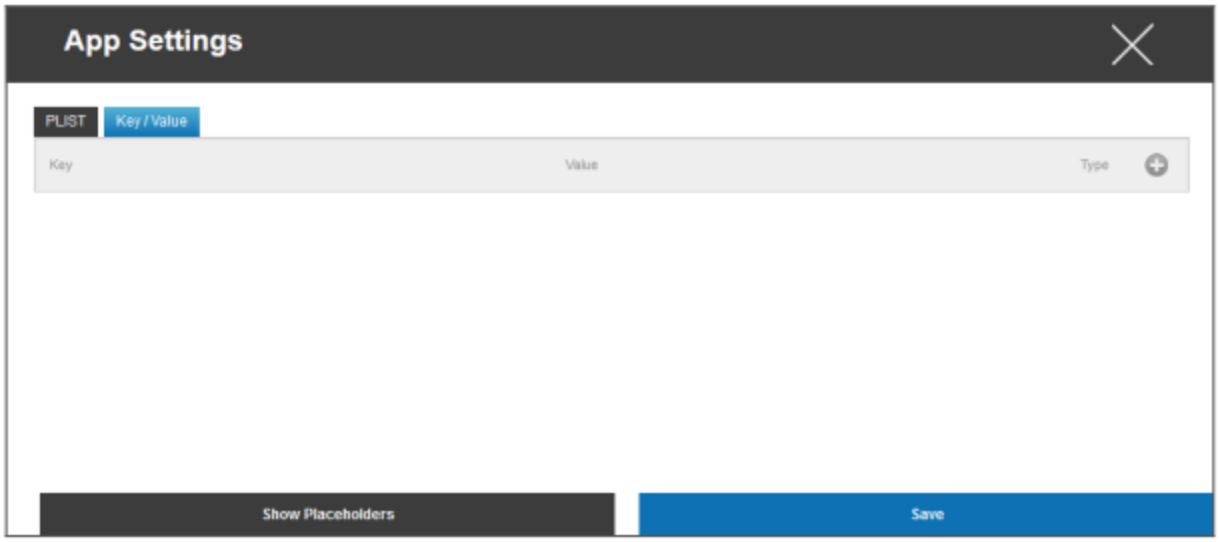
インポートが成功すると、次のような表示が出ます：

をクリックすると、様々な設定を行うことができます。すると、以下のような概要が表示されます：

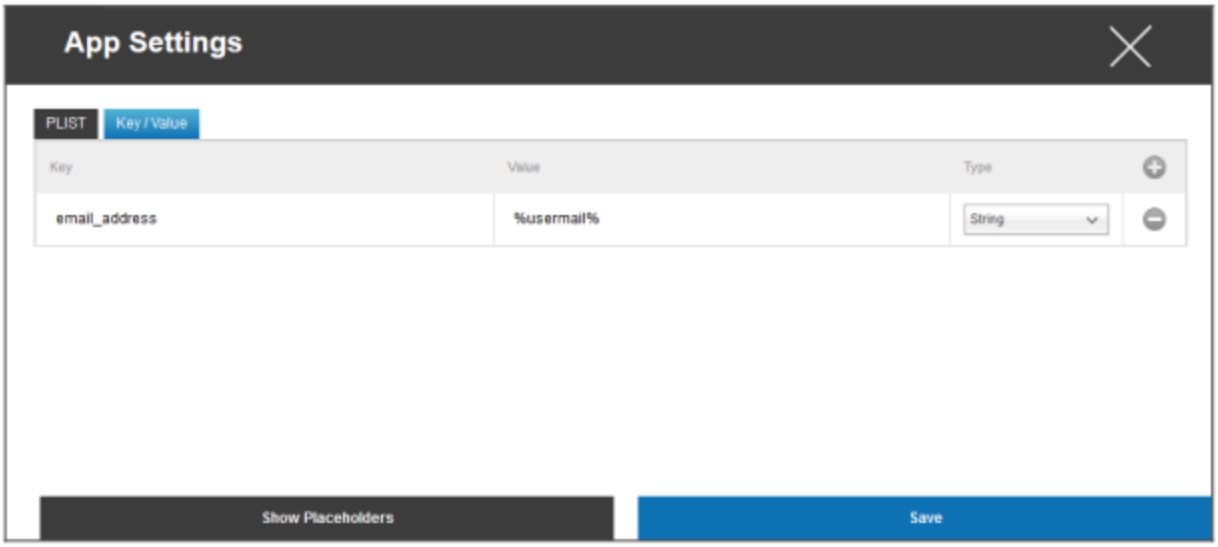


すでにPLIST（コンフィギュレーションの原文）をお持ちの場合は、ここに追加して「Save」で保存することができます。

Key / Value "では、特定のコンフィギュレーションをアプリに添付することができます。



ここで、新しいキーとその値をシンボルで設定することができる。



もちろん、AppTecのプレースホルダーはすべて自由に使うことができる。

「タイプ」の説明：

ストリング	テキスト
ブーリアン	真 / 偽
番号	番号

このマークがあれば、アプリを再び削除することができる。

エンタープライズ・アプリケーション・ストア

iTunesアプリ

このポイントでは、ユーザーのためにオプションのアプリを配布することができます。

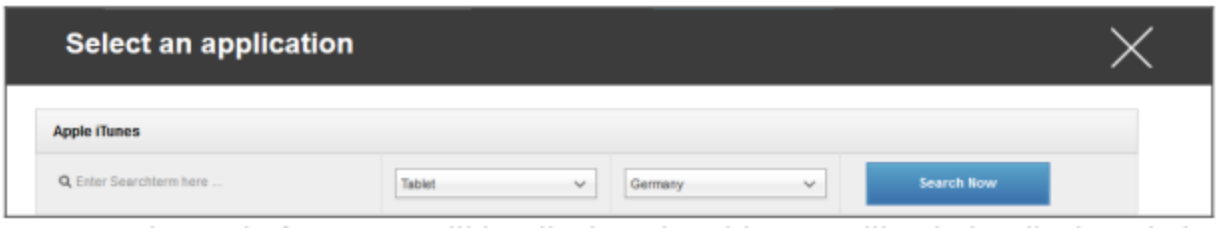
ここにアプリがあれば、AppTec360 Storeのエンドユーザーデバイスに自動的にインストールされます。

これらは単にアップル公式App Storeへのリンクである。このため、各エンドユーザーのデバイスにはApple IDが必要です。

この時点で、各ユーザーが自分のApple IDを持つことをお勧めします。

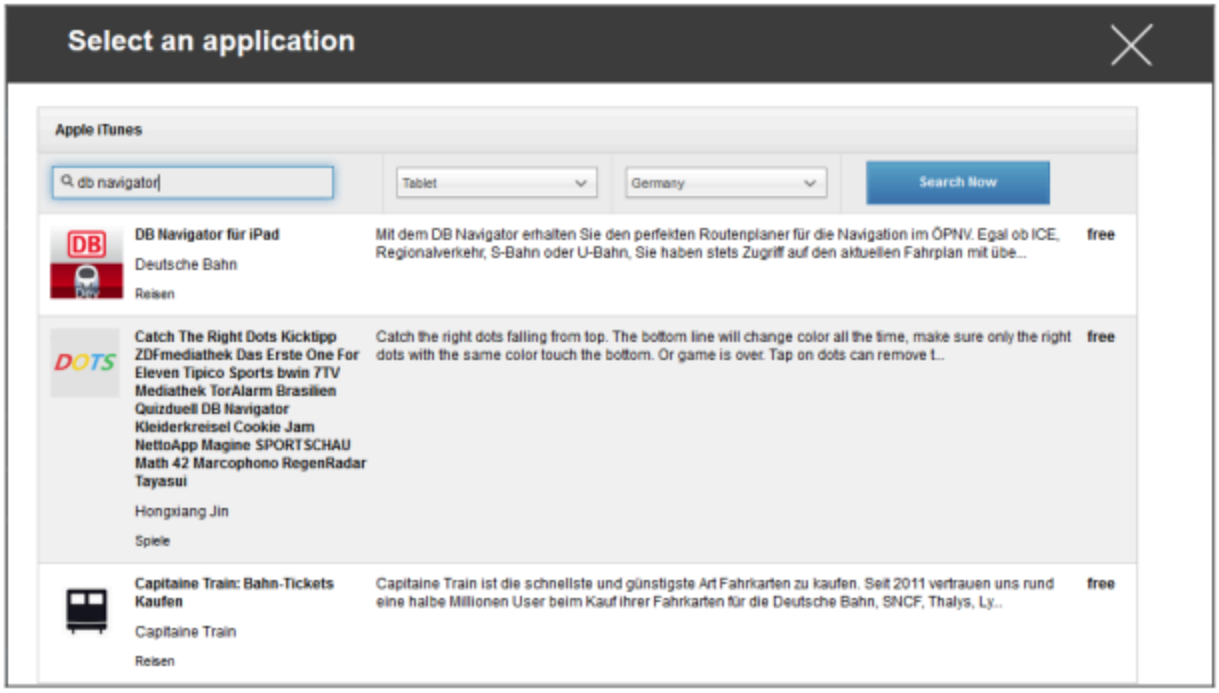
シンボルマークを使用すると、追加のAppsを追加することができます。

その後、以下のような概要のウィンドウが開きます。



無料アプリのみ表示され、有料アプリはVPN経由でのみ表示されますのでご注意ください。

Enter Search Term here ...」で、Apple App Storeにあるアプリを検索できます。



アイコンまたはアプリ名をクリックすると、追加設定を行うよう再度求められます。

最新情報	週に一度、アプリのアップデートがあるかどうかが判断されます。はい」の場合、アップデートがインストールされます。
MDMプロファイルの削除時にアプリを削除する	デバイス管理の削除の場合、アプリはアンインストールされます。
アプリデータのバックアップを防止	アプリ固有のデータのバックアップは作成されません。
アプリ-VPN	アプリを開いたときに起動するVPN接続を選択します。

Install "をクリックすると、アプリはEnterprise App Storeに追加され、AppTec360 AppStore経由でエンドユーザーデバイスにインストールできます。

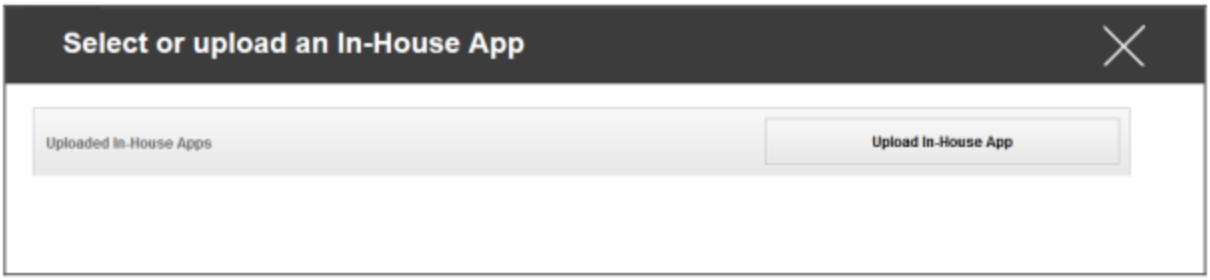
App-Storeインポートに成功すると、次のような概要が表示されます：

インハウス

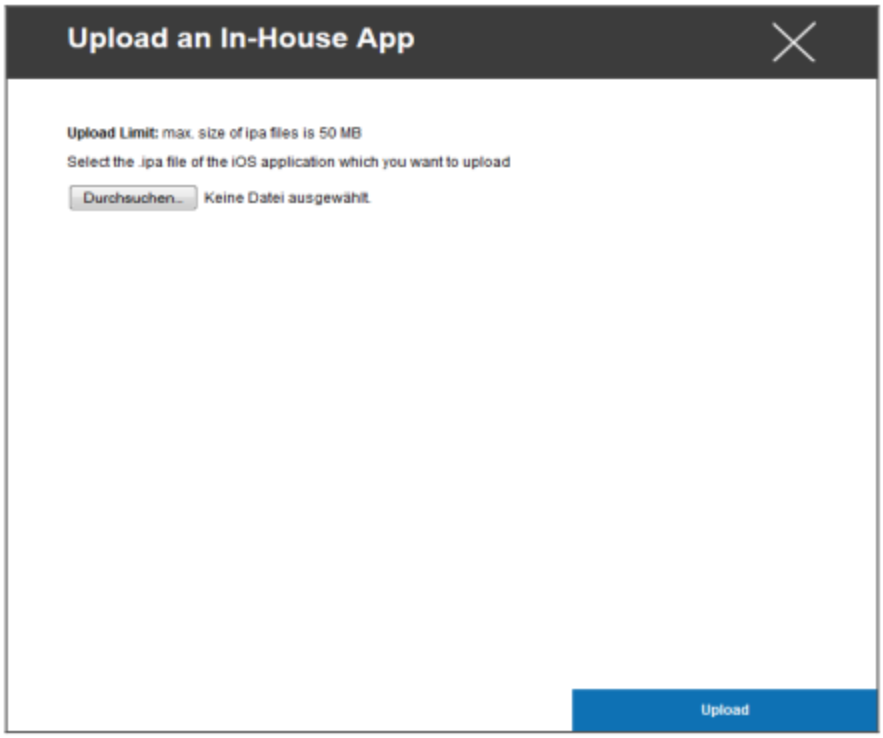
In-House」では、社内で開発したアプリをアップロードして配布することができます。

このシンボルがあれば、インハウスアプリを追加で配布できる。

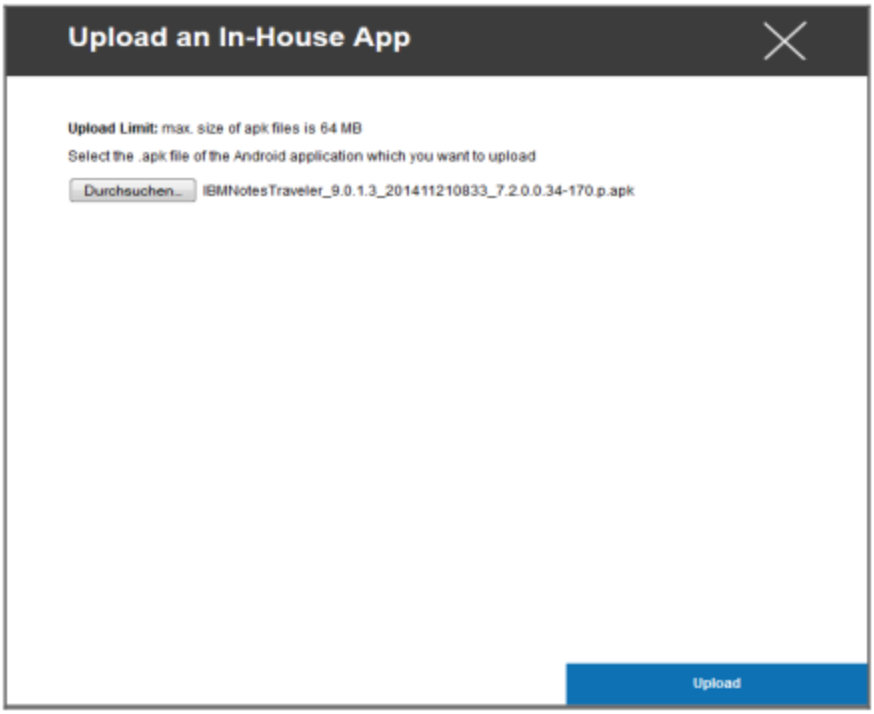
In-House Appを配信したことがない場合は、次のような概要が表示されます：



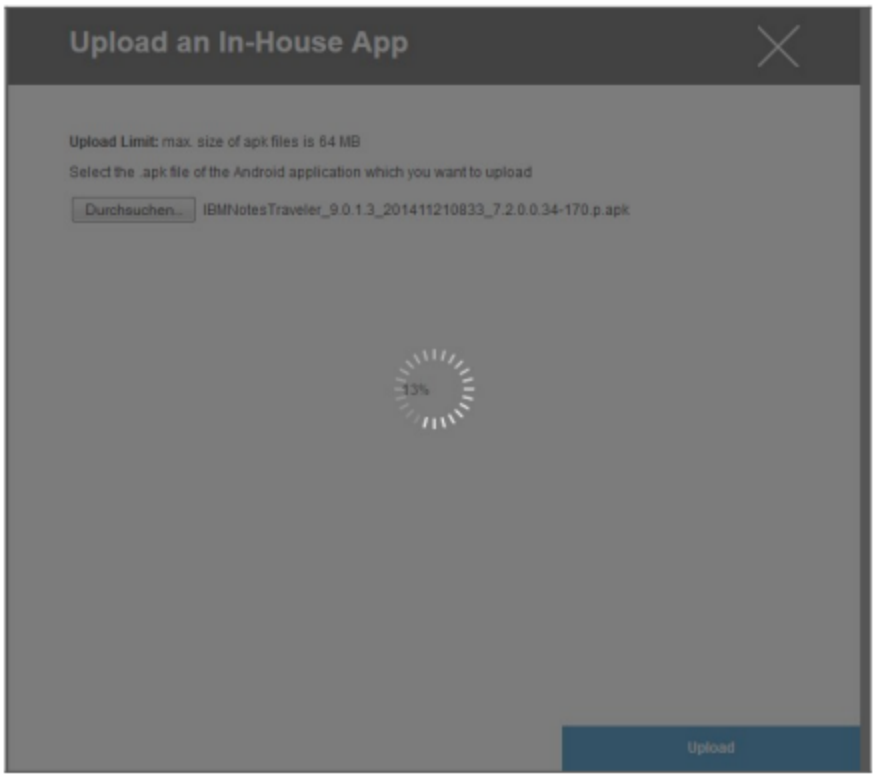
社内アプリのアップロード」をクリックすると、以下のような概要が表示されます：



検索...」で.ipaファイルを選択し、「アップロード」をクリックします。



アプリがアップロードされます。円の中央には、アプリのアップロード済み率が表示されます。



社内アプリのアップロードが正常に実行されると、アプリカタログに新しくアップロードされたアプリが表示されます。

ユーザーは、エンドユーザーのデバイス上のAppTec360 Storeの「社内」カテゴリで、このアプリを確認し、インストールするオプションがあります。

公開されているApple AppStore Appを使用しないため、エンドユーザー端末にApple IDを保存する必要はありません。

キオスク・モード

iOSのキオスク・モードは監視モードでのみ利用可能

キオスクモードでは、アプリまたはURLを事前に定義することができ、このアプリ/URLのみを実行/訪問することができます。

さらに、キオスク・モードでは様々なハードウェア・ボタンを無効にすることができます。

アプリケーション・タイプ

パッケージ

キオスク・モードでアプリを起動したい場合は、"Application Type "で "Package "を選択します。

キオスク・アプリケーション	キオスクモードで起動するアプリを選択するには、ここをクリックしてください。 現在のアプリ管理の概要がわかります。 Apple iTunes Apps」と「iOS In-House Apps」を選択できます。

URL

キオスク・モードでURLを起動したい場合は、"Application Type "で "URL "を選択します。

URL	次に、目的のURLアドレスを定義する。
同一原産地ポリシー	この機能が有効な場合、ユーザーは事前に定義されたURLのサブページのみを閲覧することができます。 例えば、次のようなURLを定義したとする： www.mypage.com、ユーザーはwww.mypage.com/subpage。
ホワイトリストのURL	ここでホワイトリストを管理することができ、以下のURLはすべて許可されます。 1行につき1URLまで URLはhttp:/またはhttps:// で始まる必要があります。
ブラックリストに掲載されたURL	ここでブラックリストを管理することができ、これらのURLはすべて許可されません。 1行につき1URLまで URLはhttp:/またはhttps:// で始まる必要があります。
非アクティブ時のブラウザ消去	操作がない場合、ブラウザのキャッシュは空になります。
終了パスワード 有効	この機能を有効にすると、ユーザーは事前に設定したパスワードでキオスクモードを終了することができます。
終了パスワード	これは、あなたが事前に設定したパスワードです。

キオスクモードの設定

予定されたキオスク・モード	キオスクモードを設定することで、あらかじめ設定した時間に自動的にキオスクモードを開始・終了することができます。
開始時間	開始時間
時間 (分	キオスクモードを再度終了するまでの時間 (分単位
タッチを無効にする	アクティブの場合、タッチスクリーンは非アクティブになる
デバイスの回転を無効にする	有効になっている場合、自動画面適応は解除されます。
リンガースイッチを無効にする	有効になると、リンガースイッチは解除されます。それ以降の動作は、事前に設定された機能に依存します。
ボリュームボタンを無効にする	アクティブにすると、音量ボタンは無効になります。
スリープ解除ボタン	作動している場合、オン / オフスイッチは解除される
オートロックを無効にする	アクティブにすると、デバイスはスタンバイに切り替わりません。
ボイスオーバーを有効にする	音声アシスタントが起動します。
ズームを有効にする	有効にすると、ズームが有効になる
色の反転を有効にする	アクティブにすると、反転表示モードがアクティブになる
アシストタッチを有効にする	起動すると、AssistiveTouchが起動します。
スピーク選択を有効にする	有効になっている場合、スピーチの選択が有効になる
モノラル音声を有効にする	アクティブにすると、モノラル音声がアクティブになります。
ボイスオーバー	有効になっている場合、ユーザーはVoiceOverを有効にすることができます。
ズーム	有効にすると、ユーザーはズーム
色の反転	有効にすると、ユーザーは色の反転を有効にすることができます。
アシスト・タッチ	アクティブにすると、ユーザーはアシストタッチを有効にすることができます。

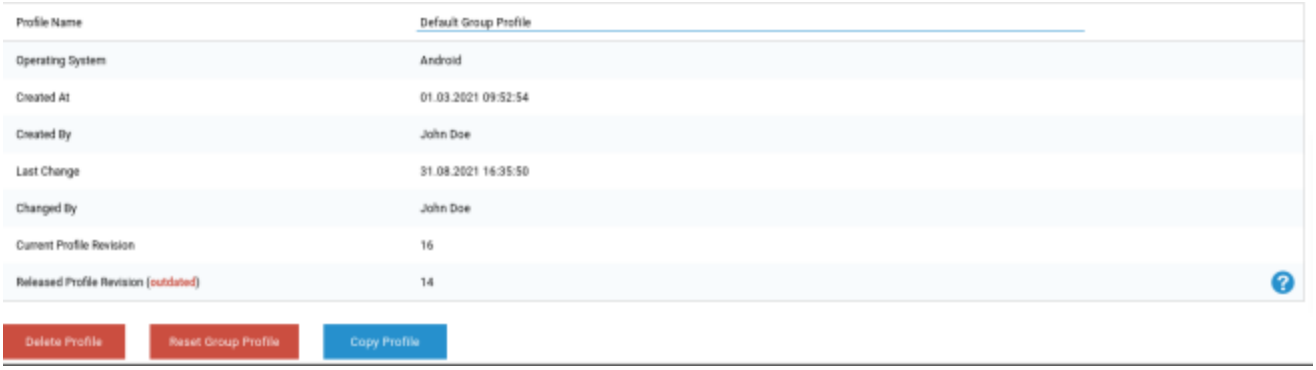
Android Enterprise – フルマネージド・デバイス構成

現在選択されているのがグループプロファイルかデバイスかによって、概要とそのサブポイントが異なります！

一般

グループプロフィールの概要（グループレベルのみ）

グループプロフィールを開くと、プロフィールの概要が表示されます。



プロフィール名	プロフィールの名前（ここで変更可能）
オペレーティングシステム	対象OS
作成日時	創造の時
作成者	プロフィールの作成者
最後の変更	プロフィールの最終変更時刻
変更履歴	最後の変更を行ったアカウント
現在のプロフィール改訂	保存されたプロファイル状態の修正
プロフィール改訂版をリリース	割り当てられたプロファイルのリビジョン（"Assign now"）。ラベルのテキストの後ろに"(outdated) "と表示されている場合は、プロファイルを保存したものの、まだ割り当てていないことを意味します。

デバイスの概要 (デバイスレベルのみ)

デバイスを選択すると、選択したデバイスの概要が表示されます：

デバイス名	デバイス名
所在地	位置座標
電話番号	電話番号
割り当てられた必須アプリ	割り当てられた必須アプリの数
OSバージョン	デバイスのOSバージョン
オペレーティングシステム	オペレーティング・システム (アンドロイド・エンタープライズ)
シリアル番号	デバイスのシリアル番号
デバイスの所有権	企業用またはプライベート用デバイス
デバイス・タイプ	AEワーク管理デバイス
ルーツ	デバイスがルート化されているかどうかを示すステータス
準拠	ガイドライン準拠
IPアドレス	デバイスのIPアドレス
ラストシーン	デバイスが最後にAppTecに接続した時点
ラスト・プッシュ	最後のプッシュがデバイスに送信された時点
AEデバイス・オーナー・モード	はい
ユーザー割り当て	このデバイスが割り当てられているユーザーまたはグループ

コンフィグ改訂（デバイスレベルのみ）

ここで、どのグループプロファイルがデバイスに割り当てられているかの概要が表示されます。

グループプロフィールをクリックすると、そのプロフィールに直接アクセスでき、設定を行うことができます。

このマークがあれば、配布されたアプリをグループプロファイルの設定に戻すことができる。

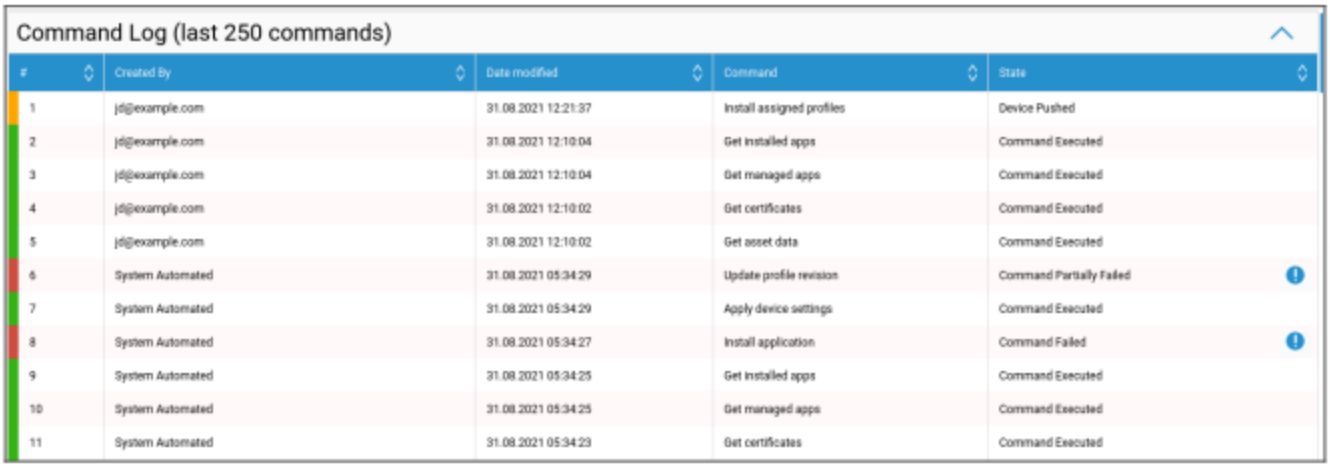
このマークがあれば、使用中のアプリをすべてグループプロファイルの設定に戻すことができます。

"Newer Revision available "は、グループプロファイルが変更され保存されたが、割り当てられていないことを示します。グループプロファイルの変更をデバイスに適用するには、グループレベルで "Assign now "を使用してグループプロファイルを割り当てる必要があります。

デバイスログ（デバイスレベルのみ）

コマンドログ

ここでは、デバイスに対して発行されたコマンドとそのステータスを確認することができます。



System Automated」によって作成されたコマンドは、システムによって自動的に作成される。

可能なコマンドステータス

デバイスが押される	プッシュリクエストは、EMM サーバーに接続するようデバイスに指示するため、プッシュサービス (APNS など) に送信されました。
コマンド作成	コマンドがシステム内に作成された。
コマンド送信	コマンドは、サーバーに接続された後、デバイスに送信された。
コマンド実行	コマンドは正常に実行された。
コマンド失敗	コマンドが失敗しました。*
コマンド一部失敗	デバイスのOSによっては、いくつかのコマンドがグループ化されることがある。 このコマンドグループの一部は失敗した。*
コマンドは実行されたが、最終的に失敗	コマンドは実行されたが、もしかしたら実行されていなかったかもしれない。
コマンド・リパッシュ	コマンドはユーザーによってリプッシュされた。
廃棄	コマンドが破棄された。例えば、他のコマンドに取って代わられたとか、デバイスが再登録されて古いコマンドが削除されたとか。

メッセージの後ろにエクスクラメーションマークが表示されている場合は、カーソルをアイコンの上に置くと詳細情報を得ることができます。

デバイス設定

クライアント設定

ここでは、Androidデバイスの以下の設定を行うことができます：

コンプライアンス違反の時間	強制アクションが適用されるユーザー応答タイムアウト制限。
コンプライアンス・タイムアウト後の強制措置	ユーザーがデバイスのステータスに準拠するアクションを実行しない場合の強制アクション
データ収集頻度	デバイス/GPS情報の収集頻度
デバイスのハートビート周波数	デバイスがAppTec360 Serverにコンタクトする間隔 最短1分 最大24時間
位置情報の更新を有効にする	有効になっている場合、デバイスは位置情報の更新をAppTec360 Serverに送信します。
場所 更新時間	デバイスが AppTec360 に位置情報の更新を送信する時間間隔を決定します。
位置情報の更新にGoogle Location Accuracyを使う	有効にすると、位置情報の更新にネットワークの位置情報が使用されます。
位置情報の更新にGPSロケーションを使用	アクティブにすると、位置情報の更新にGPSが使用されます。
モック（偽）ロケを許可する	サードパーティアプリによる位置情報の偽造を許可する
ロスト・コネクション	有効にすると、デバイスがハートビート間隔内に MDM サーバーへの接続を取得しない場合のアクションを指定できます。たとえば、デバイスのハートビート時間が5分の場合、午前10時35分にサーバーに接続します。その後、デバイスはWi-Fi範囲から外れます。次の午前10時40分のハートビートは失敗し、指定されたアクションが実行されます。
アクション	デバイスが非準拠となった場合に直ちに取られるべき措置。 • ロック・デバイス = ロック装置 • デバイスのワイプ = デバイスが工場出荷時の設定に復元されます。

	• デバイスとSDカードのワイプ = デバイスは工場出荷時の設定に復元され、SDカードのストレージは削除されます。
しきい値	指定したアクションのトリガーに必要な、失敗したハートビートの閾値を指定することができます。

ポリシー実施モード	デフォルト：	ユーザーには、未解決のアクションを実行するよう定期的にプロンプトが表示されます。
	怠惰なポリシーの実施：	未解決のアクションの実行をユーザーに促すことはありません。すべての未解決のアクションはAppTec360 Clientに表示されます。
	積極的なポリシー実施：	ユーザーは、未解決のアクションを実行するようノンストッププロンプトが表示される。
AppTec360 バージョンロック	有効にすると、AppTec360 MDM Clientのバージョンコードを指定できる。AppTec360クライアントは、指定されたバージョンにのみ更新されます。新しいバージョンは無視されます。ダウングレードはできません。	
バージョンコード	ロックオンされるAppTec360 MDM Clientのバージョンコード。	
AppTec360の通知を無効にする	無効にした場合、AppTec360クライアントは通知バーに通知を表示しません。そのため、ユーザーはタスクマネージャー経由でAppTec360クライアントを閉じることができます。AppTec360 クライアントを閉じた場合、キオスクモードやアプリのブラックリスト/ホワイトリストを含むいくつかの機能は正常に動作しません。 Samsung デバイスは AppTec360 クライアントの保護メカニズムを提供します。KNOX APIをサポートするSamsungデバイスでは、通知はデフォルトで無効になっています。 アンドロイド8.0以上の端末では、この通知が無効になることはありません。	

壁紙

カスタム壁紙の設定	カスタム壁紙の有効/無効
壁紙	カラーコードまたは画像を使用する壁紙モードを設定する。
色の指定	例えば、#000000は黒、#ffffffは白です。
画像を壁紙に設定する	壁紙にしたい画像ファイルをアップロードする

資産管理 (デバイスレベルのみ)

デバイス情報

モデル	機器モデル名
オペレーティングシステム	OS
OSバージョン	OSバージョン
シリアル番号	シリアル番号
デバイス名	デバイス名
バッテリーの状態	バッテリーの状態
フリー/トータルメモリー	空き/総メモリ
サムスン金庫	様々な設定オプションに必要なサムスンSAFEインターフェース
利用可能なSDカード	SDカードあり
エミュレートされたSDカード	エミュレートされたSDカード
リムーバブルSDカード	SDカード取り外し可能
SD空き/総メモリ	SD空き容量/SDカード空き容量

Wi-Fi

IPアドレス	デバイスIPアドレス
WiFi MAC	WiFiのMACアドレス

セルラー

ステータス	ステータス（SIMカード装着）
電話番号	電話番号
ローミング（音声/データ）	音声/データのローミング
ローミング状況	現在のローミング状況
IPアドレス	IPアドレス
オペレーター/キャリア	オペレーター/キャリア
セルラー技術	セルラー技術
IMEI	IMEI番号
国際ID	これはSIMカードのIDであり、多くの場合、スマートカードまたは集積回路カード（ICC）でもある。
移動加入者識別番号	IMSI（International Mobile Subscriber Identity）は、GSMおよびUMTSモバイル・ネットワークにおいて、ネットワーク・ユーザーの明確な識別を提供する。 IMSIは最大15桁で構成され、以下のように設定される： • 携帯国番号（MCC）、3桁 • モバイル・ネットワーク・コード（MNC）、2桁または3桁 • 携帯電話加入者識別番号（MSIN）、1～10桁
現在のMCC/MNC	SIM MCC/MNC」を参照。
SIM MCC/MNC	モバイル国コードは、E.212標準に従ってITUによって設定された、確立された国識別子です。これは、モバイル・ネットワーク・コード（MNC）と連動してモバイル・ネットワークを識別します。 SIMカードの国/モバイルネットワークコードを意味する。 別のモバイルネットワークにローミングする場合、論理的には、「現在のMCC/MNC」と「SIM MCC/MNC」は異なる。

ブルートゥース

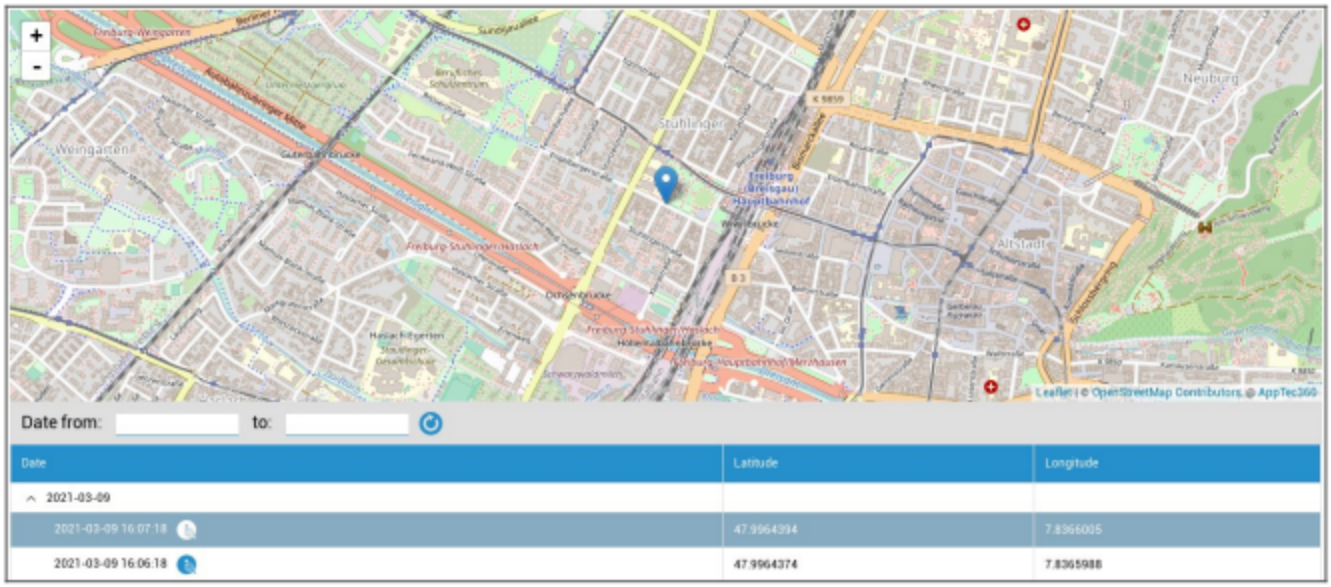
ブルートゥースMAC	ブルートゥースMACアドレス

セキュリティ管理

盗難防止（デバイスレベルのみ）

GPS情報（デバイスレベルのみ）

ここでデバイスの現在地/最終位置を設定できます。ローカライズは1つまたは2つのパスワードで保護することができます：一般設定 - プライバシー - GPSアクセス



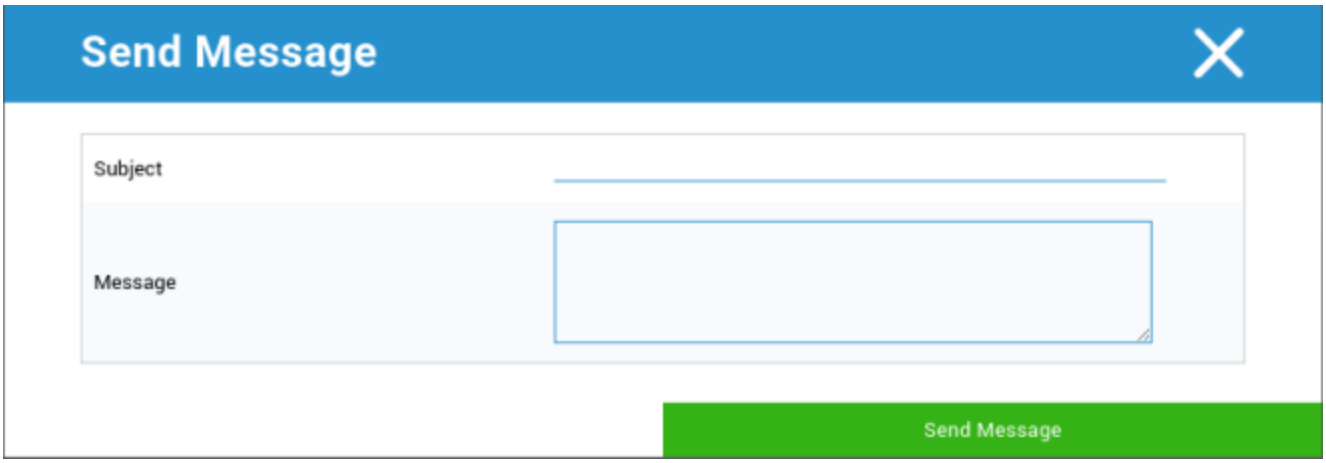
ワイプ＆ロック（デバイスレベルのみ）

ワイプ＆ロック」では、以下の3つのアクションを実行できます：

フルワイプ	デバイスを工場出荷時の設定に戻す（企業および個人データは削除される）
エンタープライズ・ワイプ	企業データのみがエンドユーザーデバイスから削除される（AppTec360によって提供されたすべてのアプリ、データなど）
ロック画面	スクリーンロックが有効になっている場合、デバイスパスワード/PINでデバイスのロックを解除すれば十分です。

メッセージ (デバイスレベルのみ)

ここで件名とメッセージを入力し、エンドユーザーデバイスに送信することができます。



セキュリティ設定

デバイスのパスコード

パスコード」では、デバイスのパスワードを設定することができます。

最小パスワード長	パスワードに最低限必要な記号の数を定める。	
パスワードの品質	特定せず	このポリシーにはパスワードに関する要件はない。
	バイオメトリックの弱さ	この方針は、低セキュリティのバイオメトリクス認識技術を許容する。これは、3 桁の暗証番号程度まで個人の身元を認識できる技術を意味する (誤検出は 1,000 分の 1 以下) 。
	何か	このポリシーは、何らかのパスワードやパターンを設定することを要求するが、特定のルールを強制するものではない。
	アルファベット	ユーザーは、少なくともアルファベット (またはその他の記号) 文字を含むパスワードを入力しなければならない。
	英数字	ユーザーは、少なくとも数字とアルファベット (またはその他の記号) の両方を含むパスワードを入力しなければならない。
	コンプレックス	デフォルトでは、ユーザーは少なくとも文字、数字、特殊記号を含むパスワードを入力しなければならない。このパスワード品質では、パスワードは、少なくとも大文字を含むなど、さまざまな文字のセットを含むように制限することができます。
最小パスワード長	パスワードに必要な文字数を設定します。例えば、PINやパスワードに最低6文字を要求することができます。	
パスワードに最低限必要な数字	パスワードに最低限必要な数字	
パスワードに最低限必要な小文字	パスワードに最低限必要な小文字	
パスワードに最低限必要な大文字	パスワードに最低限必要な大文字	

パスワードに最低限必要な文字以外の文字	パスワードに最低限必要な文字以外の文字
パスワードに最低限必要な記号	パスワードに最低限必要な記号

最大非アクティブ時間ロック	タイムロックまでの最大ユーザー非アクティブ時間
パスワード有効期限タイムアウト	パスワードの有効期限が切れると、新しいパスワードを発行しなければならない。
パスワード履歴の制限	以前に使用されたパスワードのうち、許可されていないパスワードの数
パスワードの最大試行回数	デバイスの完全消去が実行されるまでに、パスワードが誤って入力される頻度を設定します。
生体認証を許可する	指紋または虹彩スキャンによる認証が可能。Samsung KNOX 2.1以上のみ対応

アンチウイルス

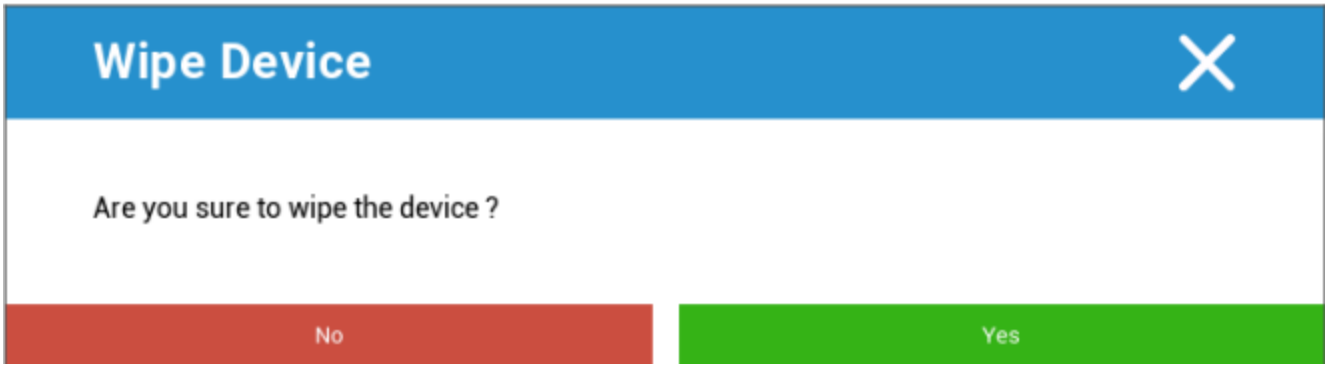
自動スキャン	定期的な自動スキャンを有効にする
スキャン間隔	検査間隔 (クイック / フル)
全自動スキャン	完全自動スキャンを有効にする
自動アップデート	自動アップデートを有効にする
更新チェック間隔	アプリとデータベースの更新頻度 (ウイルス / 破損コード)
アプリの保護	アプリの自動スキャンを有効にする
SDカード保護	SDカードの自動スキャンを有効にする
Wi-Fiのみのアップデート	有効にすると、デバイスがWi-Fiネットワークに正常に接続された場合にのみ、アップデートが適用されます。

エンド・オブ・ライフ (デバイス・レベルのみ)

ワイプ (デバイスレベルのみ)

ワイプ」では、デバイスを工場出荷時の設定に戻すことができる。ここで、企業や個人データはエンドユーザーのデバイスから削除されます。

マイナス記号」をクリックすると、次のようなメッセージが表示される：



はい」でワイプを実行できる。

Wipe Report "の下に以下の項目が表示される。

で拭いた。	誰がワイプを行ったかの履歴
日付	日付
ステータス	ステータス (ワイプが正常に実行された場合など)

制限の設定

制限事項

ここでは、さまざまなことを制限したり、ブロックしたりすることができる。

カメラを有効にする	カメラの使用を許可する	
強制自動同期	オン	同期が恒久的に有効になる
	オフ	同期が永久に解除される
	ユーザーの選択	ユーザーが選択
フォース・ブルートゥース	オン	ブルートゥースが常時有効
	オフ	ブルートゥースが永久に解除される
	ユーザーの選択	ユーザーが選択
フォースGPS	オン	GPSが常時作動
	オフ	GPSは永久に解除される
	ユーザーの選択	ユーザーが選択
フォース・ネットワークの位置	オン	恒久的なインターネット・ローカライズ
	オフ	インターネット・ローカライズの永久停止
	ユーザーの選択	ユーザーが選択

セキュリティ		
共有場所の不許可	位置情報の共有を許可しないユーザーを指定します。	
セーフブートの禁止	ユーザーがデバイスをセーフブートモードにリブートすることを許可されないかどうかを指定します。	
ネットワークリセットを許可しない	ユーザーが [設定] からネットワーク設定をリセットすることを禁止するかどうかを指定します。	
工場出荷時のリセットを許可しない	ユーザーがデバイスをリセットすることを禁止するかどうかを指定します。	
ADBを有効にする	ADB経由でPCに接続可能	
キーガードを無効にする	キーガードを無効にする	
デバイス所有者のロックスクリーン情報	ロック画面に表示するデバイスの所有者情報を設定します。	
コンプライアンスの実施	モード プロンプト ユーザー	ユーザーは、必要なアクションを実行するように求められます。
	モード・ロックダウン・コンテナ	すべての要件を満たすまで、すべてのアプリを非表示にする

アプリ管理	
クロスプロファイルのアプリリンクを許可する	親プロファイルのアプリが管理プロファイルからのウェブリンクを処理できるようにします。
アプリの制御を許可しない	ユーザーが設定やランチャーでアプリケーションを変更できないようにするかどうかを指定します。
アプリのインストールを許可しない	ユーザーがアプリケーションをインストールできないようにするかどうかを指定します。
アプリのアンインストールを許可しない	ユーザーがアプリケーションをアンインストールできないようにするかどうかを指定します。
ランタイム許可ポリシー	アプリからの新しい許可リクエストの処理方法を指定します。
不明なソースを許可する	有効にすると、ユーザーは.apkファイルをインストールしてアプリをサイドロードできる。

コネクティビティ	
モバイルネットワーク設定を許可しない	ユーザーがモバイルネットワークの設定を許可されないかどうかを指定します。
テザリング禁止設定	ユーザーがテザリングとポータブルホットスポットの設定を許可しないかどうかを指定します。
VPN設定を許可しない	ユーザーがVPNを設定することを禁止するかどうかを指定します。
Wifi設定を許可しない	ユーザーが WiFi アクセスポイントを変更できないようにするかどうかを指定します。
発信NFCビームの不許可	アプリからデータを転送するためにNFCを使用することを禁止するかどうかを指定します。
WiFi設定のロック	この設定は、デバイス所有者アプリによって作成されたWiFi設定をロックダウン（つまり、設定アプリでもなく、デバイス所有者アプリによってのみ編集または削除可能）するかどうかを制御します。
データローミングを有効にする	データローミングを有効にする

ブルートゥース	
ブルートゥースを許可しない	デバイスでブルートゥースが許可されていないかどうかを指定します。Android 8.0が必要です。
Bluetoothの共有を許可しない	デバイス上で発信ブルートゥース共有が禁止されているかどうかを指定します。Android 8.0が必要です。
Bluetooth設定を無効にする	ユーザーがブルートゥースを設定することを禁止するかどうかを指定します。

アカウント管理	
管理プロファイルの追加を許可しない	ユーザーが管理プロファイルを追加できないようにするかどうかを指定します。Android 8.0が必要です。
ユーザーの追加を許可しない	ユーザが新規ユーザを追加できないようにするかどうかを指定します。
管理プロファイルの削除を許可しない	このユーザーの管理プロファイルを、プロファイル所有者以外に削除できるかどうかを指定します。Android 8.0が必要です。
口座変更の不許可	Authenticator によってプログラム的に追加されない限り、ユーザがアカウントを追加および削除できないようにするかどうかを指定します。

テレフォニー	
発信を許可しない	ユーザーが電話を発信できないように指定します。
SMSを拒否する	ユーザーがSMSメッセージを送受信できないように指定します。

システム	
ウィンドウの作成を許可しない	アプリケーション・ウィンドウ以外のウィンドウを作成しないように指定します。
ユーザーアイコンの設定を許可しない	ユーザーが自分のアイコンを変更できないようにするかどうかを指定します。
壁紙の設定を許可しない	壁紙の設定を禁止するユーザー制限。
ステータスバーを無効にする	ステータスバーを無効にすると、通知、クイック設定、その他の画面オーバーレイがブロックされ、単一使用のデバイスから脱出できるようになる。
オートタイムを有効にする	自動的に時刻を設定する。
自動タイムゾーンを有効にする	タイムゾーンを自動的に設定する。
コンセントに接続したまま	電源に接続されている間、デバイスはアクティブな状態を保ちます。

ストレージ	
アプリ検証を無効にする	ユーザーがアプリケーション検証を無効にすることを許可するかどうかを指定します。
物理メディアのマウントを許可しない	物理的な外部メディアのマウントを禁止するかどうかを指定します。
バックアップサービスを有効にする	バックアップ・サービスは、デバイス上のすべてのバックアップおよび復元メカニズムを管理します。これをFalseに設定すると、データのバックアップやリストアができなくなります。バックアップサービスはデフォルトでオフになっています。Android 8.0が必要です。
USBマスストレージを有効にする	USBマスストレージの使用を有効にする。

キーボード	
自動入力を許可しない	ユーザーが自動入力サービスの使用を許可されていないかどうかを指定します。Android 8.0が必要です。
プロファイル間のコピー＆ペーストを禁止する	このプロファイルのクリップボードにコピーされた内容を、関連プロファイルに貼り付けることができるかどうかを指定します。

サウンド	
出来高調整を認めない	ユーザーがマスター音量を調整できないようにするかどうかを指定します。
マイクのミュート解除を許可しない	ユーザーがマイクの音量を調整できないようにするかどうかを指定します。
ミュート装置	ミュート装置。

証明書管理

ここでは、Trusted 証明書と Identity 証明書をデバイスに配布できる。

Trusted 証明書を配布するには Android 8 以上、Identity 証明書を配布するには Android 9 以上が必要である。

を使えば、複数の証明書を追加できる。

信頼できる証明書はPEM形式である必要がある。

アイデンティティ証明書は PKCS12 形式である必要がある。

コネクション管理

無線LAN

この設定を行うには、エンドユーザーデバイスの事前設定を行い、内部アクセス
ポイントにアクセスします。

サービスセット識別子（SSID）	接続するネットワークのSSID
隠しネットワーク	APがSSIDをブロードキャストしない場合は、アクティブにする。

セキュリティ・タイプ

APのセキュリティ・タイプを確立する

ウェップ

パスワード	APのパスワード

WPA/WPA2

パスワード	APのパスワード

802.1x EAP

EAPメソッド

PWD	アイデンティティ	アイデンティティ
	パスワード	パスワード

ピーエーピー	フェーズ2認証プロトコル	なし	追加プロトコルなし
		MSCHAPV2	MSCHAPV2プロトコル
		GTC	GTCプロトコル
	CA証明書	CA 証明書	
	アイデンティティ	アイデンティティ	
	匿名アイデンティティ	匿名ID	
	パスワード	パスワード	

TTLS	フェーズ2認証プロトコル	なし	追加プロトコルなし
		PAP	PAPプロトコル
		エムエスシーハップ	MSCHAPプロトコル
		MSCHAPV2	MSCHAPV2プロトコル
		GTC	GTCプロトコル
	CA証明書	CA証明書	
	アイデンティティ	アイデンティティ	
	匿名アイデンティティ	匿名アイデンティティ	
	パスワード	パスワード	

TLS	CA証明書	CA 証明書
	アイデンティティ	アイデンティティ
	パスワード	パスワード

かそうへいいきもう

接続名	VPN接続の名前

VPNタイプ

かそうへいいきもう

VPNクライアント

AppTec360 VPNクライアント	
ゲートウェイの設定	ゲートウェイVPN設定を選択（「**一般設定**」>「**ユニバーサルゲートウェイ**」>「**VPN設定**」を参照）
常時接続VPN	ネイティブ・ロックダウンを有効にする
AppTec360のロックダウンを有効にする	AppTec360のロックダウンを有効にする

内蔵（サムスン製デバイスでのみ使用可能）			
接続タイプ	PPTP	サーバー	サーバー
		PPTP暗号化を有効にする	PPTP暗号化を有効にする
	L2TP / IPSec PSK	サーバー	サーバー
		IPSec事前共有キー	IPSec事前共有キー
		L2TPシークレットを有効にする	L2TPシークレットを有効にする
		L2TP シークレット	L2TP シークレット
	IPSec XAuth PSK	サーバー	サーバー
		IPSec識別子	IPSec識別子
		IPSec事前共有キー	IPSec事前共有キー
DNS検索ドメイン	DNS検索ドメイン		
エキスパート設定	DNSサーバー	DNSサーバー	
	転送ルート	転送ルート	

オープンVPN		
サーバー	サーバー	
OpenVPNプロファイル	OpenVPNプロファイル	
OpenVPNアプリ	Android用OpenVPN（推奨）	
	OpenVPNコネクト	
エキスパート設定	DNSサーバー	DNSサーバー
	転送ルート	転送ルート

サムスン / ストロングスワン			
接続タイプ	PPTP	サーバー	サーバー
		ユーザー名	ユーザー名
		パスワード	パスワード
		PPTP暗号化を有効にする	PPTP暗号化を有効にする
	L2TP / IPSec PSK	サーバー	サーバー
		IPSec事前共有キー	IPSec事前共有キー
		ユーザー名	ユーザー名
		パスワード	パスワード
		L2TPシークレットを有効にする	L2TP シークレット
	IPSec XAuth PSK	サーバー	サーバー
		IPSec識別子	IPSec識別子
		IPSec事前共有キー	IPSec事前共有キー
		ユーザー名	ユーザー名
		パスワード	パスワード
エキスパート設定	DNSサーバー	DNSサーバー	
	転送ルート	転送ルート	

シスコエニーコネクト		
サーバー	サーバー	
証明書モード	無効	無効
	自動	自動
エキスパート設定	DNSサーバー	DNSサーバー
	転送ルート	転送ルート

アプリごとのVPN

VPNクライアント

AppTec360 VPNクライアント		
ゲートウェイの設定	ゲートウェイVPN設定を選択（「**一般設定**」>「**ユニバーサルゲートウェイ**」>「**VPN設定**」を参照）	
VPNアプリ	VPNアプリ	
常時接続VPN	ネイティブ・ロックダウンを有効にする	常時接続VPN
AppTec360のロックダウンを有効にする	AppTec360のロックダウンを有効にする	

サムスン / ストロングスワン			
接続タイプ	PPTP	サーバー	サーバー
		VPNアプリ	VPNアプリ
		ユーザー名	ユーザー名
		パスワード	パスワード
		PPTP暗号化を有効にする	PPTP暗号化を有効にする
	L2TP / IPSec PSK	サーバー	サーバー
		VPNアプリ	VPNアプリ
		IPSec事前共有キー	IPSec事前共有キー
		ユーザー名	ユーザー名
		パスワード	パスワード
		L2TPシークレットを有効にする	L2TP シークレット
	IPSec XAuth PSK	サーバー	サーバー
		VPNアプリ	VPNアプリ
		IPSec識別子	IPSec識別子
		IPSec事前共有キー	IPSec事前共有キー
		ユーザー名	ユーザー名
		パスワード	パスワード
エキスパート設定	DNSサーバー	DNSサーバー	
	転送ルート	転送ルート	

制限事項

ここでは、接続管理に関する制限を設定することができます。

データローミングを許可する	ローミング中のモバイルデータを許可する
強制データローミング	有効にすると、モバイルデータのローミングが恒久的に有効になります（お勧めしません！）。 この設定は "Allow Data Roaming "設定を上書きする！
以下の設定はSAFE 2.x以降でのみ有効です。	
緊急電話のみ許可	緊急電話のみ許可
WiFiを許可する	WiFiを許可する
WiFiネットワークの最低セキュリティレベル	WiFiネットワークの最小セキュリティレベル オープン = あらゆるタイプのWiFiが利用可能
ユーザーによるWiFiネットワークの追加を禁止	ユーザー自身がWiFiネットワークを追加することはできません。 この設定は、WiFiプロファイルが "接続管理 "で定義されている場合にのみ可能です。
SMSとMMSを許可する	All = すべてのSMSおよびMMSトラフィックが許可されます。 着信SMSのみ = 着信SMSメッセージのみが許可されます。 発信SMSのみ = 発信SMSメッセージのみ許可 None = SMS / MMSトラフィックを許可しない
ローミング中の同期を許可する	ローミング中の同期を許可する オン = 作動 オフ = 無効 ユーザーの選択 = ユーザーの選択
音声ローミングを許可する	音声ローミングを許可する オン = 作動 オフ = 無効 ユーザーチョイス = ユーザーの選択
システムのhttpプロキシサーバーを使用する	HTTPプロキシサーバーの使用は、システムの設定で提供され、接続されたネットワーク（WiFiまたはAPN）に依存します

PIM管理

Gmailエクスチェンジ

情報この設定はGmailアプリに適用されます。そのため、Gmailを承認してインストールする必要があります。

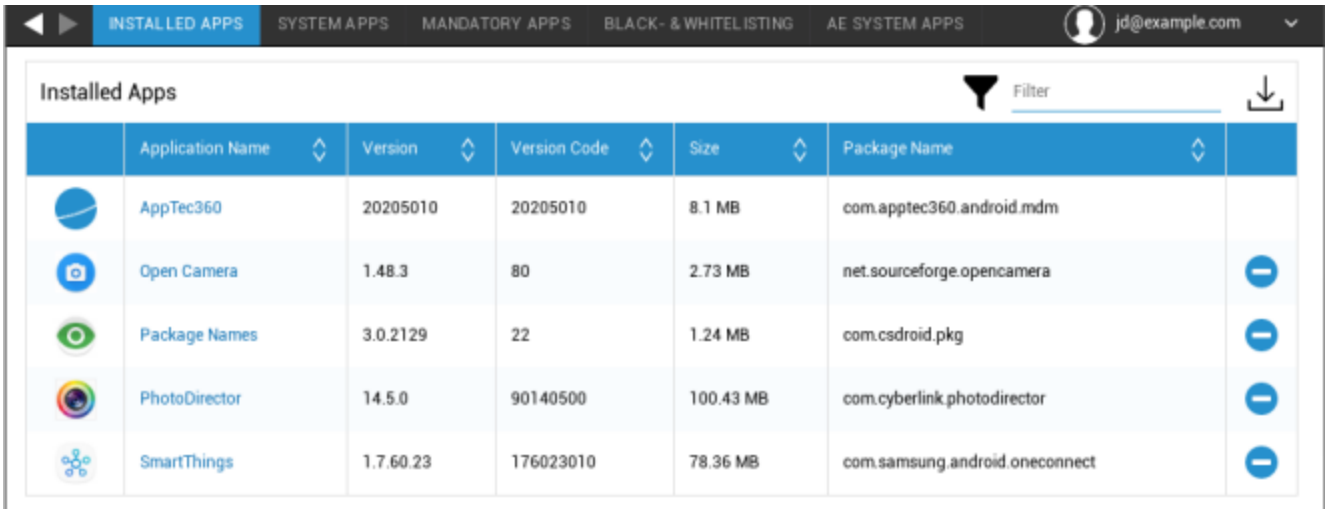
電子メールアドレス	提供されたユーザーのEメールアドレス プレースホルダ "に注意してください。このプレースホルダは、資格情報を扱うために使用することができ、すべてのデバイスで手動で変更を実行することはありません。 クリックするだけで、自分の目で見ることができる。
サーバーホスト名	Exchangeサーバーのサーバーアドレス
ログイン名	各エンドユーザーデバイスのログイン名。
署名	署名を添付することができます。
同期する前の日数	メールのシンクバックを決定する日数
デバイス識別子	EAS DeviceID を含む文字列。これは EAS プロトコルの一部であり、以下の環境で使用できます。
セキュア・ソケット・レイヤー（SSL）の使用	SSL接続を使用する
すべての証明書を受け入れる	すべての証明書が受け入れられます。Exchangeサーバーが自己署名証明書を使用している場合は、このオプションを選択してください。

アプリ管理

エンタープライズアプリマネージャー

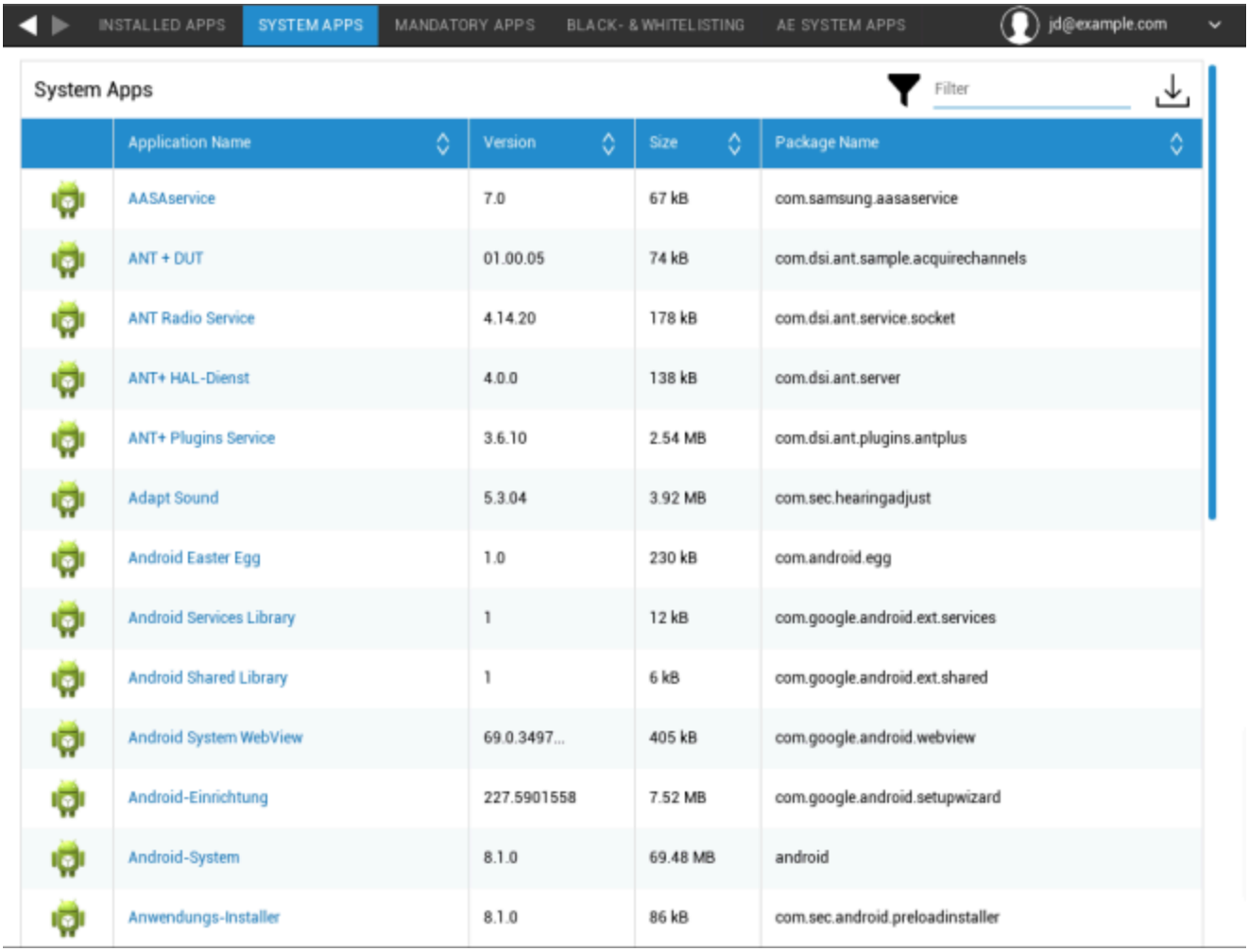
インストール済みアプリ (デバイスレベルのみ)

ここでは、エンドユーザーデバイスに現在インストールされているすべてのアプリが表示されます。



システムアプリ (デバイスレベルのみ)

システムアプリ」の下には、デバイスメーカーがエンドユーザー・デバイスにインストール済みのすべてのアプリとサービスが表示されます。

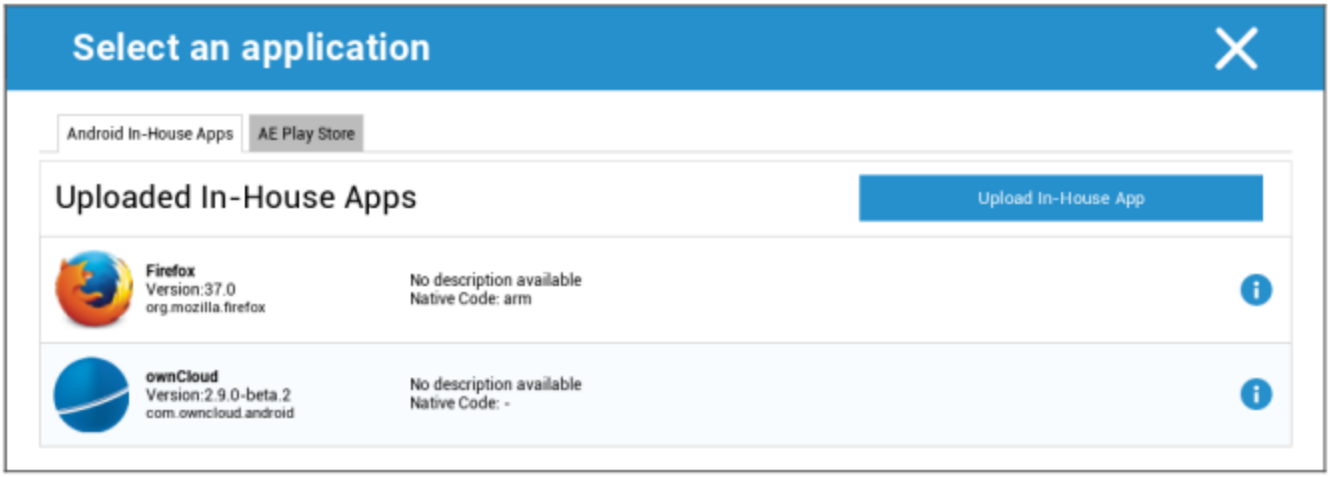


必須アプリ

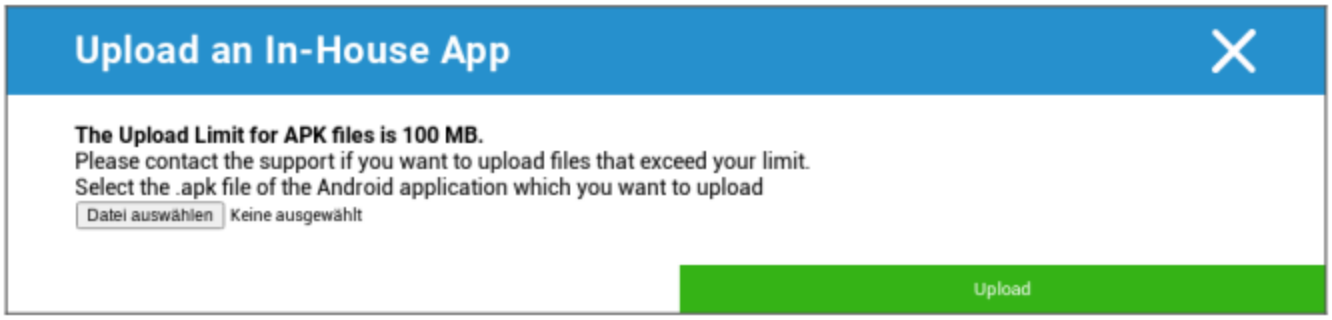
必須アプリ」では、必須アプリを設定することができます。ユーザーは、この指定アプリをインストールするよう継続的に求められます。

を介して、必須アプリを定義することができる。

これは、一般設定でアップロードした "Android In-House Apps "から社内アプリを使用することができます。

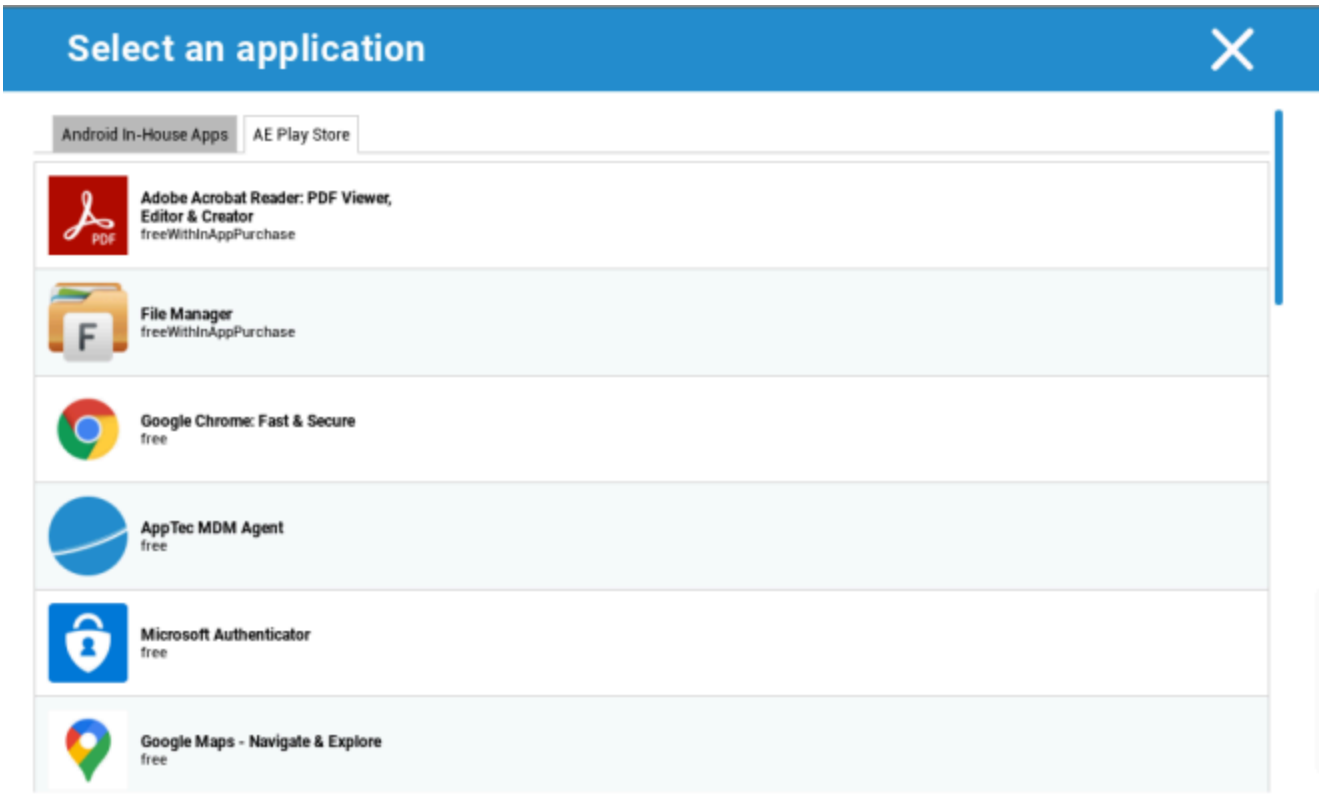


Upload In-House App "で直接apkファイルを選択してアップロードすることもできます。



In-House Appをインストールする場合、"Keep up to date "を有効にすることができます。これが有効になっており、社内アプリDBに新しいバージョンが定義されている場合、アプリはデバイス上で更新されます。

または、Google Work Play Storeの "AE Play Store "アプリでもよい。



このタブには、承認された「AE Playストアアプリ」のみが表示されます。

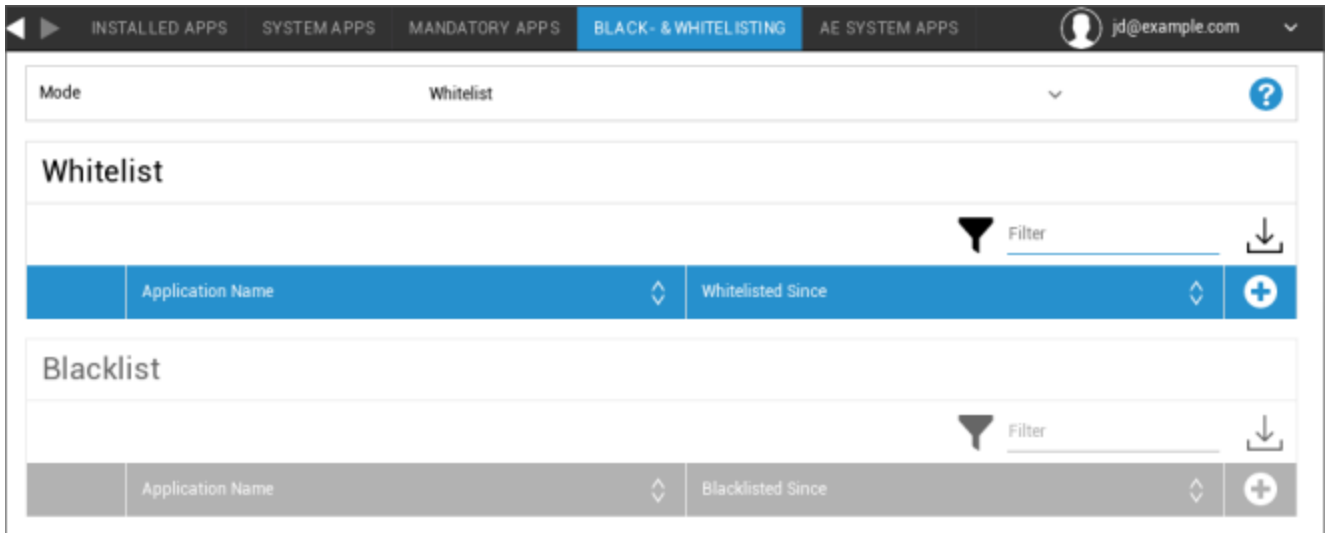
AE Playストアアプリ」を承認するには、「一般設定」→「アプリ管理」→「AE Play」に進んでください。

Store "ボタンをクリックしてアプリを追加すると、"Play Store Apps "タブにリダイレクトされます（または、
"Play Store Apps "タブに直接移動することもできます）。

Playストアのアプリ」タブでは、アプリを検索することができます。アプリをクリックすると、アプリのページが
、ここで「承認」をクリックしてアプリを承認することができます。

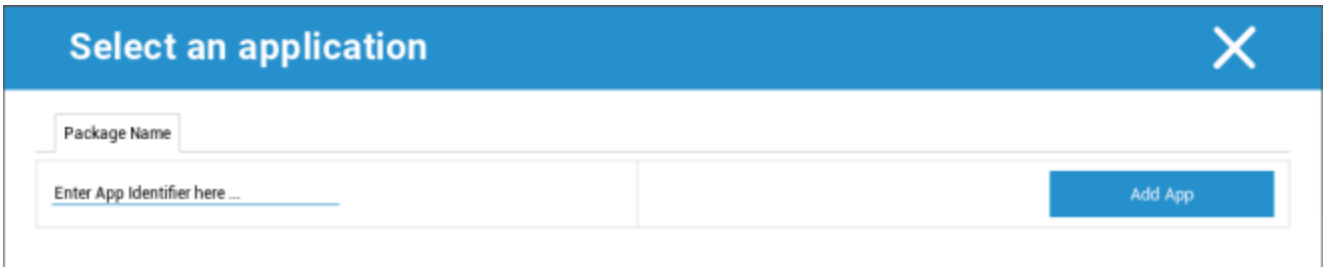
ブラックリストとホワイトリスト

Black- & Whitelisting "では、"Whitelist "モードと "Blacklist "モードを選択できます。



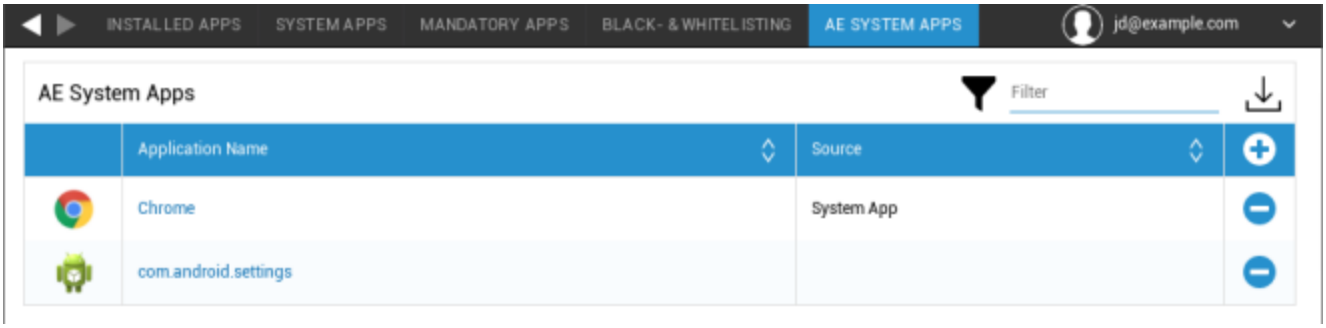
ホワイトリスト	エンドユーザーデバイスにインストールできるのは、リストに追加されたアプリとサービスのみです。エンドユーザーデバイスにすでにプリインストールされている場合は、アクティベートされ、ユーザーが実行できるように設定されます。
	リストに追加されていないその他のアプリは、エンドユーザーデバイスにインストールできません。エンドユーザーデバイスにすでにプリインストールされている場合は、無効化され、ユーザーが実行できないように設定されます。
ブラックリスト	リストに追加されたアプリやサービスは、エンドユーザーデバイスにインストールできません。エンドユーザーデバイスにすでにプリインストールされている場合は、無効化され、ユーザーが実行できないように設定されます。
	リストに追加されていない他のすべてのアプリは、エンドユーザーデバイスにインストールすることができます。エンドユーザーデバイスにすでにプリインストールされている場合は、アクティベートされ、ユーザーが実行できるように設定されます。

を介して、現在使用中のリストにアプリやサービスを追加します。
「Packagename」を定義することができます：

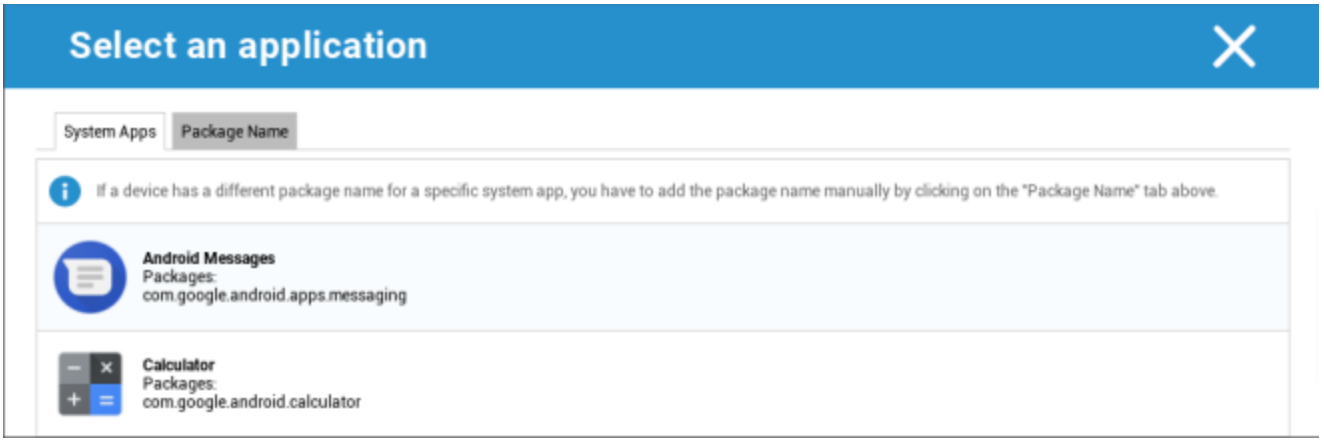

Select an application
Package Name
Enter App Identifier here ...
Add App

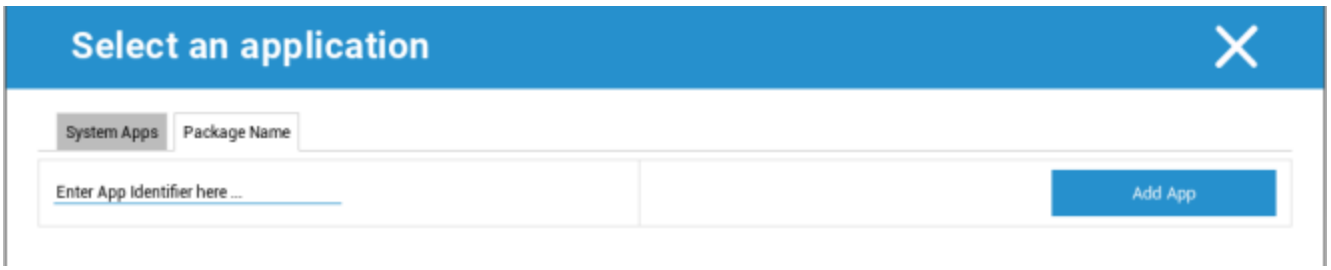
AEシステムアプリ

ここでは、デバイス上で有効化されるべき特定のシステムアプリを含むリストを定義することができます。



ボタンをクリックすると、グーグルが提供する可能なシステムアプリのリストから選択するか、有効化すべきシステムアプリのパッケージ名を直接入力することができる。





Googleが提供するリストにあるシステムアプリは、システムアプリになりうるアプリに過ぎず、必ずしもお使いの端末のシステムアプリである必要はないことにご留意ください。

ただし、このリストはすでにプリインストールされているアプリにのみ影響する。

端末にプリインストールされていないアプリを追加しても、Googleが提供するリストからアプリを追加しても、アプリのパッケージ名を直接入力しても、端末に影響はありません。

制限と設定

アプリ管理設定

ここでは、アプリのアップデートに関するデバイスの動作を設定できます。

更新頻度	AppTec360 Clientがアプリのアップデートを検索する間隔を指定します。デフォルト値は24時間です。
Wi-Fi しきい値	指定サイズ以上のアプリはWi-Fi経由でダウンロードされます。Wi-Fiのみ」を選択すると、すべてのアプリがWi-Fi経由でダウンロードされます。

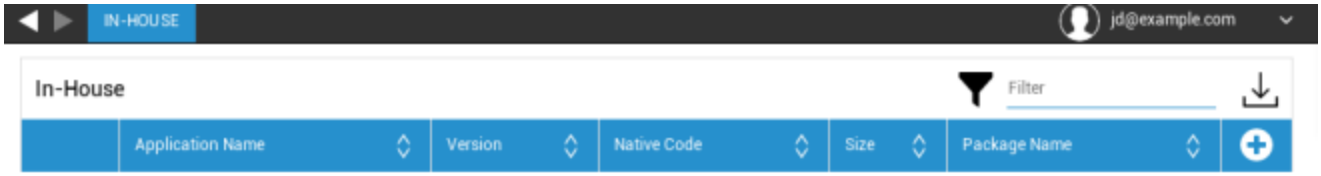
エンタープライズ・アプリケーション・ストア

インハウス

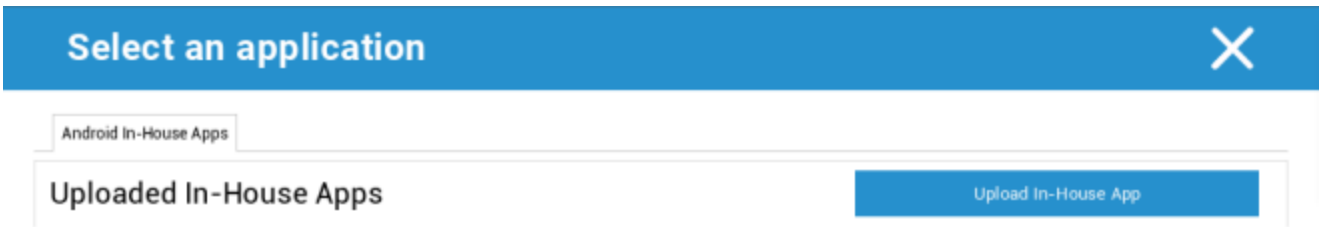
In-House（社内開発）」では、社内で開発したアプリをアップロードして配布することができます。

このシンボルがあれば、インハウスアプリを追加で配布できる。

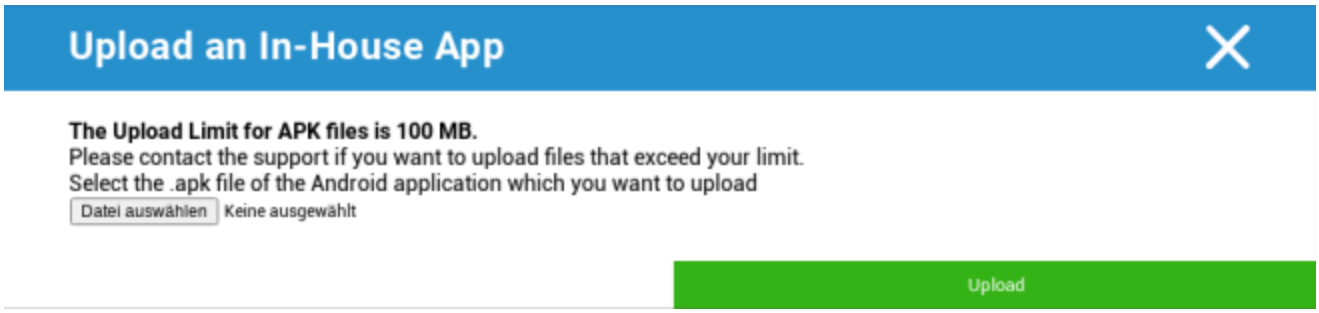
社内アプリをインストールする場合、「Keep up to date」を有効にすることができます。
が有効になっており、社内アプリDBで新しいバージョンを定義している場合、アプリはデバイス上で
更新されます。



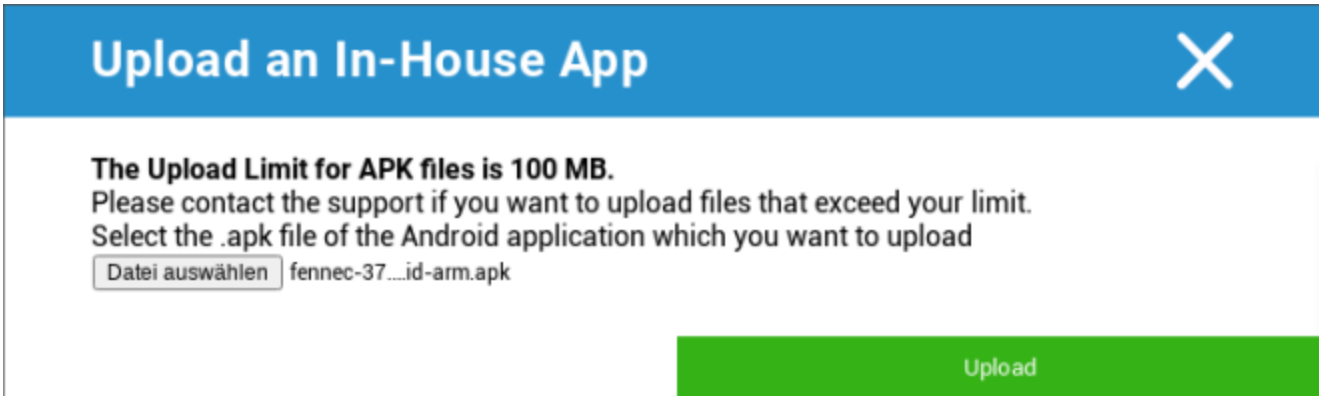
In-House Appsを配布していない場合は、以下の概要が表示されます：



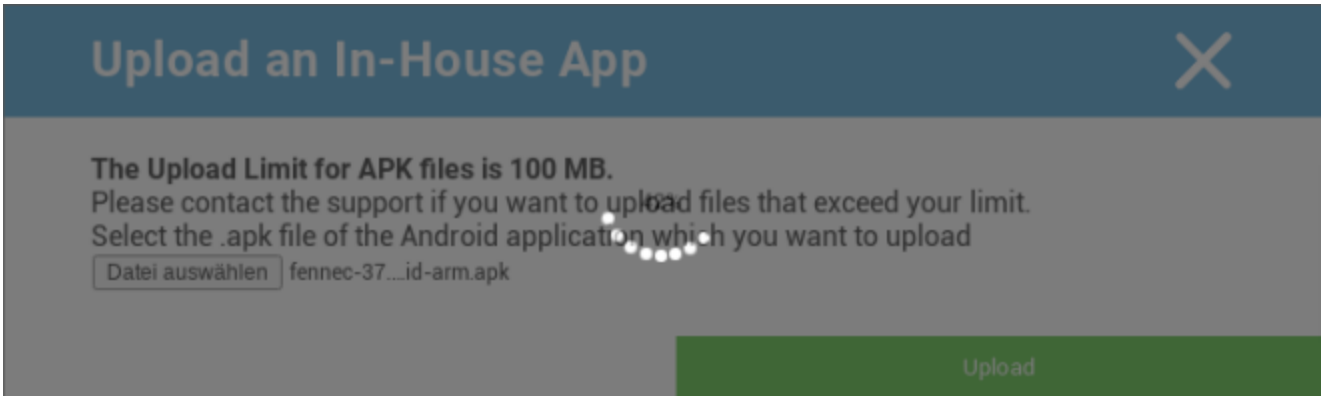
社内アプリのアップロード」をクリックすると、以下のような概要が表示されます：



Search... "で.apkファイルを選択し、"Upload "をクリックします。



アプリがアップロードされ、円の中央にパーセンテージのインジケータが表示されます。
、アプリのどれだけがすでにアップロードされたかを示しています。



社内アプリのアップロードが成功すると、アップロードされたアプリがアプリカタログで
。

ユーザーは、エンドユーザー
デバイスの AppTec360 Store の「社内」カテゴリで、このアプリを確認し、インストールするオプションがあります。

Google PlayStoreアプリを使用しないため、エンドユーザーの端末にGoogle
IDを保存する必要はありません。

エンタープライズPlayストア

AE Playストア

ここでは、Android Enterprise Playstore にアプリを追加できます。アプリを追加する前に、AE 管理者アカウントで
アプリを承認する必要があります。

アプリの承認については、「必須アプリ」の説明を参照してください。

キオスクモード＆ランチャー

キオスク・モード

キオスク・モードでは、アプリやURLを事前に定義することができます。そうすれば、
、このアプリやURLを実行/訪問することが排他的に可能になります。

同様に、様々なハードウェアボタンは、キオスクモードで無効にすることができます。

自動スタート	プロファイルがエンドユーザーデバイスに到達すると同時に、自動的にキオスクモードを開始します。
キオスクモードの予定？	キオスクモードの時間を設定することができ、設定した時間に自動的に開始・終了します。
開始時間	開始時間
時間（分	キオスクモードが再び終了するまでの時間（分単位

アプリケーション・タイプ	
シングルアプリ	キオスクモードでアプリを起動したい場合は、"Application Type "で"Package "を選択します。
キオスク・アプリケーション	キオスクモードで起動するアプリを選択するには、ここをクリックします。 通常のアプリ管理の概要をご覧いただけます。 Google Play ストア」、「Android 社内アプリ」、「パッケージ名」から選択できます。

アプリケーション・タイプ	
URL	キオスク・モードでURLを起動したい場合は、"Application Type "で "URL "を選択します。 次に、希望のURLアドレスを定義します。
非アクティブの後にブラウザをクリアする	ここでは、キオスクモードを再起動する時間間隔を分単位で定義できます。
ウェブキャッシュとクッキーを消去する	この機能を有効にすると、キオスクモードの再起動後、ウェブキャッシュ（クッキーとキャッシュされた画像）が消去されます。
同一原産地ポリシー	この機能が有効な場合、ユーザーは定義されたURLのサブページのみを閲覧することができます。 例えば、次のURLを定義したとする。www.mypage.comすると、ユーザーはwww.mypage.com/subpage。
ホワイトリストのURL	ここでホワイトリストを維持することができ、これらのURLはすべて許可されます。 1行につき1URLまで URLはhttp:/またはhttps:// で始まる必要があります。
ブラックリストに掲載されたURL	ここでブラックリストを管理することができます。 1行につき1URLまで URLはhttp:/またはhttps:// で始まる必要があります。
画面の向き	この設定は画面調整に関連する オートマティック = 自動 ポートレート = 縦型 ランドスケープ = 風景モード

マルチアプリ	マルチアプリ」キオスクモードを選択した場合、AppTec360 Launcher の使用が強制されます。
アプリ	アプリケーションキオスクアプリとしてPlaystoreまたは社内アプリを選択します。パッケージ名を入力することも可能です。選択したキオスクアプリはデバイスにインストールされている必要があります。キオスクアプリケーショ ンを必須として設定することを忘れないでください。 ホームスクリーンへのショートカット：オン」に設定すると、ホームスクリーンにショートカットが作成されます。オフ」に設定しても、アプリはアプリ一覧に表示されます。

終了パスワード 有効	この機能を有効にすると、ユーザーが事前に設定したパスワードでキオスクモードを終了することができます。
終了パスワード	これは、あなたが事前に設定したパスワードです。
ステータスバーの自動折りたたみ	このオプションを有効にすると、ステータスバーが自動的にカラー表示になります。このオプションを使用すると、ユーザーはステータスバーの情報を見ることができますが、その機能にアクセスすることはできません。
ステータスバーを無効にする	ステータスバーには、通知、ショートカット、情報が表示されます。SAFE 4.0以上を搭載したSamsung製デバイスでのみ利用可能です。
ボリュームキーを無効にする	ボリュームキーを無効にする（SAFE 3.0以上のSamsungデバイスでのみ使用可能）
オン / オフスイッチの無効化	オン/オフスイッチを無効にする（SAFE 3.0以上のSamsungデバイスでのみ使用可能）
ホームボタンを無効にする	ホームボタンを無効にする。この機能が有効になっている場合、キオスクモードはAppTec360 コンソールでのみ終了できます。 (SAFE3.0以上のSamsungデバイスでのみ利用可能)
ナビゲーションバーを無効にする	ナビゲーションバー（戻る/メニュー）を無効にすることができます。 この機能が有効になっている場合、キオスクモードは AppTec360 コンソールでのみ終了できます。 (SAFE3.0以上のSamsungデバイスでのみ利用可能)

AppTec360 ランチャー

AppTec360 Launcherを有効にする	オンAppTec360 Launcherを有効にします。ユーザーはこれをデフォルトランチャーとして1回設定する必要があります。 注：キオスクモードが有効で、キオスクモードが "Multi App "に設定されている場合、AppTec360ランチャーの使用が強制されます。
大きなアイコン	オンランチャーにアプリのアイコンを大きく表示します。
AppTec360アプリのアイコンを隠す	オンAppTec360アプリを完全に隠す
AppTec360ストアアイコンを隠す	オンAppTec360 Enterprise AppStoreを完全に非表示にします。

AppTec360の設定

AppTec360設定アプリを有効にする	AppTec360設定アプリは、WiFiとBluetooth接続を制御します。
マルチアプリで設定を有効にする キオスク・モード	有効な場合、ユーザーはマルチアプリキオスクモードがアクティブである間、AppTec360設定アプリにアクセスできます。

リモコン

スプラッシュトップ

デバイスのリモートコントロールセッションを開始するには、アプリ**管理** → **エンタープライズアプリマネージャー** → **必須アプリに**アプリ「Splashtop Streamer」を追加し、デバイスにインストールする必要があります。

その後、Splashtop の以下の設定を行います：

Splashtopを有効にする	有効な場合、AppTec360 は Splashtop アプリを構成し、リモートコントロールを許可します。
コードのデプロイ	https://my.splashtop.comにアクセスし、Splashtop アカウントにログインします。コンピュータの追加」をクリックし、表示されたページから12桁のデプロイコードをコピーします。
カスタムデプロイ・ゲートウェイを設定しますか？	ゲートウェイの展開
ゲートウェイ・ドメイン / ホストの展開	ゲートウェイの展開
証明書の検証	証明書の検証

その後、コンテキストメニュー (デバイスが選択されている場合、検索バーの横の歯車、またはツリー内のデバイスを右クリック) のオプションSplashtopリモートコントロールを使用して、リモートコントロールセッションを開始することができます。

チームビューアー

デバイスのリモートコントロールセッションを開始するには、**[アプリ管理]→[Enterprise App Manager]→[必須アプリ]**にアプリ「TeamViewer QuickSupport」を追加して、デバイスにインストールする必要があります。

次に、コンテキストメニュー(デバイスが選択されている場合は検索バーの横の歯車、ま たはツリー内のデバイスを右クリック)の[**TeamViewer リモートコントロール**]オプショ ンを使用して、リモートコントロールセッションを開始できます。

コンテンツ管理

コンテンツボックス

ここでContentBoxをアクティブにすることができます。

ContentBoxを有効にする」を「オン」に切り替えるとすぐに、別のContentBoxアプリがエンドユーザーデバイスに
、自動的にインストールされます。

セキュアブラウザ

ここでは、AppTec360 Secure Browser の設定を構成できます。

セキュア・ブラウザ "のセクションを "オン "に切り替えるとすぐに、別個のブラウザ・アプリが、エンドユーザー・デバイスに自動的にインストールされます。

パスワードが必要	ブラウザーにアクセスするためにパスワードを設定し、使用することをユーザーに要求する。
最低限必要なパスワードの長さ	パスワードに必要な文字数を設定する
必要なパスワードの品質	必要なパスワードの品質を設定する
ダウンロードを制限する / で開く	
アップロードの制限	
ホワイトリストのアップロード	アップロードが常に許可されるURLのリスト。
コピーを許可する	ウェブページ内のテキストのコピー、切り取り、共有を許可する。
スクリーンキャプチャを許可する	スクリーンショットのキャプチャを許可する。
データ・クリーンアップの頻度	すべてのユーザーデータ (履歴、キャッシュなど) を自動的に削除する頻度を選択します。
会社のしおり	ブックマークは、ブラウザのブックマークにある「会社のブックマーク」フォルダに表示されます。 ユーザーは編集できない。
アドレスバーを隠す	
ブラウザ内ホワイトリスト (ユニバーサルゲートウェイなし)	クライアント側のURLホワイトリストを有効にする。 • 会社のブックマークは常にホワイトリストに登録される • 100URLのみ対応 • 無制限のブラックリストおよびホワイトリスト登録には、ユニバーサルゲートウェイをご利用ください。
ホワイトリストのURL	許可されたURLのリスト。
ゲートウェイベースのブラックリストとホワイトリスト	ブラックリストには以下の条件がある： • AppTec360ユニバーサルゲートウェイが動作していること (「一般設定」→「ユニバーサルゲートウェイ)

	• DNSサーバーを指定したVPN設定（「一般設定」→「ユニバーサルゲートウェイ」→「VPN設定） • ブラックリストの設定（「一般設定」→「ユニバーサルゲートウェイ」→「ドメインブラックリスト） • プロファイル内の有効なVPN接続（「接続管理」→「VPN）

追加API

サムスンKNOX

制限事項

SDカードを許可する	
SDカードの書き込みを許可する	
スクリーンキャプチャを許可する	
クリップボードを許可する	
Google Cloudで設定とアプリデータをバックアップ	
アプリの再インストール時にGoogle Cloudから設定を復元する	
USBデバッグを許可する	
グーグルクラッシュレポートを許可する	
ファクトリーリセットを許可する	
OTAアップグレードを許可する	
USBホスト・ストレージを許可する	有効にすると、ユーザーは任意のペンドライブ（ポータブルUSBストレージ）、外付けHD、またはセキュアデジタル（SD）カードリーダーを接続することができ、それはデバイス上のストレージドライブとしてマウントされます。
USBメディアプレーヤーを許可する(MTP,PTP)	
マイクを許可する	サードパーティ製アプリケーションのマイクを無効にする
NFC（近距離無線通信）を許可する	

不明なソースを許可する（APKサイドローディング）	有効にすると、アプリ（APKファイル）のサイドローディングが許可されます。 この設定を無効にすると、ソース不明からのAPKのインストールを許可する際に、ユーザーは手動で有効にする必要があります。
ユーザー作成を許可する	有効な場合、ユーザーはデバイス上に複数のアカウントを作成することができます。

電子メール

電子メールアドレス	
受信サーバープロトコル	
受信サーバーアドレス	
受信サーバーポート	
受信サーバーのログイン名/ユーザー名	
受信サーバーのパスワード	
受信サーバーがSSLを使用	
受信サーバーはTLSを使用	
受信サーバーはすべての証明書を受け入れる	
送信サーバー・プロトコル	
送信サーバーアドレス	
送信サーバーポート	
送信サーバーが余分な認証情報を使用	無効の場合、システムは受信認証情報を送信サーバーにも使用する。
送信サーバーのログイン名/ユーザー名	
送信サーバーパスワード	
送信サーバーはSSLを使用	
送信サーバーはTLSを使用	
送信サーバーがすべての証明書を受け入れる	
セット署名	
署名	注：デバイスによっては、署名をHTML形式で指定する必要があります。
新着電子メールの受信通知	

交換

電子メールアドレス	
サーバーホスト名	Exchangeサーバーのホスト名
ログイン名	Exchange サーバーへのログインに使用するユーザー名。
ドメイン	ACL Gateway Configuration が有効で、Domain フィールドが空でない場合、AppTec360 Universal Gateway は以下の名前「DomainLogin Name」でデバイスを認証する。
パスワード	
同期する前の日数	
eメールの同期頻度	
ローミング中の同期	
セット署名	
署名	注：デバイスによっては、署名をHTML形式で指定する必要があります。
デフォルトアカウント	
セキュア・ソケット・レイヤー（SSL）の使用	
トランスポート・レイヤー・セキュリティ（TLS）を使用する	
すべての証明書を受け入れる	

APN

APN表示名	
アクセスポイント名	APN名
送信サーバー・プロトコル	
MCC - モバイル国コード	インストールされているSIMのmmcを使用する場合は空のままにする
MNC - モバイル・ネットワーク・コード	インストールされているSIMのmncを使用する場合は空のままにします。
サーバーアドレス	
サーバーポート番号	
サーバー・プロキシ・アドレス	
MMSサーバーアドレス	デフォルトは空のまま
MMSポート番号	デフォルトは空のまま
MMSプロキシアドレス	デフォルトは空のまま
ユーザー名	
パスワード	
アクセス・ポイント・タイプ	使用可能なタイプは "default"、"mms"、"supl"。
	NULLまたは空文字列が渡された場合、デフォルトで "default,supl,mms "が使用される。
	デフォルトは空のまま。
優先APN	

ブルートゥース

Bluetoothによるデバイス検出を許可する	
Bluetoothペアリングを許可する	
Bluetoothヘッドセットを許可する	
Bluetoothハンズフリーデバイスを許可する	
BluetoothのA2DPデバイスを許可する	A2DP（アドバンスト・オーディオ・ディストリビューション・プロファイル）により、機器間でオーディオ・ストリーミングが可能
発信を許可する	
ブルートゥースによるデータ転送を許可する	
Bluetoothテザリングを許可する	
ブルートゥースによるコンピュータへの接続を許可する	

接続

緊急通話のみ許可Wi-Fiを許可する	
Wi-Fiネットワークの最低セキュリティレベル	
Wi-Fiネットワークの追加を禁止	この制限は、接続管理の下に少なくとも1つのアクティブなWi-Fiプロファイルが定義されている場合にのみ有効です。
SMSとMMSを許可する	
ローミング中の同期を許可する	
音声ローミングを許可する	

Android Enterprise – ワークプロファイル（COPE）付きフルマネージドデバイス

COPEの一般的説明

COPEとは、**Corporate Owned Personally Enabledの**略。

COPE モードでは、Android デバイスを**Android Enterprise - コンテナ**プロファイルを統合した **Android Enterprise - Fully Managed Device** として登録できます。

これは、**Android Enterprise - Fully Managed Device**として登録済みで、**Android Enterprise - Container が**追加でセットアップされている Android デバイス、または**Android Enterprise - Fully Managed Device**として直接登録され、その上に**Android Enterprise - Container が**セットアップされている新規登録 Android デバイスのいずれかです。

COPEモードは、Android 8、9、10を搭載したデバイスでのみ利用可能です。

COPEデバイスのプロファイル設定

COPEモード自体のConfigurationプロファイルはないため、**Android Enterprise - Fully Managed Deviceと Android Enterprise - Containerの**設定はCOPEプロファイル内で2つのプロファイルに分かれています。コンソールの左側にあるそれぞれのボタンをクリックすることで、各プロファイルの設定を2つのプロファイルに切り替えることができます：

どちらのプロファイルも、各プロファイルの説明に従って設定することができる：

Android Enterprise - フルマネージド・デバイス

Android Enterprise - コンテナ

AEフルマネージド・デバイスに戻す

Android Enterprise - Containerプロファイルは、「**モバイル管理**」の説明に従って削除できます。

コンテナプロファイルを削除することで、COPEプロファイルは**Android Enterprise - Fully Managed Device**プロファイルに変換されます。

Android Enterprise – コンテナの構成

現在選択されているのがグループプロファイルかデバイスかによって、概要とそのサブポイントが異なります！

一般

プロフィール概要（プロフィールレベルのみ）

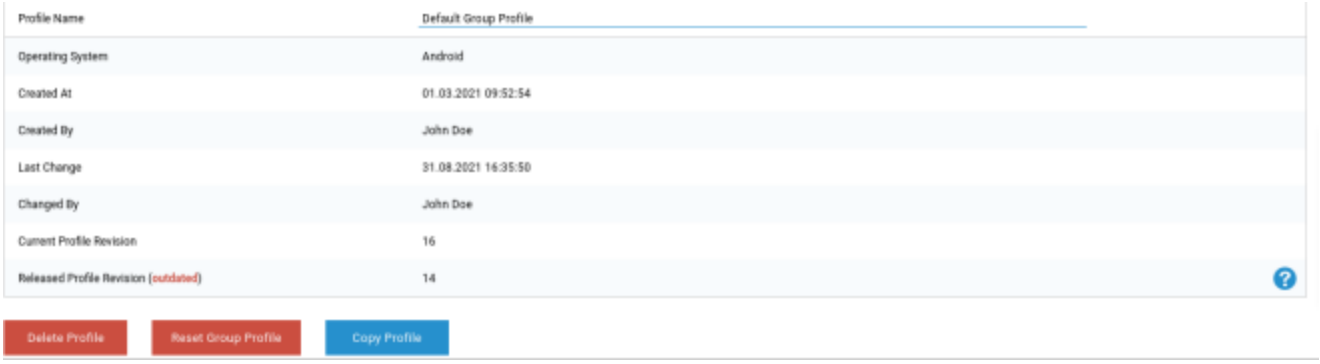
プロフィールに入ると、名前、OS、作成日、作者など、プロフィールの簡単な概要が表示されます。

プロフィール名	プロフィール名 - ここで直接名前を変更できます。
オペレーティングシステム	プロファイルに有効なOS
作成日時	作成日
作成者	作成者
最後の変更	最終変更日
変更履歴	このプロファイルの最後の変更を実行したユーザー
現在のプロフィール改訂	プロフィールの更新回数
プロフィール改訂版をリリース	プロファイルがすでに更新され、デバイスが割り当てられた回数

プロフィール削除	プロフィール削除
グループプロファイルのリセット	グループプロファイルのリセット
コピープロフィール	コピープロフィール

グループプロフィールの概要（グループレベルのみ）

グループプロフィールを開くと、プロフィールの概要が表示されます。



プロフィール名	プロフィールの名前（ここで変更可能）
オペレーティングシステム	対象OS
作成日時	創造の時
作成者	プロフィールの作成者
最後の変更	プロフィールの最終変更時刻
変更履歴	最後の変更を行ったアカウント
現在のプロフィール改訂	保存されたプロファイル状態の修正
プロフィール改訂版をリリース	割り当てられたプロファイルのリビジョン（"Assign now"）。ラベルのテキストの後ろに"(outdated) "と表示されている場合は、プロファイルを保存したものの、まだ割り当てていないことを意味します。

デバイスの概要（デバイスレベルのみ）

デバイスを選択すると、選択したデバイスの概要が表示されます：

デバイス名	デバイス名
所在地	位置座標
電話番号	電話番号
割り当てられた必須アプリ	割り当てられた必須アプリの数
OSバージョン	デバイスのOSバージョン
オペレーティングシステム	オペレーティング・システム（アンドロイド・エンタープライズ）
シリアル番号	デバイスのシリアル番号
デバイスの所有権	企業用またはプライベート用デバイス
デバイス・タイプ	AEワーク管理デバイス
ルーツ	デバイスがルート化されているかどうかを示すステータス
準拠	ガイドライン準拠
IPアドレス	デバイスのIPアドレス
ラストシーン	デバイスが最後にAppTecに接続した時点
ラスト・プッシュ	最後のプッシュがデバイスに送信された時点
ユーザー割り当て	このデバイスが割り当てられているユーザーまたはグループ

コンフィグ改訂

ここで、どのグループプロファイルがデバイスに割り当てられているかの概要が表示されます。

グループプロフィールをクリックすると、そのプロフィールに直接アクセスでき、設定を行うことができます。

このマークがあれば、配布されたアプリをグループプロファイルの設定に戻すことができる。

このマークがあれば、使用中のアプリをすべてグループプロファイルの設定に戻すことができます。

"Newer Revision available "は、グループプロファイルが変更され保存されたが、割り当てられていないことを示します。グループプロファイルの変更をデバイスに適用するには、グループレベルで

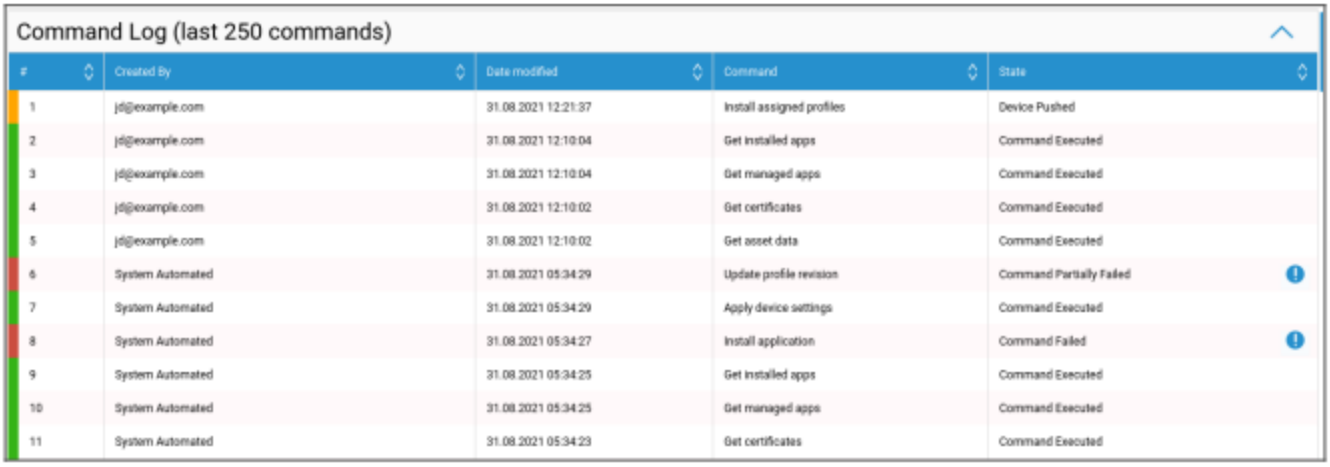
"Assign now "を使用してグループプロファイルを割り当てる必要があります。

デバイスログ (デバイスレベルのみ)

ここでは、様々なデバイスログが表示されます。必要であれば、ここで直接エラーの原因を見つけることができます。

コマンドログ

ここでは、デバイスに対して発行されたコマンドとそのステータスを確認することができます。



可能なコマンドステータス

デバイスが押される	プッシュリクエストは、EMM サーバーに接続するようデバイスに指示するため、プッシュサービス（APNS など）に送信されました。
コマンド作成	コマンドがシステム内に作成された。
コマンド送信	コマンドは、サーバーに接続された後、デバイスに送信された。
コマンド実行	コマンドは正常に実行された。
コマンド失敗	コマンドが失敗しました。*
コマンド一部失敗	デバイスのOSによっては、いくつかのコマンドがグループ化されることがある。 このコマンドグループの一部は失敗した。*
コマンドは実行されたが、最終的に失敗	コマンドは実行されたが、もしかしたら実行されていなかったかもしれない。
コマンド・リパッシュ	コマンドはユーザーによってリプッシュされた。
廃棄	コマンドが破棄された。例えば、他のコマンドに取って代わられたとか、デバイスが再登録されて古いコマンドが削除されたとか。

*メッセージの後ろにエクスクラメーションマークが表示されている場合は、カーソルをアイコンの上に置くと詳細な情報を得ることができます。

デバイス設定

クライアント設定

ここでは、Androidデバイスの以下の設定を行うことができます：

コンプライアンス違反の時間	強制アクションが適用されるユーザー応答タイムアウト制限。
コンプライアンス・タイムアウト後の強制措置	適合デバイスのステータスにつながるアクションをユーザーが実行しない場合の強制アクション
データ収集頻度	デバイス/GPS情報の収集頻度
デバイスのハートビート周波数	デバイスがAppTecサーバーに連絡する間隔 最短1分 最大24時間
位置情報の更新を有効にする	アクティブにすると、デバイスは位置情報の更新をAppTecサーバーに送信します。
場所 更新時間	デバイスがAppTecに位置情報の更新を送信する時間間隔を決定します。
位置情報の更新にGoogle Location Accuracyを使う	有効にすると、位置情報の更新にネットワークの位置情報が使用されます。
位置情報の更新にGPSロケーションを使用	アクティブにすると、位置情報の更新にGPSが使用されます。
モック（偽）ロケを許可する	サードパーティアプリによる位置情報の偽造を許可する
ロスト・コネクション	有効にすると、デバイスがハートビート間隔内に MDM サーバーへの接続を取得しない場合のアクションを指定できます。たとえば、デバイスのハートビート時間が5分の場合、午前10時35分にサーバーに接続します。その後、デバイスはWi-Fi範囲から外れます。次の午前10時40分のハートビートは失敗し、指定されたアクションが実行されます。

アクション	デバイスが非準拠となった場合に直ちに取られるべき措置。 • Lock Device = ロック・デバイス • デバイスのワイプ = デバイスが工場出荷時の設定に復元されます。 • デバイスとSDカードのワイプ = デバイスは工場出荷時の設定に復元され、SDカードのストレージは削除されます。
しきい値	指定したアクションのトリガーに必要な、失敗したハートビートの閾値を指定できます。

ポリシー実施モード	デフォルト：	ユーザーには、未解決のアクションを実行するよう定期的にプロンプトが表示されます。
	怠惰なポリシーの実施：	未解決のアクションの実行をユーザーに促すことはありません。すべての未解決のアクションはAppTec Clientに表示されます。
	積極的なポリシー実施：	ユーザーは、未解決のアクションを実行するようノンストッププロンプトが表示される。
AppTecバージョンロック	有効にすると、AppTecアプリのバージョンコードを指定できます。AppTecクライアントは、指定されたバージョンにのみアップデートします。新しいバージョンは無視されます。ダウングレードはできません。	
バージョンコード	ロックオンされるAppTecアプリのバージョンコード。	
AppTec通知を無効にする	無効にすると、AppTecクライアントは通知バーに通知を表示しません。そのため、ユーザーはタスクマネージャーでAppTecクライアントを閉じることができます。AppTecクライアントを閉じると、キオスクモードやアプリのブラックリスト/ホワイトリストなどのいくつかの機能が正しく動作しなくなります。 Samsungデバイスは、AppTecクライアントの保護メカニズムを提供します。KNOX APIをサポートするSamsungデバイスでは、通知はデフォルトで無効になっています。アンドロイド8.0以上の端末では、この通知が無効になることはありません。	

壁紙

カスタム壁紙の設定	カスタム壁紙の有効/無効
壁紙	カラーコードまたは画像を使用する壁紙モードを設定する。
色の指定	背景色を16進数で指定する（例：#000000は黒、#ffffffは白）。
画像を壁紙に設定する	壁紙にしたい画像ファイルをアップロードする

資産管理 (デバイスレベルのみ)

デバイス情報

モデル	機器モデル名
オペレーティングシステム	OS
OSバージョン	OSバージョン
シリアル番号	シリアル番号
デバイス名	デバイス名
バッテリーの状態	バッテリーの状態
フリー/トータルメモリー	空き/総メモリ
サムスン金庫	様々な設定オプションに必要なサムスンSAFEインターフェース
利用可能なSDカード	SDカードあり
エミュレートされたSDカード	エミュレートされたSDカード
リムーバブルSDカード	SDカード取り外し可能
SD空き/総メモリ	SD空き容量/SDカード空き容量

Wi-Fi

IPアドレス	デバイスIPアドレス
WiFi MAC	WiFiのMACアドレス

セルラー

ステータス	ステータス（SIMカード装着）
電話番号	電話番号
ローミング（音声/データ）	音声/データのローミング
ローミング状況	現在のローミング状況
IPアドレス	IPアドレス
オペレーター/キャリア	オペレーター/キャリア
セルラー技術	セルラー技術
IMEI	IMEI番号
国際ID	これはSIMカードのIDであり、多くの場合、スマートカードまたは集積回路カード（ICC）でもある。
移動加入者識別番号	IMSI（International Mobile Subscriber Identity）は、GSMおよびUMTSモバイル・ネットワークにおいて、ネットワーク・ユーザーの明確な識別を提供する。 IMSIは最大15桁で構成され、以下のように設定される： • 携帯国番号（MCC）、3桁 • モバイル・ネットワーク・コード（MNC）、2桁または3桁 • 携帯電話加入者識別番号（MSIN）、1～10桁
現在のMCC/MNC	SIM MCC/MNC」を参照。
SIM MCC/MNC	モバイル国コードは、E.212標準に従ってITUによって設定された、確立された国識別子です。これは、モバイル・ネットワーク・コード（MNC）と連動してモバイル・ネットワークを識別します。 SIMカードの国/モバイルネットワークコードを意味する。 別のモバイルネットワークにローミングする場合、論理的には、「現在のMCC/MNC」と「SIM MCC/MNC」は異なる。

ブルートゥース

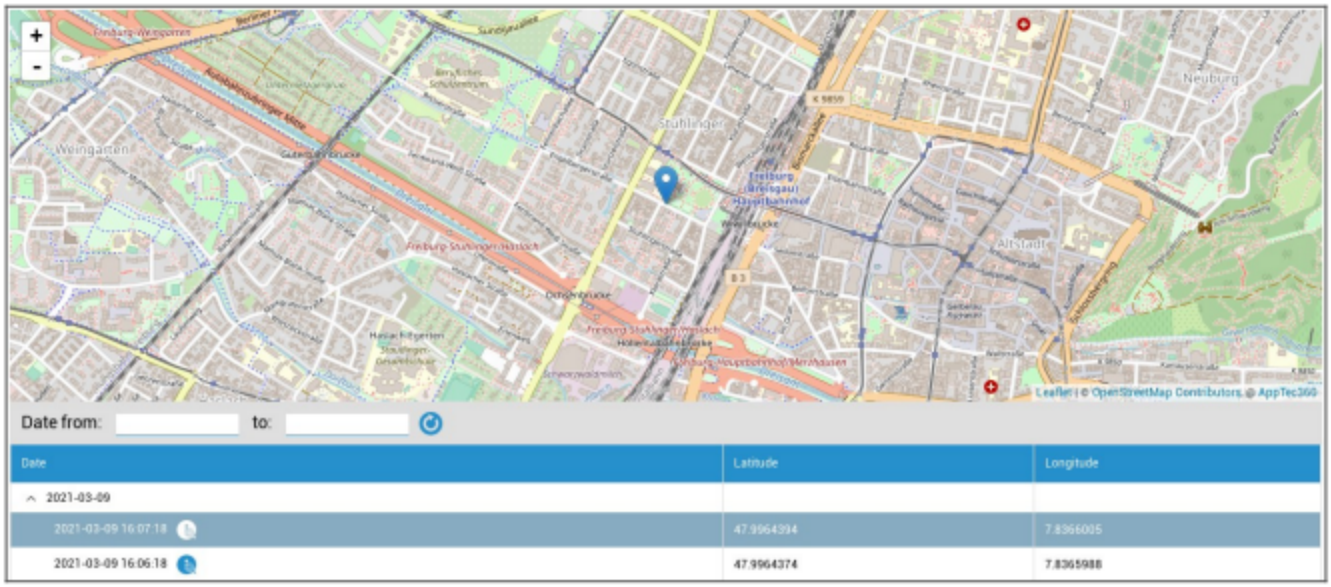
ブルートゥースMAC	ブルートゥースMACアドレス

セキュリティ管理

盗難防止（デバイスレベルのみ）

GPS情報（デバイスレベルのみ）

ここでデバイスの現在地/最終位置を設定できます。ローカライズは1つまたは2つのパスワードで保護することができます：一般設定 - プライバシー - GPSアクセス



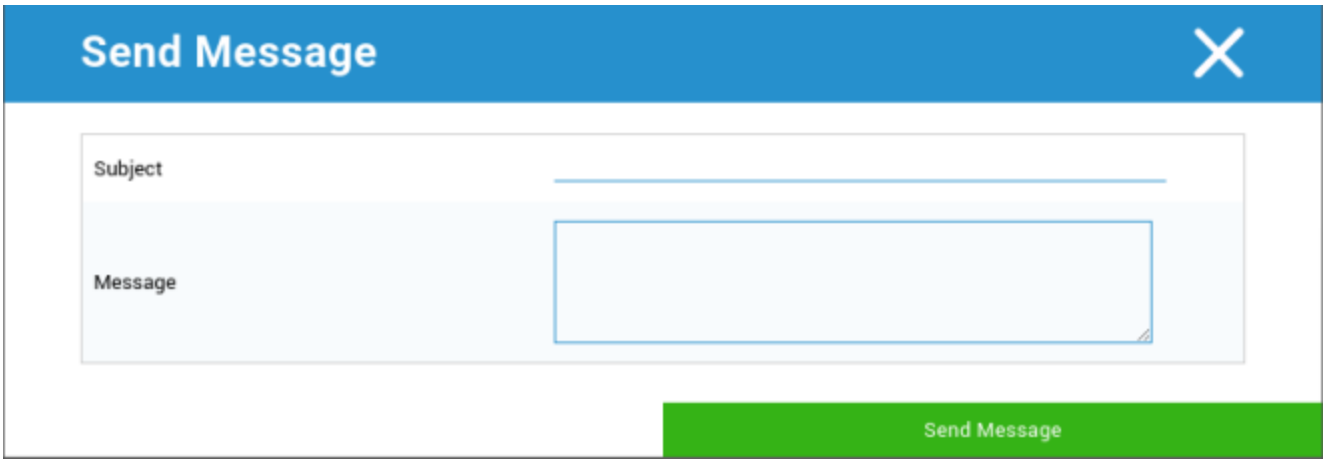
ワイプ＆ロック（デバイスレベルのみ）

ワイプ＆ロック」では、以下の3つのアクションを実行できます：

フルワイプ	デバイスは工場出荷時の設定に復元されます（企業データだけでなく個人データも削除されます）。拡張ワークプロファイルでのみ機能
エンタープライズ・ワイプ	エンドユーザーデバイスから企業データのみを削除（AppTecが提供したすべてのアプリ、データなど）
ロック画面	スクリーンロックが有効になっている場合、デバイスパスワード/PINでデバイスのロックを解除すれば十分です。

メッセージ (デバイスレベルのみ)

ここで件名とメッセージを入力し、エンドユーザーデバイスに送信することができます。



セキュリティ設定

デバイスのパスコード

パスコード」では、デバイスのパスワードを設定することができます。

最小パスワード長	パスワードに最低限必要な記号の数を定める。	
パスワードの品質	特定せず	このポリシーにはパスワードに関する要件はない。
	バイオメトリックの弱さ	この方針は、低セキュリティのバイオメトリクス認識技術を許容する。これは、3 桁の暗証番号程度まで個人の身元を認識できる技術を意味する (誤検出は 1,000 分の 1 以下) 。
	何か	このポリシーは、何らかのパスワードやパターンを設定することを要求するが、特定のルールを強制するものではない。
	アルファベット	ユーザーは、少なくともアルファベット (またはその他の記号) 文字を含むパスワードを入力しなければならない。
	英数字	ユーザーは、少なくとも数字とアルファベット (またはその他の記号) の両方を含むパスワードを入力しなければならない。
	コンプレックス	デフォルトでは、ユーザーは少なくとも文字、数字、特殊記号を含むパスワードを入力しなければならない。このパスワード品質では、パスワードは、少なくとも大文字を含むなど、さまざまな文字のセットを含むように制限することができます。
最小パスワード長	パスワードに必要な文字数を設定します。例えば、PINやパスワードに最低6文字を要求することができます。	
パスワードに最低限必要な数字	パスワードに最低限必要な数字	
パスワードに最低限必要な小文字	パスワードに最低限必要な小文字	
パスワードに最低限必要な大文字	パスワードに最低限必要な大文字	

パスワードに最低限必要な文字以外の文字	パスワードに最低限必要な文字以外の文字
パスワードに最低限必要な記号	パスワードに最低限必要な記号

最大非アクティブ時間ロック	タイムロックまでの最大ユーザー非アクティブ時間
パスワード有効期限タイムアウト	パスワードの有効期限が切れると、新しいパスワードを発行しなければならない。
パスワード履歴の制限	以前に使用されたパスワードのうち、許可されていないパスワードの数
パスワードの最大試行回数	デバイスの完全消去が実行されるまでに、パスワードが誤って入力される頻度を設定します。
生体認証を許可する	指紋または虹彩スキャンによる認証が可能。Samsung KNOX 2.1以上のみ対応

コンテナ・パスコード

パスコード」では、コンテナのパスワードを設定することができ、以下の設定オプションが利用可能です。

最小パスワード長	パスワードに最低限必要な記号の数を定める。	
パスワードの品質	特定せず	このポリシーにはパスワードに関する要件はない。
	バイオメトリックの弱さ	この方針は、低セキュリティのバイオメトリクス認識技術を許容する。これは、3 桁の暗証番号程度まで個人の身元を認識できる技術を意味する (誤検出は 1,000 分の 1 以下) 。
	何か	このポリシーは、何らかのパスワードやパターンを設定することを要求するが、特定のルールを強制するものではない。
	アルファベット	ユーザーは、少なくともアルファベット (またはその他の記号) 文字を含むパスワードを入力しなければならない。
	英数字	ユーザーは、少なくとも数字とアルファベット (またはその他の記号) の両方を含むパスワードを入力しなければならない。
	コンプレックス	デフォルトでは、ユーザーは少なくとも文字、数字、特殊記号を含むパスワードを入力しなければならない。このパスワード品質では、パスワードは、少なくとも大文字を含むなど、さまざまな文字のセットを含むように制限することができます。
最小パスワード長	パスワードに必要な文字数を設定します。例えば、PINやパスワードに最低6文字を要求することができます。	
パスワードに最低限必要な数字	パスワードに最低限必要な数字	
パスワードに最低限必要な小文字	パスワードに最低限必要な小文字	
パスワードに最低限必要な大文字	パスワードに最低限必要な大文字	
パスワードに最低限必要な	パスワードに最低限必要な文字以外の文字	

文字以外の文字	
パスワードに最低限必要な記号	パスワードに最低限必要な記号

最大非アクティブ時間ロック	タイムロックまでの最大ユーザー非アクティブ時間
パスワード有効期限タイムアウト	パスワードの有効期限が切れると、新しいパスワードを発行しなければならない。
パスワード履歴の制限	以前に使用されたパスワードのうち、許可されていないパスワードの数
パスワードの最大試行回数	デバイスの完全消去が実行されるまでに、パスワードが誤って入力される頻度を設定します。

アンチウイルス

自動スキャン	定期的な自動スキャンを有効にする
スキャン間隔	検査間隔 (クイック / フル)
全自動スキャン	完全自動スキャンを有効にする
自動アップデート	自動アップデートを有効にする
更新チェック間隔	アプリとデータベースの更新頻度 (ウイルス / 破損コード)
アプリの保護	アプリの自動スキャンを有効にする
SDカード保護	SDカードの自動スキャンを有効にする
Wi-Fiのみのアップデート	有効にすると、デバイスがWi-Fiネットワークに正常に接続された場合にのみ、アップデートが適用されます。

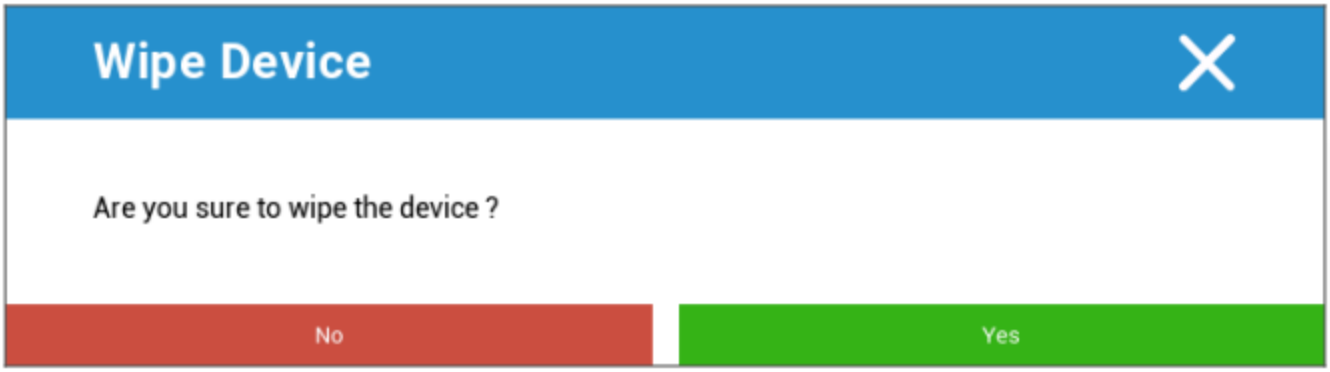
エンド・オブ・ライフ（デバイス・レベルのみ）

ワイプ（デバイスレベルのみ）

Wipe（ワイプ）」では、デバイスを工場出荷時の設定に戻すことができます（Enhanced Work Profileの場合のみ）。

ここでは、企業データだけでなく個人データもエンドユーザー・デバイス上で削除される。

マイナス記号」をクリックすると、次のようなメッセージが表示される：



はい」でワイプを実行できる。

Wipe Report "の下に以下の項目が表示される。

で拭いた。	誰がワイプを行ったかの履歴
日付	日付
ステータス	ステータス（ワイプが正常に実行された場合など）

制限の設定

制限事項

ここでは、さまざまなことを制限したり、ブロックしたりすることができる。

コンプライアンスの実施	ユーザーを促すモード - ユーザーは必要なアクションを実行するよう促されます。 モードロックダウンコンテナ - すべての要件を満たすまで、すべてのアプリを非表示にします。
ランタイム許可ポリシー	新しいパーミッションのリクエストをユーザーに促す 常に新しい許可要求を許可する 常に新しい許可要求を拒否する 警告パーミッションが自動的に設定されている場合、アプリによってはパーミッションの認識に問題があります。常にパーミッションを許可しているにもかかわらず、アプリがパーミッションが不足していると言って問題が発生する場合は、この設定を「プロンプト・ユーザー」にしてアプリを再インストールしてください。
クリップボードの送信を許可する	コンテナ内部から外部へのコピー＆ペーストを許可する。
発信者番号通知を許可する	コンテナ内の連絡先に基づいて着信の名前を表示する
コンタクト検索解決を許可する	通話時にコンテナの連絡先から名前を検索できるようにする
Bluetoothコンタクト共有を許可する	車内でコンテナの接触が可能
発信NFCビームの不許可	コンテナのNFCを無効にする
不明なソースを許可する	有効にすると、ユーザーは.apkファイルをインストールしてアプリをサイドロードできる。
USBデバッグを許可する	有効にすると、ユーザーはUSBデバッグを有効にすることができます。
口座変更の不許可	コンテナ内のアカウントの作成、削除、変更を許可しない。 アプリによっては、期待通りに動作させるためにアカウントを作成または変更する必要があることに留意してください。

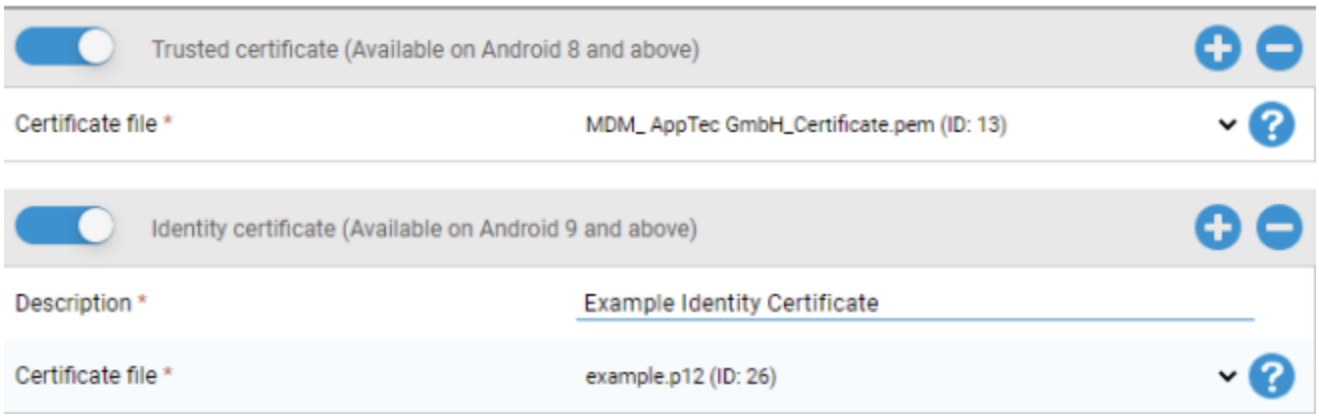
ワークプロファイルの制限。Android 11以上のデバイスでのみ利用可能。

カメラの使用禁止	作業プロファイルでカメラが許可されていないかどうかを指定します。
ブルートゥースを許可しない	作業プロファイルでブルートゥースを禁止するかどうかを指定します。
ファクトリーリセット保護を有効にする	一般設定」→「Android設定」→「Androidエンタープライズ」→「工場出荷時のリセット保護」で定義したGoogleアカウントにAndroidの工場出荷時のリセット保護を上書きするには、これを有効にします。これを有効にしてデバイスをリセットすると、設定したGoogleアカウントを提供してデバイスを再度セットアップする必要があります。
コントロールOSアップデート	更新の動作を自動、ウィンドウ表示、または延期に設定するには、これを有効にします。
更新ポリシー	自動: アップデートが利用可能になり次第、自動的にインストールします。ウィンドウ表示：毎日のメンテナンスウィンドウ内に自動的にインストールします。また、ウィンドウ内でPlayアプリが更新されるように設定されます。これは、フォアグラウンドに固定されたアプリが Play によって更新される唯一の方法であるため、キオスク端末に強く推奨されます。延期：自動インストールを最大30日間延期します。

個人プロフィールの制限。Android 11以上のデバイスでのみ利用可能。	
カメラの使用禁止	個人プロファイルでカメラを禁止するかどうかを指定します。
ブルートゥースを許可しない	個人プロファイルでブルートゥースを禁止するかどうかを指定します。
不明なソースを許可する	有効にすると、ワークプロファイルユーザーは、.apkファイルをインストールすることでアプリをサイドロードできます。

証明書管理

ここでは、信頼済み証明書とアイデンティティ証明書をデバイスに配布することができます。信頼できる証明書を配布するにはAndroid 8以上、アイデンティティ証明書を配布するにはAndroid 9以上が必要です。



を使えば、複数の証明書を追加できる。

信頼できる証明書はPEM形式である必要がある。

アイデンティティ証明書は PKCS12 形式である必要がある。

コネクション管理

無線LAN

この設定を行うには、エンドユーザーデバイスの事前設定を行い、内部アクセス
ポイントにアクセスします。

サービスセット識別子（SSID）	接続するネットワークのSSID
隠しネットワーク	APがSSIDをブロードキャストしない場合は、アクティブにする。

セキュリティ・タイプ

APのセキュリティ・タイプを確立する

ウェップ

パスワード	APのパスワード

WPA/WPA2

パスワード	APのパスワード

802.1x EAP

EAPメソッド

PWD	アイデンティティ	アイデンティティ
	パスワード	パスワード

ピーエーピー	フェーズ2認証プロトコル	なし	追加プロトコルなし
		MSCHAPV2	MSCHAPV2プロトコル
		GTC	GTCプロトコル
	CA証明書	CA 証明書	
	アイデンティティ	アイデンティティ	
	匿名アイデンティティ	匿名ID	
	パスワード	パスワード	

TTLS	フェーズ2認証プロトコル	なし	追加プロトコルなし
		PAP	PAPプロトコル
		エムエスシーハップ	MSCHAPプロトコル
		MSCHAPV2	MSCHAPV2プロトコル
		GTC	GTCプロトコル
	CA証明書	CA証明書	
	アイデンティティ	アイデンティティ	
	匿名アイデンティティ	匿名アイデンティティ	
	パスワード	パスワード	

TLS	CA証明書	CA 証明書
	アイデンティティ	アイデンティティ
	パスワード	パスワード

かそうへいいきもう

接続名	VPN接続の名前

VPNタイプ

かそうへいいきもう

VPNクライアント

AppTec VPNクライアント	
ゲートウェイの設定	ゲートウェイVPN設定を選択（「**一般設定**」>「**ユニバーサルゲートウェイ**」>「**VPN設定**」を参照）
常時接続VPN	ネイティブ・ロックダウンを有効にする
AppTecロックダウンを有効にする	AppTecロックダウンを有効にする

内蔵（サムスン製デバイスでのみ使用可能）			
接続タイプ	PPTP	サーバー	サーバー
		PPTP暗号化を有効にする	PPTP暗号化を有効にする
	L2TP / IPSec PSK	サーバー	サーバー
		IPSec事前共有キー	IPSec事前共有キー
		L2TPシークレットを有効にする	L2TPシークレットを有効にする
		L2TP シークレット	L2TP シークレット
	IPSec XAuth PSK	サーバー	サーバー
		IPSec識別子	IPSec識別子
		IPSec事前共有キー	IPSec事前共有キー
DNS検索ドメイン	DNS検索ドメイン		
エキスパート設定	DNSサーバー	DNSサーバー	
	転送ルート	転送ルート	

オープンVPN		
サーバー	サーバー	
OpenVPNプロファイル	OpenVPNプロファイル	
OpenVPNアプリ	Android用OpenVPN（推奨）	
	OpenVPNコネクト	
エキスパート設定	DNSサーバー	DNSサーバー
	転送ルート	転送ルート

サムスン / ストロングスワン			
接続タイプ	PPTP	サーバー	サーバー
		ユーザー名	ユーザー名
		パスワード	パスワード
		PPTP暗号化を有効にする	PPTP暗号化を有効にする
	L2TP / IPSec PSK	サーバー	サーバー
		IPSec事前共有キー	IPSec事前共有キー
		ユーザー名	ユーザー名
		パスワード	パスワード
		L2TPシークレットを有効にする	L2TP シークレット
	IPSec XAuth PSK	サーバー	サーバー
		IPSec識別子	IPSec識別子
		IPSec事前共有キー	IPSec事前共有キー
		ユーザー名	ユーザー名
		パスワード	パスワード
エキスパート設定	DNSサーバー	DNSサーバー	
	転送ルート	転送ルート	

シスコエニーコネクト		
サーバー	サーバー	
証明書モード	無効	無効
	自動	自動
エキスパート設定	DNSサーバー	DNSサーバー
	転送ルート	転送ルート

アプリごとのVPN

VPNクライアント

AppTec VPNクライアント		
ゲートウェイの設定	ゲートウェイVPN設定を選択（「**一般設定**」>「**ユニバーサルゲートウェイ**」>「**VPN設定**」を参照）	
VPNアプリ	VPNアプリ	
常時接続VPN	ネイティブ・ロックダウンを有効にする	常時接続VPN
AppTecロックダウンを有効にする	AppTecロックダウンを有効にする	

サムスン / ストロングスワン			
接続タイプ	PPTP	サーバー	サーバー
		VPNアプリ	VPNアプリ
		ユーザー名	ユーザー名
		パスワード	パスワード
		PPTP暗号化を有効にする	PPTP暗号化を有効にする
	L2TP / IPSec PSK	サーバー	サーバー
		VPNアプリ	VPNアプリ
		IPSec事前共有キー	IPSec事前共有キー
		ユーザー名	ユーザー名
		パスワード	パスワード
		L2TPシークレットを有効にする	L2TP シークレット
	IPSec XAuth PSK	サーバー	サーバー
		VPNアプリ	VPNアプリ
		IPSec識別子	IPSec識別子
		IPSec事前共有キー	IPSec事前共有キー
		ユーザー名	ユーザー名
		パスワード	パスワード
エキスパート設定	DNSサーバー	DNSサーバー	
	転送ルート	転送ルート	

制限事項

ここでは、接続管理に関する制限を設定できます。

データローミングを許可する	ローミング中のモバイルデータを許可する
強制データローミング	有効にすると、モバイルデータのローミングが恒久的に有効になります（お勧めしません！）。 この設定は "Allow Data Roaming "設定を上書きする！
システムのhttpプロキシサーバーを使用する	HTTPプロキシサーバーの使用は、システムの設定で提供され、接続されたネットワーク（WiFiまたはAPN）に依存します

PIM管理

Gmailエクスチェンジ

情報この設定はGmailアプリに適用されます。そのため、Gmailを承認してインストールする必要があります。

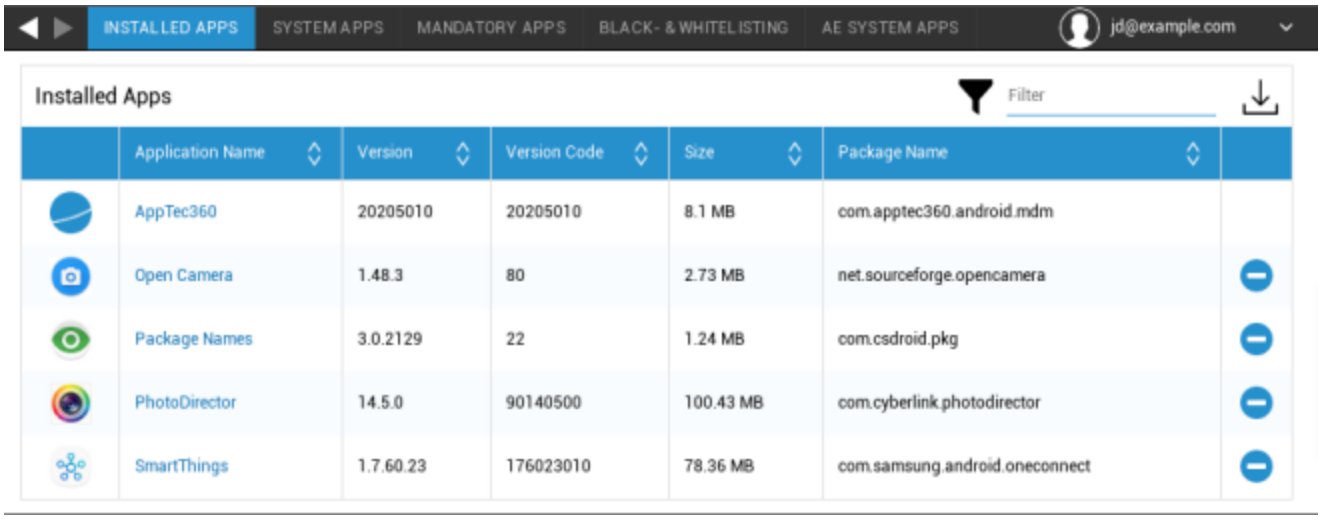
電子メールアドレス	提供されたユーザーのEメールアドレス プレースホルダ "に注意してください。このプレースホルダは、資格情報を扱うために使用することができ、すべてのデバイスで手動で変更を実行することはありません。 クリックするだけで、自分の目で見ることができる。
サーバーホスト名	Exchangeサーバーのサーバーアドレス
ログイン名	各エンドユーザーデバイスのログイン名。
署名	署名を添付することができます。
同期する前の日数	メールのシンクバックを決定する日数
デバイス識別子	EAS DeviceID を含む文字列。これは EAS プロトコルの一部であり、以下の環境で使用できます。
セキュア・ソケット・レイヤー（SSL）の使用	SSL接続を使用する
すべての証明書を受け入れる	すべての証明書が受け入れられます。Exchangeサーバーが自己署名証明書を使用している場合は、このオプションを選択してください。
管理されていないアカウントを許可する	この管理対象構成で指定されたアカウント以外の Exchange アカウントをユーザーが追加または削除できるようにします。この設定を有効にすると、ユーザーが他の Exchange アカウントを Gmail に追加できないようにすることはできません。また、他のアプリとユーザーが追加した Exchange アカウント間のデータ共有を制御することもできません。この設定は、ユーザーが Gmail で複数の仕事用 Exchange アカウントを維持する必要がある場合にのみ有効にしてください。
クライアント証明書	クライアント証明書。メールサーバーがこの証明書の存在を期待している場合のみ必要です。

アプリ管理

エンタープライズアプリマネージャー

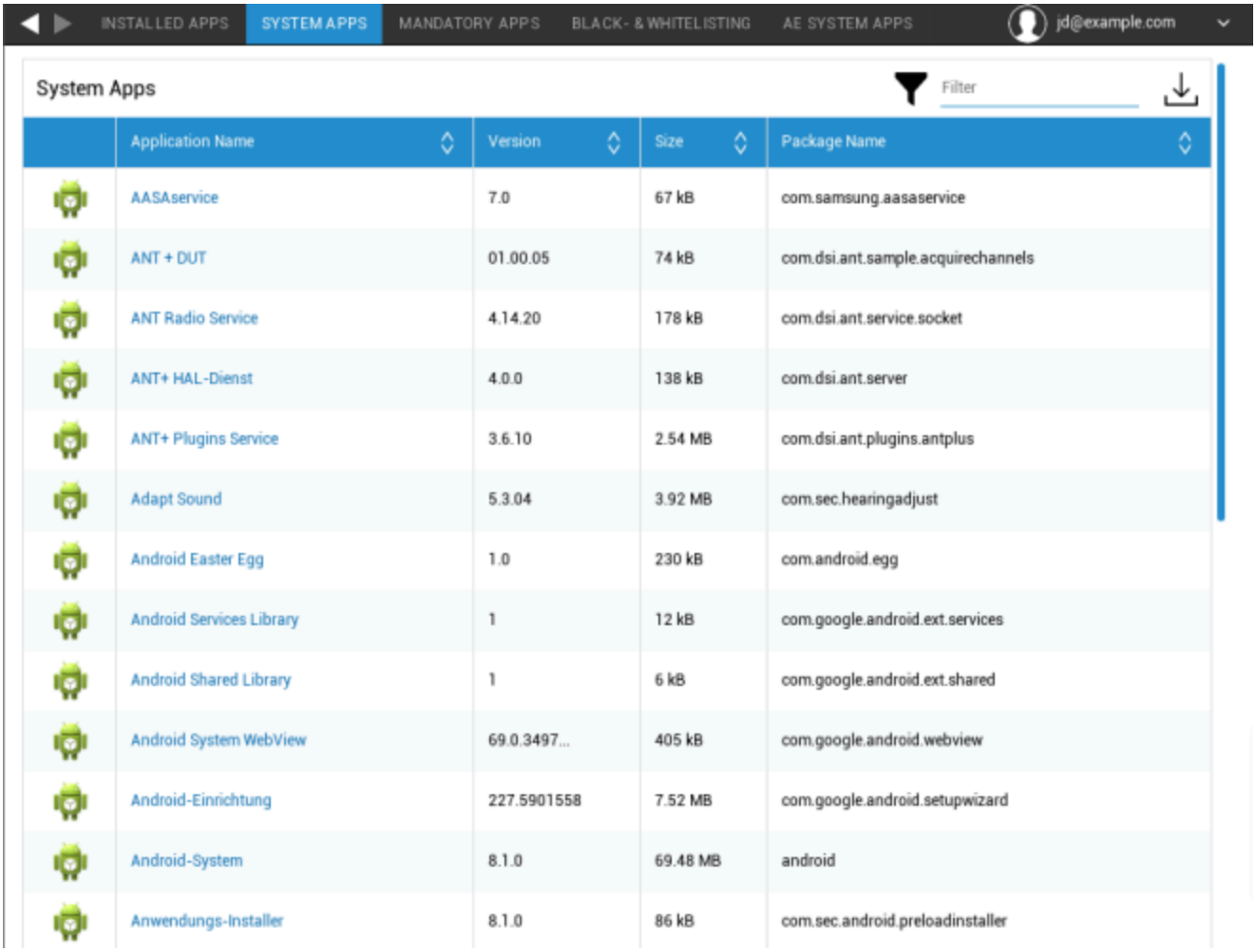
インストール済みアプリ (デバイスレベルのみ)

ここでは、現在コンテナにインストールされているすべてのアプリが表示されます。



システムアプリ (デバイスレベルのみ)

システムアプリ」の下には、デバイスメーカーがエンドユーザー・デバイスにインストール済みのすべてのアプリとサービスが表示されます。

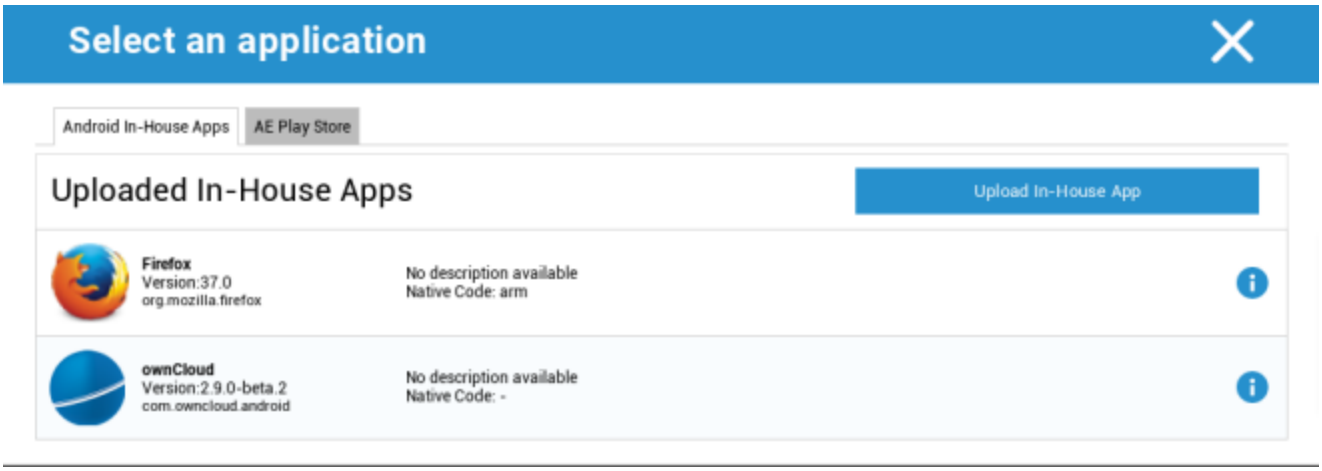


必須アプリ

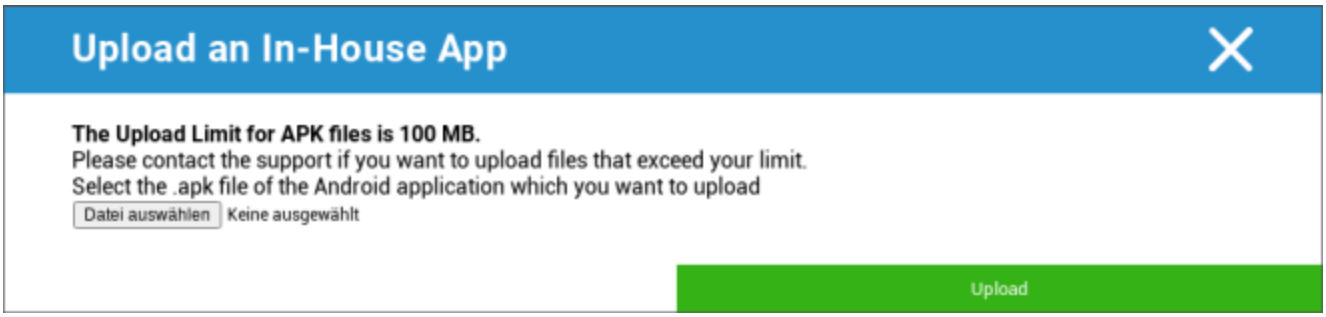
必須アプリ]では、必須アプリを設定できます。社内アプリの場合、ユーザーはこの指定アプリをインストールするよう継続的に求められます。Playストアアプリは自動的にインストールされます。

を介して、必須アプリを定義することができる。

これは、一般設定でアップロードした "Android In-House Apps "から社内アプリを使用することができます。

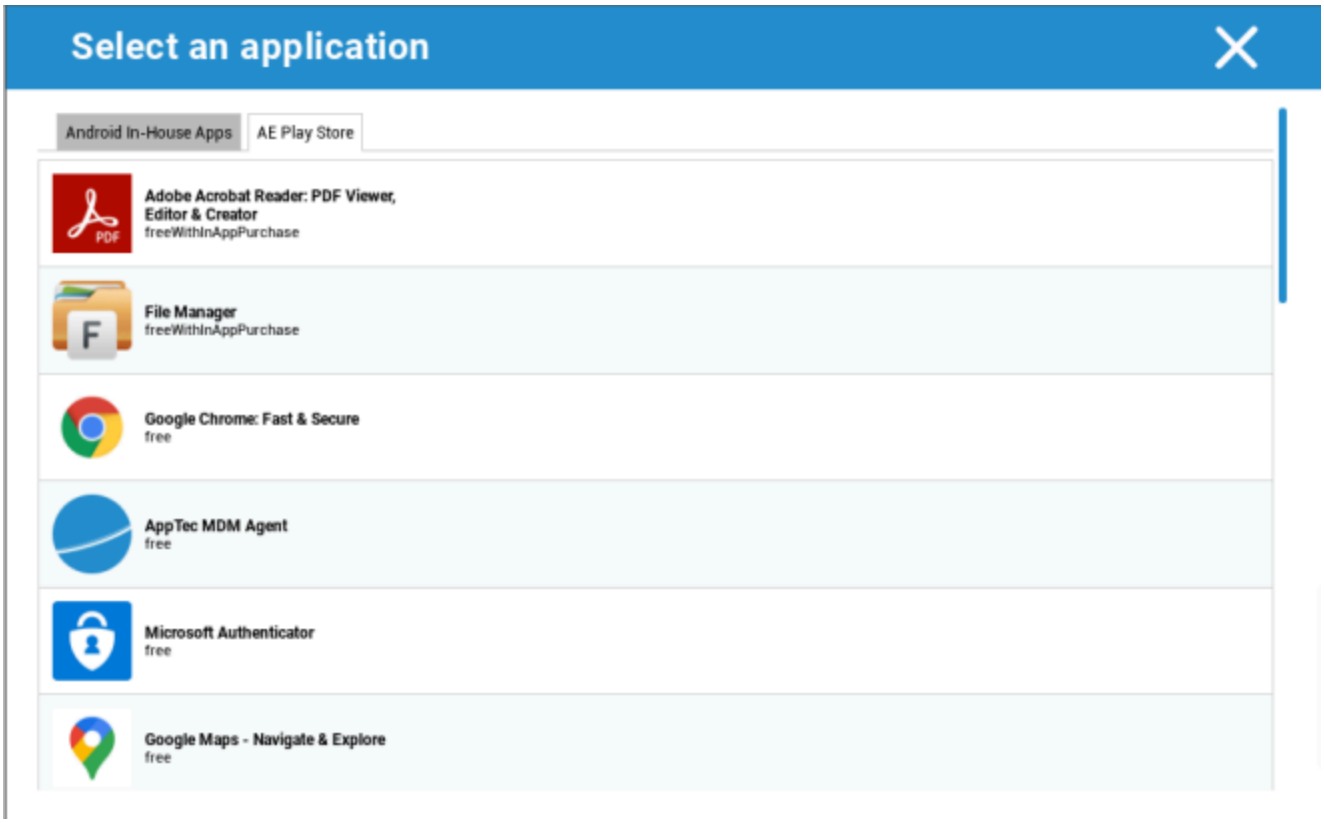


Upload In-House App "で直接apkファイルを選択してアップロードすることもできます。



In-House Appをインストールする場合、"Keep up to date "を有効にすることができます。これが有効になっており、社内アプリDBに新しいバージョンが定義されている場合、アプリはデバイス上で更新されます。

または、Google Work Play Storeの "AE Play Store "アプリでもよい。



このタブには、承認された「AE Playストアアプリ」のみが表示されます。

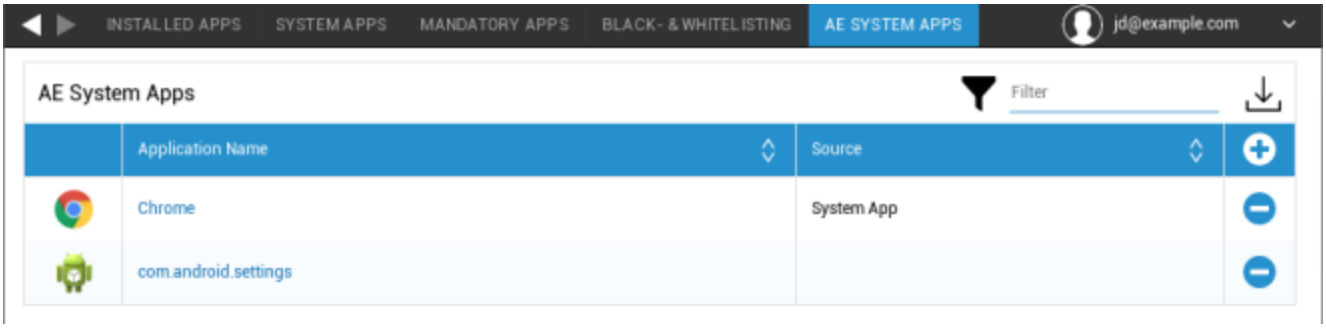
AE Playストアアプリ」を承認するには、「一般設定」→「アプリ管理」→「AE Play」に進んでください。

Store "ボタンをクリックしてアプリを追加すると、"Play Store Apps "タブにリダイレクトされます（または、直接 "Play Store Apps "タブに移動することもできます）。

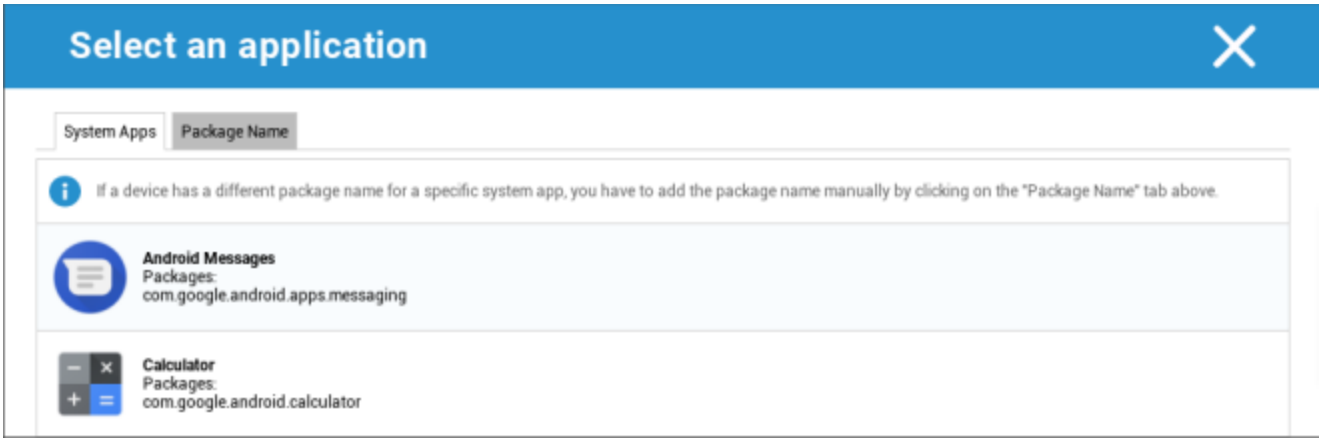
Playストアのアプリ」タブでは、アプリを検索することができます。アプリをクリックすると、アプリのページが開き、ここで「承認」をクリックしてアプリを承認することができます。

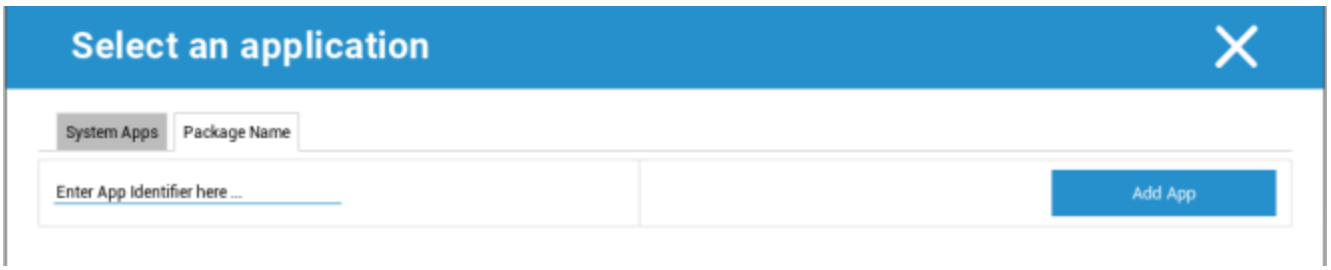
AEシステムアプリ

ここでは、デバイス上で有効化されるべき特定のシステムアプリを含むリストを定義することができます。



ボタンをクリックすると、グーグルが提供する可能なシステムアプリのリストから選択するか、有効化すべきシステムアプリのパッケージ名を直接入力することができる。





Googleが提供するリストにあるシステムアプリは、システムアプリになりうるアプリに過ぎず、必ずしもお使いの端末のシステムアプリである必要はないことにご留意ください。

ただし、このリストはすでにプリインストールされているアプリにのみ影響する。

端末にプリインストールされていないアプリを追加しても、Googleが提供するリストからアプリを追加しても、アプリのパッケージ名を直接入力しても、端末に影響はありません。

制限と設定

アプリ管理設定

ここでは、アプリのアップデートに関するデバイスの動作を設定できます。

更新頻度	AppTec Clientがアプリのアップデートを検索する間隔を指定します。デフォルト値は24時間です。
Wi-Fi しきい値	指定サイズ以上のアプリはWi-Fi経由でダウンロードされます。Wi-Fiのみ」を選択すると、すべてのアプリがWi-Fi経由でダウンロードされます。

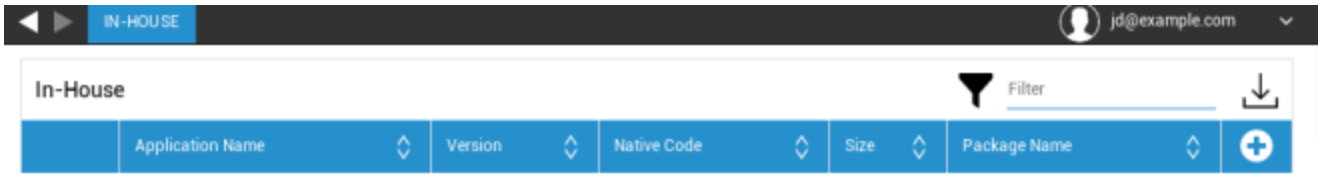
エンタープライズ・アプリケーション・ストア

インハウス

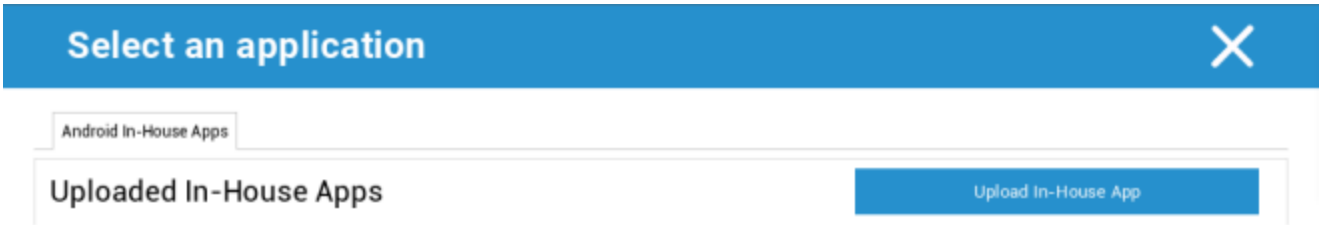
In-House（社内開発）」では、社内で開発したアプリをアップロードして配布することができます。

このシンボルがあれば、インハウスアプリを追加で配布できる。

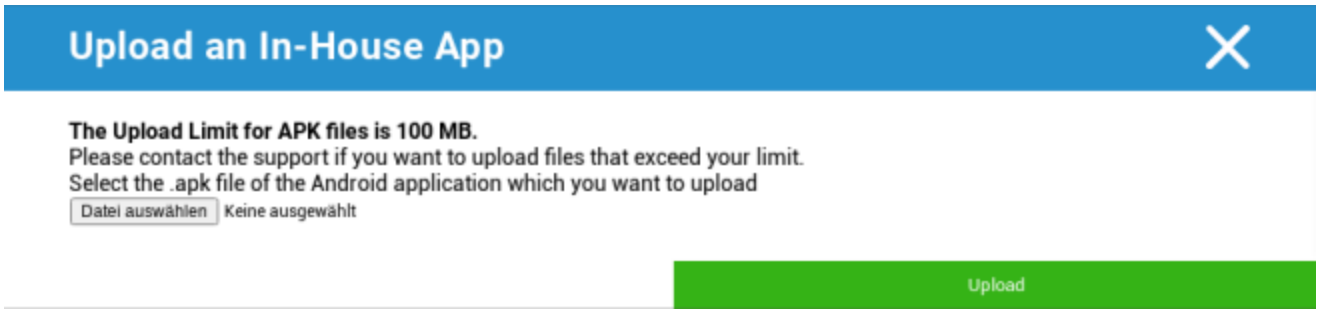
In-House Appをインストールする場合、"Keep up to date "を有効にすることができます。これが有効になっており、社内アプリDBに新しいバージョンが定義されている場合、アプリはデバイス上で更新されます。



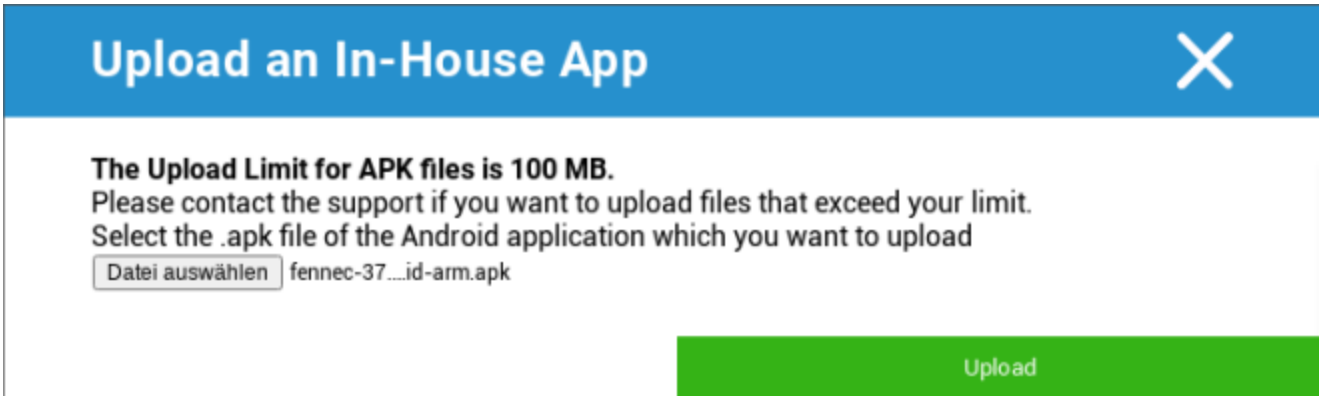
In-House Appsを配布していない場合は、以下の概要が表示されます：



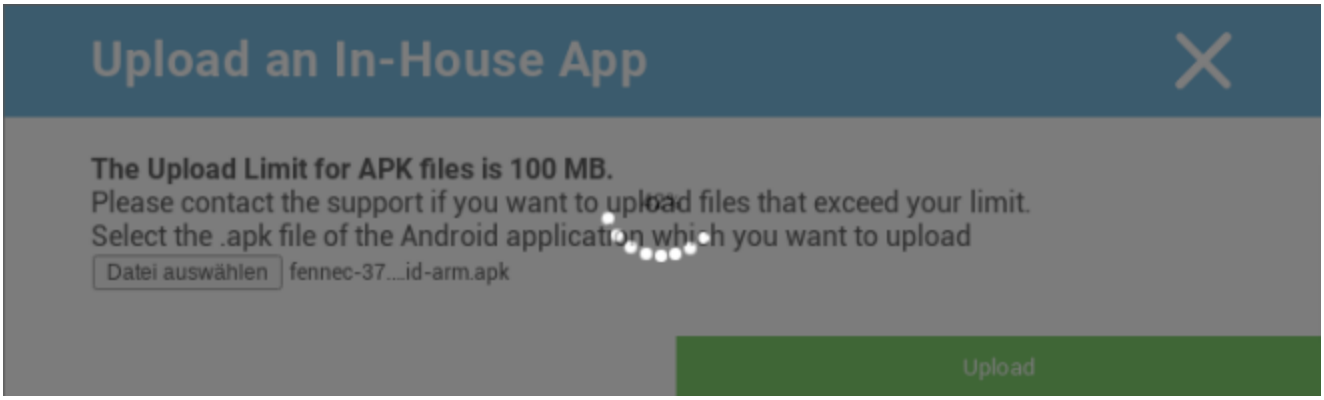
社内アプリのアップロード」をクリックすると、以下のような概要が表示されます：



Search... "で.apkファイルを選択し、"Upload "をクリックします。



アプリがアップロードされ、サークルの中央には、アプリのアップロード済み量を示すパーセンテージのインジケータが表示されます。



社内アプリのアップロードが成功すると、アップロードされたアプリをアプリカタログで見つけることができます。

ユーザーは、エンドユーザーのデバイス上のAppTec Storeの「In-House」カテゴリで、このアプリを確認し、インストールするオプションがあります。

Google PlayStoreアプリを使用しないため、エンドユーザーの端末にGoogle IDを保存する必要はありません。

エンタープライズPlayストア

AE Playストア

Android Enterprise Playstoreにアプリを追加することができます。アプリを追加する前に、AE 管理者アカウントでアプリを承認する必要があります。

アプリの承認については、「必須アプリ」の説明を参照してください。

コンテンツ管理

コンテンツボックス

ここでContentBoxをアクティブにすることができます。

ContentBoxを有効にする "を "オン "に切り替えると、エンドユーザーのデバイスにContentBoxアプリが自動的にインストールされます。

セキュアブラウザ

ここでは、AppTec Secure Browser の設定を構成できます。

セキュアブラウザ "のセクションを "オン "に切り替えるとすぐに、別のブラウザアプリがエンドユーザーデバイスに自動的にインストールされます。

パスワードが必要	ブラウザーにアクセスするためにパスワードを設定し、使用することをユーザーに要求する。
最低限必要なパスワードの長さ	パスワードに必要な文字数を設定する
必要なパスワードの品質	必要なパスワードの品質を設定する
ダウンロードを制限する / で開く	
アップロードの制限	
ホワイトリストのアップロード	アップロードが常に許可されるURLのリスト。
コピーを許可する	ウェブページ内のテキストのコピー、切り取り、共有を許可する。
スクリーンキャプチャを許可する	スクリーンショットのキャプチャを許可する。
データ・クリーンアップの頻度	すべてのユーザーデータ (履歴、キャッシュなど) を自動的に削除する頻度を選択します。
会社のしおり	ブックマークは、ブラウザのブックマークにある「会社のブックマーク」フォルダに表示されます。 ユーザーは編集できない。
アドレスバーを隠す	
ブラウザ内ホワイトリスト (ユニバーサルゲートウェイなし)	クライアント側のURLホワイトリストを有効にする。 • 会社のブックマークは常にホワイトリストに登録される • 100URLのみ対応 • 無制限のブラックリストおよびホワイトリスト登録には、ユニバーサルゲートウェイをご利用ください。
ホワイトリストのURL	許可されたURLのリスト。
ゲートウェイベースのブラックリストとホワイトリスト	ブラックリストには以下の条件がある： • 動作するAppTecユニバーサルゲートウェイ (「一般設定」→「ユニバーサルゲートウェイ)

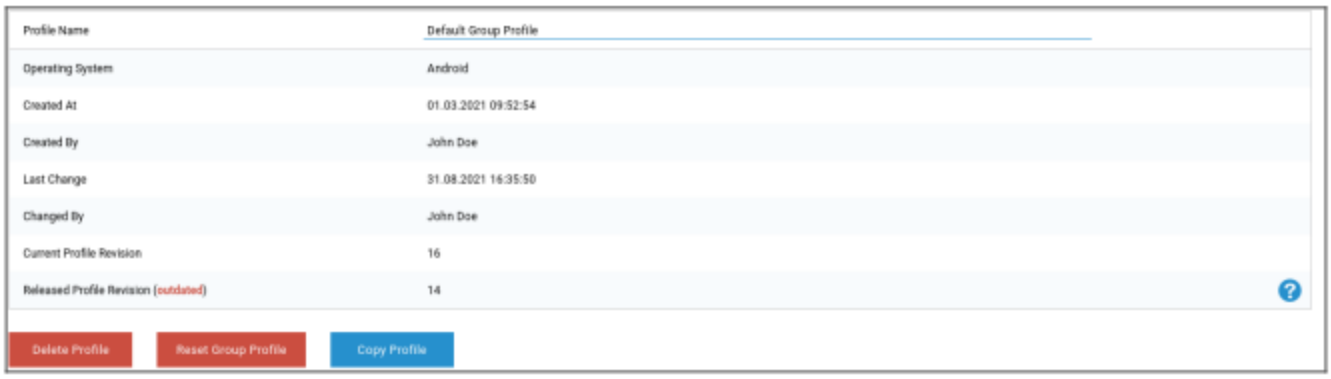
	• DNSサーバーを指定したVPN設定（「一般設定」→「ユニバーサルゲートウェイ」→「VPN設定） • ブラックリストの設定（「一般設定」→「ユニバーサルゲートウェイ」→「ドメインブラックリスト） • プロファイル内の有効なVPN接続（「接続管理」→「VPN）

アンドロイドの設定

一般

グループプロフィールの概要（グループレベルのみ）

グループプロフィールを開くと、プロフィールの概要が表示されます。



プロフィール名	プロフィールの名前（ここで変更可能）
オペレーティングシステム	対象OS
作成日時	創造の時
作成者	プロフィールの作成者
最後の変更	プロフィールの最終変更時刻
変更履歴	最後の変更を行ったアカウント
現在のプロフィール改訂	保存されたプロファイル状態の修正
プロフィール改訂版をリリース	割り当てられたプロファイルのリビジョン（"Assign now"）。ラベルのテキストの後ろに"(outdated) "と表示されている場合は、プロファイルを保存したものの、まだ割り当てていないことを意味します。

デバイスの概要 (デバイスレベルのみ)

デバイスを選択すると、選択したデバイスの概要が表示されます：

デバイス名	デバイス名
最終所在地	最後に確認されたGPS座標
電話番号	電話番号
割り当てられた必須アプリ	割り当てられた必須アプリの数
OSバージョン	デバイスのOSバージョン
オペレーティングシステム	オペレーティングシステム (Android / iOS / Windows Phone)
シリアル番号	デバイスのシリアル番号
デバイスの所有権	企業用またはプライベート用デバイス
デバイス・タイプ	電話またはタブレット
ルーツ	デバイスがルート化されているかどうかを示すステータス
準拠	ガイドライン準拠
IPアドレス	IPアドレス
ラストシーン	デバイスが最後にAppTecに接続した時点
ラスト・プッシュ	サーバーがデバイスにプッシュを送信した時点
ユーザー割り当て	別のユーザーにデバイスを割り当てるためのドロップダウン

コンフィグ改訂（デバイスレベルのみ）

ここで、どのグループプロファイルがデバイスに割り当てられているかの概要が表示されます。

グループプロフィールをクリックすると、そのプロフィールに直接アクセスし、設定を行うことができます。

このマークがあれば、割り当てられたアプリをグループプロファイルの設定に戻すことができます。

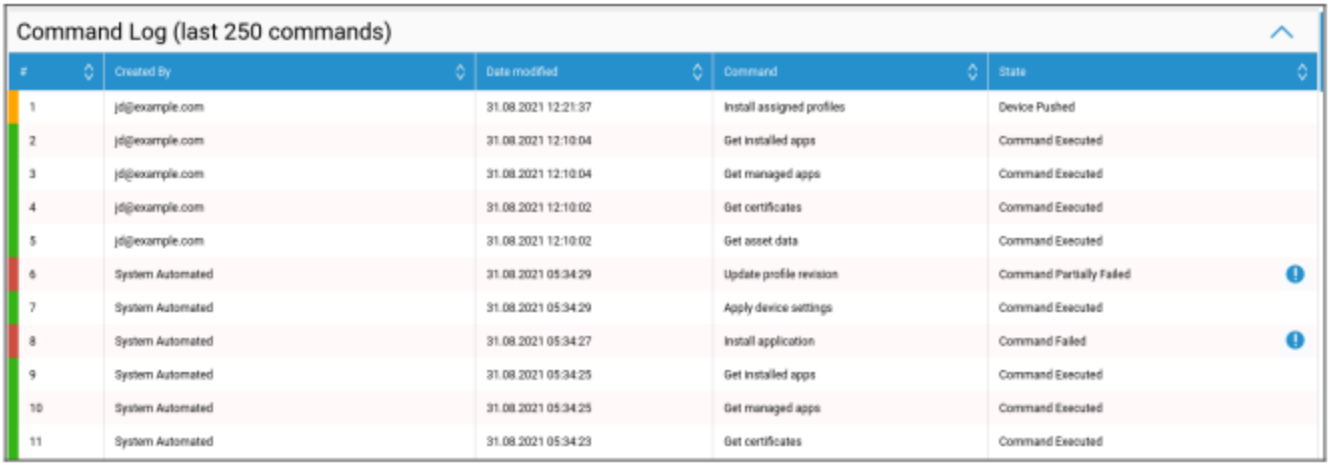
この記号を使えば、デバイスのプロファイルをリセットして、設定を一切なしにすることができる。

"Newer Revision available "は、グループプロファイルが変更され保存されたが、割り当てられていないことを示します。グループプロファイルの変更をデバイスに適用するには、グループレベルで "Assign now "を使用してグループプロファイルを割り当てる必要があります。

デバイスログ（デバイスレベルのみ）

コマンドログ

ここでは、デバイスに対して発行されたコマンドとそのステータスを確認することができます。



System Automated」によって作成されたコマンドは、システムによって自動的に作成される。

可能なコマンドステータス

デバイスが押される	プッシュリクエストは、EMM サーバーに接続するようデバイスに指示するため、プッシュサービス (APNS など) に送信されました。
コマンド作成	コマンドがシステム内に作成された。
コマンド送信	コマンドは、サーバーに接続された後、デバイスに送信された。
コマンド実行	コマンドは正常に実行された。
コマンド失敗	コマンドが失敗しました。*
コマンド一部失敗	デバイスのOSによっては、いくつかのコマンドがグループ化されることがある。 このコマンドグループの一部は失敗した。*
コマンドは実行されたが、最終的に失敗	コマンドは実行されたが、もしかしたら実行されていなかったかもしれない。
コマンド・リパッシュ	コマンドはユーザーによってリプッシュされた。
廃棄	コマンドが破棄された。例えば、他のコマンドに取って代わられたとか、デバイスが再登録されて古いコマンドが削除されたとか。

*メッセージの後ろにエクスクラメーションマークが表示されている場合は、カーソルをアイコンの上に置くと詳細な情報を得ることができます。

デバイス設定

クライアント設定

ここでは、Androidデバイスの以下の設定を行うことができます：

デバイス管理を無効にした後の警告メッセージ	デバイス管理を無効にした後に警告メッセージが表示される
コンプライアンス違反の時間	デバイスが準拠していない場合、「準拠後の強制措置」が実行される期限。 最短1分 最大24時間
コンプライアンス・タイムアウト後の強制措置	デバイスが非準拠となった場合に直ちに取られるべき措置。 • 何もしない = 何もしない • ロック・デバイス = ロック装置 • デバイスのワイプ = デバイスが工場出荷時の設定に復元されます。
データ収集頻度	デバイス/GPS情報の収集頻度
デバイスのハートビート周波数	デバイスがAppTec360 Serverにコンタクトする間隔 最短1分 最大24時間
位置情報の更新を有効にする	有効になっている場合、デバイスは位置情報の更新をAppTec360 Serverに送信します。
場所 更新時間	デバイスがAppTecに位置情報の更新を送信する時間間隔を決定します。
位置情報の更新にGoogle Location Accuracyを使う	有効にすると、Google位置情報精度（旧ネットワーク位置情報）が位置情報の更新に使用されます。
位置情報の更新にGPSロケーションを使用	アクティブにすると、位置情報の更新にGPSが使用されます。
モック（偽）ロケを許可する	サードパーティアプリによる位置情報の偽造を許可する
ロスト・コネクション	一定の心拍数が経過した後に実行される特定のアクションを設定できます。
ポリシー実施モード	AppTec360 Clientが、ユーザー入力を必要とする特定のアクションの実行を、どの程度積極的にユーザーに求めるかを定義します。

	Interval (Default) = 間隔をあけて問い合わせる。 アラートが表示されない = 必要な操作のポップアップが表示されない。AppTec360 Clientを手動で開いて、必要なアクションがあるかどうかを確認する必要があります。 コンスタントアラート = ユーザーは必要なアクションのみを実行できます。AppTec360 Clientは、ユーザーがそれを避けようとすると、強制的にフォアグラウンドになります。
AppTec360 バージョンロック	AppTec360クライアントのバージョンを定義します。

壁紙

ここでは、カスタム壁紙を定義することができます。

"Specify a Color"（色の指定）では、16進数で色を定義できます（例：#000000）。指定できるのは16進数のみです。

「画像を壁紙に設定」では、画像をアップロードすることができます。ランチャーやOSのバージョンが異なる端末では、動作が異なりますのでご注意ください。サイズや比率は端末によって異なるため、一般的な目安はありません。

ファイル形式はJPG（またはJPEG）またはPNGを使用してください。

資産管理（デバイスレベルのみ）

資産管理

デバイス情報

モデル	機器モデル名
オペレーティングシステム	OS
OSバージョン	OSバージョン
AEサポート	Android Enterpriseのサポート (コンテナおよびフルマネージド)
シリアル番号	シリアル番号
デバイス名	デバイス名
バッテリーの状態	バッテリーの状態
フリー/トータルメモリー	空き/総メモリ
サムスンKNOX	サムスンKNOX APIレベル
利用可能なSDカード	SDカードあり
エミュレートされたSDカード	エミュレートされたSDカード
リムーバブルSDカード	SDカード取り外し可能
SD空き/総メモリ	SD空き容量/SDカード空き容量

Wi-Fi

IPアドレス	デバイスIPアドレス
WiFi MAC	WiFiのMACアドレス

セルラー

ステータス	ステータス（SIMカード装着）
電話番号	電話番号
ローミング（音声/データ）	音声/データのローミング
ローミング状況	現在のローミング状況
IPアドレス	IPアドレス
オペレーター/キャリア	オペレーター/キャリア
セルラー技術	セルラー技術
IMEI	IMEI番号
国際ID	これはSIMカードのIDであり、多くの場合、スマートカードまたは集積回路カード（ICC）でもある。
移動加入者識別番号	IMSI（International Mobile Subscriber Identity）は、GSMおよびUMTSモバイル・ネットワークにおいて、ネットワーク・ユーザーの明確な識別を提供する。 IMSIは最大15桁で構成され、以下のように設定される： • 携帯国番号（MCC）、3桁 • モバイル・ネットワーク・コード（MNC）、2桁または3桁 • 携帯電話加入者識別番号（MSIN）、1～10桁
現在のMCC/MNC	SIM MCC/MNC」を参照。
SIM MCC/MNC	モバイル国コードは、E.212標準に従ってITUによって設定された、確立された国識別子です。これは、モバイル・ネットワーク・コード（MNC）と連動してモバイル・ネットワークを識別します。 SIMカードの国/モバイルネットワークコードを意味する。 別のモバイルネットワークにローミングする場合、論理的には、「現在のMCC/MNC」と「SIM MCC/MNC」は異なる。

ブルートゥース

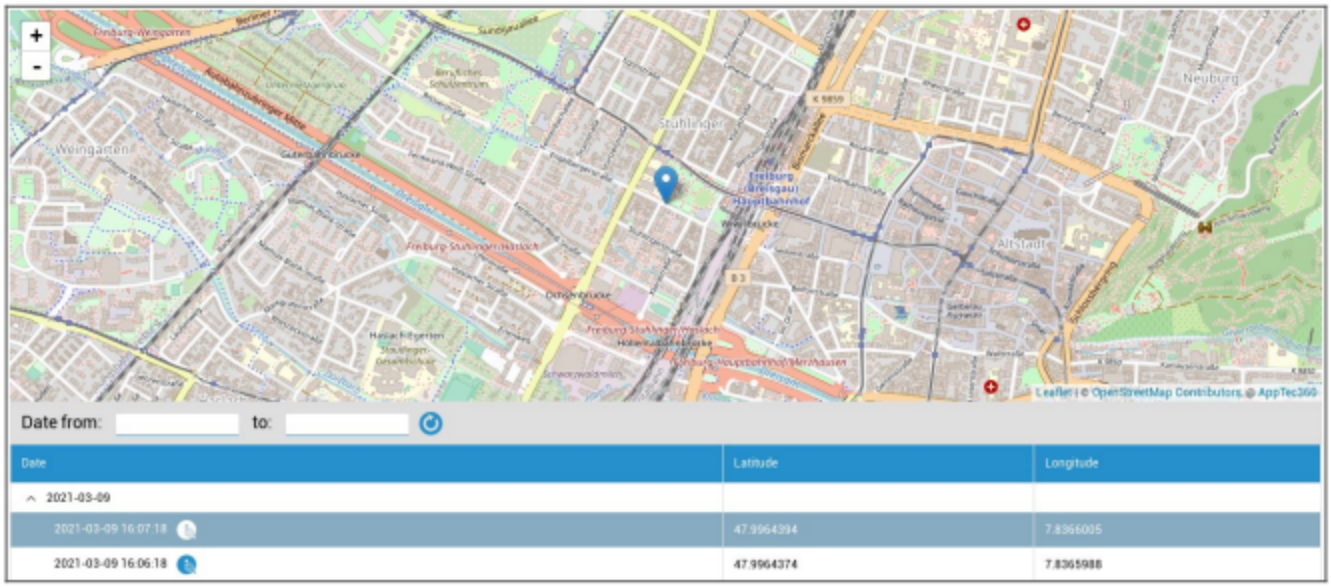
ブルートゥースMAC	ブルートゥースMACアドレス

セキュリティ管理

盗難防止（デバイスレベルのみ）

GPS情報（デバイスレベルのみ）

ここでデバイスの現在地/最終位置を設定できます。ローカライズは1つまたは2つのパスワードで保護することができます：一般設定 - プライバシー - GPSアクセス



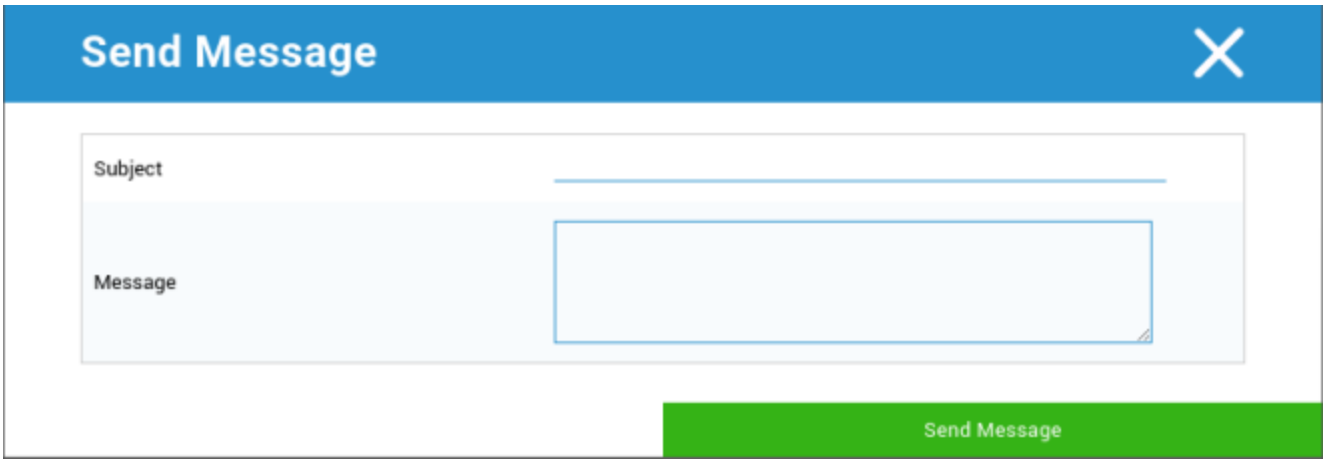
ワイプ＆ロック（デバイスレベルのみ）

ワイプ＆ロック」では、以下の3つのアクションを実行できます：

フルワイプ	デバイスを工場出荷時の設定に戻す（企業および個人データは削除される）
エンタープライズ・ワイプ	企業データのみがエンドユーザーデバイスから削除される（AppTec360によって提供されたすべてのアプリ、データなど）
ロック画面	スクリーンロックが有効になっている場合、デバイスパスワード/PINでデバイスのロックを解除すれば十分です。

メッセージ（デバイスレベルのみ）

件名とメッセージを記入して、エンドユーザーデバイスに送信できます。このメッセージはAppTec360 Clientに表示されます。



セキュリティ設定

パスコード

パスコード」では、デバイスのパスワードを設定することができます。

最小パスワード長	パスワードに最低限必要な記号の数を定める。
パスワードの品質	パスワード強度 不特定 = 特定しない どのパスワードもOK = どのパスワードも受け入れられる at least numeric characters = 少なくとも数字が含まれていなければならない。 少なくとも複雑な文字 = 少なくとも特殊文字を含むこと at least alphanumerical characters = 少なくとも英数字を含むこと。 at least alphabetic characters = 少なくともアルファベット文字を含むこと。
最大非アクティブ時間ロック	画面の最大タイムアウト。これはユーザーが選択できる最大値のみを設定します。
パスワードに最低限必要な小文字	パスワードに最低限必要な小文字
パスワードに最低限必要な大文字	パスワードに最低限必要な大文字
パスワードに最低限必要な文字以外の文字	パスワードに最低限必要な文字以外の文字
パスワードに最低限必要な数字	パスワードに最低限必要な数字
パスワードに最低限必要な記号	パスワードに最低限必要な記号
パスワード有効期限タイムアウト	パスワードの有効期限が切れると、新しいパスワードを発行しなければならない。
パスワード履歴の制限	以前に使用されたパスワードのうち、許可されていないパスワードの数
パスワードの最大試行回数	デバイスの完全消去が実行されるまでに、パスワードが誤って入力される頻度を設定します。

暗号化

このポイントでは、デバイスの内部メモリだけでなく、SDカードのメモリも暗号化することができます。

ストレージの暗号化が必要	この設定を有効にすると、デバイスがこの機能をサポートしている限り、デバイスのメモリは暗号化されます。 デバイスのメモリが初めて暗号化されると、暗号化を解除することはできなくなります。 同様に、パスワードポリシーは自動的に6つの英数字記号に切り替わります。
SDカードの暗号化が必要	この設定はサムスン製デバイスにのみ適用されます！ この設定が有効な場合、外部SDカードは暗号化され、エンドユーザーデバイスでのみ手動で暗号化を解除することができます。 同様に、パスワードポリシーは自動的に6つの英数字記号に切り替わります。

アンチウイルス

AntiVirusを有効にすると、デバイスにIkarusがインストールされます。これには、一般設定 → アプリ管理 → サードパーティアプリで入力できる別のライセンスが必要ですのでご注意ください。

自動スキャン	Ikarusが自動的にスキャンを行うかどうかと、スキャンを行う頻度を定義します。 フル自動スキャン」を有効にすると、フルスキャンが実行されます。それ以外の場合はクイックスキャンが実行されます
自動アップデート	ウイルスデータベースの自動更新を有効にし、その頻度を設定する。
アプリの保護	ファイルのみをスキャンする通常のスキャンに加え、アプリのスキャンを有効にする。
SDカード保護	SDカード保護を有効にします。これがないと、スキャンはローカル ストレージに制限されます。
Wi-Fiのみのアップデート	Wi-Fiへのアップデートを制限

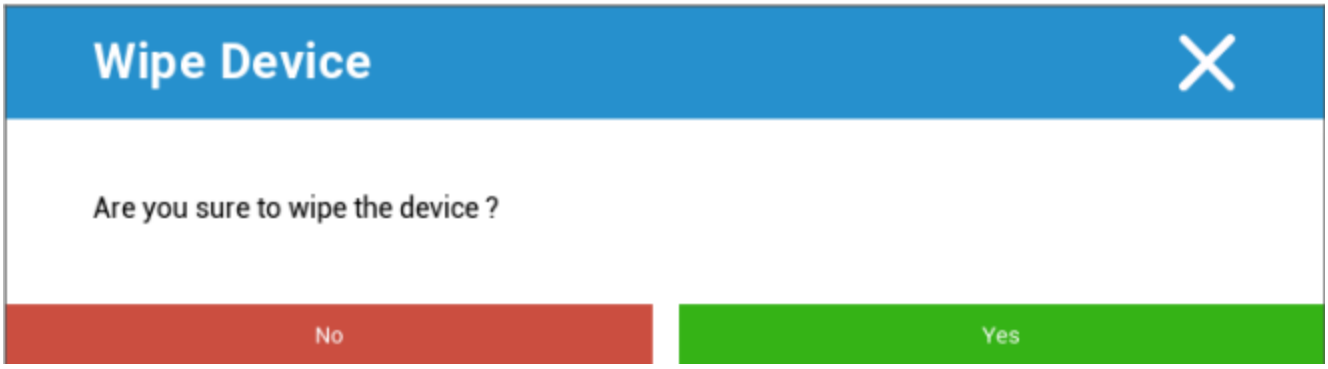
エンド・オブ・ライフ (デバイス・レベルのみ)

ワイプ (デバイスレベルのみ)

ワイプ」では、デバイスを工場出荷時の設定に戻すことができる。ここで、企業や個人データはエンドユーザーのデバイスから削除されます。

マイナス記号」をクリックすると、次のようなメッセージが表示されます。

SDカードも消去？	SDカードのメモリも消去されます。



はい」でワイプを実行できる。

Wipe Report "の下に以下の項目が表示される。

で拭いた。	誰がワイプを行ったかの履歴
日付	日付
ステータス	ステータス (ワイプが正常に実行された場合など)

制限の設定

制限事項

ここでは、さまざまなことを制限したり、ブロックしたりすることができる。

カメラを有効にする	カメラの使用を許可する
強制自動同期	シンク」インターフェイス関連 オン = 同期が常時有効 オフ = 同期は永久に解除される ユーザーチョイス = ユーザーが選択
フォース・ブルートゥース	オン = ブルートゥースが常時有効 オフ = ブルートゥースは永久に解除される ユーザーチョイス = ユーザーが選択
フォースGPS	オン = GPSが常時作動 オフ = GPSは永久に解除される ユーザーチョイス = ユーザーが選択
グーグルの位置情報精度を強制する	オン = 恒久的なインターネット・ローカライズ オフ = インターネット・ローカライズの永久停止 ユーザーチョイス = ユーザーが選択

KNOX 1.0以上のインターフェイスを搭載したSamsungデバイスの場合、以下の設定オプションが利用できます。

SDカードを許可する	SDカードを許可する
SDカードの書き込みを許可する	SDカードへの「書き込み」を許可する
スクリーンキャプチャを許可する	スクリーンキャプチャを許可する
クリップボードを許可する	クリップボードを許可する
Google Cloudで設定とアプリデータをバックアップ	オフ = Googleバックアップを無効にする オン = Googleバックアップを有効にする ユーザーチョイス = ユーザーが選択
USBデバッグを許可する	USBデバッグを許可する（デバイスログ（ADB）の作成などに使用される）
グーグルクラッシュレポートを許可する	アプリからGoogleクラッシュレポートの送信を許可する
ファクトリーリセットを許可する	デバイスを工場出荷時の設定に戻すことができます。
OTAアップグレードを許可する	オーバー・ザ・エアー」アップデートを許可する
USBホスト・ストレージを許可する	起動すれば、HDやSDカードリーダーなどのUSBメモリーを接続できます。
USBメディアプレーヤーを許可する(MTP,PTP)	USBメディアプレーヤーを許可する(MTP,PTP)
マイクを許可する	オン = サードパーティアプリのマイクを許可する オフ = サードパーティアプリのマイクをブロックする ユーザーの選択 = サードパーティアプリがマイクにアクセスできる場合、ユーザーは選択できる。
NFC（近距離無線通信）を許可する	NFCを許可する
不明なソースを許可する（APKサイドローディング）	有効にすると、アプリ（APKファイル）のサイドローディングが許可されます。 この設定を無効にすると、ソース不明からのAPKのインストールを許可する際に、ユーザーは手動で有効にする必要があります。
ユーザー作成を許可する	複数ユーザーの作成が可能

AEデバイス所有者

(デバイスはAndroid Enterprise Device Owner Modeである必要があります) デバイスは「Android」デバイスとしてではなく、「Android Enterprise」デバイスとして作成することをお勧めします。

セキュリティ	
共有場所の不許可	位置情報の共有を許可しないユーザーを指定します。
セーフブートの禁止	ユーザーがデバイスをセーフブートモードにリブートすることを許可されないかどうかを指定します。
ネットワークリセットを許可しない	ユーザーが [設定] からネットワーク設定をリセットすることを禁止するかどうかを指定します。
工場出荷時のリセットを許可しない	ユーザーがデバイスをリセットすることを禁止するかどうかを指定します。
ADBを有効にする	ADB経由でPCに接続可能
キーガードを無効にする	キーガードを無効にする
デバイス所有者のロックスクリーン情報	ロック画面に表示するデバイスの所有者情報を設定します。
コンプライアンスの実施	ユーザーを促すモード - ユーザーは必要なアクションを実行するよう促されます。 モードロックダウンコンテナ - すべての要件を満たすまで、すべてのアプリを非表示にします。

アプリ管理	
クロスプロファイルのアプリリンクを許可する	親プロファイルのアプリが管理プロファイルからのウェブリンクを処理できるようにします。
アプリの制御を許可しない	ユーザーが設定やランチャーでアプリケーションを変更できないようにするかどうかを指定します。
アプリのインストールを許可しない	ユーザーがアプリケーションをインストールできないようにするかどうかを指定します。
アプリのアンインストールを許可しない	ユーザーがアプリケーションをアンインストールできないようにするかどうかを指定します。
ランタイム許可ポリシー	アプリからの新しい許可リクエストの処理方法を指定します。
不明なソースを許可する	有効にすると、ユーザーは.apkファイルをインストールしてアプリをサイドロードできる。

コネクティビティ	
モバイルネットワーク設定を許可しない	ユーザーがモバイルネットワークの設定を許可されないかどうかを指定します。
テザリング禁止設定	ユーザーがテザリングとポータブルホットスポットの設定を許可しないかどうかを指定します。
VPN設定を許可しない	ユーザーがVPNを設定することを禁止するかどうかを指定します。
Wifi設定を許可しない	ユーザーが WiFi アクセスポイントを変更できないようにするかどうかを指定します。
発信NFCビームの不許可	アプリからデータを転送するためにNFCを使用することを禁止するかどうかを指定します。
WiFi設定のロック	この設定は、デバイス所有者アプリによって作成されたWiFi設定をロックダウン（つまり、設定アプリでもなく、デバイス所有者アプリによってのみ編集または削除可能）するかどうかを制御します。
データローミングを有効にする	データローミングを有効にする

ブルートゥース	
ブルートゥースを許可しない	デバイスでブルートゥースが許可されていないかどうかを指定します。Android 8.0が必要です。
Bluetoothの共有を許可しない	デバイス上で発信ブルートゥース共有が禁止されているかどうかを指定します。Android 8.0が必要です。
Bluetooth設定を無効にする	ユーザーがブルートゥースを設定することを禁止するかどうかを指定します。

アカウント管理	
管理プロファイルの追加を許可しない	ユーザーが管理プロファイルを追加できないようにするかどうかを指定します。Android 8.0が必要です。
ユーザーの追加を許可しない	ユーザが新規ユーザを追加できないようにするかどうかを指定します。
管理プロファイルの削除を許可しない	このユーザーの管理プロファイルを、プロファイル所有者以外に削除できるかどうかを指定します。Android 8.0が必要です。
口座変更の不許可	Authenticator によってプログラム的に追加されない限り、ユーザがアカウントを追加および削除できないようにするかどうかを指定します。

テレフォニー	
発信を許可しない	ユーザーが電話を発信できないように指定します。
SMSを拒否する	ユーザーがSMSメッセージを送受信できないように指定します。

システム	
ウィンドウの作成を許可しない	アプリケーション・ウィンドウ以外のウィンドウを作成しないように指定します。
ユーザーアイコンの設定を許可しない	ユーザーが自分のアイコンを変更できないようにするかどうかを指定します。
壁紙の設定を許可しない	壁紙の設定を禁止するユーザー制限。
ステータスバーを無効にする	ステータスバーを無効にすると、通知、クイック設定、その他の画面オーバーレイがブロックされ、単一使用のデバイスから脱出できるようになる。
オートタイムを有効にする	自動的に時刻を設定する。
自動タイムゾーンを有効にする	タイムゾーンを自動的に設定する。
コンセントに接続したまま	電源に接続されている間、デバイスはアクティブな状態を保ちます。

ストレージ	
アプリ検証を無効にする	ユーザーがアプリケーション検証を無効にすることを許可するかどうかを指定します。

物理メディアのマウントを許可しない	物理的な外部メディアのマウントを禁止するかどうかを指定します。
バックアップサービスを有効にする	バックアップ・サービスは、デバイス上のすべてのバックアップおよび復元メカニズムを管理します。これをFalseに設定すると、データのバックアップやリストアができなくなります。バックアップサービスはデフォルトでオフになっています。Android 8.0が必要です。
USBマスストレージを有効にする	USBマスストレージの使用を有効にする。

キーボード	
自動入力を許可しない	ユーザーが自動入力サービスの使用を許可されていないかどうかを指定します。Android 8.0が必要です。
プロファイル間のコピー＆ペーストを禁止する	このプロファイルのクリップボードにコピーされた内容を、関連プロファイルに貼り付けることができるかどうかを指定します。

サウンド	
出来高調整を認めない	ユーザーがマスター音量を調整できないようにするかどうかを指定します。
マイクのミュート解除を許可しない	ユーザーがマイクの音量を調整できないようにするかどうかを指定します。
ミュート装置	ミュート装置。

システム・アップデート・ポリシー	
OSアップデートの制御	更新の動作を自動、ウィンドウ表示、または延期に設定するには、これを有効にします。

BYODコンテナ

アンドロイド・エンタープライズ

アンドロイド・エンタープライズ

Android Enterpriseを有効にする	Android Enterprise（AE）を有効にする。AEはAndroid 5.1以降でサポートされています。
コンプライアンスの実施	ユーザーを促すモード - ユーザーは必要なアクションを実行するよう促されます。 モードロックダウンコンテナ - すべての要件を満たすまで、すべてのアプリを非表示にします。
ランタイム許可ポリシー	新しいパーミッションのリクエストをユーザーに促す 常に新しい許可要求を許可する 常に新しい許可要求を拒否する 警告パーミッションが自動的に設定されている場合、アプリによってはパーミッションの認識に問題があります。常にパーミッションを許可しているにもかかわらず、アプリがパーミッションが不足していると言って問題が発生する場合は、この設定を「プロンプト・ユーザー」にしてアプリを再インストールしてください。
クリップボードの送信を許可する	コンテナ内部から外部へのコピー＆ペーストを許可する。
発信者番号通知を許可する	コンテナ内の連絡先に基づいて着信の名前を表示する
コンタクト検索解決を許可する	通話時にコンテナの連絡先から名前を検索できるようにする
Bluetoothコンタクト共有を許可する	車内でコンテナの接触が可能
発信NFCビームの不許可	コンテナのNFCを無効にする
不明なソースを許可する	有効にすると、ユーザーは.apkファイルをインストールしてアプリをサイドロードできる。
USBデバッグを許可する	有効にすると、ユーザーはUSBデバッグを有効にすることができます。

口座変更の不許可	コンテナ内のアカウントの作成、削除、変更を許可しない。 アプリによっては、期待通りに動作させるためにアカウントを作成または変更する必要があることに留意してください。

Gmailエクスチェンジ

コンテナ内のGmailを設定できるようにします。この設定を有効にしても、アプリは自動的にインストールされません。このアプリを必須アプリとして追加する必要があります。

メールアドレス	メールアドレス
サーバーホスト名	サーバーホスト名
ログイン名	ログイン名
署名	署名
同期する前の日数	同期する前の日数。
デバイス識別子	EAS識別子。お使いの環境で必要ない場合は空のままにしてください。
セキュア・ソケット・レイヤー（SSL）の使用	SSLの使用を有効にします。無効にするとセキュリティが低下する場合があります。
すべての証明書を受け入れる	すべての証明書を受け入れる。これを有効にするとセキュリティが低下する可能性があります。
管理されていないアカウントを許可する	アカウントの追加を許可する
クライアント証明書	Exchangeサーバーがクライアント証明書を必要とする場合は、クライアント証明書をアップロードします。

AEシステムアプリ

ここで、Android Enterprise Container の System Apps を有効にすることができます。指定したアプリがシステムのストレージになければ何も起こらないことに注意してください。

コンテナ・パスコード

アンドロイド7.0以上のみ

コンテナに特定のパスワード要件を設定できるようにする。

最小パスワード長	パスワードに最低限必要な記号の数を定める。
パスワードの品質	パスワード強度 不特定 = 特定しない どのパスワードもOK = どのパスワードも受け入れられる at least numeric characters = 少なくとも数字が含まれていなければならない。 少なくとも複雑な文字 = 少なくとも特殊文字を含むこと at least alphanumerical characters = 少なくとも英数字を含むこと。 at least alphabetic characters = 少なくともアルファベット文字を含むこと。
最大非アクティブ時間ロック	コンテナがロックされるまでの最大時間。これは、ユーザーが選択できる最大値のみを設定します。
パスワードに最低限必要な小文字	パスワードに最低限必要な小文字
パスワードに最低限必要な大文字	パスワードに最低限必要な大文字
パスワードに最低限必要な文字以外の文字	パスワードに最低限必要な文字以外の文字
パスワードに最低限必要な数字	パスワードに最低限必要な数字
パスワードに最低限必要な記号	パスワードに最低限必要な記号
パスワード有効期限タイムアウト	パスワードの有効期限が切れると、新しいパスワードを発行しなければならない。
パスワード履歴の制限	以前に使用されたパスワードのうち、許可されていないパスワードの数
パスワードの最大試行回数	コンテナが削除されるまでに、パスワードが誤って入力される頻度を設定する。

サムスンKNOX

アクティベーション

ここでは、Samsung KNOXコンテナを有効にすることができます。Android 10以降ではSamsungからのサポートは終了していますのでご注意ください。Android 10以降でAndroid Enterpriseコンテナを使用する

ノックスのパスコード

デバイスのパスワード設定に関するガイドラインを確立する。

最小パスワード長	パスワードに必要な記号の数を設定します。
パスワードの品質	パスワード強度 どのパスワードもOK = どのパスワードもOK 少なくとも数字が必要 = 最低限の数字が必要 少なくとも複雑な文字 = 最低限の特殊文字が存在すること 少なくとも英数字が必要 = 最低限の英数字が存在すること 少なくともアルファベット文字 = 最低限のアルファベット文字が存在すること
最低限必要な複雑な文字	最低限複雑な文字が必要
最大非アクティブタイムアウト	キーボードがロックされるまでの、ユーザー非アクティブ時の最大タイムアウト時間
指紋認証を許可する	指紋認証を許可する
虹彩認証を許可する	虹彩認証の許可
パスワードの最大年齢	パスワードの有効期限を設定し、新しいパスワードを発行する。
保存されたパスワードの履歴	許可されていない旧パスワードの数
パスワードの最大試行回数	デバイスの完全消去が行われるまでに、パスワードが間違って送信される可能性がある回数を設定する。

ノックス・セキュリティ

特定のデバイスの機能を制限する

カメラを有効にする	カメラの使用を許可する
サムスンKNOXアプリストアを許可する	Samsung KNOX App Storeの使用を許可する。
Google Playサービスを許可する	Google Playサービスを許可する
ブラウザを許可する	ネイティブ・ブラウザの使用を許可する
スクリーンショットを許可する	スクリーンショットの作成を許可する

連絡先のインポートを許可する	有効にすると、KNOXコンテナからデバイスの連絡先へのアクセスが許可されます。
連絡先のエクスポートを許可する	有効にすると、デバイスからKNOXコンタクトへのアクセスが許可されます。
カレンダーのインポートを許可する	有効にすると、KNOXコンテナからデバイスカレンダーへのアクセスが許可されます。
カレンダーのエクスポートを許可する	有効にすると、デバイスからKNOXカレンダーへのアクセスが許可されます。
非セキュアキーパッドを許可する	非セキュア・キーパッドの使用を許可する
ファイルのインポートを有効にする	KNOXコンテナへのファイルインポートを有効にする
ファイルエクスポートを有効にする	KNOXコンテナからのファイルエクスポートを有効にする

ノックス・エクスチェンジ

ここでは、KNOX コンテナの Exchange プロファイルを設定できます。

電子メールアドレス	提供されたユーザーのEメールアドレス プレースホルダ "に注意してください。このプレースホルダは、資格情報を扱うために使用することができ、すべてのデバイスで手動で変更を実行することはありません。 **プレースホルダーを表示**」をクリックすると、プレースホルダーを表示することができます。
サーバーホスト名	Exchangeサーバーのサーバーアドレス
ログイン名	各エンドユーザーデバイスのログイン名。ここでは「プレースホルダ」にも注意してください。
ドメイン	ドメインアドレス
パスワード（デバイスレベルのみ）	オプションとして、個々のデバイスにパスワードを提供することができます。このパスワードが空のままである場合、ユーザーは Exchange パスワードを入力するよう求められます。
同期する前の日数	メールのシンクバックを決定する日数
署名	署名の添付が可能
デフォルトアカウント	このメールアカウントが標準アカウントであることを証明する。
セキュア・ソケット・レイヤー（SSL）の使用	SSL接続を使用する
トランスポート・レイヤー・セキュリティ（TLS）を使用する	TLS接続を使用する
すべての証明書を受け入れる	すべての証明書が受け入れられます。Exchangeサーバーが自己署名証明書を使用している場合は、このオプションを選択してください。

ノックスeメール

電子メールアドレス	提供されたユーザーのEメールアドレス プレースホルダ "に注意してください。このプレースホルダは、資格情報を扱うために使用することができ、すべてのデバイスで手動で変更を実行することはありません。 **プレースホルダーを表示**」をクリックすると、プレースホルダーを表示することができます。
受信サーバープロトコル	受信サーバープロトコル IMAPまたはPOP
受信サーバーアドレス	受信サーバーアドレス
受信サーバーポート	受信サーバーポート
受信サーバーのログイン名/ユーザー名	受信サーバーのログイン名/ユーザー名
受信サーバーのパスワード	受信サーバーのパスワード
受信サーバーがSSLを使用	受信サーバーがSSLを使用
受信サーバーはTLSを使用	受信サーバーはTLSを使用
受信サーバーはすべての証明書を受け入れる	着信サーバーはすべてのタイプの証明書を受け入れる
送信サーバー・プロトコル	送信サーバー・プロトコル SMTP
送信サーバーポート	送信サーバーポート
送信サーバーが余分な認証情報を使用	送信サーバーの追加認証情報。これが "off "に設定されている場合、受信サーバーの設定が使用されます。
送信サーバーのログイン名/ユーザー名	送信サーバーのログイン名/ユーザー名
送信サーバーのパスワード	送信サーバーのパスワード
送信サーバーはSSLを使用	送信サーバーはSSLを使用

送信サーバーはTLSを使用	送信サーバーはTLSを使用
送信サーバーがすべての証明書を受け入れる	送信サーバーはすべてのタイプの証明書を受け入れる
署名	ここに署名を添付することができる。
新着電子メールの受信通知	新着電子メールの受信通知

ノックスアプリ

エンドユーザーデバイスに配布するアプリをここで設定します。アプリはKNOXコンテナで利用できるようになります。アプリを追加するには、[必須アプリ]メニューの手順に従ってください。

アプリケーション名	アプリケーション名
必須	アプリが追加された時点
ソース	アプリの提供元（Playストア｜インハウス）

マークをクリックすると、それぞれのアプリを再度削除することができます。

コネクション管理

無線LAN

この設定を行うには、エンドユーザーデバイスの事前設定を行い、内部アクセスポイントにアクセスします。

サービスセット識別子（SSID）	接続するネットワークのSSID
隠しネットワーク	APがSSIDをブロードキャストしない場合は、アクティブにする。
セキュリティ・タイプ	APのセキュリティ・タイプを確立する

セキュリティ・タイプ

ウェップ

パスワード	APのパスワード

WPA/WPA2

パスワード	APのパスワード

802.1x EAP

EAPメソッド	

PWD	アイデンティティ	アイデンティティ
	パスワード	パスワード

ピーエーピー	フェーズ2認証プロトコル	なし	追加プロトコルなし
		MSCHAPV2	MSCHAPV2プロトコル
		GTC	GTCプロトコル
	CA証明書	CA 証明書	
	アイデンティティ	アイデンティティ	
	匿名アイデンティティ	匿名ID	
	パスワード	パスワード	

EAPメソッド	

TTLS	フェーズ2認証プロトコル	なし	追加プロトコルなし
		PAP	PAPプロトコル
		エムエスシーハップ	MSCHAPプロトコル
		MSCHAPV2	MSCHAPV2プロトコル
		GTC	GTCプロトコル
	CA証明書	CA 証明書	
	アイデンティティ	アイデンティティ	
	匿名アイデンティティ	匿名アイデンティティ	
	パスワード	パスワード	

TLS	CA証明書	CA 証明書
	アイデンティティ	アイデンティティ
	パスワード	パスワード

かそうへいいきもう

接続タイプ	VPN接続タイプを確立する

VPNタイプで「アプリ単位VPN」を選択すると、利用可能なVPNクライアントが変更されます。アプリ単位VPNは、VPNを特定のアプリに限定し、特定のアプリが起動されると自動的にVPN接続を開始します。

AppTec360 VPNクライアント	AppTec360 VPNクライアントとユニバーサルゲートウェイを組み合わせて使用します。
接続名	VPN接続名
ゲートウェイの設定	ユニバーサルゲートウェイのVPN構成を選択する
常時接続VPN	VPNを常時アクティブにし、全トラフィックがVPNを経由するようにする。
ネイティブ・ロックダウンを有効にする	デバイスがVPNに接続されていないとき、すべてのネットワーキングをブロックする。適切に設定されていない場合、接続が完全に失われる可能性があるため、慎重に使用してください。Android 7以上のAndroid Enterpriseのみ
AppTec360のロックダウンを有効にする	VPN接続が開始されるまで、すべてのアプリの使用をブロックする

Cisco AnyConnect	
接続名	VPN接続名
サーバー	サーバーアドレス
証明書モード	無効 = 機能停止 オートマティック = 自動

L2TP (KNOXのみ)	サムスン製端末でのみ利用可能
接続名	接続名
サーバー	サーバーアドレス
L2TPシークレットを有効にする	
DNS検索ドメイン	DNS検索ドメイン

接続タイプ	**VPN接続タイプを確立する**

PPTP (KNOXのみ)	サムスン製端末でのみ利用可能
接続名	VPN接続名
サーバー	サーバーアドレス
暗号化を有効にする	暗号化を有効にする
DNS検索ドメイン	DNS検索ドメイン

L2TP / IPSec PSK (KNOXのみ)	サムスン製端末でのみ利用可能
接続名	VPN接続名
サーバー	サーバーアドレス
IPSec事前共有キー	認証用の事前共有鍵
L2TPシークレットを有効にする	
L2TP シークレット	
DNS検索ドメイン	DNS検索ドメイン

IPSec XAuth PSK (KNOXのみ)	サムスン製端末でのみ利用可能
接続名	VPN接続名
サーバー	サーバーアドレス
IPSec識別子	接続ユーザー名
IPSec事前共有キー	接続用パスワード
DNS検索ドメイン	DNS検索ドメイン

オープンVPN	
接続名	接続名

OpenVPNプロファイル	.ovpnファイルの内容がコピーされる場所は以下の通りである。
OpenVPNアプリ	OpenVPNを使用するためのアプリは2種類あります。 OpenVPN for Android」アプリをお勧めします。別の方法として、"OpenVPN Connect "アプリを使用することもできます。

制限事項

ここでは、接続管理に関する制限を設定することができます。

データローミングを許可する	ローミング中のモバイルデータを許可する
強制データローミング	有効にすると、モバイルデータのローミングが恒久的に有効になります（お勧めしません！）。 この設定は "Allow Data Roaming "設定を上書きする！
以下の設定は、Samsung KNOX 2.0以降でのみ利用可能です。	
緊急電話のみ許可	緊急電話のみ許可
WiFiを許可する	WiFiを許可する
WiFiネットワークの最低セキュリティレベル	WiFiネットワークの最小セキュリティレベル オープン = あらゆるタイプのWiFiが利用可能
ユーザーによるWiFiネットワークの追加を禁止	ユーザー自身がWiFiネットワークを追加することはできません。 この設定は、WiFiプロファイルが "接続管理 "で定義されている場合にのみ可能です。
SMSとMMSを許可する	All = すべてのSMSおよびMMSトラフィックが許可されます。 着信SMSのみ = 着信SMSメッセージのみが許可されます。 発信SMSのみ = 発信SMSメッセージのみ許可 None = SMS / MMSトラフィックを許可しない
ローミング中の同期を許可する	ローミング中の同期を許可する オン = 作動 オフ = 無効 ユーザーの選択 = ユーザーの選択
音声ローミングを許可する	音声ローミングを許可する オン = 作動 オフ = 無効 ユーザーチョイス = ユーザーの選択
システムのhttpプロキシサーバーを使用する	HTTPプロキシサーバーの使用は、システムの設定で提供され、接続されたネットワーク（WiFiまたはAPN）に依存します

APN

以下の設定は、Samsung SAFE 2.0以降でのみ有効です！

APN表示名	APN表示名	
アクセスポイント名	APN名	
送信サーバー・プロトコル	未設定	
	なし	
	PAP	PAPプロトコル
	チャップ	CHAPプロトコル
	PAPまたはCHAP	PAPまたはCHAPプロトコルのいずれか
MCC - モバイル国コード	挿入されたSIMカードのMCCを使用する場合は、このフィールドを空白にしてください。	
MNC - モバイル・ネットワーク・コード	挿入されたSIMカードのMCCを使用する場合は、このフィールドを空白にしてください。	
サーバーアドレス	サーバーアドレス	
サーバーポート番号	サーバーポート番号	
サーバー・プロキシ・アドレス	サーバー・プロキシ・アドレス	
MMSサーバーアドレス	MMSサーバーのアドレス、スタンダードの場合は空白にしてください。	
MMSポート番号	MMSポート番号	
MMSプロキシアドレス	MMSプロキシアドレス	
ユーザー名	ユーザー名	
パスワード	パスワード	
アクセス・ポイント・タイプ	許可されるタイプは以下の通り："default"、"mms"、"supl"このフィールドが空白の場合、"default,supl,mms "が使用されます。	
優先APN	APNが望ましい	

ブルートゥース

ここではBluetoothの各種設定が行えます。

以下の設定は、Samsung KNOX 1.0以降でのみ有効です！

Bluetoothによるデバイス検出を許可する	Bluetooth経由でのデバイス検出を許可する
Bluetoothペアリングを許可する	Bluetoothペアリングを許可する
Bluetoothヘッドセットを許可する	Bluetoothヘッドセットを許可する
Bluetoothハンズフリーデバイスを許可する	Bluetoothハンズフリーデバイスを許可する
BluetoothのA2DPデバイスを許可する	デバイス間でBluetooth A2DPオーディオ・ストリーミングを許可する
発信を許可する	BT経由での発信を許可する
ブルートゥースによるデータ転送を許可する	ブルートゥースによるデータ転送
Bluetoothテザリングを許可する	デバイスをモデムとして使用可能（Bluetoothインターネット接続）
ブルートゥースによるコンピュータへの接続を許可する	ブルートゥースによるコンピュータへの接続を許可する

PIM管理

交換

Samsung KNOX 1.0以上でのみ使用可能！

電子メールアドレス	提供されたユーザーのEメールアドレス プレースホルダ "に注意してください。このプレースホルダは、資格情報を扱うために使用することができ、すべてのデバイスで手動で変更を実行することはありません。 **プレースホルダーを表示**」をクリックすると、プレースホルダーを表示することができます。
サーバーホスト名	Exchangeサーバーのサーバーアドレス
ログイン名	各エンドユーザーデバイスのログイン名。
ドメイン	ドメインアドレス
パスワード（デバイスレベルのみ）	オプションで、個々のデバイスにパスワードを提供することができます。このパスワードが空のままである場合、ユーザーは Exchange パスワードを入力するよう求められます。
同期する前の日数	メールのシンクバックを決定する日数
署名	署名を添付することができます。
デフォルトアカウント	このメールアカウントが標準アカウントであることを確定する。
セキュア・ソケット・レイヤー（SSL）の使用	SSL接続を使用する
トランスポート・レイヤー・セキュリティ（TLS）を使用する	TLS接続を使用する
すべての証明書を受け入れる	すべての証明書が受け入れられます。Exchangeサーバーが自己署名証明書を使用している場合は、このオプションを選択してください。

電子メール

ここで、IMAPとPOPアカウントをそれぞれのエンドユーザーデバイスに配布することができます。

以下の設定は、Samsung KNOX 1.0以降でのみ有効です！		
電子メールアドレス	提供されたユーザーのEメールアドレス プレースホルダ "に注意してください。このプレースホルダは、資格情報を扱うために使用することができ、すべてのデバイスで手動で変更を実行することはありません。 **プレースホルダーを表示**」をクリックすると、プレースホルダーを表示することができます。	
受信サーバープロトコル	受信サーバープロトコル	IMAPまたはPOP
受信サーバーアドレス	受信サーバーアドレス	
受信サーバーポート	受信サーバーポート	
受信サーバーのログイン名/ユーザー名	受信サーバーのログイン名/ユーザー名	
受信サーバーのパスワード（デバイスレベルのみ）	受信サーバーのパスワード（デバイスレベルのみ）	
受信サーバーがSSLを使用	受信サーバーがSSLを使用	
受信サーバーはTLSを使用	受信サーバーはTLSを使用	
受信サーバーはすべての証明書を受け入れる	着信サーバーはすべてのタイプの証明書を受け入れる	
送信サーバー・プロトコル	送信サーバー・プロトコル	SMTP
送信サーバーポート	送信サーバーポート	
送信サーバーが余分な認証情報を使用	送信サーバーの追加認証情報。これが "off "に設定されている場合、受信サーバーの設定が使用されます。	
送信サーバーのログイン名/ユーザー名	送信サーバーのログイン名/ユーザー名	
送信サーバーのパスワード（デバイスレベル	送信サーバーのパスワード	

のみ)	
送信サーバーはSSLを使用	送信サーバーはSSLを使用
送信サーバーはTLSを使用	送信サーバーはTLSを使用
送信サーバーがすべての証明書を受け入れる	送信サーバーはすべてのタイプの証明書を受け入れる
署名	署名はここに添付することができます。
新着電子メールの受信通知	新着メールの受信を通知

AE Gmail Exchange

情報この設定はGmailアプリに適用されます。そのため、Gmailを承認してインストールする必要があります。

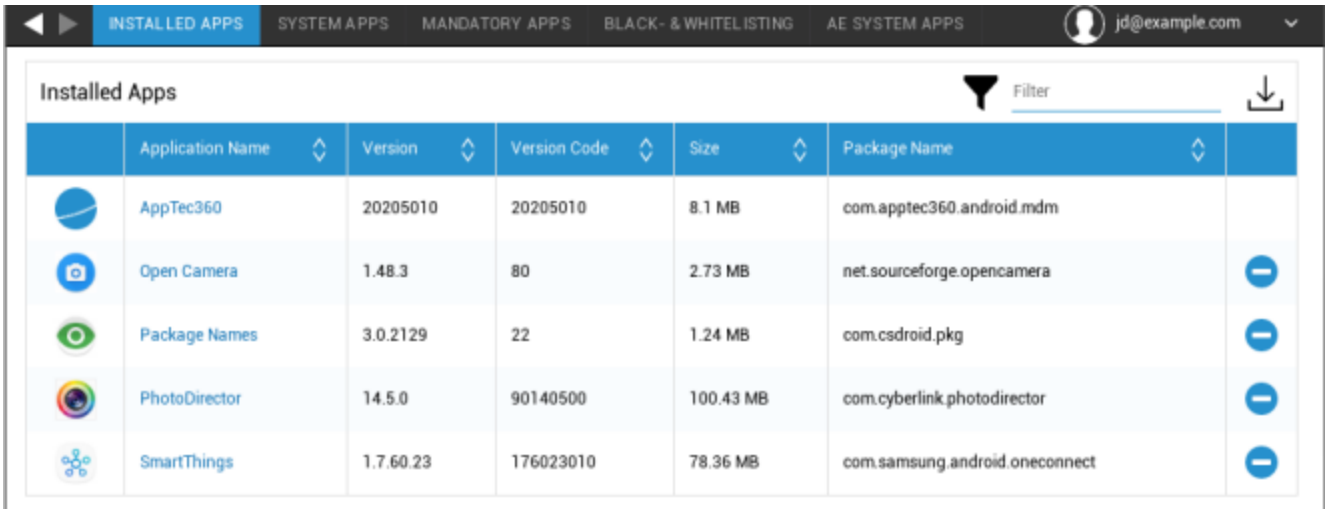
電子メールアドレス	提供されたユーザーのEメールアドレス プレースホルダ "に注意してください。このプレースホルダは、資格情報を扱うために使用することができ、すべてのデバイスで手動で変更を実行することはありません。 プレースホルダーを表示」をクリックすると、プレースホルダーを表示することができます。
サーバーホスト名	Exchangeサーバーのサーバーアドレス
ログイン名	各エンドユーザーデバイスのログイン名。
署名	署名を添付することができます。
同期する前の日数	メールのシンクバックを決定する日数
デバイス識別子	EAS識別子。お使いの環境で必要ない場合は空のままにしてください。
セキュア・ソケット・レイヤー（SSL）の使用	SSL接続を使用する
すべての証明書を受け入れる	すべての証明書が受け入れられます。Exchangeサーバーが自己署名証明書を使用している場合は、このオプションを選択してください。
管理されていないアカウントを許可する	アカウントの追加を許可する
クライアント証明書	Exchangeサーバーがクライアント証明書を必要とする場合は、クライアント証明書をアップロードします。

アプリ管理

エンタープライズアプリマネージャー

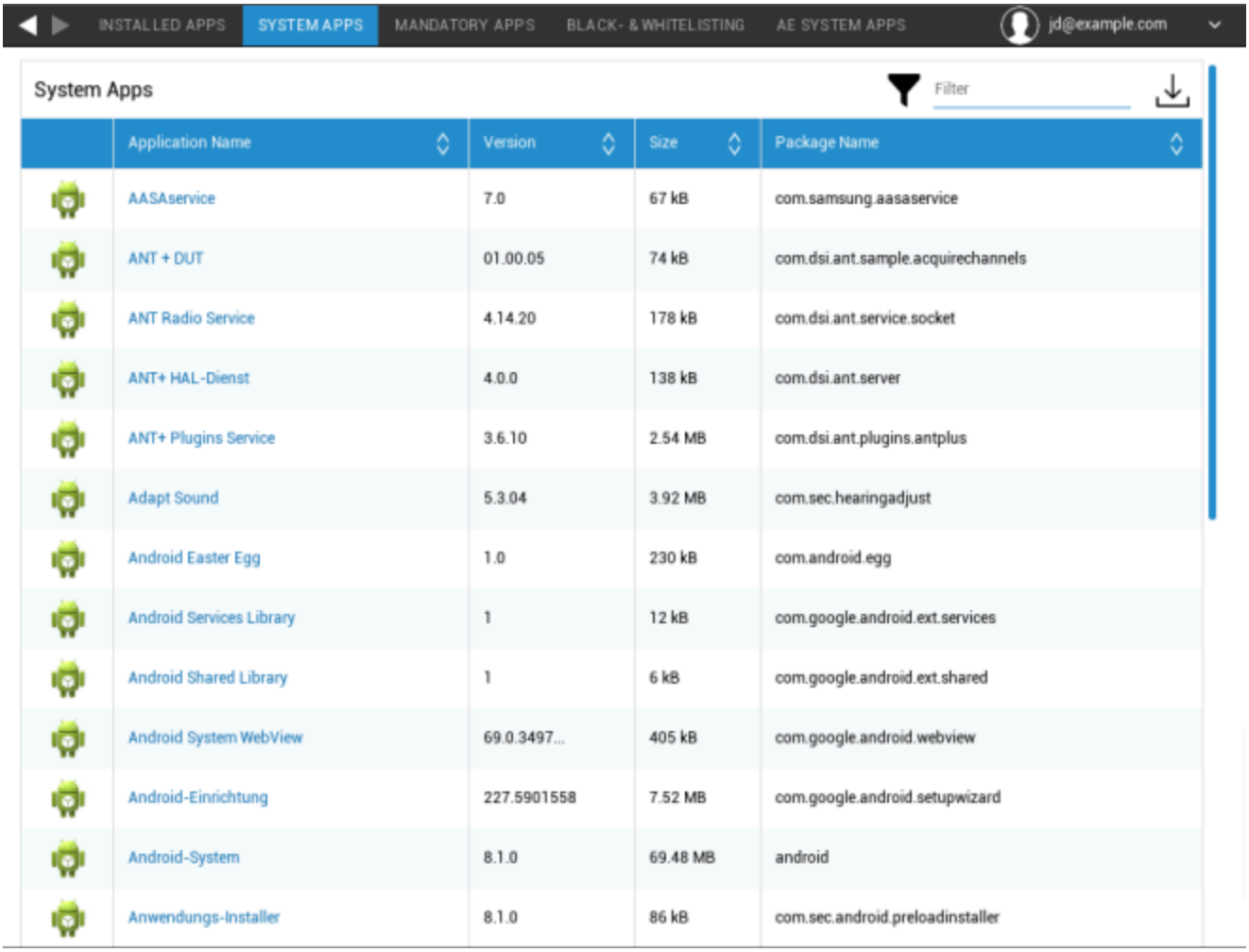
インストール済みアプリ（デバイスレベルのみ）

ここでは、エンドユーザーデバイスに現在インストールされているすべてのアプリが表示されます。


INSTALLED APPS
SYSTEM APPS
MANDATORY APPS
BLACK- & WHITELISTING
AE SYSTEM APPS
jd@example.com
Installed Apps
Filter
Application Name
Version
Version Code
Size
Package Name
AppTec360
20205010
20205010
8.1 MB
com.apptec360.android.mdm
Open Camera
1.48.3
80
2.73 MB
net.sourceforge.opencamera
Package Names
3.0.2129
22
1.24 MB
com.csdroid.pkg
PhotoDirector
14.5.0
90140500
100.43 MB
com.cyberlink.photodirector
SmartThings
1.7.60.23
176023010
78.36 MB
com.samsung.android.oneconnect

システムアプリ (デバイスレベルのみ)

システムアプリ」の下に、プリインストールされているすべてのシステムがパッケージ名とバージョンとともにリストアップされる。



Application Name	Version	Size	Package Name
AASAservice	7.0	67 kB	com.samsung.aasaservice
ANT + DUT	01.00.05	74 kB	com.dsi.ant.sample.acquirechannels
ANT Radio Service	4.14.20	178 kB	com.dsi.ant.service.socket
ANT+ HAL-Dienst	4.0.0	138 kB	com.dsi.ant.server
ANT+ Plugins Service	3.6.10	2.54 MB	com.dsi.ant.plugins.antplus
Adapt Sound	5.3.04	3.92 MB	com.sec.hearingadjust
Android Easter Egg	1.0	230 kB	com.android.egg
Android Services Library	1	12 kB	com.google.android.ext.services
Android Shared Library	1	6 kB	com.google.android.ext.shared
Android System WebView	69.0.3497...	405 kB	com.google.android.webview
Android-Einrichtung	227.5901558	7.52 MB	com.google.android.setupwizard
Android-System	8.1.0	69.48 MB	android
Anwendungs-Installer	8.1.0	86 kB	com.sec.android.preloadinstaller

必須アプリ

必須アプリでは、デバイスにインストールする必要があるアプリを定義できます。設定とデバイスに応じて、アプリは自動的にインストールされるか、ユーザーにインストールを促すプロンプトが表示されます。

アプリの管理を容易にするため、Android Enterpriseを使用することをお勧めします。

シナリオは以下の通り：

通常のPlayストアアプリ

Playストアアプリのインストールには、常にユーザーの操作が必要です。また、端末にGoogleアカウントを設定する必要があります。

社内アプリのインストール

サムスン・デバイスでは、これらのアプリは静かにインストールされます。唯一の例外はコンテナで、ユーザーがインストールを確認する必要があります。

それ以外のシナリオでは、ユーザーはアプリのインストールを確認しなければならない。

AndroidエンタープライズPlayストアアプリ

これらのアプリは、ユーザーが操作することなく、常に静かにインストールされます。

必須アプリを追加するには、「+」をクリックし、リストから必要なアプリを選択します。デバイスがAndroid Enterpriseでフルマネージドまたはコンテナとして設定されている場合、「Google Play Store」タブからアプリをインストールすることはできませんのでご注意ください。

Android Enterpriseを使用している場合は、「AE Playストア」からアプリを選択します。ここでアプリを利用できるようにするには、「一般設定」→「AE Playストア」→「Playストアアプリ」でGoogle Enterprise Playストアでアプリを確認します。

必須アプリを削除すると、そのアプリもデバイスからアンインストールされます。

必須アプリ一覧でアプリ名をクリックし、「configuration」タブに移動してアプリを設定できます。これにはAndroid Enterpriseを使用する必要があり、アプリはこれをサポートする必要があります。そのため、利用できるオプションは選択したアプリによって異なります。

AEシステムアプリ

ここでは、Android Enterpriseデバイスのシステムアプリを有効にすることができます。指定したアプリがシステムのストレージになければ何も起こらないことに注意してください。296

制限と設定

ブラックリストとホワイトリスト

ここでブラックリストまたはホワイトリストを定義できます。ブラックリストにあるアプリはすべてブロックされます。ホワイトリストにないアプリはすべてブロックされます。空のブラックリストは何もブロックせず、空のホワイトリストはすべてをブロックします*。

**必須アプリと Enterprise App Store からのアプリはすべて、自動的にホワイトリストに登録されます。手動で追加する必要はありません。*

をクリックすると、ブラックリストまたはホワイトリストに追加したいアプリを検索するか、パッケージ名を手動で入力することができます。

システアプリの制限

システアプリの制限」では、プリインストールされたアプリやサービスをブロックすることができます。

ブラウザを無効にする	標準ブラウザを無効にする
カレンダーを無効にする	ネイティブカレンダーを無効にする
電卓を無効にする	電卓を無効にする
クロームブラウザを無効にする	Chromeブラウザを無効にする
クロックの無効化	クロックを無効にする
コンタクトを無効にする	コンタクトを無効にする
ダイヤラーを無効にする	ネイティブのダイヤラーを無効にする
電子メールを無効にする	電子メールを無効にする
交換を無効にする	Exchangeアカウントを無効にする
フェイスブックを無効にする	Facebookアプリを無効にする
ギャラリーを無効にする	ネイティブのギャラリーアプリを無効にする
Gmailを無効にする	Gmailを無効にする
グーグルブックスを無効にする	グーグルブックスを無効にする
Google Play キオスクを無効にする	Google Play キオスクを無効にする
グーグルマップを無効にする	グーグルマップを無効にする
Googleミュージックを無効にする	Googleミュージックを無効にする
Googleムービーを無効にする	Googleムービーを無効にする
Google Playストアを無効にする	Google Playストア（一般公開されているApp Store）を無効にする
グーグルプラスを無効にする	グーグルプラスを無効にする
グーグル検索を無効にする	グーグル検索を無効にする
Googleトーク / Googleハングアウトを無効にする	Googleトーク / Googleハングアウトを無効にする
音楽プレーヤーを無効にする	ネイティブの音楽プレーヤーアプリを無効にする
設定を無効にする	デバイスの設定を無効にする
シムツールキットを無効にする	Sim Toolkitサービスを無効にする
SMS/MMSを無効にする	SMS/MMSを無効にする
ストリートビューを無効にする	ストリートビューのサービスを無効にする
Youtubeを無効にする	Youtubeを無効にする

サムスンアプリ

サムスンアプリ」では、サムスンデバイス用の追加設定や制限を定義できます。

AllShare Play / Samsung Linkを無効にする	AllShare Play / Samsung Linkを無効にする
ChatONを無効にする	ChatONを無効にする
ゲームハブを無効にする	ゲームハブを無効にする
グループプレーを無効にする	グループプレーを無効にする
ヘルプを無効にする	サムスンヘルプを無効にする
KNOXを無効にする	サムスンKNOXコンテナを無効にする
メモを無効にする	ボイスメモを無効にする
マイファイルを無効にする	マイファイルを無効にする
光学式リーダーを無効にする	光学式リーダーを無効にする
ポラリスオフィスを無効にする	ポラリスオフィスを無効にする
リーダーズハブ/サムスンブックスを無効にする	リーダーズハブ/サムスンブックスを無効にする
Sメモを無効にする	サムスンのメモアプリを無効にする
Sトランスレーターを無効にする	サムスン翻訳アプリを無効にする
Sボイスを無効にする	Sボイスアシスタントを無効にする
サムスンアプリを無効にする	サムスンApp Storeを無効にする
サムスンハブを無効にする	サムスンエンターテインメントストアを無効にする
ビデオプレーヤーを無効にする	ビデオプレーヤーを無効にする
ボイスレコーダーを無効にする	ボイスレコーダーを無効にする
WatchONを無効にする	WatchON を無効にする（リモコンをシミュレートする）

ファーウェイのアプリ

Huawei Apps」では、Huaweiデバイスの追加設定や制限を定義できます。

DLNAを無効にする	DLNAを無効にする
アプリのインストーラーを無効にする	アプリのインストーラーを無効にする
ファイルマネージャーを無効にする	ファイルマネージャーを無効にする
バックアップマネージャーを無効にする	バックアップマネージャーを無効にする
システムアップデータを無効にする	システムアップデータを無効にする
ツールボックスを無効にする	ツールボックスを無効にする
天候を無効にする	天候を無効にする
FMラジオを無効にする	FMラジオを無効にする

アプリ管理設定

ここでは、InHouse Appsのアップデート動作を定義できます。

アップデートチェック頻度は、AppTec360アプリがInHouseアプリのアップデートを探す頻度を定義します。新しいバージョンが検出されると、ダウンロードされ、インストールされます。

Wi-Fiしきい値は、アプリが設定したしきい値より大きい場合、ダウンロードをWi-Fi接続に制限するかどうかを定義します。アプリのサイズが小さいか、しきい値を定義していない場合、アプリはWi-Fiでも携帯電話ネットワークでもダウンロードされます。

エンタープライズ・アプリケーション・ストア

ここで追加されたアプリ（Enterprise App Store）は、デバイスに自動的にインストールされないことにご注意ください。ユーザーは、デバイスでEnterprise App Storeを開き、アプリを手動でインストールする必要があります。

端末にアプリを自動的にインストールしたい場合は、「アプリ管理」→「Enterprise App Manager」→「必須アプリ」で必要なアプリを追加してください。

このポイントでは、オプションのアプリをユーザーに配布することができます。

プレイストア

をクリックして、Playストアアプリをストアに追加します。Android Enterpriseを使用している場合は、"App Management Enterprise Play Store "にアクセスしてください。また、ここで定義されたアプリをインストールするには、端末にGoogleアカウントが設定されている必要があります。

インハウス

In-House（社内開発）」では、社内で開発したアプリをアップロードして配布することができます。

をクリックすると、InHouseアプリがエンタープライズアプリストアに追加され、ユーザーがインストールできるようになります。このダイアログでは、新しい InHouse アプリをアップロードすることもできます。

エンタープライズPlayストア

ここで追加されたアプリ（Enterprise Play Store）は、デバイスに自動的にインストールされないことにご注意ください。ユーザーはデバイスでPlayストアを開き、手動でアプリをインストールする必要があります。

端末にアプリを自動的にインストールしたい場合は、「アプリ管理」→「Enterprise App Manager」→「必須アプリ」で必要なアプリを追加してください。

このポイントでは、オプションのアプリをユーザーに配布することができます。

Android Enterprise Playstoreにアプリを追加することができます。一般設定 → AE Play ストア → Play ストア アプリ でアプリを承認する必要があります。これらのアプリは通常のGoogle Playストアに追加されます。

また、「一般設定」→「アプリ管理」→「AE Playストア」→「ストアレイアウト」で、まずアプリのレイアウトを定義する必要があります。

アプリをストアに追加するには、レイアウトが必要です。

キオスクモード＆ランチャー

キオスク・モード

キオスクモードでは、アプリやURLを事前に定義することができます。そうすれば、このアプリやURLを実行/訪問することだけが可能になります。

同様に、様々なハードウェアボタンは、キオスクモードで無効にすることができます。

自動スタート	プロファイルがエンドユーザーデバイスに到達すると同時に、自動的にキオスクモードを開始します。
キオスクモードの予定？	キオスクモードの時間を設定することができ、設定した時間に自動的に開始・終了します。
開始時間	開始時間
時間（分	キオスクモードが再び終了するまでの時間（分単位

アプリケーション・タイプ

シングルアプリ	キオスクモードでアプリを起動したい場合は、"Application Type "で"Package "を選択します。
キオスク・アプリケーション	キオスクモードで起動するアプリを選択するには、ここをクリックします。 通常のアプリ管理の概要をご覧いただけます。 Google Play ストア」、「Android 社内アプリ」、「パッケージ名」から選択できます。

アプリケーション・タイプ

URL	キオスク・モードでURLを起動したい場合は、"Application Type "で "URL "を選択します。 次に、希望のURLアドレスを定義します。
非アクティブの後にブラウザをクリアする	ここでは、キオスクモードを再起動する時間間隔を分単位で定義できます。
ウェブキャッシュとクッキーを消去する	この機能を有効にすると、キオスクモードの再起動後、ウェブキャッシュ（クッキーとキャッシュされた画像）が消去されます。
同一原産地ポリシー	この機能が有効な場合、ユーザーは定義されたURLのサブページのみを閲覧することができます。 例えば、次のURLを定義したとする。www.mypage.comすると、ユーザーはwww.mypage.com/subpage。
ホワイトリストのURL	ここでホワイトリストを維持することができ、これらのURLはすべて許可されます。 1行につき1URLまで URLはhttp:/またはhttps:// で始まる必要があります。
ブラックリストに掲載されたURL	ここでブラックリストを管理することができます。 1行につき1URLまで URLはhttp:/またはhttps:// で始まる必要があります。
画面の向き	この設定は画面調整に関連する オートマティック = 自動 ポートレート = 縦型 ランドスケープ = 風景モード

マルチアプリ	マルチアプリ」キオスクモードを選択した場合、AppTec360 Launcher の使用が強制されます。
アプリ	アプリケーションキオスクアプリとしてPlaystoreまたは社内アプリを選択します。パッケージ名を入力することも可能です。選択したキオスクアプリはデバイスにインストールされている必要があります。キオスクアプリケーショ ンを必須として設定することを忘れないでください。 ホームスクリーンへのショートカット：オン」に設定すると、ホームスクリーンにショートカットが作成されます。オフ」に設定しても、アプリはアプリ一覧に表示されます。

終了パスワード 有効	この機能を有効にすると、ユーザーが事前に設定したパスワードでキオスクモードを終了することができます。
終了パスワード	これは、あなたが事前に設定したパスワードです。
ステータスバーの自動折りたたみ	このオプションを有効にすると、ステータスバーが自動的にカラー表示になります。このオプションを使用すると、ユーザーはステータスバーの情報を見ることができますが、その機能にアクセスすることはできません。
ステータスバーを無効にする	ステータスバーには、通知、ショートカット、情報が表示されます。KNOX 1.0以上のSamsungデバイスでのみ使用できます。
ボリュームキーを無効にする	ボリュームキーを無効にする（KNOX 1.0以上のSamsung製デバイスでのみ使用可能）
オン / オフスイッチの無効化	オン/オフスイッチの無効化（KNOX 1.0以上を搭載したSamsungデバイスでのみ使用可能）
ホームボタンを無効にする	ホームボタンを無効にする。この機能が有効になっている場合、キオスクモードはAppTec360 コンソールでのみ終了できます。 (KNOX1.0以上のSamsungデバイスでのみ利用可能)
ナビゲーションバーを無効にする	ナビゲーションバー（戻る/メニュー）を無効にすることができます。 この機能が有効になっている場合、キオスクモードは AppTec360 コンソールでのみ終了できます。 (KNOX1.0以上のSamsungデバイスでのみ利用可能)

アプリのアップデート設定	
アプリのアップデートを許可する	キオスクモードが有効な場合でも、アプリのアップデートを促すメッセージが表示されます。Samsung KNOXを搭載したデバイスでは、アプリは静かに更新されます。
更新ウィンドウ	ユーザーがアプリのアップデートをインストールするよう促される間隔を設定します。

チームビューアー	
無人アクセスを有効にする	有効にすると、管理者はユーザーの操作なしでデバイスをリモートコントロールできます。TeamViewer Hostアプリをデバイスにインストールする必要があります。

AppTec360 ランチャー

AppTec360 Launcherを有効にする	オンAppTec360 Launcherを有効にします。ユーザーはこれをデフォルトランチャーとして1回設定する必要があります。 注：キオスクモードが有効で、キオスクモードが "Multi App "に設定されている場合、AppTec360ランチャーの使用が強制されます。
大きなアイコン	オンランチャーにアプリのアイコンを大きく表示します。
AppTec360アプリのアイコンを隠す	オンAppTec360アプリを完全に隠す
AppTec360ストアアイコンを隠す	オンAppTec360 Enterprise AppStoreを完全に非表示にします。

AppTec360の設定

AppTec360設定アプリを有効にする	AppTec360設定アプリは、WiFiとBluetooth接続を制御します。
マルチアプリで設定を有効にする キオスク・モード	有効な場合、ユーザーはマルチアプリキオスクモードがアクティブである間、AppTec360設定アプリにアクセスできます。

リモコン

スプラッシュトップ

Splashtop Setupの現在のステータスが表示されます。Splashtop を使用してデバイスにリモートアクセスするために必要な手順が表示されます。ここでは、Splashtop ウェブサイトから取得できるデプロイコードを入力する必要もあります。デプロイコードはデバイスに接続するために必要です。

チームビューアー

Teamviewer セットアップの現在のステータスが表示されます。Teamviewer 経由でデバイスにリモートアクセスするために必要な手順が表示されます。

コンテンツ管理

コンテンツボックス

ここで、このデバイスのContentboxを有効にすることができます。有効にすると、Contentboxアプリがデバイスにインストールされます。

セキュアブラウザ

ここで、このデバイスのセキュアブラウザを有効にできます。有効にすると、セキュアブラウザアプリがデバイスにインストールされます。このブラウザは、ニーズに合わせてデバイス上でウェブブラウザを提供するように構成できます。

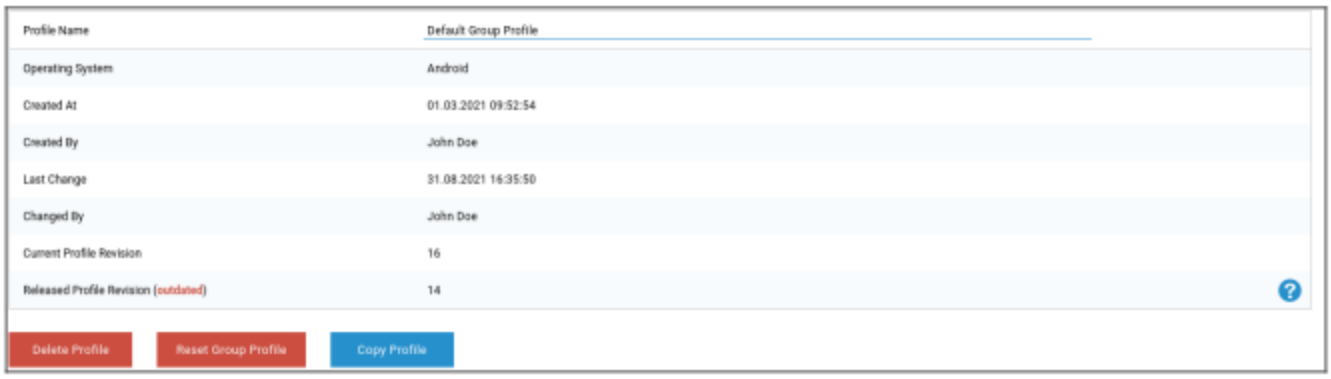
パスワードが必要	ブラウザーにアクセスするためにパスワードを設定し、使用することをユーザーに要求する。
ダウンロードを制限する / で開く	ウェブサイトからのダウンロードをブロック
アップロードの制限	特定のURLへのアップロードを制限します。URLを指定しない場合は、アップロードを完全にブロックします。
コピーを許可する	ウェブページ内のテキストのコピー、切り取り、共有を許可する。
スクリーンキャプチャを許可する	スクリーンショットのキャプチャを許可する。
データ・クリーンアップの頻度	すべてのユーザーデータ (履歴、キャッシュなど) を自動的に削除する頻度を選択します。
会社のしおり	ブックマークは、ブラウザのブックマーク内の「会社のブックマーク」フォルダに表示されます。ユーザーが編集することはできません。
アドレスバーを隠す	アドレスバーを非表示にし、ユーザーが訪問しているURLを表示しないようにする。
ブラウザ内ホワイトリスト (ユニバーサルゲートウェイなし)	クライアント側でURLのホワイトリスト化が可能。- 会社のブックマークは常にホワイトリストに登録されます。
ゲートウェイベースのブラックリストとホワイトリスト	ブラックリストには以下の要件があります：- AppTec360 Universal Gatewayが動作していること (「一般設定」→「Universal Gateway」) - 指定されたDNSサーバーでVPN設定が動作していること (「一般設定」→「Universal Gateway」→「VPN設定」) - ブラックリスト設定 (「一般設定」→「Universal Gateway」→「ドメインブラックリスト」) - プロファイルで有効なVPN接続があること (「接続管理」→「VPN」)。

構成 Windows 10 PC

一般

グループプロフィールの概要（グループレベルのみ）

グループプロフィールを開くと、プロフィールの概要が表示されます。



プロフィール名	プロフィールの名前（ここで変更可能）
オペレーティングシステム	対象OS
作成日時	創造の時
作成者	プロフィールの作成者
最後の変更	プロフィールの最終変更時刻
変更履歴	最後の変更を行ったアカウント
現在のプロフィール改訂	保存されたプロファイル状態の修正
プロフィール改訂版をリリース	割り当てられたプロファイルのリビジョン（"Assign now"）。ラベルのテキストの後ろに"(outdated) "と表示されている場合は、プロファイルを保存したものの、まだ割り当てていないことを意味します。

デバイスの概要 (デバイスレベルのみ)

デバイスの概要：

PC名	PC名
クライアント	デバイス Windows タイプ
最終所在地	デバイスが最後に確認された位置の緯度と経度
割り当てられた必須アプリ	デバイスに割り当てられた必須アプリの数
PC UID	PCのUID
OS版	Windows Editionを表示します。
OSバージョン	現在インストールされているWindowsのバージョン
OSビルド	現在のWindowsビルド
オペレーティングシステム	現在インストールされているオペレーティング・システム
シリアル番号	デバイスのシリアル番号
デバイスの所有権	設定されたオーナーシップ・タイプ
デバイス・タイプ	デバイスのタイプ
ルーツ	デバイスがルート化されているかどうかを示す
準拠	デバイスが準拠しているかどうかを示す
ラストシーン	プロフィールに変更が加えられた日時
ユーザー割り当て	このデバイスが現在割り当てられているユーザーまたはグループを表示します。 ドロップダウンリストから別のユーザーまたはグループを選択することで、デバイスを移動できます。

設定

自動更新を許可する	OSの自動アップデートを許可するかしないか。

コンフィグ改訂（デバイスレベルのみ）

ここで、どのグループプロファイルがデバイスに割り当てられているかの概要が表示されます。

グループプロフィールをクリックすると、そのプロフィールに直接アクセスし、設定を行うことができます。

このマークがあれば、割り当てられたアプリをグループプロファイルの設定に戻すことができます。

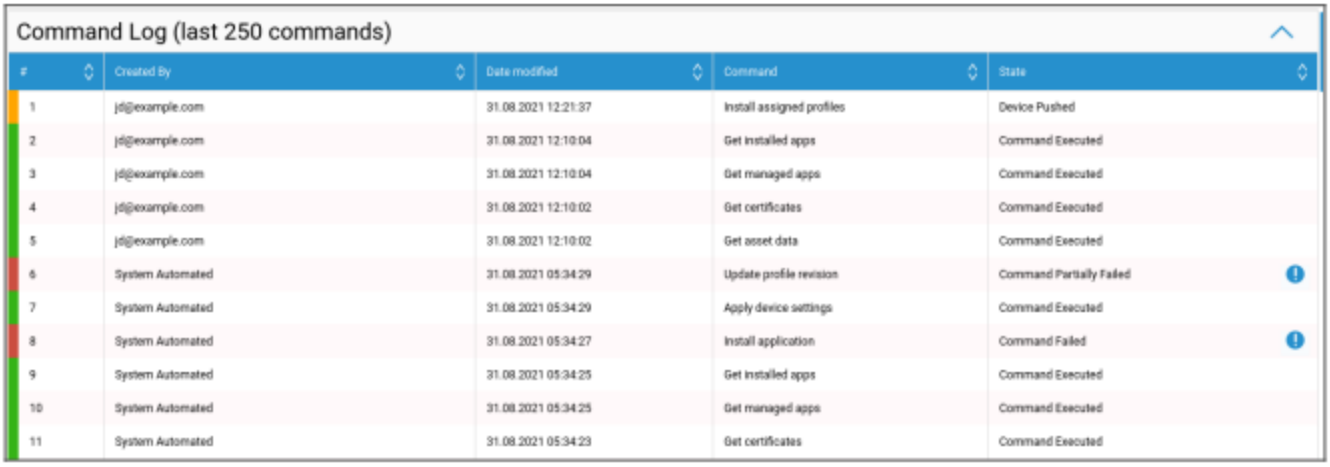
この記号を使えば、デバイスのプロファイルをリセットして、設定を一切なしにすることができる。

"Newer Revision available "は、グループプロファイルが変更され保存されたが、割り当てられていないことを示します。グループプロファイルの変更をデバイスに適用するには、グループレベルで "Assign now "を使用してグループプロファイルを割り当てる必要があります。

デバイスログ（デバイスレベルのみ）

コマンドログ

ここでは、デバイスに対して発行されたコマンドとそのステータスを確認することができます。



System Automated」によって作成されたコマンドは、システムによって自動的に作成される。

可能なコマンドステータス

デバイスが押される	プッシュリクエストは、EMM サーバーに接続するようデバイスに指示するため、プッシュサービス（APNS など）に送信されました。
コマンド作成	コマンドがシステム内に作成された。
コマンド送信	コマンドは、サーバーに接続された後、デバイスに送信された。
コマンド実行	コマンドは正常に実行された。
コマンド失敗	コマンドが失敗しました。*
コマンド一部失敗	デバイスのOSによっては、いくつかのコマンドがグループ化されることがある。 このコマンドグループの一部は失敗した。*
コマンドは実行されたが、最終的に失敗	コマンドは実行されたが、もしかしたら実行されていなかったかもしれない。
コマンド・リパッシュ	コマンドはユーザーによってリプッシュされた。
廃棄	コマンドが破棄された。例えば、他のコマンドに取って代わられたとか、デバイスが再登録されて古いコマンドが削除されたとか。

*メッセージの後ろにエクスクラメーションマークが表示されている場合は、カーソルをアイコンの上に置くと詳細な情報を得ることができます。

資産管理（デバイスレベルのみ）

デバイス情報

メーカー	機器メーカー
モデル	デバイスモデル
モデル番号	モデル番号
オペレーティングシステム	オペレーティングシステム
OSバージョン	OSバージョン
シリアル番号	シリアル番号
ExchangeID	ExchangeID
合計RAM	合計RAM
ディスプレイ解像度	ディスプレイ解像度
電話言語	デバイス言語
ファームウェア・バージョン	ファームウェアバージョン
DMクライアントバージョン	デバイス管理クライアントのバージョン
ハードウェア・バージョン	デバイスのハードウェアバージョン
CPUアーキテクチャ	CPUアーキテクチャ（プロセッサタイプ）

セルラー

SIMキャリアネットワーク	キャリアネットワーク
電話番号	電話番号
ローミング状況	ローミング状況
IMEI	IMEI
移動加入者識別番号	移動加入者識別番号
モデム・ファームウェア	モデム・ファームウェア

同期情報

インスタントDMコネクション	デバイスはすぐにAppTecへの接続を作成する必要があります。
初回リトライ時間	最初の接続のリトライ時間
接続の再試行	コネクション・マネージャーからの切断またはWinInetレベルのエラーが発生した後の、新規接続の再試行回数
最大睡眠時間	パッケージ送信エラー後の最大スリープ時間
最初の同期再試行	入団後の第1ステージの時間
最初の再試行間隔	入団後の第1ステージの時間
2回目の同期リトライ	入団後の第2ステージの時間
秒リトライ間隔	入団後の第2ステージの時間
通常の同期再試行	入学後の追加ステージの時間
通常の再試行間隔	入学後の追加ステージの時間

セキュリティ管理

盗難防止 (デバイスレベルのみ)

GPS情報 (デバイスレベルのみ)

ここでデバイスの現在地/最終位置を設定できます。ローカライズは1つまたは2つのパスワードで保護できます：参照："一般設定" > "プライバシー" > "GPSアクセス"

GPS設定

GPS追跡を有効にする	GPS情報の定期的な同期を有効にする。
トラッキング間隔	GPS情報の同期間隔を設定します。

セキュリティ設定

パスコード

最小パスワード長	最小パスワード長	
パスワードの構成	パスワードが含まなければならない特定の文字の数を指定します。 これらは大文字、小文字、数字、特殊記号で構成される。	
パスワードの品質	ここでは、パスワードの品質を設定することができます	
	英数字	数字とアルファベットのみ
	数値	数字のみ
	数字または英数字	数字または数字と文字
最大休止時間ロック	デバイスがロックされるまでの無操作時間。ユーザーはこの時間経過後、デバイスのパスワードを入力してデバイスのロックを解除する必要があります。	
パスワードの有効期限	新しいパスワードを設定するまでの時間を設定します。	
パスワード履歴の制限	過去に使用されたパスワードの数。	
失敗したパスワードの最大試行回数	デバイスの完全消去が実行されるまでのパスワード誤入力回数	

アンチウイルス

アンチウイルス設定 - スキャン設定の設定	
スキャンの種類	クイックスキャンとフルスキャンのどちらを実行するかを選択します。
スキャン開始の設定	Windows Defenderがスキャンを開始する時間帯を選択します。
スキャン周波数	Windows Defenderのスキャンを実行する日を選択します。
署名の更新頻度	署名をチェックする間隔を時間単位で指定します。

スキャンするファイルの種類を設定する	
アーカイブファイルのスキャンを許可する	アクセス時にアーカイブ（.zipなど）のスキャンを許可または禁止する。
スクリプトのスキャンを許可する	Windows Defenderのスクリプトスキャン機能を許可または禁止します。
電子メールのスキャンを許可する	電子メールのスキャンを許可または拒否する。
ネットワークファイルのスキャンを許可する	ネットワークファイルのスキャンを許可または禁止する。
マップされたネットワークドライブの完全スキャンを許可する	マップされたネットワークドライブのスキャンを許可または禁止する（フルスキャンが有効な場合のみ有効）。
双方向スキャンを制御	どのファイル群を監視するかを制御する。
リムーバブルドライブの完全スキャンを許可する	リムーバブルドライブの完全スキャンを許可または禁止します。完全スキャンが開始された場合のみ。

スキャンから除外するファイルの種類	
スキャンするファイルの種類を無視する	ファイル拡張子のタイプのセットを定義します。各フィールドの各ファイル拡張子。
ディレクトリパスを無視する	ディレクトリパスをスキャンしないように定義する。1フィールドにつき1パス。例 例："C:◆Example"、"C:◆Windows"、"C:◆Users"。
スキャンからプロセスを除外する	特定のプロセスによって開かれたファイルを Microsoft Defender アンチウイルスのスキャンから除外します。.フィールドごとに1つのパスを指定します。 例"C:◆myFile.exe"、"C:◆WindowsmyProcess.exe"、 "C:◆myScript.bat

追加設定	
リアルタイム監視	Windows Defenderリアルタイム監視機能の許可または不許可
行動モニタリングの許可	Windows動作監視機能の許可または不許可
クラウド保護を許可する	Windows Defenderが検出した問題について、Microsoftに情報を送信することを許可または拒否します。マイクロソフトはその情報を分析し、デバイスに影響を及ぼしている問題の詳細を知り、改善された解決策を提供します。
	サンプル送付時の動作
Windows DefenderのIOAV保護を許可する	Windows DefenderのIOAV保護を許可または拒否する
ディフェンダーの「オンアクセス保護」UIへのアクセスを許可する	
平均CPU負荷率	Windows Defenderスキャンの平均CPU負荷率(パーセント)

マルウェアへの対応	
深刻度が低い	重大度レベルごとに、デバイスがマルウェアをどのように処理するかを定義できます。 利用可能なオプションは以下の通り： • クリーン • 検疫 • 削除 • 許可する • ユーザー定義 • ブロック
中程度の重症度	
深刻度が高い	
重症度	
クリーニングされたマルウェアを保持する日数	隔離されたファイル/アイテムがシステムに保存される日数。デフォルト値は 0 で、アイテムは隔離され、自動的には削除されません。最大値は 90 です。

セキュリティセンター

Windows セキュリティセンター - Windows セキュリティの設定	
ウイルス＆脅威保護UIを無効にする	
ランサムウェアのデータ復元UIを隠す	
アカウント保護UIを無効にする	
ファイアウォールとネットワーク保護UIを無効にする	
アプリとブラウザのコントロールUIを無効にする	
エクスプロイト・プロテクションの変更を許可しない	ユーザーがエクスプロイト保護設定を変更できないようにする
デバイスセキュリティUIを無効にする	
TPMのトラブルシューティングを隠す	TPMのトラブルシューティング設定を隠す
TPMクリアボタンを無効にする	
デバイスのパフォーマンスとヘルスUIを無効にする	
ファミリーオプションUIを無効にする	

トーストのカスタマイズ	
カスタマイズされたサポート情報を有効にする	セキュリティセンターアプリの右下に、御社用にカスタマイズされたサポート連絡先を表示できるようにする。
Eメールアドレス	会社のEメールアドレスを設定する
会社名	会社名の設定
会社電話	会社の電話を設定する
ヘルプURL	会社のヘルプURLを設定する

追加設定	
通知を無効にする	Windows Defenderセキュリティセンター通知の表示を無効にする。
TPMファームウェア・アップデートの推奨を隠す	脆弱なファームウェアが検出された場合、TPM ファームウェアを更新するよう推奨することを隠す。
会社名と連絡先オプションの表示	Windows Defenderセキュリティセンターの連絡先カードに、会社名と連絡先オプションを表示します。
セキュアブートを隠す	セキュリティ・ブート・エリアを隠す。
セキュリティ通知領域のコントロールを隠す	Windowsセキュリティ通知領域コントロールを隠す。

ファイアウォールの設定

ファイアウォールの設定 - グローバル設定	
認証セットを無視する	認証セットで指定された認証スイートのすべてをサポートしていない場合は、認証セット全体を無視する。
パケットキューイングの種類	IPsec トンネルゲートウェイシナリオの暗号化された受信とクリアフォワードパスの両方で、受信側のソフトウェアのスケーリングがどのように有効になるかを指定する。
ステートフルFTPフィルタリングを無効にする	これが無効の場合、セカンダリ接続を許可するステートフルなファイル転送プロトコル（FTP）フィルタリングは実行されません。
セキュリティ・アソシエーションのアイドル時間	このフィールドは、セキュリティ・アソシエーションのアイドル時 間を秒単位で設定する。この指定された時間、ネットワーク・トラフィックが表示されないと、セキュリティ・アソシエーションは削除される。
共有鍵エンコーディング	共有鍵のエンコーディングを設定する
IPSecの例外	インターネットプロトコルの例外設定
証明書失効リストのチェック	

ファイアウォールプロファイル (ドメインプロファイル / プライベートプロファイル / パブリックプロファイル)	
このプロファイルのファイアウォールを有効にする	
通知を無効にする	アプリケーションがポートのリッスンをブロックされた場合、ユーザーへの通知を表示しないようにする。
マルチキャストブロードキャストに対するユニキャストレスポンスをブロックする	
許可されたアプリケーション・ファイアウォール・ルールの実施	このルールが適用されない場合、ローカルストア内の許可されたアプリケーションファイアウォールルールは無視され、適用されません。
グローバルポートファイアウォールルールの適用	これが強制されない場合、ローカル ストアのグローバル ポート ファイアウォール ルールは無視され、強制されません。この設定は、グループ ポリシー ストアで設定または列挙されている場合、または GroupPolicyRSoPStore から列挙されている場合にのみ意味を持ちます。
ファイアウォールルールの適用	このルールが適用されない場合、ローカルストアからのファイアウォールルールは無視され、適用されません。
接続セキュリティ・ルールの実施	これが実行されないと、ローカルストアからの接続セキュリティルールは無視され、実行されない。
デフォルトのアウトバウンドアクション	ファイアウォールがアウトバウンド接続に対してデフォルトで行うアクション
デフォルトの受信アクション	ファイアウォールがインバウンド接続に対してデフォルトで行うアクション
ステルスモードを無効にする	ステルスモードは、Windowsファイアウォールのメカニズムで、悪意のあるユーザーがネットワークコンピューターやそのコンピューターが実行するサービスに関する情報を発見するのを防ぐのに役立つ。
未承諾トラフィックに応答しないようにする	無効の場合、ファイアウォールのステルスモードのルールは、トラフィックがIPsecによって保護されている場合、ホストコンピュータが未承諾のネットワークトラフィックに応答することを妨げてはならない。

ファイアウォールルール

ファイアウォールルール	
名称	ルール名
説明	ルールの説明
アクション	このルールがトラフィックをブロックするか、許可するかを指定します。ブロック]オプションは、MDMサーバーとデバイス間のトラフィックもブロックする可能性があることを考慮してください（残りの設定による）。
ディレクション	
エッジトラバーサルを有効にする（**Directionが インバウンドトラフィックに**設定されている場合のみ有効）	特定のインバウンドトラフィックが、Teredoトンネリング技術を使用して、NATや他のエッジデバイスを通してトンネリングすることが許可されていることを示す。

プログラムとサービス	
アプリケーションを定義する。	有効になっていない場合は、すべてのアプリケーションを考慮します。
パッケージファミリー名	ルールが適用されるパッケージファミリ名。
アプリケーションのファイルパス	ルールが適用されるC:¨WindowsSystemAppacheNotepad.exeのような完全なアプリケーション。
完全修飾バイナリ名	ルールを適用する完全修飾バイナリ名。FQBNは以下の形式の文字列である：{PublisherProductFilename,Version}の形式の文字列である。
サービス名	サービス名（例："EventLog"）を入力します。Powershellで "Get-Service "コマンドを実行すると、サービス名のリストを取得できます。

プロトコルとポート				
プロトコル	ルールが使用するプロトコル。			
	利用可能な値： - どんなものでも - カスタム - ホポート - アイシーエムピーブイフォー - アイジーエムピー - TCP - UDP - アイピーブイシックス - IPv6ルート - IPv6-フラグ - GRE - アイシーエムピーブイシックス - IPv6-NoNext - IPv6オプション - VRRP - PGM - L2TP	カスタム	0 ~ 255のプロトコル番号を入れる。	プロトコル番号
		TCPまたはUDPに設定した場合	ローカルポートを指定する。	ルールが使用するローカルポート。
			地方港	単一ポートまたはポート範囲。 例：100-120,200,300-320。
			リモートポートを指定する。	ルールが使用するリモートポート。
			リモートポート	単一ポートまたはポート範囲。 例：100-120,200,300-320。

スコープ	
ローカルIPを指定、それ以外は任意のIP	ローカルIPの集合。-で区切られたIPの範囲も指定できます。
ローカルIPアドレス	単一のIPの集合、または-で区切られたIPの範囲
リモートIPを指定、それ以外は任意のリモートIP	リモートIPのセットを指定する。"-"で区切られたIPの範囲を指定することもできる。
リモートIPアドレス	単一のIPまたはIPの範囲を指定する
トークン	リモートアドレスとともに設定できるトークン。トークンIntranet、RmtIntranet、Ply2Rendersは、Windows 10、バージョン1809以降でサポートされています。

詳細設定	
プロファイルを指定する。	無効の場合、すべてのプロファイルが使用される
ドメイン	ドメイン・プロフィール
プライベート	プライベートプロフィール
パブリック	公開プロフィール
インターフェイスを指定する。	無効の場合、すべてのインターフェイスが使用される
ローカルエリアネットワーク	ローカル・エリア・ネットワーク・インターフェース
リモートアクセス	リモート・アクセス・インターフェース
ワイヤレス	ワイヤレス・インターフェース

地元の校長	
承認されたローカルユーザーを追加する	このルールを使用するローカルユーザーのリストを追加できるようにする。
認定ユーザー	このルールの認可ローカルユーザのリスト。ユーザは、PC_NAMEUSERNAMEなどのSDDL (Security Description Definition language) 形式でなければならない。サービス名がこのルールを使用するように設定されている場合、このフィールドを埋めてはならない。

制限の設定

デバイスの機能

SDカードを許可する	SDカードの使用を許可する
カメラを許可する	カメラの使用を許可する
位置情報サービスを許可する	デバイスの位置情報サービスを許可する
アプリのサイドロードを許可する	提供元不明のアプリのインストールを許可する
開発者モードを許可する	開発者モードを許可する
携帯電話のデータローミングを許可する	携帯電話のデータローミングを許可する
コルタナを許可する	音声アシスタント「コルタナ」を許可する
位置情報の検索を許可する	位置情報を使った検索を許可する
マイクロソフト以外の電子メールアカウントの追加を許可する	ユーザーがMSA以外の電子メールアカウントを追加できるかどうかを指定します。
マイクロソフトアカウント接続を許可する	電子メールに関連しない接続認証およびサービスにMSAアカウントを使用することを許可するかどうかを指定します。

設定の同期を許可する	デバイス全体で設定の同期が可能
企業保護ドメイン名	企業ドメイン名を"; "で区切って指定する。
ユーザーがシステムの復元を無効にできるようにする	システムの復元を無効にします。 **警告だ！** この機能は、企業または組織が所有または提供するデバイス、またはユーザーが所有するデバイスで、デバイスが企業によって完全に管理されることをユーザーが許可している場合にのみ使用する必要があります。このポリシー設定を無効にすると、システムの復元はオフになり、システムの復元ウィザードにアクセスできなくなります。システムの復元を構成したり、システムの保護を通じて復元ポイントを作成したりするオプションも無効になります。
ユーザーの登録解除を許可する	ユーザーがデバイスからコーポレート部分を削除し、AppTec360 サーバーから切断できるようにします。この場合、デバイスを管理することができなくなります。 **警告だ！** この機能は、企業または組織が所有または提供するデバイス、またはユーザーが所有するデバイスで、デバイスが企業によって完全に管理されることをユーザーが許可している場合にのみ使用する必要があります。このポリシー設定を無効にすると、ユーザーは MDM 登録を削除できなくなります。 ユーザーがワークプレイスコントロールパネル経由でワークプレイスアカウントを削除できるかどうかを指定します。MDMサーバーは常にリモートでアカウントを削除できます。

ビットロッカー

ビットロッカーの設定

一般設定	
デバイスの暗号化を要求する	Windowsのエディションとシステム構成によっては、ユーザーにデバイスの暗号化を有効にするよう促す： - 他のプロバイダーからの暗号化が有効になっていないことを確認する。 - BitLocker Drive Encryptionをオフにしてから、BitLockerをオンに戻します。
暗号化方式	
オペレーティング・システム・ドライブの暗号化方法	
固定データ・ドライブの暗号化方式	
リムーバブル・データ・ドライブの暗号化方法	
サードパーティのディスク暗号化に関する警告を無効にする	デバイスで使用されているサードパーティのディスク暗号化サービスに関する警告プロンプトを無効にします。 Windows 10のバージョン1803から、この設定はAzure Active Directoryに参加しているデバイスでのみサポートされています。
管理者以外のユーザーがログインしている間、暗号化を実行することを許可する。	Azure Active Directoryに参加しているデバイスのみサポート

AppTec360 拡張機能	
サイレント暗号化	Require device encryption "を選択すると、AppTec360 Management Serviceはデバイスドライブの自動サイレント暗号化を実行します。
ユーザー認証情報の自動生成	暗号化されたOSドライブは、自動的に生成されたユーザー認証情報で保護されます。 TPMが利用可能な場合はTPM PIN、または6桁のテキストパスワード。 生成された認証情報は、指定されたデバイスに登録された電子メール・アドレスに送信される。 このオプションがオフの場合、サイレント暗号化にはTPMを使うしかない。 この場合、TPMを搭載していないデバイスでは、サイレント暗号化は失敗する。
固定ドライブの暗号化	利用可能な固定データドライブも暗号化され、OSドライブに保存されたキーを使用して「自動ロック解除」で保護されます。

OSドライブ設定		
起動時に追加認証を要求する	この設定では、BitLocker がコンピュータの起動時に毎回認証を必要とするかどうかを設定できます。 この設定はBitLockerのセットアップ時に適用されます。 この設定を有効にすると、ユーザは BitLocker セットアップ・ウィザードで高度なスタートアップ・オプションを構成できます。	
互換性のあるTPMなしでBitLockerをブロックする		
TPMのみ		
TPMとPIN		
TPMとキー		
TPM、キー、PIN	PIN と USB フラッシュドライブ (キー) の使用を要求する場合は、BitLocker Drive Encryption セットアップウィザードではなく、コマンドラインツール「manage-bde」を使用して BitLocker をセットアップする必要があります。	

最低暗証番号の長さが必要	
	最小文字数

プリブート・リカバリーのメッセージとURLを設定する	OSドライブがロックされているときに、ブート前のキーリカバリ画面に表示されるリカバリメッセージ全体を設定するか、既存のURLを置き換えます。

	注意：すべての文字や言語がプリブートでサポートされているわけではありません。使用する文字がプリブート回復画面に正しく表示されることをテストすることを強くお勧めします。
	プリブート・リカバリー・メッセージ・オプション
	カスタムリカバリーメッセージ
	カスタム・リカバリURL

OSドライブの回復オプション		この設定により、必要な認証情報がない場合に、BitLocker で保護されたオペレーティング・システム・ドライブを回復する方法を制御できます。 この設定はBitLockerのセットアップ時に適用されます。 デフォルトでは、証明書ベースのデータ回復エージェントが許可され、回復パスワードと回復キーを含む回復オプションはユーザーが指定でき、回復情報はAD DSにバックアップされない。
	ブロック証明書ベースのデータ復元エージェント	BitLocker で保護されたオペレーティング・システム・ドライブでデータ復元エージェントを使用できるかどうかを指定します。 データ復旧エージェントを使用する前に、グループ・ポリシー管理コンソールまたはローカル・グループ・ポリシー・エディタの公開鍵ポリシー項目から追加する必要があります。 データ復元エージェントの追加に関する詳細については、Microsoft TechNet の『BitLocker Drive Encryption Deployment Guide』を参照してください。
	BitLocker 復旧パスワード設定	
	BitLocker回復キーの設定	
	BitLockerリカバリ情報をActive Directoryドメインサービスに保存する	
	AD DS BitLockerリカバリストレージの構成	キーパッケージの保存は、物理的に破損したドライブからのデータ復旧をサポートする。
	リカバリーデータをAD DSに保存する必要がある	コンピュータがドメインに接続されていない限り、ユーザーがBitLockerを有効にできないようにする。

固定ドライブ設定	
固定ドライブの復元オプション	この設定により、必要な認証情報がない場合に BitLocker で保護された固定ドライブをどのように復元するかを制御できます。 この設定はBitLockerのセットアップ時に適用されます。 デフォルトでは、証明書ベースのデータ回復エージェントが許可され、回復パスワードと回復キーを含む回復オプションはユーザーが指定でき、回復情報はAD DSにバックアップされない。
ブロック証明書ベースのデータ復元エージェント	
BitLocker 復旧パスワード設定	
BitLocker回復キーの設定	
BitLockerリカバリ情報をActive Directoryドメインサービスに保存する	
AD DS BitLockerリカバリストレージの構成	キーパッケージの保存は、物理的に破損したドライブからのデータ復旧をサポートする。
リカバリーデータをAD DSに保存する必要がある	コンピュータがドメインに接続され、AD DSへのBitLockerリカバリ情報のバックアップが成功しない限り、ユーザがBitLockerを有効にできないようにする。 注：回復パスワードは自動的に生成されます。
保護されていない固定ドライブへの書き込みアクセスを拒否する	

リムーバブルドライブの設定	
保護されていないリムーバブルドライブへの書き込みアクセスを拒否する	Bitlockerで保護されていないリムーバブルデータドライブへの書き込みアクセスを拒否します。注意：グループポリシーで「リムーバブルディスク：グループポリシーで「書き込みアクセスの拒否」が有効になっている場合、このポリシー設定は無視されます。
別の組織で設定されたデバイスへの書き込みアクセスを拒否する	コンピュータの識別フィールドと一致する識別フィールドを持つドライブにのみ、書き込みアクセスが与えられます。これらのフィールドは、「組織に固有の識別子を提供する」グループポリシー設定によって定義されます。

ビットロッカーの状態

ここでは、BitLocker暗号化ドライブの現在の状態を見ることができます。

C [OS Drive]
暗号化ステータス
暗号化(%)
保護状況
暗号化方式
キープロテクター
回復パスワード

回復パスワードを回転させる」ボタンをクリックすると、BitLocker 回復パスワードを回転させることができます。

証明書管理

証明書リスト

表示されているデバイスにインストールされている証明書のリストです。

証明書の構成

ここでは、証明書とそのデバイスへのインストール方法を設定できます。

信頼できる証明書	
説明	証明書の内容
スコープ	証明書の展開範囲現在のユーザーとデバイス
証明書ストア	「信頼できない証明書」は、Windows 10のバージョン1803からのみ利用可能です。
証明書ファイル	PKCS#1ファイルのアップロード

身分証明書			
説明	証明書の内容		
スコープ	証明書の展開範囲現在のユーザーとデバイス		
キーロケーション	秘密鍵をインストールする鍵ストレージ・プロバイダ。		
		TPM。TPMが存在しない場合は失敗	
	TPM。TPMが存在しない場合は、ソフトウェアKSPにフォールバックする。		
	ソフトウェア・キー・ストレージ・プロバイダー	秘密鍵をエクスポート可能にする	
	ビジネス向け Windows Hello	容器名	Windows Hello for Business（旧称：Microsoft Passport for Work）のコンテナ名を指定します。
		PINプロンプトテキスト	証明書の登録時に Windows Hello for Business PIN プロンプトに表示するカスタム テキストを指定します。
資格	PKCS#12ファイルのアップロード		

SCEP

説明	SCEP サーバーの説明			
配備範囲	証明書の展開範囲現在のデバイスとユーザー			
SCEPサーバーのURL	SCEP を通じて証明書を発行する 1 つ以上のサーバ			
テーマ	X.500名の表現。例："C=US, O=Microsoft Corporation, CN=foo, 1.2.5.3=bar"			
主題の別名	タイプ	メールアドレス		
		DNS		
		ユーアールアイ		
		ユーザー・プリンシパル名 (UPN)		
CAフィンガープリント	認証局証明書の SHA1 フィンガープリント。E.g. 31:8F:1E:78:5C:D5:12:9F:7E:3B:AD:F3:1C:C0:19:03:96:43:A9:E5			
有効期間単位	日、月、年			
有効期間				
チャレンジ	自動登録のための事前共有シークレットとして使用されます。			
リトライ	サーバーが PENDING 応答を送信した場合に、デバイスが再試行する回数。デフォルト値は 5、最大値は 30。			
リトライ遅延	再試行までの待ち時間。デフォルト値は5で、最小値は1である。			
キーサイズ	キーサイズ (ビット			
ハッシュアルゴリズム	ハッシュアルゴリズム・ファミリー			
主な用途	Key usage extensionは、証明書に含まれる鍵の目的 (暗号化、署名など) を定義する。少なくとも「電子署名」または「鍵の暗号化」のいずれかを選択する必要がある。			
拡張キーの使用	SCEP サーバー構成に従う。対応する OID のリストを指定する。例：1.3.6.1.5.5.7.3.2 (Client Authentication)			

キーロケーション	秘密鍵をインストールする鍵ストレージ・プロバイダ。		
		TPM。TPMが存在しない場合は失敗	
	TPM。TPMが存在しない場合は、ソフトウェアKSPにフォールバックする。		
	ソフトウェア・キー・ストレージ・プロバイダー		
	ビジネス向け Windows Hello	容器名	Windows Hello for Business (旧称：Microsoft Passport for Work) のコンテナ名を指定します。
		PINプロンプトテキスト	証明書の登録時に Windows Hello for Business PIN プロンプトに表示するカスタム テキストを指定します。

コネクション管理

無線LAN

この設定では、内部アクセス・ポイントにアクセスするためのエンドユーザー・デバイスの事前設定を行います。

サービスセット識別子（SSID）	接続先のネットワークのSSID
オートジョイン	ネットワークへの自動参加を有効にする
隠しネットワーク	APがSSIDをブロードキャストしない場合は、アクティブにする。

セキュリティ・タイプ

APセキュリティ・タイプを確立する

WEPオープンシステム	
パスワード	APのパスワード

WPA PSK	
パスワード	APのパスワード

WPA EAP	
認証タイプ	認証タイプ。"PEAP-MSCAHPv2 "でのみ可能。
高速再接続	デバイスは、アクセス・ポイント間を切り替えることができ、再度認証する必要はありません。
ゲストアクセス	ユーザーはアカウントを持っていないため、ゲストとして登録する必要があります。
検疫チェック	クライアントはNAP（ネットワーク・アクセス保護）チェックを行い、その結果をシステムと共有しなければならない。
暗号バインディングを要求する	認証は暗号バインディングによってのみ可能である。
サーバー検証	クライアントは、サーバ証明書が有効かどうかをチェックする。有効であれば、接続が確立される。
証明書の発行を促す	ユーザが信頼できない証明書を受け入れることを許可する。
サーバー名	ネットワーク認証と認可を提供するRADIUSサーバーの名前を表示するオプションを提供します。

WPA2-PSK	
パスワード	APパスワード

WPA2 EAP	
認証タイプ	認証タイプ。"PEAP-MSCAHPv2 "でのみ可能。
高速再接続	
ゲストアクセス	
検疫チェック	ネットワークアクセス保護 NAP を有効にする
暗号バインディングを要求する	認証は暗号バインディングによってのみ可能である。
サーバー検証	
証明書の発行を促す	検証済みのサーバー証明書、名前、またはルート証明書認証（CA）の入力を求めるプロンプトが表示されます。
サーバー名	デバイスが信頼すべきサーバーのリスト
なし	セキュリティが確立されていない
プロキシサーバーの使用	プロキシサーバーの使用
サーバーアドレス	プロキシサーバーのアドレス
サーバーポート	プロキシサーバーのサーバーポート

プロキシサーバーの使用

プロキシサーバーの使用を有効にする。

サーバーアドレス	このネットワークで使用されているプロキシサーバーのアドレス。
サーバーポート	このネットワークで使用されているプロキシサーバーのポート。

Wifiの制限

ここで様々なWifi制限を定義することができます。

WiFiを許可する	WiFiの許可/拒否
インターネット共有を許可する	ホットスポットの使用を許可する
WiFiセンス・ホットスポットへの自動接続を許可する	WiFiセンス・ホットスポットへの自動接続を許可する
WiFiの手動設定を許可する	AppTecによって定義されていないWiFiネットワークへの接続を許可する。
WLANスキャン周波数	WLAN スキャン間隔を設定します。値が大きいほど、WIFIネットワークを認識する能力が高くなります。

かそうへいいきもう

VPN接続を設定するために、ここで適切な設定を行います。

接続名	表示された接続名		
VPNタイプ	アプリごとのVPN接続は、特定のアプリのトラフィックを保護するために使用されます。		
	かそうへいいきもう	常にオン	これにより、サインイン時に自動的にVPNが接続され、ユーザーが手動で切断するまで接続が維持される。
	アプリごとのVPN	VPNアプリ	このVPN接続を使用するアプリを定義する
		アプリごとのロックダウン	アプリごとのロックダウンは、選択したアプリがこのVPN接続経由でのみ接続できるようにします。 この機能はWindows Defender Firewallに依存します。
	WIPプロフィール	この接続のWIPドメイン	エンタープライズID。このVPNプロファイルをWindows情報保護（WIP）ポリシーと接続するために必要です。

接続タイプ

AppTec360 VPN	
AppTec360 VPN」では、アプリのサイドローディングを許可する必要があります。セキュリティ管理」→「制限設定」→「端末機能」の「アプリのサイドロードを許可」を有効にしてください。	
ゲートウェイの設定	VPN接続にブラックリストを設定するには、DNSサーバーを指定したVPN設定を選択してください。VPN設定は、「一般設定」→「ユニバーサルゲートウェイ」→「VPN設定」で設定できます。

アイケイビーツー		
サーバー	VPNサーバー一覧	
デバイス・トンネル	ユーザーのログオン前に接続を有効にする。	
認証方法	イーエーピー	EAP XML
	機械証明書	
暗号化アルゴリズム		
完全性チェック・アルゴリズム		
ディフィー・ヘルマン群		
暗号変換アルゴリズム		
認証変換アルゴリズム		
完全前方秘匿（PFS）グループ		

PPTP		
サーバー	VPNサーバー一覧	
認証方法	イーエーピー	EAP XML

L2TP		
サーバー	VPNサーバー一覧	
認証方法	イーエーピー	EAP XML
暗号化アルゴリズム		
完全性チェック・アルゴリズム		
ディフィー・ヘルマン群		
暗号変換アルゴリズム		
認証変換アルゴリズム		
完全前方秘匿（PFS）グループ		

自動		
サーバー	VPNサーバー一覧	
認証方法	イーエーピー	EAP XML

一般的なVPN構成

ログオンのたびに認証情報を記憶	
内部DNSにIPアドレスを登録する	
ネットワーク・トラフィック・フィルタリング・ルール	VPN接続を定義されたルールセットに制限する。
DNSサフィックス検索リスト	短い名前をルーティングするためのDNS検索リストに追加するDNSサフィックス。
名前解決ポリシーテーブル（NRPT）ルール	名前解決ポリシーテーブル(NRPT)のルールは、VPN接続時にDNSがどのように名前を解決するかを定義します。
信頼できるネットワーク検出	信頼できるネットワークを識別するためのDNSサフィックスのリスト。
スプリット・トンネリング	スプリット・トンネリングとは、トラフィックがネットワーク・スタックによって決定された任意のインターフェイスを通過できることを意味する。
トンネリングルートの分割	VPNインターフェースのルーティングテーブルに追加するルートのリスト。
プロキシの設定	このネットワークで使用するプロキシを設定します。
代理アドレス	完全修飾ホスト名またはIPアドレスとしてのプロキシサーバーアドレス。
ポート	プロキシサーバーのポート。
プロキシ自動設定URL	URLからプロキシ設定を自動的に取得する。

VPNの制限

ここでは、様々なVPN制限を定義することができます。

VPN設定を許可する	このガイドラインは、ユーザーがVPN設定を解除したり変更したりすることを許可/禁止するものです。
セルラー経由のVPNを許可する	デバイスがモバイルデータを使用している場合、VPN接続の確立を許可/禁止する。
携帯電話でのVPNローミングを許可する	デバイスがローミング中の場合、VPN接続の確立を許可/禁止する。

ブルートゥース

ブルートゥースを許可するか禁止するかを設定します。

ブルートゥースを許可する	ブルートゥースの有効化/無効化

PIM管理

Exchangeアクティブ同期

エンドユーザーデバイスのActiveSyncアカウントのセットアップ

口座名	メールアカウント名
サーバーホスト名	サーバーアドレス/FQDN
ドメイン名	サーバードメイン
メールアドレス	メールアドレス
ユーザー名	ユーザー名
ユーザーパスワード	オプションとして、ここでユーザーにパスワードを添付することもできます。
SSLの使用	SSL接続を使用する
同期間隔	ここで同期間隔を設定することができる 手動同期 = ユーザーは電子メールをダウンロードし、手動で同期を実行する必要があります。
メール年齢フィルター	メールが同期されるまでの時間 フィルターなし = 無制限
ログレベル	ActiveSyncトラフィックのロギング・レベルの設定
メールの同期	有効 = メールが同期される
連絡先の同期	アクティブ = 連絡先が同期される
カレンダーの同期	アクティブ化 = カレンダーが同期されている
タスクの同期	アクティブ化 = タスクが同期化される

電子メール

エンドユーザーデバイス上のPOP3/IMAP4アカウントの確立。

口座詳細	メールアカウント名
送信者名	表示される送信者名
ドメイン名	メールアカウントのドメイン名
メールアドレス	ユーザーメールアドレス
ユーザー名	ユーザー名
ユーザーパスワード	オプションとして、ここでユーザーにパスワードを添付することもできます。
代替送信サーバー認証情報	送信サーバーに他の認証情報が必要な場合は、ここで定義することができる。
送信ドメイン名	送信ドメイン名
送信サーバーユーザー名	送信サーバーのユーザー名
送信サーバーパスワード	送信サーバーのパスワード
電子メールプロトコル	POP3またはIMAP4をプロトコルとして使用可能
受信メールサーバーホスト名	受信メールサーバーホスト名
受信メールにSSLを使用する	受信メールにSSLを使用する
送信メールサーバーホスト名	送信メールサーバーホスト名
送信メールにSSLを使用する	送信メールにSSLを使用する
送信サーバー認証	発信サーバー認証が必要
同期間隔	ここで同期間隔を設定することができる 手動同期 = ユーザーは電子メールをダウンロードし、手動で同期を実行する必要があります。
メール年齢フィルター	メールが同期されるまでの時間 フィルターなし = 無制限

アプリ管理

エンタープライズアプリマネージャー

インストール済みアプリ

表示されているデバイスに現在インストールされているアプリのリストです。

必須アプリ

ここでは、デバイスに必須のアプリのリストを設定できます。

このリストは、デバイスがMDMに接続するたびにチェックされ、アプリがアンインストールされたか、以前にインストールされたことがないかにかかわらず、デバイスにインストールされていないアプリをすべてインストールします。

Windows 10の社内アプリをアップロードしてこのリストに追加するか、「一般設定」→「アプリ管理」→「Microsoft Office」で事前に設定が必要なMicrosoft Officeの設定を追加することができる。

シスアプリの制限

受信トレイアプリ
アラームと時計を許可する
電卓を許可する
カメラを許可する
コンタクトサポートを許可する
コルタナを許可する
ファイルエクスプローラーを許可する
開始を許可する
グルーヴ音楽を許可する
地図を許可する
メッセージングを許可する
マイクロソフト・エッジを許可する
映画とテレビを許可する
お金を許す
ニュース
OneDriveを許可する
OneNoteを許可する
Outlookのカレンダーとメールを許可する
人々を許可する
電話を許可する
写真を許可する
パワーポイントを許可する
設定を許可する
スカイプを許可する
スポーツ
ストア
ボイスレコーダーを許可する
ウォレットを許可する
天気予報

ウィンドウズ・フィードバック・ハブを許可する
ワードを許可する
Xboxを許可する

設定ページ
アカウントを許可 職場
高度な情報を許可する
アプリコーナーを許可する
ブロックとフィルタを許可する
カラープロファイルを許可する
走行モードの許可
電子メールとアカウントの許可
イコライザーを許可する
キーボードを許可する
ナビゲーションバーを許可する
ネットワークの機内モードを許可する
ネットワークのインターネット共有を許可する
ネットワークサービスを許可する
ネットワークWi-Fiを許可する
PCシステムのブルートゥースを許可する
デバイスの評価を許可する
復元アップデートを許可する
共有を許可する
スタートを許可する
時間言語
許可時間 地域
Windowsデフォルトのロック画面を許可する
仕事または学校のアカウントを許可する

ブラックリストとホワイトリスト

Black- & Whitelisting "では、"Whitelist "モードと "Blacklist "モードを選択できます。

ホワイトリスト	エンドユーザーデバイスにインストールできるのは、リストに追加されたアプリとサービスのみです。エンドユーザーデバイスにすでにプリインストールされている場合は、アクティベートされ、ユーザーが実行できるように設定されます。
	リストに追加されていないその他のアプリは、エンドユーザーデバイスにインストールできません。エンドユーザーデバイスにすでにプリインストールされている場合は、無効化され、ユーザーが実行できないように設定されます。
ブラックリスト	リストに追加されたアプリやサービスは、エンドユーザーデバイスにインストールできません。エンドユーザーデバイスにすでにプリインストールされている場合は、無効化され、ユーザーが実行できないように設定されます。
	リストに追加されていない他のすべてのアプリは、エンドユーザーデバイスにインストールすることができます。エンドユーザーデバイスにすでにプリインストールされている場合は、アクティベートされ、ユーザーが実行できるように設定されます。

を介して、現在使用中のリストにアプリやサービスを追加します。

を介して、現在アクティブでないリストにアプリやサービスを追加します。

Windows App Store」からアプリを追加するか、「アプリ識別子」を直接入力してブラックリストまたはホワイトリストに追加することができます。

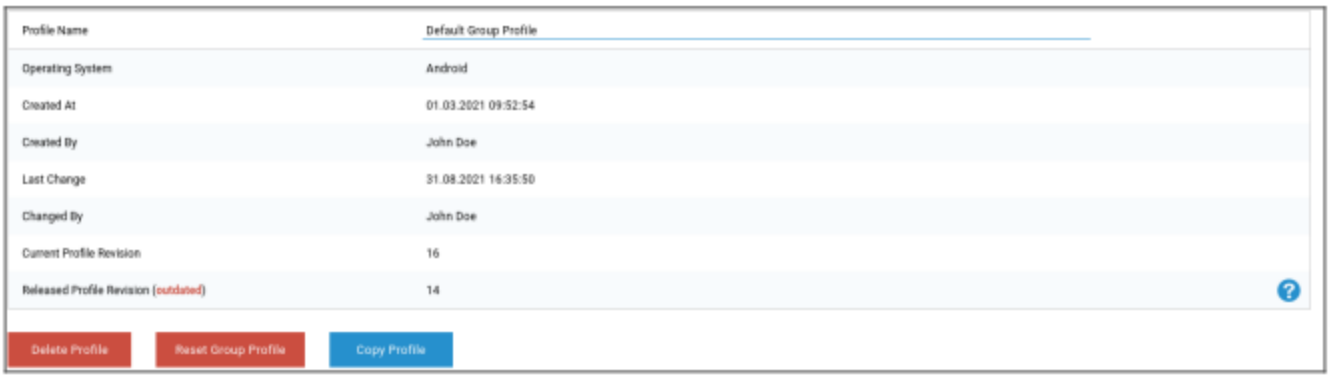
MacOSの設定

プロファイルとデバイスのどちらを選択したかによって、表示とそのサブポイントが異なります！

一般

グループプロフィールの概要（グループレベルのみ）

グループプロフィールを開くと、プロフィールの概要が表示されます。



プロフィール名	プロフィールの名前（ここで変更可能）
オペレーティングシステム	対象OS
作成日時	創造の時
作成者	プロフィールの作成者
最後の変更	プロフィールの最終変更時刻
変更履歴	最後の変更を行ったアカウント
現在のプロフィール改訂	保存されたプロファイル状態の修正
プロフィール改訂版をリリース	割り当てられたプロファイルのリビジョン（"Assign now"）。ラベルのテキストの後ろに"(outdated) "と表示されている場合は、プロファイルを保存したものの、まだ割り当てていないことを意味します。

デバイスの概要（デバイスレベルのみ）

デバイスの概要

デバイス名	デバイス名
モデル	モデル
オペレーティングシステム	オペレーティングシステム
シリアル番号	装置のシリアル番号
デバイスの所有権	設定されたオーナーシップ・タイプ
デバイス・タイプ	デバイスのタイプ
準拠	デバイスが準拠しているかどうかを示す
IPアドレス	サーバーに接続したデバイスのIPアドレス
ラストシーン	デバイスからの最終接続時間
ラスト・プッシュ	デバイスに最後にプッシュされた時間
割り当て	ここでは、デバイスを別のユーザーまたはグループに移動できます。

コンフィグ改訂（デバイスレベルのみ）

ここで、どのグループプロファイルがデバイスに割り当てられているかの概要が表示されます。

グループプロフィールをクリックすると、そのプロフィールに直接アクセスし、設定を行うことができます。

このマークがあれば、割り当てられたアプリをグループプロファイルの設定に戻すことができます。

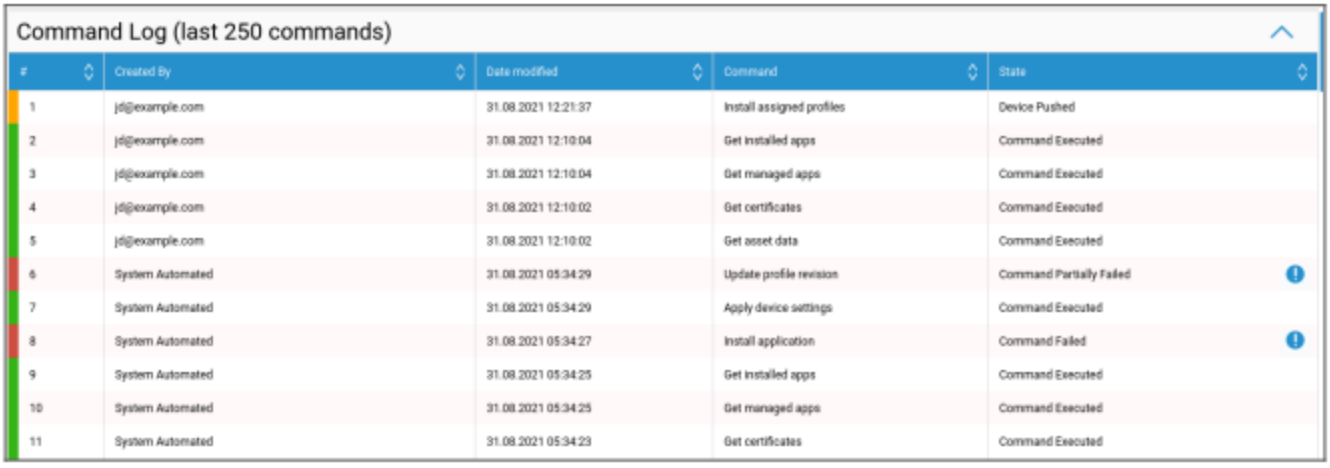
この記号を使えば、デバイスのプロファイルをリセットして、設定を一切なしにすることができる。

"Newer Revision available "は、グループプロファイルが変更され保存されたが、割り当てられていないことを示します。グループプロファイルの変更をデバイスに適用するには、グループレベルで "Assign now "を使用してグループプロファイルを割り当てる必要があります。

デバイスログ（デバイスレベルのみ）

コマンドログ

ここでは、デバイスに対して発行されたコマンドとそのステータスを確認することができます。



System Automated」によって作成されたコマンドは、システムによって自動的に作成される。

可能なコマンドステータス

デバイスが押される	プッシュリクエストは、EMM サーバーに接続するようデバイスに指示するため、プッシュサービス (APNS など) に送信されました。
コマンド作成	コマンドがシステム内に作成された。
コマンド送信	コマンドは、サーバーに接続された後、デバイスに送信された。
コマンド実行	コマンドは正常に実行された。
コマンド失敗	コマンドが失敗しました。*
コマンド一部失敗	デバイスのOSによっては、いくつかのコマンドがグループ化されることがある。 このコマンドグループの一部は失敗した。*
コマンドは実行されたが、最終的に失敗	コマンドは実行されたが、もしかしたら実行されていなかったかもしれない。
コマンド・リパッシュ	コマンドはユーザーによってリプッシュされた。
廃棄	コマンドが破棄された。例えば、他のコマンドに取って代わられたとか、デバイスが再登録されて古いコマンドが削除されたとか。

*メッセージの後ろにエクスクラメーションマークが表示されている場合は、カーソルをアイコンの上に置くと詳細な情報を得ることができます。

資産管理 (デバイスレベルのみ)

デバイス情報

モデル番号	モデル番号
ホスト名	ホスト名
ローカルホスト名	ローカルホスト名
オペレーティングシステム	オペレーティングシステム
OSバージョン	OSバージョン
ユーディーアイディー	ユーディーアイディー
フリー/トータルメモリー	フリー/トータルメモリー

WiFi

IPアドレス	IPアドレス
WiFi MAC	WiFi MAC

セルラー

電話番号	電話番号
ローミング状況	ローミング状況
ローミング (音声/データ)	ローミング (音声/データ)
IPアドレス	IPアドレス
オペレーター/キャリア	オペレーター/キャリア
SIMキャリアネットワーク	キャリアネットワーク
キャリア版	キャリア版
国際ID	国際ID
現在のMCC/MNC	現在のMCC/MNC
SIM MCC/MNC	SIM MCC/MNC

ブルートゥース

ブルートゥースMAC	ブルートゥースMAC

アップデート管理 (デバイスレベルのみ)

更新情報

このタブには、デバイスのシステム・アップデート設定に関する情報が表示されます。

オートチェック有効	システムが自動的にアップデートをチェックしている場合。
アプリの自動アップデートが有効	システムが自動的にアプリのアップデートをインストールする場合。
OSの自動アップデートが有効	システムが自動的にOSアップデートをインストールする場合。
自動セキュリティ・アップデートが有効	システムが自動的にセキュリティアップデートをインストールする場合。
アプリ更新のバックグラウンドダウンロードが可能に	システムがバックグラウンドでアプリのアップデートをダウンロードする場合。
カタログURL	クライアントが使用しているソフトウェア・アップデート・カタログのURL。
デフォルト・カタログ	yes」の場合、Catalogがデフォルトのカタログとなる。
定期点検の実施	はい」の場合、新しいスキャンを開始する。
前回のスキャン日	最後のソフトウェア更新スキャンの日付。
前回の検査結果	前回のソフトウェア・アップデート・スキャンの結果コード。

セキュリティ管理

盗難防止

ワイプ＆ロック

フルワイプ	デバイスを工場出荷状態にリセットするコマンドを送信する
エンタープライズ・ワイプ	デバイスからMDMを削除し、すべてのMDMデータ（アカウント、アプリなど）を削除する。
ロック画面	デバイスをロック画面に戻す

セキュリティ設定

パスコード

コードの無効化が許可される	ユーザーにPINを設定させるかどうかを決定する。この値を設定するだけで、(他の値ではなく)長さや品質を指定することなく、ユーザーにパスコードの入力を強制します。
シンプルな値	ユーザーが同じ、エスカレーション、縮小番号文字列（例：1234、1111）を使用できるようにする。
英数字が必要	パスワードには少なくとも1文字が含まれていなければならない
最小パスコード長	パスワードの最小長
複雑な文字の最小数	パスワードに含まれる英数字記号の最小数
最大パスコード年齢	パスワードを変更しなければならない日数
最大オートロック	デバイスがロックされる最大時間
デバイス・ロックの最大猶予期間	ロック解除時にパスコードの入力を求めずにデバイスをロックできる時間
最大パスコード日数（1～730日、またはなし）	パスコードを変更しなければならない日数
パスコード履歴（1～50個、またはなし）	再利用前のユニークなパスコード数

証明書

PKCS#1	
説明	証明書の説明を入力する
資格	pkcs1ファイルのアップロード

PKCS#12	
説明	証明書の説明を入力する
資格	pkcs12 ファイルのアップロード

制限の設定

デバイスの機能

カメラを許可する	カメラの使用を許可する
ゲームセンターを許可する	Falseの場合、Game Centerは無効になり、ホーム画面からアイコンが削除されます。
マルチプレイヤーゲームの許可	偽の場合、マルチプレイヤーゲームを禁止する。
Game Centerフレンドの追加を許可する	Falseの場合、Game Centerへのフレンド追加を禁止します。
iCloudフォトライブラリを許可する	falseに設定すると、iCloud Photo Libraryが無効になります。iCloudフォトライブラリからデバイスへのダウンロードが完了していない写真は、ローカルストレージから削除されます。
Touch IDを許可する	Falseの場合、Touch IDによるデバイスのロック解除を防ぎます。

iCloud

iCloudペアリング中に特定の機能をブロックする

ドキュメントの同期を許可する	ドキュメントの同期を許可する
iCloudキーチェーンの同期を許可する	iCloudキーチェーンの同期を許可する
iCloudメモを許可する	偽の場合、MacOSのiCloud Notesサービスを無効にします。
iCloud BTMMを許可する	Falseの場合、MacOSのBack to My Mac iCloudサービスを無効にします。
iCloud FMMを許可する	Falseの場合、MacOSの「Macを探す」iCloudサービスを無効にします。
iCloudブックマークを許可する	Falseの場合、MacOSのiCloudブックマーク同期を無効にします。
iCloudメールを許可する	Falseの場合、MacOS MailのiCloudサービスを無効にします。
iCloudカレンダーを許可する	Falseの場合、MacOS CloudのiCloudサービスを無効にします。
iCloudリマインダーを許可する	Falseの場合、iCloudリマインダーサービスを無効にします。
iCloudアドレス帳を許可する	Falseの場合、MacOSのiCloudアドレス帳サービスを無効にします。

メディア・マネジメント

ログアウト時のイジェクト	ログアウト時にすべてのリムーバブルメディアを取り出す
ネットワークを許可する	ネットワークメディアへのアクセスを許可する
内蔵ディスクを許可する	内蔵ディスクのアクセスを許可する。
認証が必要	このメディアの使用には認証が必要
読み取り専用	ユーザーはメディアからデータを読み取ることしかできません。
外付けディスクを許可する	外付けディスクのアクセスを許可する。
認証が必要	このメディアの使用には認証が必要
読み取り専用	ユーザーはメディアからデータを読み取ることしかできません。
ディスクイメージの使用を許可する	画像へのアクセスを許可する。
認証が必要	このメディアの使用には認証が必要
読み取り専用	ユーザーはメディアからデータを読み取ることしかできません。
DVD-RAMの使用を許可する	DVD-RAMディスクのアクセスを許可する。
認証が必要	このメディアの使用には認証が必要
読み取り専用	ユーザーはメディアからデータを読み取ることしかできません。
DVDの使用を許可する	DVDディスクのアクセスを許可する。
認証が必要	このメディアの使用には認証が必要
CDの使用を許可する	CDディスクのアクセスを許可する。
認証が必要	このメディアの使用には認証が必要

コネクション管理

Wi-Fi

ここでWi-Fi接続の追加と設定ができます。

サービスセット識別子（SSID）	接続先のネットワークのSSID
オートジョイン	ネットワークの自動参加を有効にする
隠しネットワーク	AP が SSID をブロードキャストしない場合に有効にする。
プロキシの設定	アクセスポイントごとのプロキシ設定
なし	プロキシサーバーを使用しない
マニュアル	手動プロキシの確立
プロキシサーバーURL	プロキシ設定にアクセスするためのアドレス
ポート	プロキシのポートを設定する
認証	プロキシで認証するためのユーザ名
パスワード	プロキシ認証用パスワード
自動	自動的にプロキシを確立する
プロキシサーバーURL	プロキシ設定ファイルのURL
セキュリティ・タイプ	APのセキュリティ・タイプを確立する
ウェップ	
パスワード	APのパスワード
WPA/WPA2	
パスワード	APのパスワード
WEPエンタープライズ WPA2エンタープライズ あらゆる企業	表 エラーを参照：以下の参照ソースが見つかりません
なし	セキュリティを確立しない
MACアドレスのランダム化を無効にする	ネットワークに接続している間、そのWi-FiネットワークのMACアドレスのランダム化を無効にします。また、プライバシー保護の警告が表示されます。

エンタープライズWi-Fiの設定

注："Security Type "がEnterprise Typeに設定されている場合のみ利用可能。

プロトコル	ターゲット・ネットワークでサポートされている認証プロトコル
TLS	使用の有効化 / 無効化
TTLS	使用の有効化 / 無効化
内部認証	使用する認証プロトコルPAP、CHAP、MSCHAP、MSCHAPv2
リープ	使用の有効化 / 無効化
ピーエーピー	使用の有効化 / 無効化
EAP-FAST	使用の有効化 / 無効化
EAP-SIM	使用の有効化 / 無効化
PAC使用	PAC（保護されたアクセス制御）の使用
提供PAC	提供PACの構成
匿名でのPAC提供	PACの匿名提供
認証	
ユーザー名	認証ユーザー名
使用しない 接続ごと パスワード	接続ごとのパスワードを使用しない
パスワード	使用するパスワード
身分証明書	認証証明書のアップロード/選択
アウター・アイデンティティー	外から見えるアイデンティティ
信頼	
信頼できる証明書 1	最初の信頼できる証明書をアップロードする
信頼できる証明書 2	2つ目の信頼できる証明書をアップロードする
信頼できる証明書 3	信頼できる第3の証明書をアップロードする
信頼できるサーバー 証明書の名称	想定されるサーバー証明書の名前 (カンマ区切りリスト)

かそうへいいきもう

選択した接続タイプによって、表示されるフィールドが異なります。

接続名	VPNプロファイル名
VPNタイプ	
かそうへいいきもう	デバイスのネットワーク・トラフィックはすべて、VPN接続を介してルーティングされる。
接続タイプ	VPN接続タイプを確立する
IPsec（シスコ）	シスコのIPsecプロトコル
L2TP	L2TPプロトコル
カスタムSSL	カスタムSSLによる接続
アイケイビーツー	IKEv2プロトコル
プロキシの設定	VPN接続用プロキシの設定
なし	代理人を立てない
マニュアル	手動でプロキシを確立する
プロキシサーバーURL	プロキシ設定へのアクセス用アドレス
ポート	プロキシのポートを設定する
認証	プロキシで認証するためのユーザ名
パスワード	プロキシ認証用パスワード
自動	自動的にプロキシを確立する
プロキシサーバーURL	プロキシ設定にアクセスするためのURL

HTTPプロキシ

プロキシ・タイプ	
マニュアル	手動でプロキシを確立する
プロキシサーバーURL	プロキシ設定にアクセスするためのアドレス
ポート	プロキシポートの確立
認証	プロキシで認証するためのユーザ名
パスワード	プロキシ認証用パスワード
自動	自動的にプロキシを確立する
プロキシPAC URL	プロキシPAC URL
PACにアクセスできない場合、直接接続を許可する。	PACに到達できない場合、（VPNを介さずに）直接接続を許可する。
プロキシをバイパスしてキャプティブ・ネットワークにアクセスできるようにする。	プロキシをバイパスしてキャプティブな内部ネットワークにアクセスできるようにする。

エアプリント

IPアドレス	プリンタIPアドレス
リソースパス	AirPrintデバイスへの明確なパス

エアプレイ

デバイス名	デバイス名
パスワード	ペアリング・パスワード
ホワイトリスト	デバイスが排他的にペアリングできるデバイスのリストを定義します。

PIM管理

Exchangeアクティブ同期

口座名	口座名
電子メールアドレス	口座の住所 (例：max@company.com)
サーバーホスト名	内部ホスト名
ログイン名	デバイスがユーザーの入力を求めるには、"Domain "と "Login Name "は空白でなければなりません。
ドメイン	デバイスがユーザーの入力を求めるには、"Domain "と "Login Name "は空白でなければなりません。 ACL Gateway Configurationが有効で、Domainフィールドが空でない場合、AppTec360 Universal Gatewayは以下の名前 "DomainLogin Name "でデバイスを認証する。
パスワード	アカウントのパスワード (例：secretUserPassword)
過去の同期メール	同期するメールの過去日数
SSLの使用	内部 Exchange ホストに SSL を使用する
アドバンスオプション	詳細オプションを表示
サーバーポート	内部ポート
サーバーパス	内部経路
外部ホスト名	外部ホスト
外部ポート	外部ポート
外部経路	外部経路
SSLを外部に使用する交換ホスト	外部 Exchange ホストに SSL を使用する

電子メール

エンドユーザーデバイスへのPOP3/IMAPアカウントのセットアップ

口座詳細	電子メールアカウント名
口座種別	
アイマップ	
パスのプレフィックス	特殊フォルダのパスプレフィックス
ポップ	
ユーザー表示名	ユーザー表示名
メールアドレス	ユーザーメールアドレス

受信メール	受信サーバーの設定
メールサーバーアドレス	メールサーバーアドレス
メールサーバーポート	メールサーバーポート
ユーザー名	それぞれのユーザー名
認証タイプ	認証タイプ
なし	認証タイプなし
パスワード (デバイスレベルのみ)	パスワードプロンプト
MDM チャレンジ・レスポンス	
エヌティーエルエム	NTLM認証
HTTP MD5 ダイジェスト	
SSLの使用	必要に応じてSSLを使用する

送信メール	送信サーバーの設定
メールサーバーアドレス	メールサーバーアドレス
メールサーバーポート	メールサーバーポート
ユーザー名	それぞれのユーザー名
認証タイプ	
なし	認証方法なし
パスワード (デバイスレベルのみ)	パスワードプロンプト
MDM チャレンジ・レスポンス	
エヌティーエルエム	NTLM認証
HTTP MD5 ダイジェスト	
SSLの使用	必要に応じてSSLを使用する
送信パスワードは受信パスワードと同じ	送信パスワードは受信パスワードと同じ
郵便でのみ使用	すべての送信メールをMail-App経由で送信する場合、有効にする。

カルダヴ

CalDavアカウントのセットアップと配布の設定

口座詳細	アカウントの表示名
ホスト名	ホスト名および/またはIPアドレス
ポート	CalDavアカウントのポート
主なURL	口座の主なURL
ユーザー名	それぞれのCalDavユーザー名
パスワード (デバイスレベルのみ)	それぞれのCalDavパスワード
SSLの使用	必要に応じてSSLを使用する

カードダヴ

CardDavアカウントのセットアップと配布の設定

口座詳細	アカウントの表示名
ホスト名	ホスト名および/またはIPアドレス
ポート	CardDavアカウントのポート
主なURL	口座の主なURL
ユーザー名	それぞれのCardDavユーザー名
パスワード (デバイスレベルのみ)	それぞれのCardDavパスワード
SSLの使用	必要に応じてSSLを使用する

ライトウェイトディレクトリアクセスプロトコル

このエリアでは、エンドユーザーデバイスとActive Directoryの間で動的な証明書交換を可能にするために、LDAP接続を設定します。

選択されたユーザーには、それぞれの読み取り権限が必要であることに注意してください。

口座詳細	口座詳細
アカウントユーザー名	LDAPアクセス用ユーザー
アカウントパスワード	LDAPアクセス用パスワード
アカウントホスト名	LDAPサーバーのホスト名/IPアドレス
SSLの使用	必要に応じてSSLを使用する

第2部では、LDAPレジストリを検索するための個々のフィルターを定義することができる。

説明	スコープ	検索ベース
フィルターの説明	LDAPレジストリの検索レベル	個々のフィルターを定義する

ダッシュボードとレポート

ダッシュボード設定

ここで既存のダッシュボードを確認したり、編集したり、新しいダッシュボードを作成することができます。各ダッシュボードには、表示するデータとグラフの設定があります。

ダッシュボード設定コントロール

パブリック	ダッシュボードの公開を設定し、他のユーザーがダッシュボードを見ることができるようにします。もちろん、ユーザーはログインしてダッシュボードを見ることができなければなりません。公開" が有効になっていない場合、作成者だけがダッシュボードを見ることができます。
デフォルト	ダッシュボードをデフォルトに設定し、次回ダッシュボードビューにアクセスしたときに自動的に開くようにします。
	ダッシュボードとグラフの表示
	ダッシュボードの削除
	ダッシュボード名と設定の編集
	ダッシュボードのコピーを作成する
	まったく新しいダッシュボードを追加

ダッシュボード・ビュー

選択したダッシュボードのデータとグラフが表示され、これらを変更することもできます。

ダッシュボード・コントロール

	ダッシュボードに表示するデータ、表示するデータ量、表示するデータのサイズを定義できます。
	ダッシュボードの概要に戻ります。
	現在開いているダッシュボードをデフォルトにリセットします。
	現在開いているダッシュボードに加えたすべての変更 (表示するデータなど) を保存します。
	チャートの種類をピラー・チャートに変更
	チャートの種類を円グラフに変更
	チャートの種類をドーナツ・チャートに変更
	チャートの種類を極域チャートに変更
	ソート順の変更

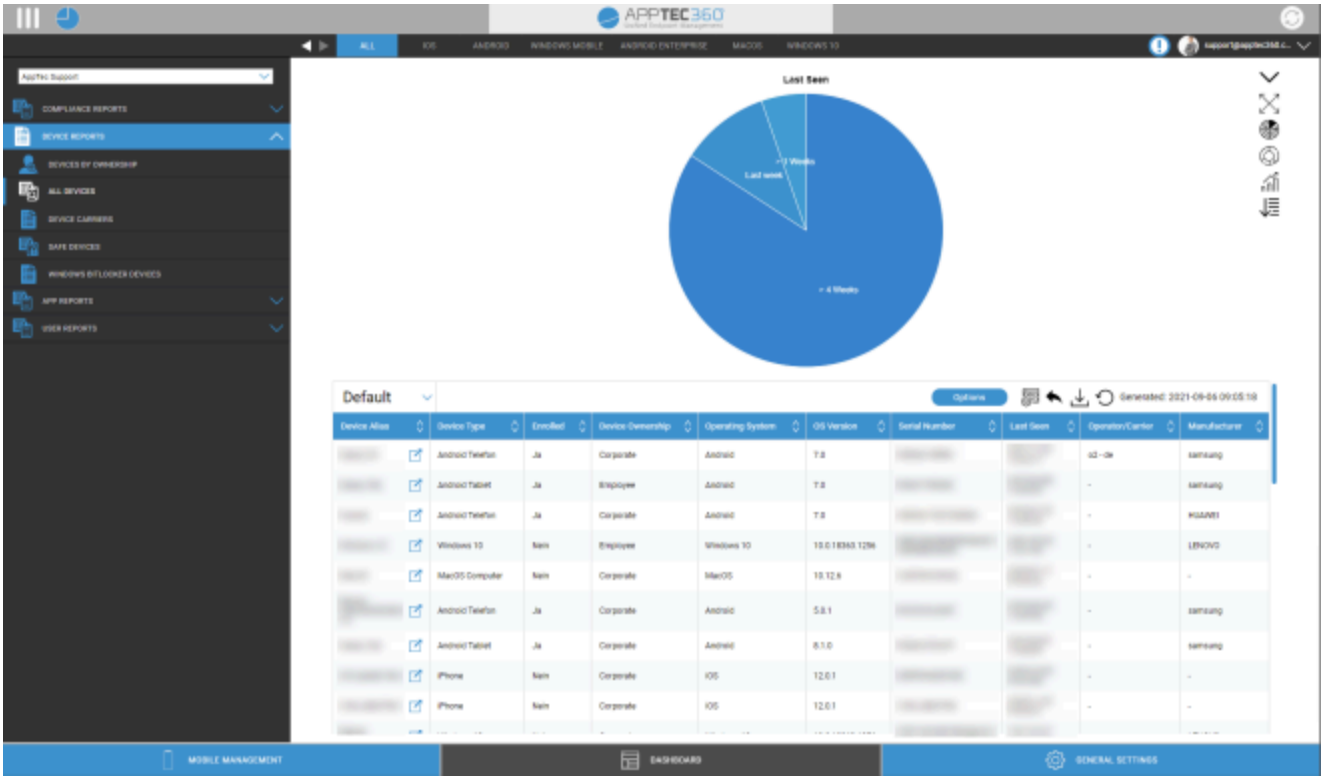
拡張レポート

拡張レポーティング」では、デバイスやユーザー情報の詳細な概要やグラフを見ることができます。

デフォルトのレポートがいくつかあるが、すべて手動で変更でき、表示するデータを追加したり削除したりできる。

どのデータを表示するかは手動でしか変更できないことに注意してください。選択されたレポートカテゴリは、これが基づいているデータを定義します。例：「デバイスレポート」の「すべてのデバイスiOS」のiOSレポートにAndroidデバイスが表示されることはありません。

左上では、レポートのデータを特定のグループ（およびそのすべてのサブグループ）に制限することができます。デフォルトでは、ルートノードに設定されているため、すべてのデバイスとユーザーを考慮に入れます。



拡張レポート・コントロール

各概要では、以下の機能を使ってレポートを自由に変更することができます：

	チャートを隠す（チャートが表示されている場合）
	チャートを表示する（チャートが非表示の場合）
	チャートの拡大（チャートが折りたたまれている場合）
	チャートの折りたたみ（チャートが展開されている場合）
	チャートの種類をピラー・チャートに変更
	チャートの種類を円グラフに変更
	チャートの種類をドーナツ・チャートに変更
	チャートの種類を極域チャートに変更
	ソート順の変更
	表示された概要について、以下の部分を修正する： • カラムの追加と削除 • 列の表示順を指定する。 • 表の上にチャートを表示する / 表示しない • チャートに使用する列を選択する • テーブルのデータにフィルタをかける
	セットアップ・マネージャーを開いて、さまざまなレポートを保存したり読み込んだりできる。
	現在開いているレポートをデフォルトにリセットする
	現在のレポートを.csvファイルとしてエクスポートする。
	データを再生成し、現在のレポートをリロードする

すべてのデフォルト・レポートのリストは次のページにあります。

コンプライアンス・レポート

根付きデバイス

root化/脱獄されたデバイスの概要。

このレポートのデフォルトの列：

デバイスエイリアス
デバイス所有者
Eメール
オペレーティングシステム
電話番号
ラストシーン
メーカー

ローミングデバイス

ローミング中の全デバイスの概要

このレポートのデフォルトの列：

デバイスエイリアス
デバイス所有者
Eメール
デバイス・タイプ
オペレーティングシステム
電話番号
ラストシーン

ローミング対応デバイス

ローミングを有効にしているが、必ずしも現在ローミング中でないすべてのデバイスの概要。

このレポートのデフォルトの列：

デバイスエイリアス
デバイス所有者
Eメール
デバイス・タイプ
オペレーティングシステム
電話番号
ラストシーン

監視対象機器

監視モードで監視されているすべてのデバイスの概要（iOSのみ）

このレポートのデフォルトの列：

デバイスエイリアス
デバイス所有者
Eメール
デバイス・タイプ
ラストシーン

非アクティブ・デバイス

過去7日間にサーバーに接続していないすべてのデバイスの概要

このレポートのデフォルトの列：

デバイスエイリアス
デバイス所有者
Eメール
デバイス・タイプ
オペレーティングシステム
ラストシーン

デバイスレポート

所有者別デバイス

ここでは、企業用デバイス (コーポレート・デバイス) と従業員用デバイス (プライベート・デバイス) として現在何台のデバイスが導入されているかを確認できます。

このレポートのデフォルトの列：

デバイスエイリアス
デバイス所有者
デバイス・タイプ
デバイスの所有権
オペレーティングシステム

すべてのデバイス

ここでは、すべてのデバイスの概要と最も重要な情報を見ることができます。

このレポートのデフォルトの列：

デバイスエイリアス
デバイス・タイプ
在籍
デバイスの所有権
オペレーティングシステム
OSバージョン
シリアル番号
ラストシーン
オペレーター/キャリア
メーカー

デバイス・キャリア

ここでは、キャリア (携帯電話会社) に関する概要を見ることができます。

このレポートのデフォルトの列：

デバイスエイリアス
デバイス所有者
Eメール
オペレーティングシステム
OSバージョン
オペレーター/キャリア

セーフデバイス

ここでは、SAFEバージョンを使用しているデバイスの概要を見ることができます。

概要および/またはSAFEはサムスンのデバイスでのみ利用可能なため、このポイントの下に通常のタブは表示されません。

このレポートのデフォルトの列：

デバイスエイリアス
デバイス所有者
Eメール
デバイス・タイプ
ラストシーン
セーフ・バージョン

Windows BitLockerデバイス

ここでは、BitLockerを使用するWindowsデバイスの概要を見ることができます。

このレポートのデフォルトの列：

デバイスエイリアス
デバイス所有者
Eメール

ビットロッカーの状態

アプリ報告

ここではアプリに関する様々な概要が得られる。これらのレポートすべてにおいて、エントリーをクリックすることで、デバイスにインストールされているバージョンとその頻度を確認することができます。このビューでは、特定のバージョンをもう一度クリックして、どのデバイスにその特定のバージョンがインストールされているかを確認することができます。

注意：システムがデバイスから最新の情報を取得するまで、時間がかかる場合があります。また、レポートは毎分更新されるわけではありません。新しいアプリやバージョンを割り当てたばかりの場合、現在のステータスを確認するには辛抱強く待つ必要があるかもしれません。レポートを手動で再読み込みすると、最新のデータが表示されます。

インストール済みアプリ

ここにインストールされているすべてのアプリの概要が表示されます。

このレポートのデフォルトの列：

名称	それぞれのアプリやサービスの名前
識別子	明確なアプリ/サービスID
総カウント数	このアプリ / サービスがエンドユーザーのデバイスにインストールされた頻度

最もインストールされているアプリ

ここでは、最も多くインストールされているアプリの概要がわかります。

このレポートのデフォルトの列：

名称	それぞれのアプリやサービスの名前
識別子	明確なアプリ/サービスID
総カウント数	このアプリ / サービスがエンドユーザーのデバイスにインストールされた頻度

必須アプリ

ここでは、必須 (義務化された必須) アプリの概要を説明する。

このレポートのデフォルトの列：

名称	それぞれのアプリやサービスの名前
識別子	明確なアプリ/サービスID
アプリ提供元	どのAppStoreが関係しているか： • Google PlayStore (アンドロイド) • iTunes AppStore (iOS)
OS	オペレーティングシステム

ブラックリスト入りアプリ

ここでは、定義されたすべてのブラックリスト入りアプリの概要が表示されます。

このレポートのデフォルトの列：

名称	それぞれのアプリやサービスの名前
識別子	明確なアプリ/サービスID
アプリ提供元	どのAppStoreが関係しているか： • Google PlayStore (アンドロイド) • iTunes AppStore (iOS)
OS	オペレーティングシステム

ユーザーレポート

料金表

ここでは、ユーザーの電話料金とSIMカードの概要がわかります。

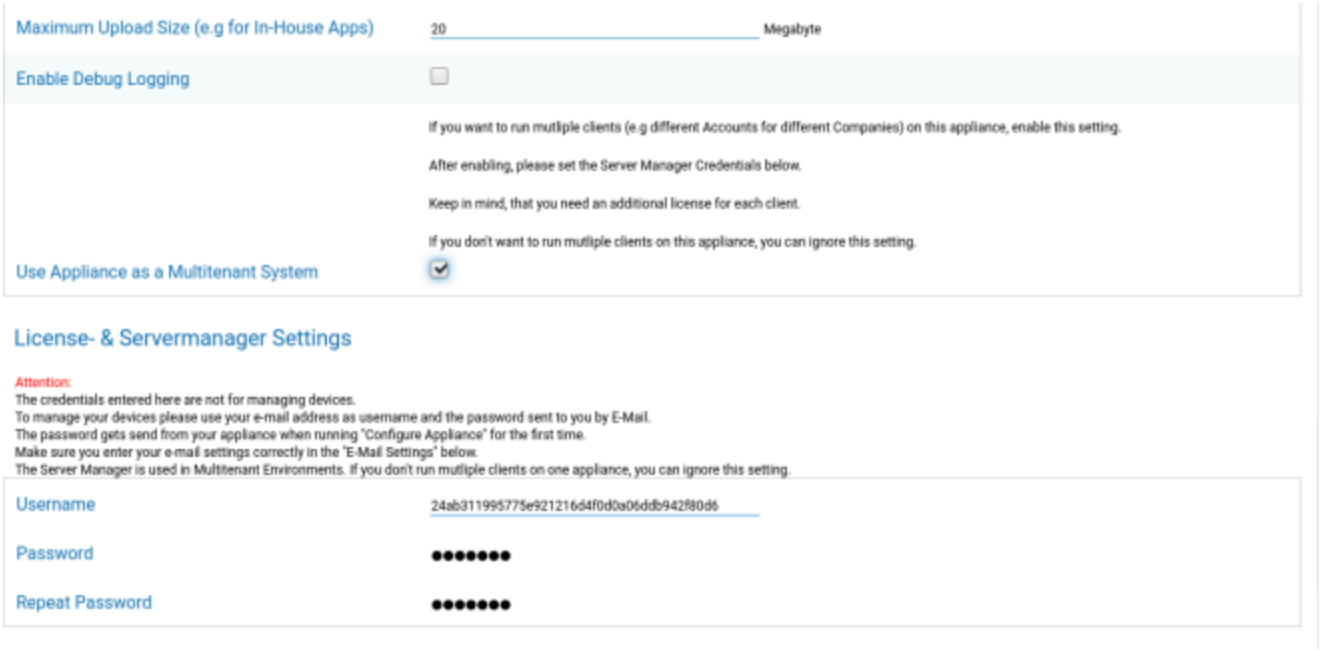
このレポートのデフォルトの列：

Eメール
名称
電話番号
キャリア
料金表
オプション
価格
契約解除
契約開始
時間中
モバイル・アンド・データ
データボリューム
マルチSIM
タイプ
simCardSerial1
simCardSerial2
simCardSerial3
ピン1
ピン2
プク1
プク2
備考

マルチテナント管理

AppTec360 EMMは、それぞれ独自のユーザーやグループ、権限、グローバル設定を持つ複数の個別のテナントをホストすることができます。

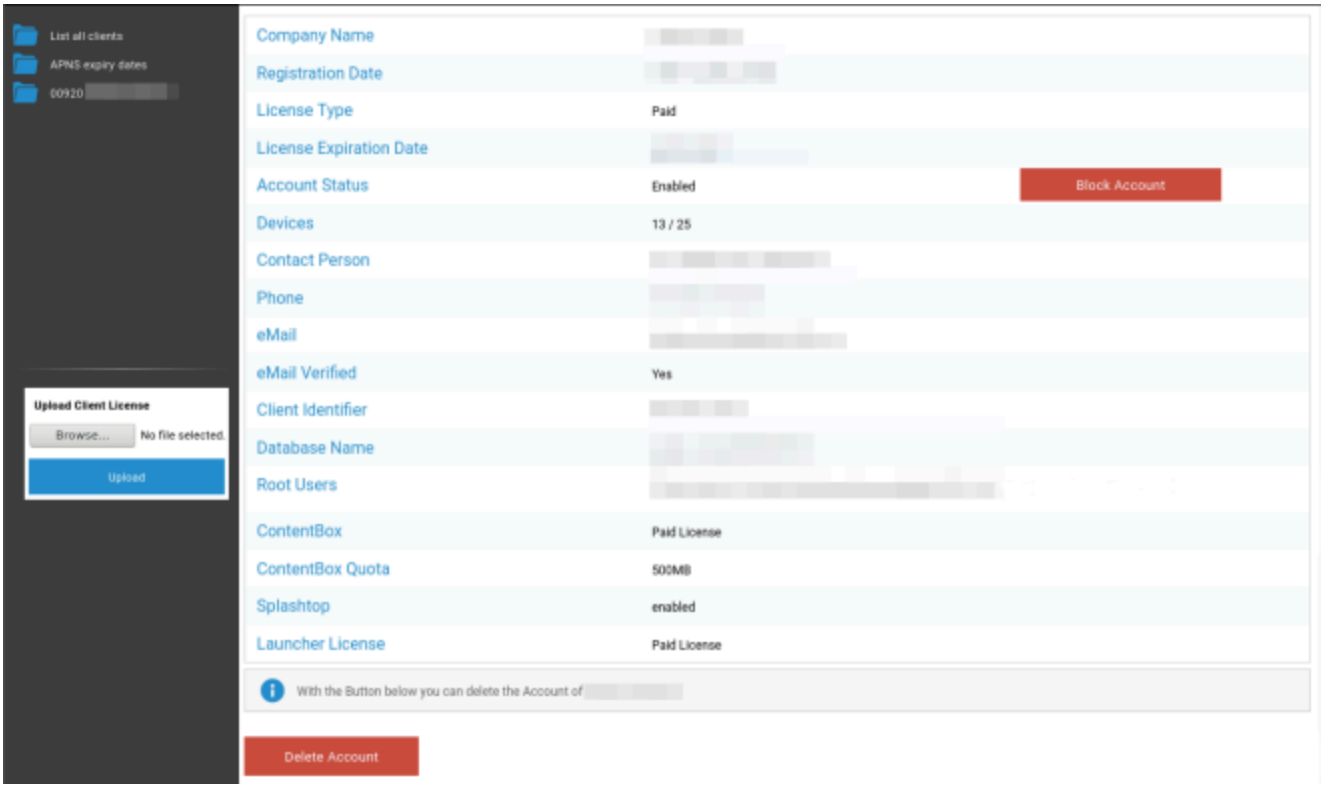
マルチテナント機能を有効にするには、アプライアンスの構成インターフェイスの「ステップ 3 - サーバー設定」で有効にする必要があります。



新しいメニューで、Servermanager用のユーザ名とパスワードを設定します。設定を保存し、「ステップ5 - ライセンス契約」の「アプライアンスの構成」を実行 して、設定を適用します。

設定が完了したら、設定した認証情報で通常のモバイル管理インターフェイスからログインできるようになります。

ログインすると、次のような画面が表示されます。



左側にはすべてのテナント（この場合はID 920のテナントのみ）が表示され、右側にはこのクライアントに関する情報が表示されます。また、アカウントへのアクセスをブロックしたり、クライアントを削除するオプションもあります（注意：これにより、そのクライアントに関連するすべてのデータが削除されます）。

左側では、新しいクライアントライセンスをアップロードすることができます。これは、既存のクライアントのライセンス更新、または自動的に新しいクライアントを作成する新しいライセンスのいずれかになります。新しいクライアントが作成されると、ライセンスが発行された電子メールアドレスにログインパスワードが記載された電子メールが自動的に送信されます。

新規または更新のクライアントライセンスを取得するには（より多くのデバイスライセンスが必要な場合など）、営業担当者にお問い合わせください。

その他の意見

すべての顧客をリストアップ

システム内の全クライアントの概要を表示します。

クライアントID	クライアントID
識別子	クライアント識別子
データベース	データベース
会社名	会社名
電子メール	担当者Eメール
確認済み	コンタクトパーソンの電子メールが認証されているかどうか
国名	国名
デバイス	登録デバイス数
登録日	ライセンス譲渡の時点
最終ログイン	最後の管理者アカウントログイン
ライセンス	ライセンスタイプ表示 (無料|有料)
CBライセンス	ContentBox ライセンス タイプ (無料|有料)
ステータス	現在のAppTec-Clientのステータス
期限切れ	ライセンスの有効期限が切れている場合は、次のように表示されます。
iOS	iOSデバイス数
アンドロイド	アンドロイド端末数
ウィンドウズ・モバイル	ウィンドウズ・モバイル・デバイス数
マックオス	MacOSデバイス数
ウィンドウズ10	Windows 10デバイス数
アンドロイド・エンタープライズ	Androidエンタープライズ・デバイス数
IOS BYOD (ユーザー登録)	IOS BYOD (ユーザー登録) デバイス数
IoT	IoTデバイス数

APNSの有効期限

すべてのクライアントのAPNS証明書の有効期限の概要を表示します。

クライアントID	クライアントID
会社名	会社名
有効期限	Apple APNS証明書の有効期限
インフォメーション	有効期限に関する情報

連絡先

その他のご質問下記までご連絡ください：

一般的な技術的質問

support@apptec360.com

+41 61 511 3210

仮想アプライアンスのインストールに関する質問

consulting@apptec360.com

+41 61 511 3214

免責事項