ZJTP202216925

Endpoint Central Cloud MDM

# スタートアップガイド

ManageEngine

## Endpoint Central Cloud MDM

2022 年 2 月 1 日発行

2024 年 3 月 27 日 更新

Copyright© ZOHO Japan Corporation. All Rights Reserved.

## 内容



(C) ZOHO Japan Corporation. All rights reserved.

■著作権について
**本ガイドの著作権は、ゾーホージャパン株式会社が所有しています。**

■注意事項
**本ガイドの内容は、改良のため、予告なく変更することがあります。**
**ゾーホージャパン株式会社は本ガイドに関しての一切の責任を負いかねます。 当社はこのガイドを**
**使用することにより引き起こされた偶発的もしくは間接的な損害についても責任を負いかねます。**

■商標一覧
・Google、Android、Google Play、Google Chrome、およびその他のマークは Google LLC の商標です。
・Apple, iPhone, App Store, およびその他マークは Apple Inc.の登録商標です。
・iPhone の商標は、アイホン株式会社のライセンスに基づき使用されています。
・iOS は Cisco Inc.のライセンスに基づき使用されています。
・Windows のロゴは Microsoft corp.の登録商標です。
・本ガイドでは、必ずしも(R)、TM は表記していません。

(C)　ZOHO Japan Corporation. All rights reserved.

# 1 はじめに

## 1 - 1 本ガイドの目的

本ガイドは ManageEngine Endpoint Central Cloud の機能の一つである MDM（モバイルデバイス管理）について説明したものです。

MDM はビジネスで利用されるモバイルデバイスを一元管理し、リスクの低減・対策に役立ちます。社用のデバイスに加えて、個人所有のデバイス（BYOD）の管理にも対応しており管理者による柔軟な運用を手助けします。

製品は次のような特徴を持ちます。

1. 幅広い OS に対応
2. 柔軟なデバイス管理が可能
3. 企業のポリシーに準拠したデバイス運用が可能
4. デバイス紛失/盗難時の対策が可能

本ガイドは、MDM の運用を検討されている方を対象に iOS または Android™デバイスの管理方法について、よく利用される機能を抜粋して紹介しています。MDM の中から製品概要を理解し、スムーズに運用を開始するための手がかりとなれば幸いです。

## 1 - 2 MDM のサポート OS

最新のサポート OS は以下の Web ページからご確認ください。

https://www.manageengine.jp/products/Endpoint_Central/system-requirements.html#cloud_MDM

なお、サムスン社製の Android デバイスは、非サムスン社製の場合に比べて、いくつか追加の機能をご利用いただけますが、本ドキュメントでは両者に共通の機能について説明いたします。

(C) ZOHO Japan Corporation. All rights reserved.

# 2 モバイルデバイス管理タブについて

## 2 - 1 管理タブの概要

タブの各機能の概要について説明します。


- ダッシュボード

  登録済みのデバイス数や、デバイスの種類の内訳を示した円グラフ、監査ログのフィードなど基本的な情報が表示されます。

- 管理

  プロファイル管理、アプリケーション管理、リモート制御や、ジオフェンシング機能など端末の管理に関わる機能を使用できます。

- インベントリ

  管理端末の資産情報の詳細を確認できます。端末の位置情報の取得もこのタブから可能です。

- 登録

  「モバイルデバイス管理」タブの管理対象を登録します。

- レポート

  取得したデバイス情報をレポートとして提供します。PDF や CSV 形式でダウンロードすることも可能です。スケジュールレポートとして製品ユーザーにメール送信することも可能です。

- 設定

  MDM に関する設定をします。「ユーザー管理」からは、MDM タブにアクセスできる製品ユーザーを登録する必要があります。

- 監査

  管理ユーザーが「モバイルデバイス管理」タブで実行した操作ログを確認できます。PDF や CSV 形式でダウンロードすることも可能です。

(C) ZOHO Japan Corporation. All rights reserved.

## 2 - 2　MDM タブにアクセス可能なユーザー

「モバイルデバイス管理」タブには、「アクセス権限」をもつユーザーのみがアクセス可能です。各ユーザーのアクセス権限（*役割）は、「設定」タブ→「ユーザーの管理」→「ユーザー」の役割の名称カラムが表示されています。少なくとも 1 つ以上のモジュールにアクセスなし以外の権限をもつ役割が、「モバイルデバイス管理」タブにアクセス可能です。


「ユーザーを追加する」をクリックすると、「モバイルデバイス管理」タブにアクセス可能な製品ユーザーを新たに追加することができます。追加時に以下の情報を入力します：


- メール

  管理者のアドレスを入力します。

- ユーザー名

  追加するユーザーの名前を入力します。

- 役割

  ユーザーに与えるアクセス権限を設定します。

(C)　ZOHO Japan Corporation. All rights reserved.

- 電話番号

  必要に応じてユーザーの電話番号を入力します。

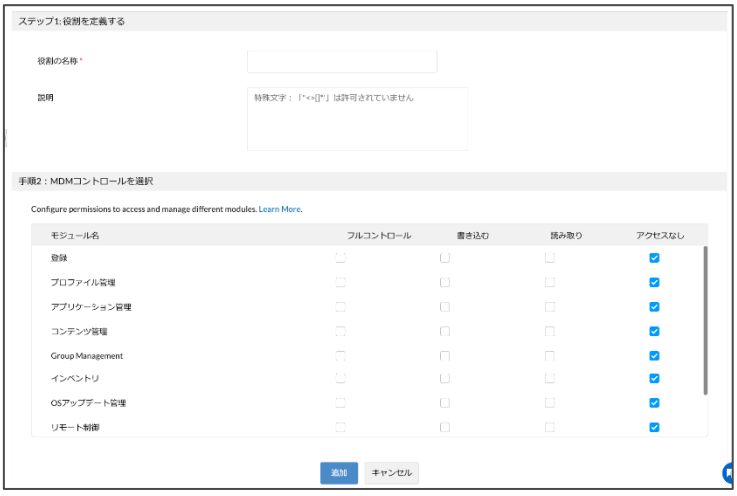
- 監理されるデバイスで

  ユーザーにすべてのデバイスへのアクセス権を与える場合「すべてのデバイス」を、一部のグループにのみアクセス権を与える場合は「選択されたグループ」を選択します。

***役割**

「設定」→「ユーザーの管理」→「役割」から利用可能な**役割**を確認できます。デフォルトで用意されている役割は Administrator, Auditor, Guest, IT Asset Manager, Technician です。「＋役割の追加」から役割を追加することができます。


役割の追加時に権限を設定します。設定可能な権限は下表の通りです。




| フルコントロール | 書き込む | 読み取り | アクセスなし |
|---|---|---|---|
| モジュール内の、すべての機能が利用できます | “配布”や“関連付け”の操作を行うことができますが、モジュール内で設定の作成や修正はできません | モジュールを閲覧することのみ可能です | ユーザーはモジュールを閲覧することができません |

各モジュールに対するアクセス権限について、より詳細な情報はこちらの Web ページ（英語）をご参照ください。

(C)　ZOHO Japan Corporation. All rights reserved.

## 3 登録

MDM を活用するための最初のステップが端末を「モバイルデバイス管理」タブに**登録**することです。

企業のさまざまなニーズに対応するために多くの登録方法を利用できます。登録方法には、プラットフォーム（iOS または Android）共通の方法と（3-1 プラットフォーム共通の登録方法）、各プラットフォームに固有の方法を提供しています（3-2 iOS の登録方法、3-3 Android の登録方法）。

登録方法によって以下のようにデバイスのタイプが分かれ、MDM で使用可能な機能が異なります。

- Workspace Management

  **プラットフォーム（iOS または Android）共通の方法**で登録した場合に該当します。業務に必要な機能を限定的に利用することができます。例えば BYOD（Bring Your Own Device）の端末を管理するために使用します。

- Full Device Management

  各**プラットフォーム固有の方法**で登録した場合に該当します。iOS では監視モード、Android では Device owner の端末として登録されます。Workspace Management の場合に比べて、デバイスを管理するためにより多くの機能を利用できます。例えば共有のデバイスや、キオスク（特定のアプリケーションの使用に制限したデバイス）、仕事用として従業員に貸与するデバイスを管理するために使用します。

Workspace Management と Full Device Management で利用可能な機能の差異は、次の Web ページをご確認ください。

▼モバイルデバイス登録方法による機能比較

https://www.manageengine.jp/support/kb/Desktop_Central_Cloud/?p=1689

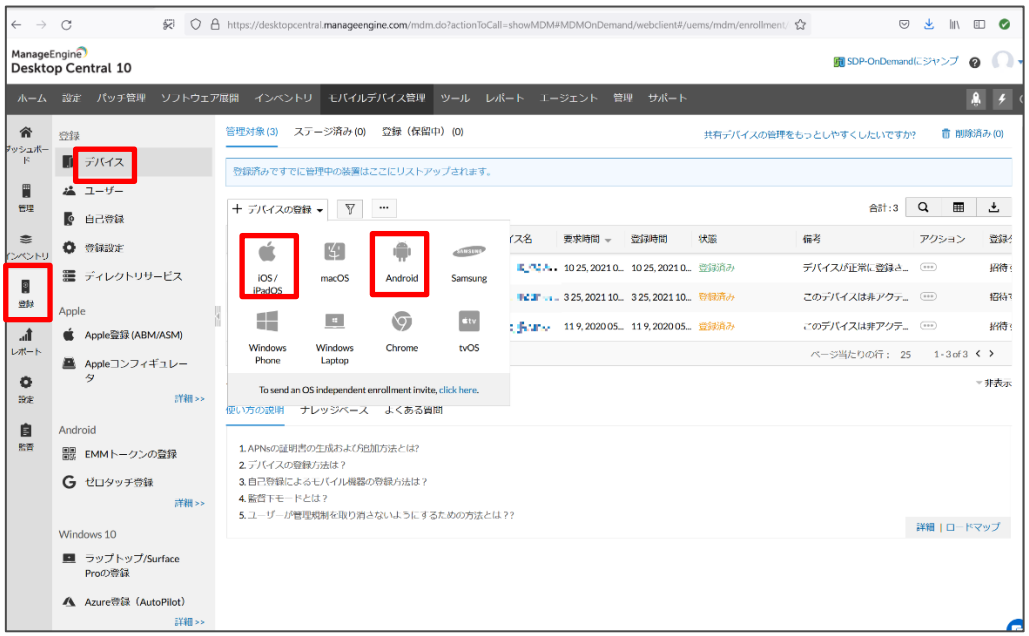
(C)　ZOHO Japan Corporation. All rights reserved.

## 3 - 1 プラットフォーム共通の登録方法

プラットフォーム共通の登録方法では、製品ユーザーが承認して一台ずつ登録する製品ユーザーまたは招待による登録と、製品ユーザーによって公開された共通の登録用リンクに、エンドユーザーがアクセスして登録する自己登録があります。**製品ユーザーまたは招待による登録**では製品ユーザーによって 1 台ずつ確実に登録することができます。**自己登録**は一度に多数のデバイスを登録する場合に有用です。

### 製品ユーザーまたは招待による登録

1．「登録」→「デバイス」→「デバイスの登録」からプラットフォーム(iOS/Android)を選択します。




2．**(A)製品ユーザーが製品画面から操作して登録する方法**と、**(B)ユーザーに登録の招待メールを送信して登録を依頼する方法**の 2 通りがあります。

**(A)製品ユーザーが製品画面から操作して登録する方法**

A-1.

- 登録するデバイス
  「自分で」を選択します
- 所有者
  端末が個人所有の場合は「個人」に、企業の所有の場合は「企業」を選択します。この設定はデバイスポリシーに関係します。
- グループに割り当てる
  登録後の端末を割り当てるグループを選択します（任意）。

(C)　ZOHO Japan Corporation. All rights reserved.


A-2. 以上の設定の完了後、「次へ」をクリックします。

A-3. 画面の指示にしたがい、ワンタイムパスワードまたはディレクトリを利用した認証を行い登録します（認証方法の変更は登録設定をご覧ください）。


**登録画面（上）iOS 、(下)Android**

(C) ZOHO Japan Corporation. All rights reserved.

**(B)ユーザーに登録の招待メールを送信して登録を依頼する方法**

B-1.

- 登録するデバイス
  「**ユーザー招待を通じて**」を選択します。
- ~までに通知する
  メールを通知方法として選択します。
- ユーザー
  招待するユーザーを設定します。
- 所有者
  端末が個人所有の場合は「個人」に、企業の所有の場合は「企業」を選択します。この設定はデバイスポリシーに関係します。
- グループに割り当てる
  登録後の端末を割り当てるグループを選択します（任意）。


登録メールテンプレートの設定から、招待メールを送る際のテンプレートを編集することができます。

B-2. 以上の設定の完了後、「登録招待を送信する」をクリックします

B-3. 招待メールの文章に従い、ユーザーが端末を登録します。登録時にワンタイムパスワードまたはディレクトリを利用した認証が必要となります（認証方法の変更は登録設定をご覧ください）。

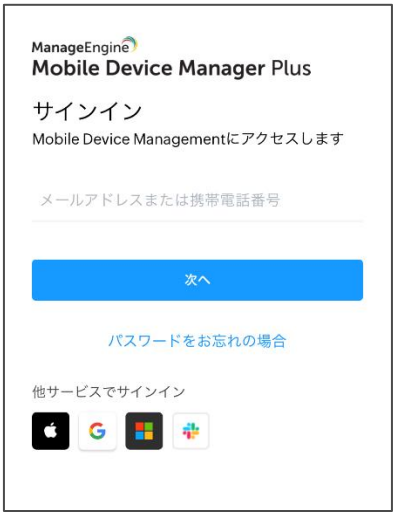
**招待メール（左）iOS、(右)Android**

(C)　ZOHO Japan Corporation. All rights reserved.

## 自己登録

自己登録では製品ユーザーが、複数のエンドユーザーに共通の登録用リンクを公開します。エンドユーザーがリンクにアクセスし、ディレクトリの資格情報を利用して認証を行うことで、登録が完了します。デフォルトでは認証情報として Zoho 認証を利用し、製品ユーザーの組織に所属するアカウントのみが登録できます。

「登録」→「自己登録」の画面右にあるリンクまたは QR コードをエンドユーザーに公開してください。


**自己登録時の認証画面：Zoho 認証**

> 自己登録で使用する URL を変更することはできません。

(C) ZOHO Japan Corporation. All rights reserved.

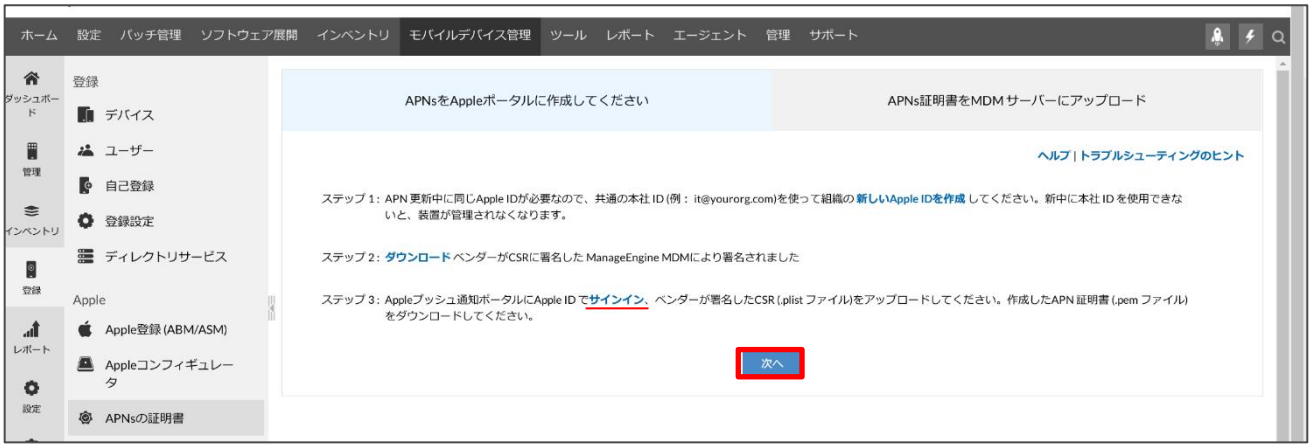
## 3 - 2　iOS の登録方法

### APNs 証明書の登録

iOS を管理するためには「登録」→「APNs の証明書」から、サーバーに **Apple Push Notification Service 証明書（APNs 証明書）**を登録する必要があります。APNs 証明書は、Apple によって提供され、発行のためには Apple ID が必要になります。本節では APNs 証明書を発行し、サーバーに登録する方法について説明します。

1. コンソール画面の「ダウンロード」をクリックし、Zoho が署名した CSR ファイルをダウンロードします。


2. コンソール画面の「サインイン」をクリックして「Apple プッシュ通知証明書ポータル」に移動後、サインインして、ページの指示に従い CSR ファイル（ステップ 1 でダウンロード済み）をアップロードします。
3. Apple から発行された APNs 証明書をダウンロードします。
4. コンソール画面で「次へ」をクリックします。




(C)　ZOHO Japan Corporation. All rights reserved.

5. ダウンロードした APNs 証明書をコンソール画面からアップロードします。画面左の青い領域にダウンロードした APNs 証明書のファイルをドラッグ&ドロップします。
6. 情報を入力します。
   - APNs の作成に使用する本社 Apple ID
     APNs 証明書作成の際に利用した Apple ID を入力します。
   - APN 有効期限のメール通知
     APNs の有効期限が切れる 3 か月前に入力したアドレス宛に通知します。
7. 入力の完了後、「アップロード」をクリックします。


以上で APNs 証明書の登録が完了します。APNs 証明書には有効期限があり、1 年ごとに更新する必要があります。

(C) ZOHO Japan Corporation. All rights reserved.

Apple Business Manager/Apple School Manager を利用した登録

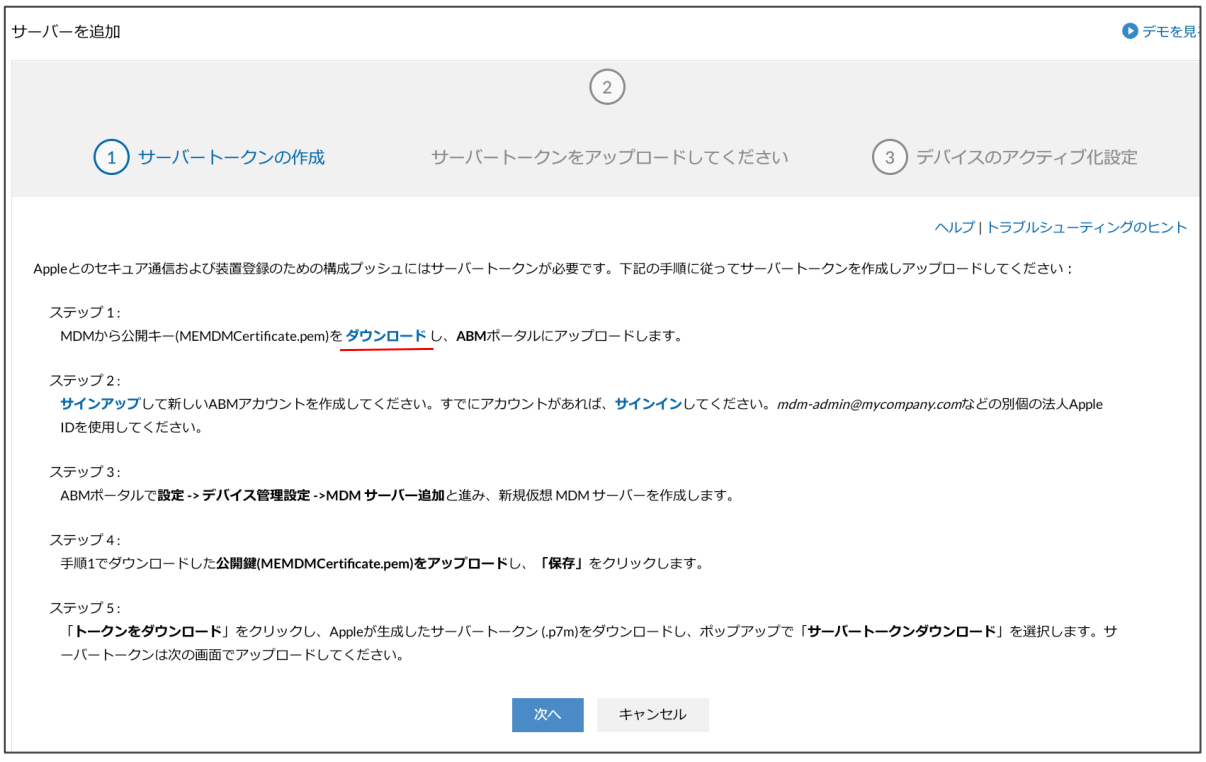
**Apple Business Manager（ABM）/Apple School Manager（ASM）** と同期して、正規のベンダーから購入した端末を「モバイルデバイス管理」タブに自動的に登録することができます。本機能で登録された端末は監視モード(Supervised mode)となります。

以下、本書では ABM を利用した場合について設定方法を説明します。ASM の場合も手順は同様ですので、必要に応じて ABM を ASM に読み替えてください。

MDM サーバーと ABM の連携方法

1. 「登録」→「Apple 登録(ABM/ASM)」→「装置を法人用に登録」を選択します。


2. コンソール画面の「ダウンロード」をクリックし”MDM_Zoho_corporation_Certificate.pem”をダウンロードします。



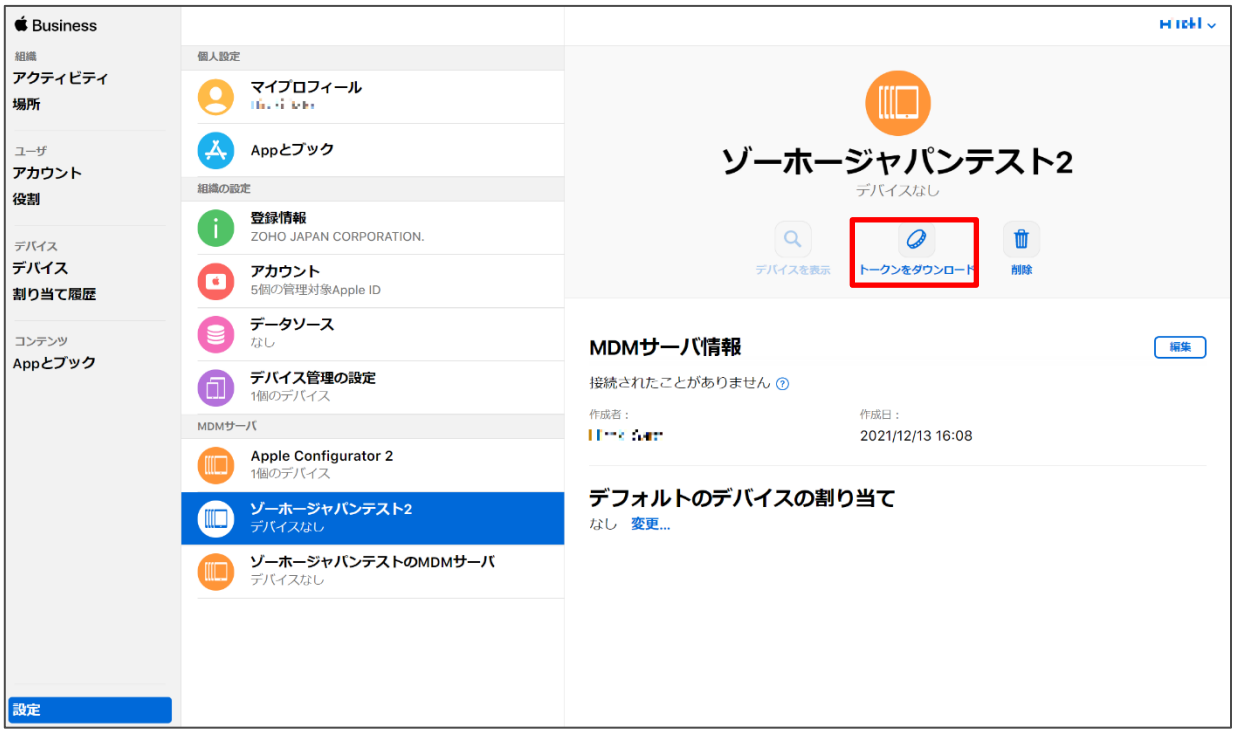

(C) ZOHO Japan Corporation. All rights reserved.

3. ABM ポータルにログインし、「設定」→「デバイス管理の設定」→「MDM サーバーの追加」をクリックします。


4. 「ファイルを選択」からステップ 2 でダウンロードした”MDM_Zoho_corporation_Certificate.pem”を選択し、「保存]をクリックします。


(C) ZOHO Japan Corporation. All rights reserved.

5. 「トークンをダウンロード」をクリックして MDM サーバーにアップロードするファイルをダウンロードします。ダウンロード後、コンソール画面で「次へ]をクリックします。



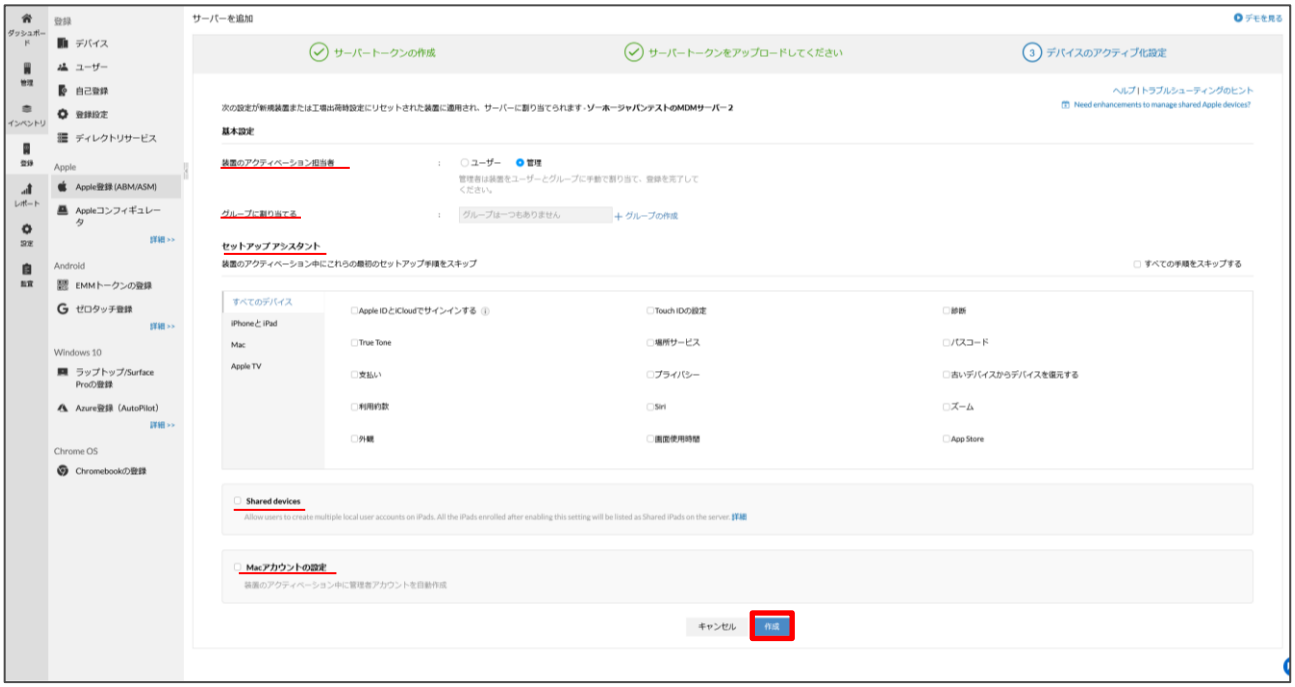


(C) ZOHO Japan Corporation. All rights reserved.

6. サーバートークンを検索するから「参照する」をクリックし、ステップ 5 でダウンロードしたファイルをアップロードします。サーバートークンの期限が切れた場合に通知するアドレスを、サーバートークンの期限切れの通知先メールアドレスに入力し、「次へ」をクリックします。


7. デバイスのアクティブ時の設定を行います。

- 装置のアクティベーション担当者
  「ユーザー」または「管理」（=製品ユーザー）を選択します。
- グループに割り当てる
  端末を割り当てるグループを選択します（任意）。
- セットアップアシスタント
  端末起動後のセットアップ時に設定をスキップする項目にチェックを入れます。




(C) ZOHO Japan Corporation. All rights reserved.

8. 以上の設定の完了後、「作成」をクリックします。

以上で Endpoint Central Cloud サーバーと ABM の連携が完了します。以後、購入端末が ABM に登録される際に、コンソールに自動で追加されます。ABM へのデバイスの登録方法は Apple の Web ページをご参照ください。
なお、ABM と連携して登録するにはデバイスのアクティベーションの前に上記操作が完了している必要があります。該当しないデバイスは工場出荷状態に初期化してください。

(C) ZOHO Japan Corporation. All rights reserved.

## Apple Configurator による登録

まだ ABM サーバーに登録されていない端末に対して、監視モード（Supervised mode）を利用した管理を行う場合、**Apple Configurator 2** を使用して端末を登録できます。ただし登録を行うと端末は初期化されます。本機能を使用するためには Apple Business Manager（ABM）のアカウントが必要になります。iPhone でアクティベーションロックが有効の場合、本登録が完了しない場合がございます。その際には、Apple ID からログアウトして、再度お試しください。

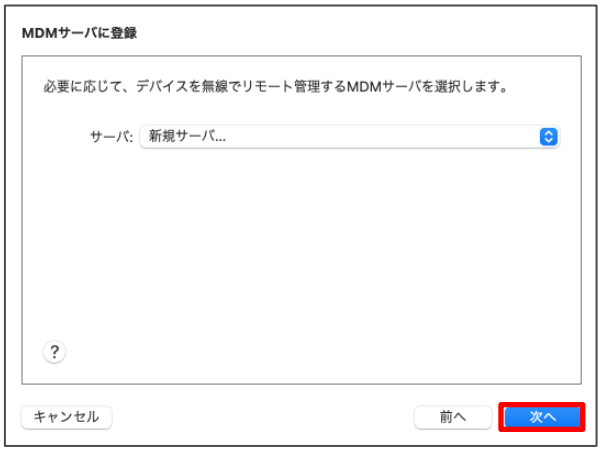
1. App Store から Apple Configurator 2 をダウンロードします。
2. 自動的に Wi-Fi に接続するプロファイルを必要に応じて作成します（このプロファイルは端末の初期化後に必要に応じて利用します）。「ファイル」→「新規プロファイル」をクリックして、左メニューから Wi-Fi を選択し、SSID や、セキュリティの種類、パスワードなど必要な情報を入力してください。入力後、「ファイル」→「保存」からプロファイルを保存します。


3. 「ファイル」→「新規ブループリント」をクリックし、新しいブループリントを作成します。その後、右クリックを押し、「準備」をクリックします。

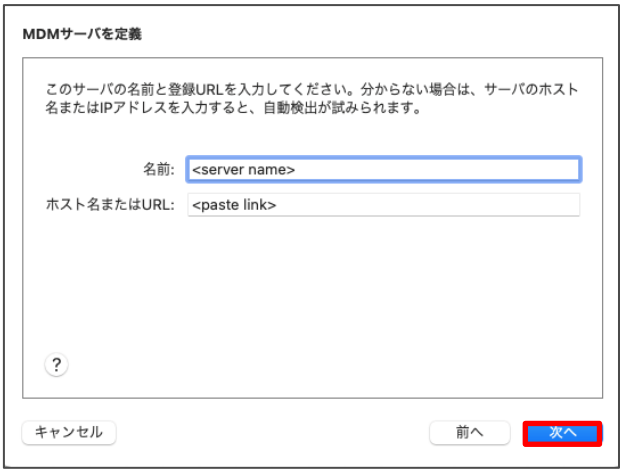

4. デバイスを準備の画面で、「準備方法」を「手動構成」に設定し、「Apple School Manager または Apple Business Manager に追加」にチェックマークを入れ、「次へ」をクリックします。

(C) ZOHO Japan Corporation. All rights reserved.


5. Apple Configurator に新規サーバーを登録します。サーバー：から新規サーバーを選択し、「次へ]をクリックします。

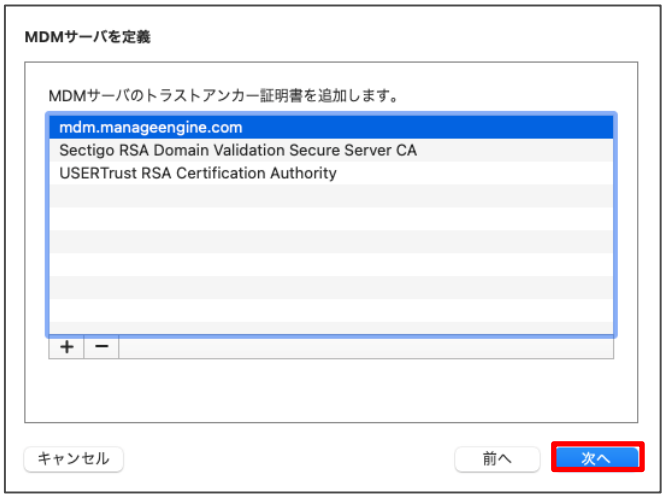



6. サーバー名を入力します。URL は、コンソール画面の「モバイルデバイス管理」タブ→「登録」→「Apple コンフィギュレーター」に表示されている URL を入力してください。




(C) ZOHO Japan Corporation. All rights reserved.


7. 信頼できる証明書が追加されていることを確認後、「次へ」をクリックしてください。



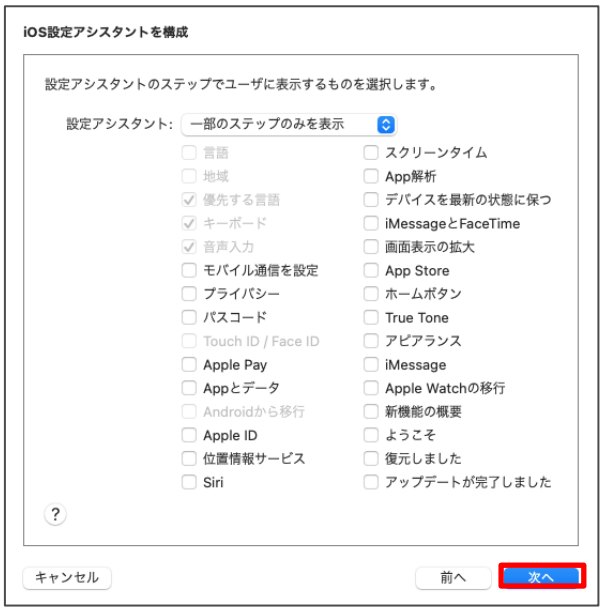

8. ABM のアカウント情報を入力します。


9. 組織に関する詳細を入力し、「次へ」をクリックします。

(C) ZOHO Japan Corporation. All rights reserved.

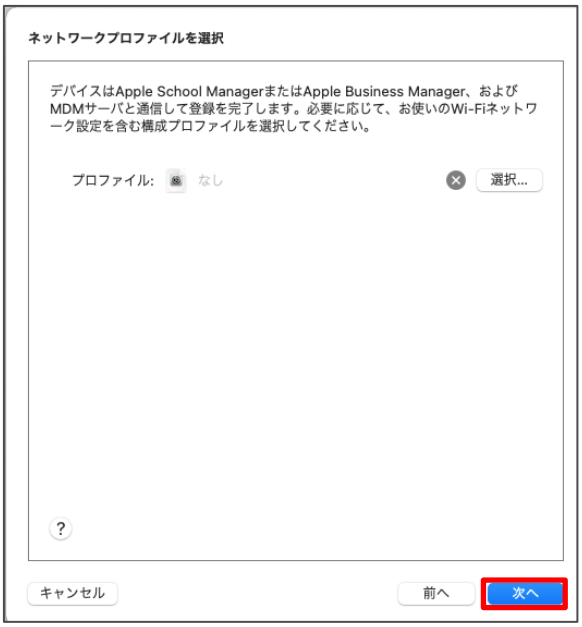
10. 「組織を作成」で「新しい監視識別情報を生成」を選択して、「次へ」クリックします。


11. 「iOS 設定アシスタントを構成」でデバイスの初期化時に、ユーザーが設定を行う項目を選択します。

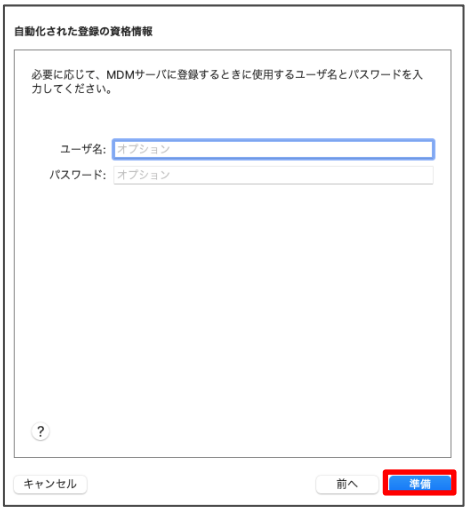



(C) ZOHO Japan Corporation. All rights reserved.

12. デバイスが登録を完了するためには、ABM および MDM サーバーとの通信が必要です。「ネットワークプロファイルを選択」で必要に応じて、ステップ 1 で作成した Wi-Fi の設定プロファイルを選択し、「次へ」をクリックします。




13. 「自動化された登録の資格情報」では何も入力せずに「準備」をクリックします。




(C) ZOHO Japan Corporation. All rights reserved.

14. 端末を PC に接続して、Configurator 上で端末を右クリックし「適用」から作成したブループリントを適用します。


以上で端末の初期化後に登録が完了します。

## 監視モード（Supervised mode）

Apple の提供する**監視モード**（**Supervised mode**）を利用することで、より高度な管理を実現できます。主に、アプリケーションのサイレントインストールや、一部プロファイルの使用（詳細はプロファイル作成時の画面上のアイコンから確認できます）のほか、キオスクモード、アプリケーションのブラックリスト登録が利用可能です。
端末を監視モードで管理するためには、Apple Business Manager を利用した登録または Apple Configurator による登録が必要であり、プラットフォーム共通の登録方法では監視モードは無効になります。

(C) ZOHO Japan Corporation. All rights reserved.

## 3 - 3　Android の登録方法

### EMM トークン

工場出荷状態の Android（6.0 以上）を対象に、ManageEngine MDM アプリケーションを自動的にインストールし、デバイスオーナーとして高度な管理を実現します。

1．　工場出荷状態の Android を起動して、画面の指示に従い、Google アカウントを入力する直前までの設定を完了します。


2．　メールアドレスに’afw#memdm’と入力します。


3．　画面の指示に従い、ManageEngine MDM のアプリケーションをインストールします。

(C)　ZOHO Japan Corporation. All rights reserved.


4 .ManageEngine MDM アプリケーションのインストール後、コンソールの**[登録]→[EMM トークンの登録]**から、表示される QR コードをスキャンし、登録を完了します。


5． 登録が完了したデバイスはコンソール上に表示されます。EMM トークンを利用して登録したデバイスは**[登録]→[EMM トークンの登録]**から確認できます。

6 .次のステップはこのデバイスをユーザーに割り当てることです。アクションカラムから、**[ユーザーの割り当て]**をクリックします。


(C) ZOHO Japan Corporation. All rights reserved.

７． 割り当てるユーザーとグループを入力します。


８． デバイスが**[登録]**→**[デバイス]**から確認できるようになり、「モバイルデバイス管理」タブで管理できるようになります。

## 管理タイプ

Android の管理形態にはプロファイルオーナー（Profile owner）とデバイスオーナー（Device owner）とレガシーオーナー（Legacy owner）の三種類あります。Android 5.0 より前の端末はレガシーオーナーに分類されます。一方で Android 5.0 以降の端末は、登録方法によってプロファイルオーナーまたはデバイスオーナーに分類されます。

プロファイルオーナーの端末は、Android が提供するワークプロファイルと呼ばれる仕事用のコンテナのみを管理することができます。そのため機能的な制限があります。プラットフォーム共通の登録方法によって登録した場合、管理形態はプロファイルオーナーになります。

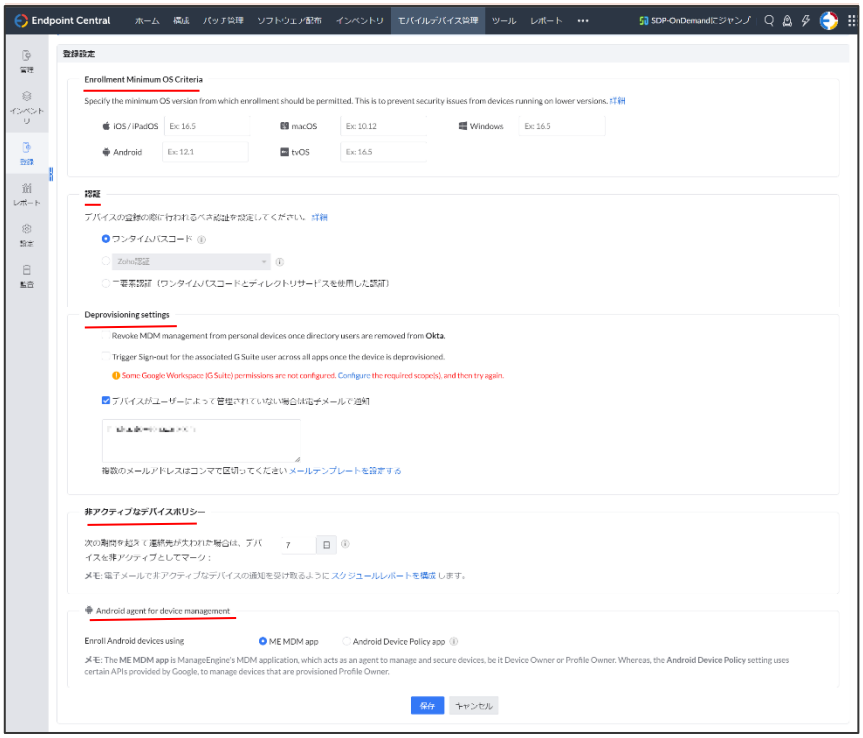
デバイスオーナーの端末はプロファイルオーナーの機能に加えて、より高度な管理が可能になります。EMM トークンによる登録を行った場合、管理形態はデバイスオーナーになります。

(C) ZOHO Japan Corporation. All rights reserved.

## 3 - 4　登録設定

「登録」→「登録設定」から、デバイス登録をする際の設定を変更できます。

- Enrollment Minimum OS Criteria
  登録する OS の基準を設定します。基準よりも古い OS は登録されません。
- 認証
  デバイスを登録する際の認証方法を選択します。"
  - ➢ ワンタイムパスコード
    登録時にユーザーはワンタイムパスコードを電子メールで受け取り、認証に用います。
  - ➢ Zoho 認証
    組織に所属する Zoho アカウントの情報を入力して認証します。
- Deprovision settings
  登録デバイスのプロビジョニング解除に関する設定です。Okta からユーザーが削除された際のデバイスのプロビジョニング解除と、ManageEngine MDM の削除（Android）または MDM プロファイルの削除（iOS）を行った際の管理者への通知を設定できます。
- 非アクティブなデバイスポリシー
  特定の期間通信がない端末を非アクティブなデバイスとして分類するための基準を指定します。デフォルトでは 7 日に指定されています。
- Android agent for device management
  アンドロイド管理に使用するアプリケーションを選択します。




(C)　ZOHO Japan Corporation. All rights reserved.

## 3 - 5　デバイスポリシー

端末登録時に端末の**所有者**を、「個人」または「企業」から選択できます。


**所有者を設定：Android デバイスを登録時**

所有者ごとに MDM で実行可能な操作に違いあり、これを**デバイスポリシー**から設定します。デフォルトのポリシーは「設定」→「プライバシーポリシー」から確認することができます。所有者が個人の場合は従業員が所有している装置に対するデフォルト設定、所有者が企業の場合は本社が所有している装置に対するデフォルト設定の欄をご確認ください。画面右上の「変更」をクリックして設定を変更することが可能です。

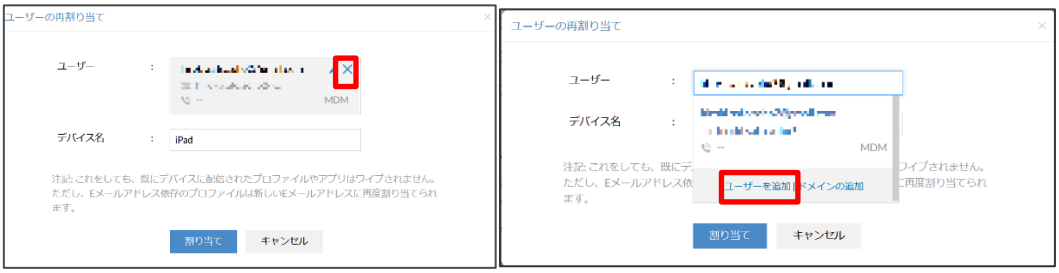

(C)　ZOHO Japan Corporation. All rights reserved.

## 3 - 6　ユーザーの再割り当て

管理対象のデバイス名とユーザー名は登録後に変更することも可能です。

1. 「登録」→「デバイス」→「アクション」カラムから「ユーザーの再割り当て」をクリックします。


2. 右上の×をクリックして、リストから既存のユーザーを選択するか「ユーザーを追加」から新規のユーザーを追加します。ユーザーを追加する場合は、ユーザー登録に必要な情報を入力します。なおここで追加したユーザーは「登録」→「ユーザー」から確認することができます。





**ユーザーを追加**

3. ユーザーを設定後、「割り当て」をクリックします。

(C)　ZOHO Japan Corporation. All rights reserved.

# 4 プロファイル

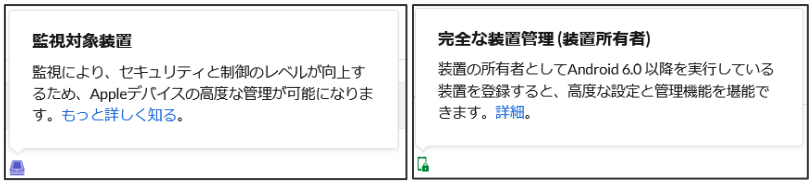
MDM では端末の設定を変更するプロファイルを作成することができます。作成したプロファイルは、端末に「関連付け」することで適用します。この章ではプロファイルの作成および関連付けする方法について説明します。

## プロファイルの作成

1．「管理」タブ→「プロファイル」→「プロファイルを作成する」から配布対象のプラットフォーム(iOS/Android)選択します。


2． 製品画面を操作して任意のプロファイルを設定し「保存」と「公開」をクリックします。下図は例として作成した Android のパスコードに関する設定項目です。


一部の設定項目は Full Device Management の端末にのみ有効です。該当する項目にはアイコンが表示されています。




**（左）監視対象（=Supervised mode）（右）完全な装置管理（=Device Owner）**

(C)　ZOHO Japan Corporation. All rights reserved.

プロファイルの関連付け

作成したプロファイルをデバイスまたは端末に関連付ける方法について説明します。

1．「管理」→「グループおよび装置」に移動します。

2． グループ/デバイスの画面から、対象となるグループ/デバイスの左にあるチェックボックスにチェックを入れ、アクションから「プロファイルを関連付ける」を選択します。


**グループに対してプロファイルを関連付ける場合**

3． 公開されたプロファイルを選択して、デバイスに関連付けします。プロファイルは端末が通信可能になると関連付けられます。

既に適用済みのプロファイルを編集した際には、編集後のプロファイルは自動的には適用されず、プロファイルの更新が必要になります。更新を行うためには「プロファイル」から該当プロファイル選択し、画面の「すべてをアップグレードする」をクリックします。


(C)　ZOHO Japan Corporation. All rights reserved.

# 5 アプリケーション

「モバイルデバイス管理」タブでは以下の手順で、アプリケーションのインストール実行できます。

1.リポジトリへ追加

インストールするアプリケーションを製品画面で設定します。管理者が手動で設定する方法と、Apple Business Manager /Managed Google Play と連携して自動で設定する方法があります。

2.リポジトリの関連付け

リポジトリ内のアプリケーションをインストールする対象を選択し、インストールを実行します。

インストールしたアプリケーションは、アップデートおよび削除も容易です。また使用可能なアプリを予め制限する機能もあります（ブラックリスト）。

## 5-1 リポジトリへ追加

アプリケーションをインストールするには、まずリポジトリにアプリケーションを追加する必要があります。追加方法には以下の 2 種類があります。

A　管理者が手動で設定する方法（コンソール画面からストアにアクセスしアプリケーションを検索して追加する方法）

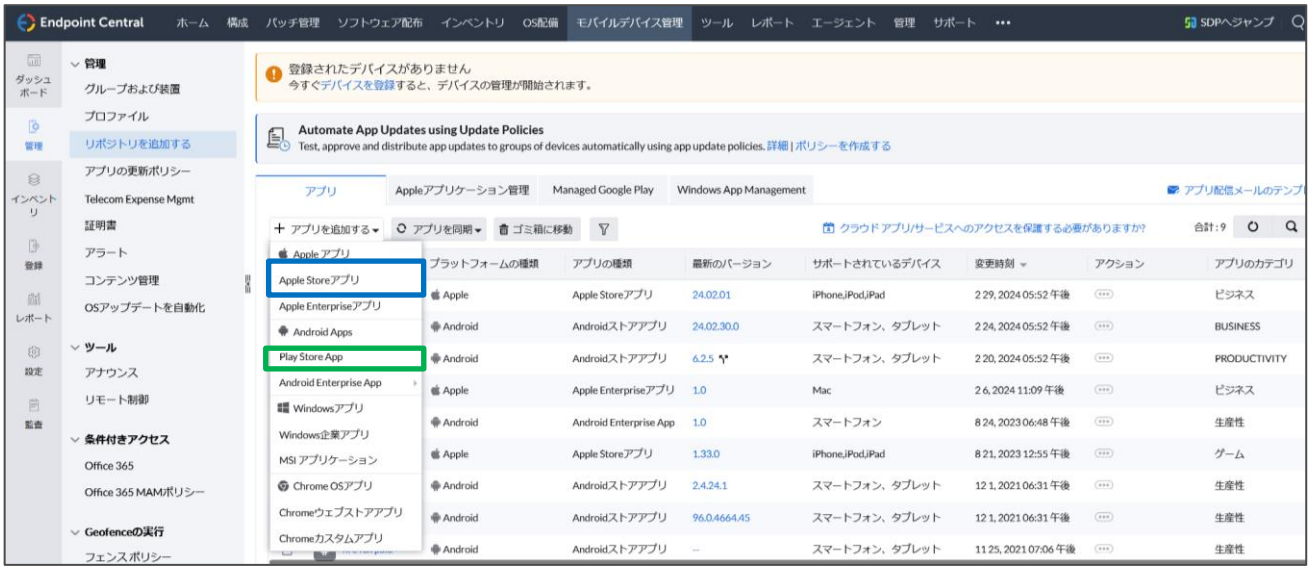
B　ベンダーの提供するサービス（Apple Business Manager/Managed Google Play）と同期して自動で追加する方法

また社内で作成したアプリケーションをアップロードしインストールする機能もございますが、本書では割愛します。

### コンソール画面からストアにアクセスしアプリケーションを検索して追加する方法

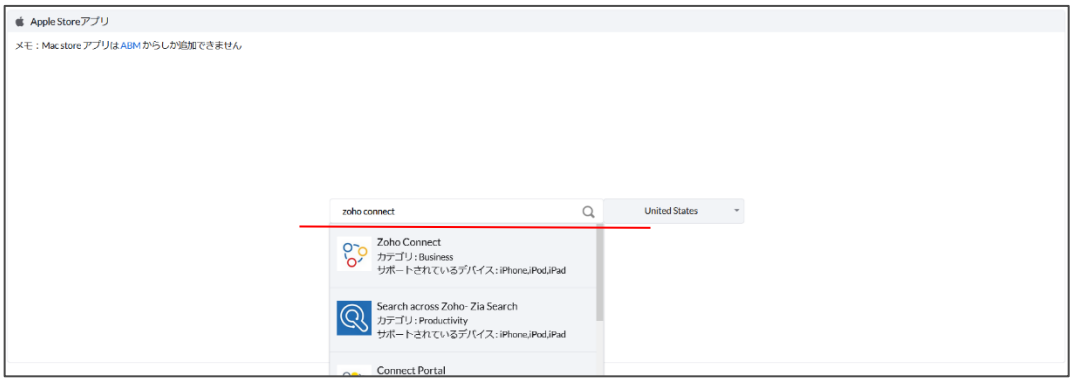
1．「管理」→「リポジトリを追加する」をクリックします。

2．「+アプリを追加する」から、「Apple Store アプリ」（iOS の場合）または「Play Store App」（Android の場合）を選択します。「Play Store App」（Android の場合）は、さらに Managed Google play を設定している場合とそうでない場合で、方法がやや異なります。

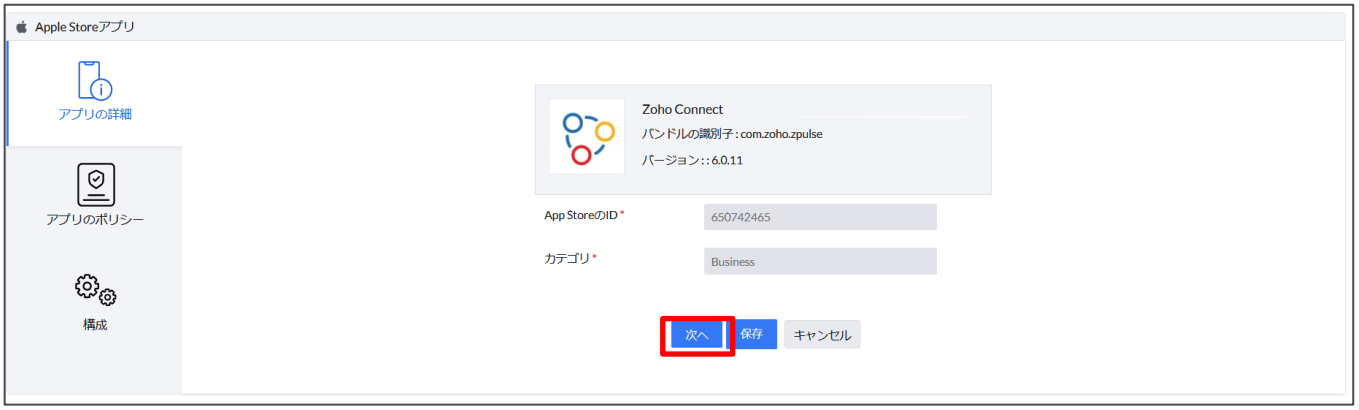



(C)　ZOHO Japan Corporation. All rights reserved.

2-1-1. 「Apple Store アプリ」（iOS の場合）「Apple Store アプリ」を選択し、検索窓からアプリケーション名を検索します。

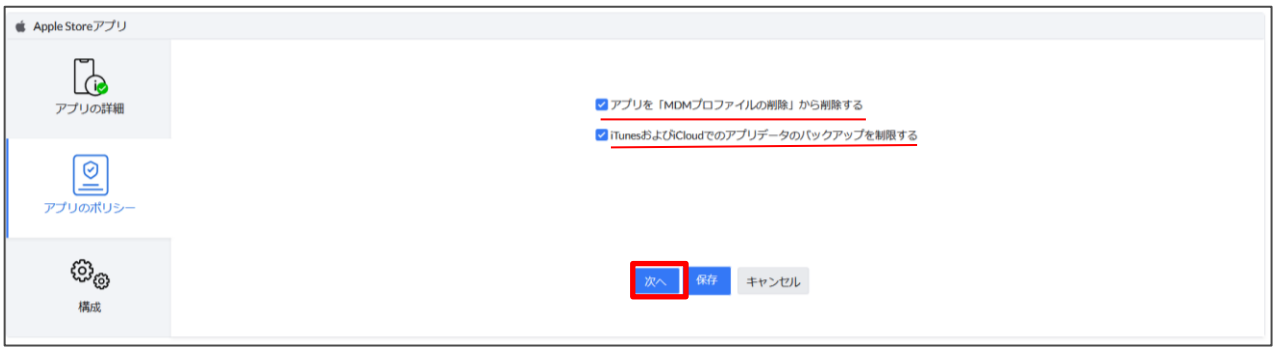



2-1-2. 選択したアプリケーションの情報が自動的に入力されます。確認したら、「次へ」を押します。



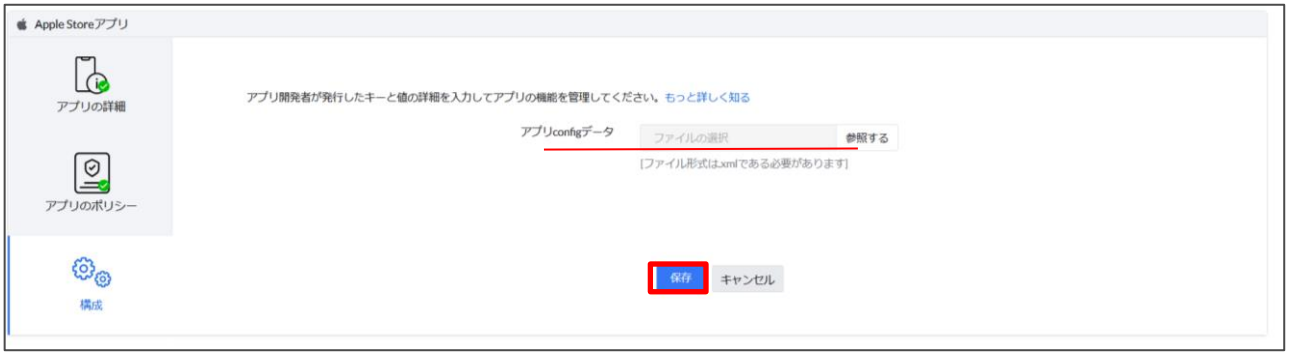

2-1-3. アプリケーションのポリシーを設定します。

- アプリを「MDM プロファイルの削除」から削除する
  iOS のプロファイル削除時にアプリケーションを削除します。
- iTunes および iCloud でのアプリデータのバックアップを制限する
  iTunes および iCloud へのアプリデータのバックアップを制限します 。




(C) ZOHO Japan Corporation. All rights reserved.

2 - 1 - 4 .　アプリ開発者によって設定ファイルの追加が要請されている場合、アプリ config データから追加して保存します。




以上で、Apple ストアのアプリケーションをリポジトリに追加することができます。

2 - 2 - 1 「Play Store App」（Android の場合）かつ Managed Google Play を設定していない場合

「Play Store App」を選択し、アプリの識別子*、ライセンスのタイプ、カテゴリ、サポートされているデバイスを入力し、保存を押します。


(C)　ZOHO Japan Corporation. All rights reserved.

*アプリの識別子の取得方法

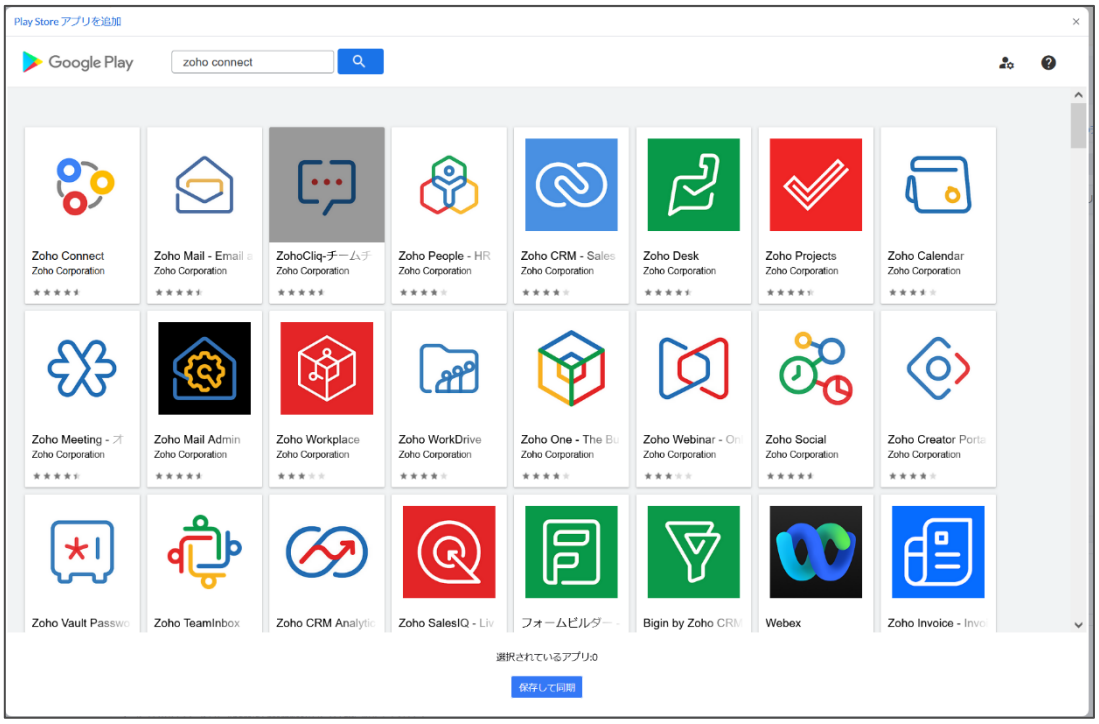
Google Play Store のインストールしたいアプリケーションのページに移動します。URL の”id=”以下が識別子になります。

（例）Google Chrome の場合、識別子は’com.android.chrome’になります。

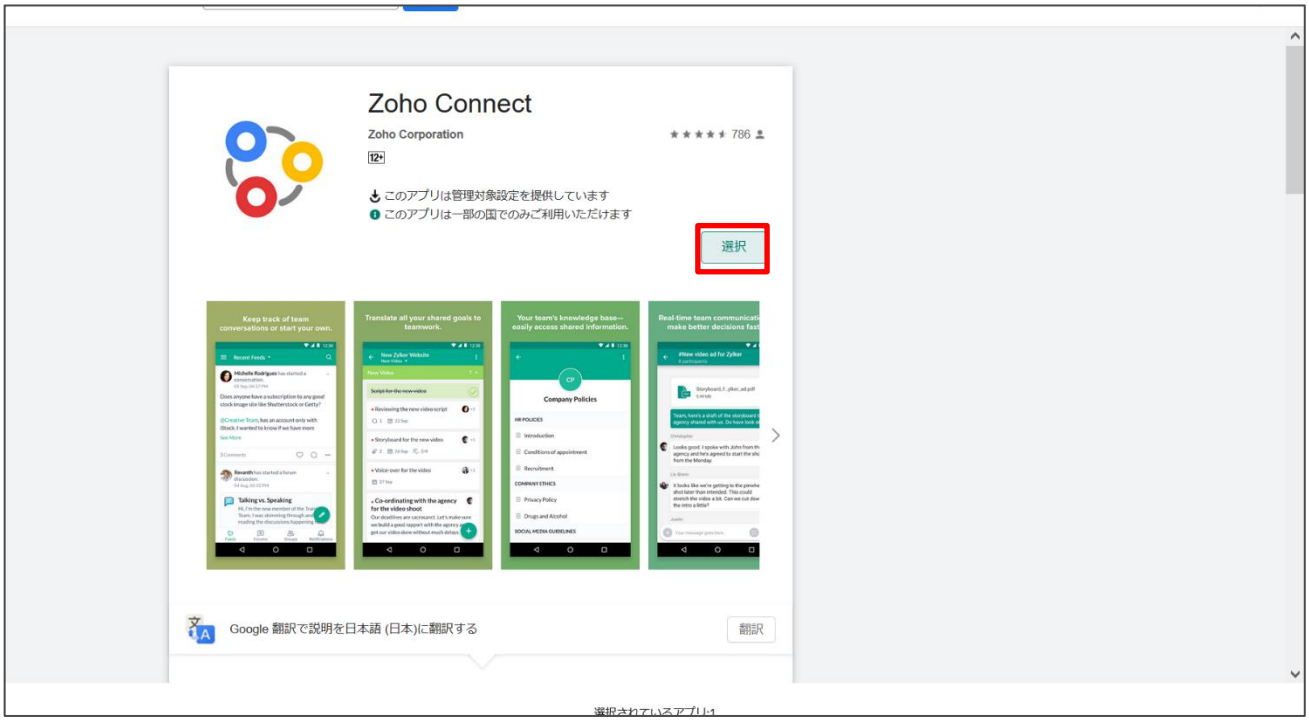

(C) ZOHO Japan Corporation. All rights reserved.

2 - 2 - 2 .「Play Store App」（Android の場合）かつ Managed Google Play を設定済みの場合

「Play Store App」を選択し、アプリケーション名を検索窓に入力します。

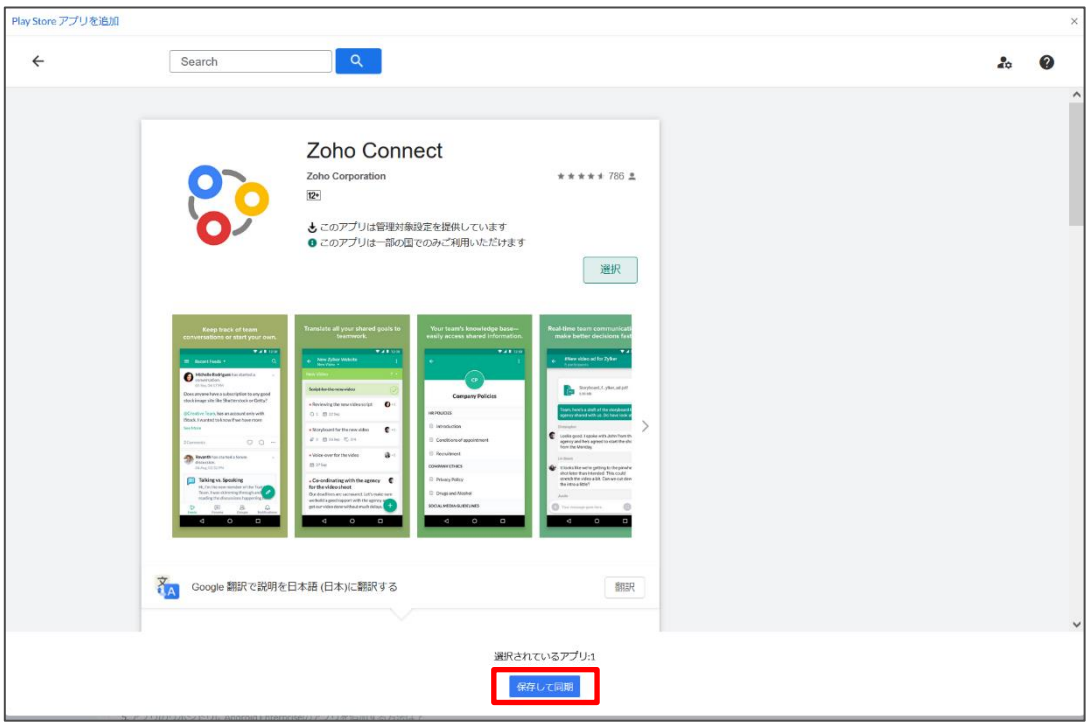



2 - 2 - 3 . 追加するアプリケーションを確認して選択をクリックします。




(C) ZOHO Japan Corporation. All rights reserved.

2-2-4. 追加するアプリケーションを選択した後、「保存して同期」をクリックすることで、対象のアプリケーションをリポジトリに追加することができます。




(C) ZOHO Japan Corporation. All rights reserved.

## Apple Business Manager（ABM）と同期

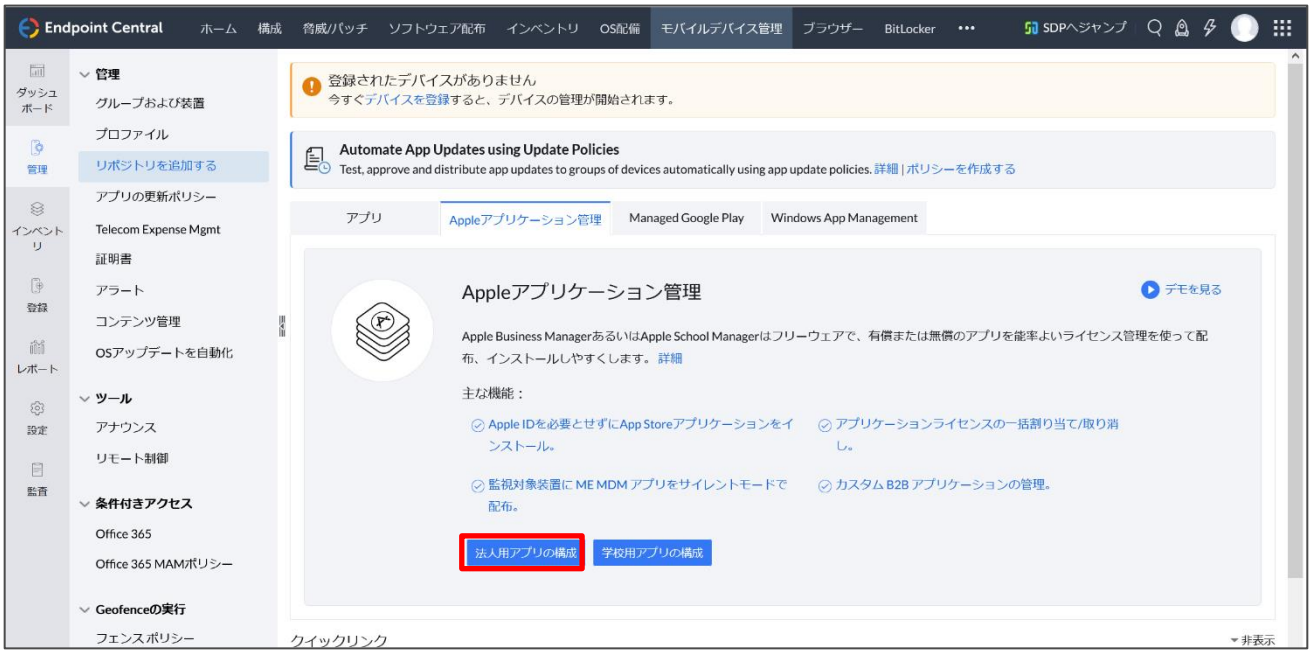
ABM のアカウントを持っている場合、購入したアプリケーションを、自動的にリポジトリに追加することができます。

1. ABM ポータルにログインし、「環境設定」→「お支払いと請求」を表示します。
2. 右下の「コンテンツトークン」の「ダウンロード」をクリックして、サーバートークンをダウンロードします。


3. Endpoint Central Cloud コンソールの「モバイルデバイス管理」→「管理」→「リポジトリを追加する」→「Apple アプリケーション管理」を表示します。

(C) ZOHO Japan Corporation. All rights reserved.

4. 「法人用アプリの構成」（ABM の場合）をクリックします。



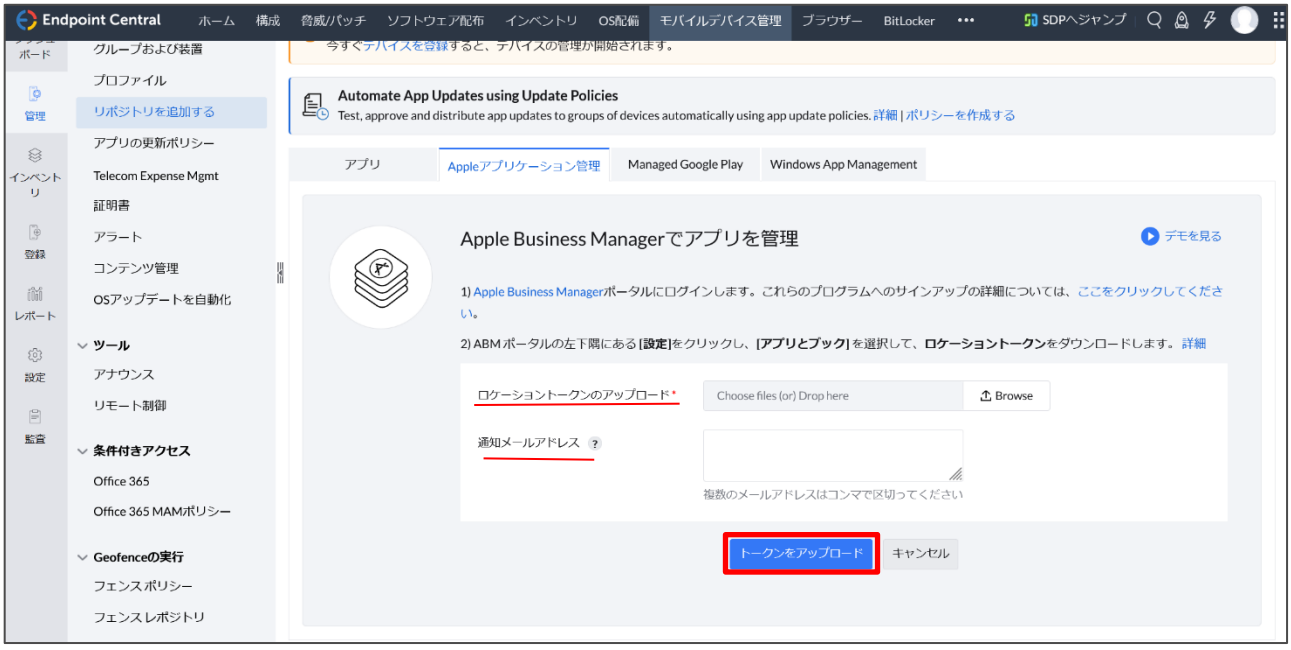

5. 画面から、サーバートークンをアップロードします。

- ロケーショントークンのアップロード

  上記でダウンロードした ABM サーバートークンを選択します。

- 通知メールアドレス

  トークンが有効期限切れした際に通知する宛先を入力します。




(C) ZOHO Japan Corporation. All rights reserved.

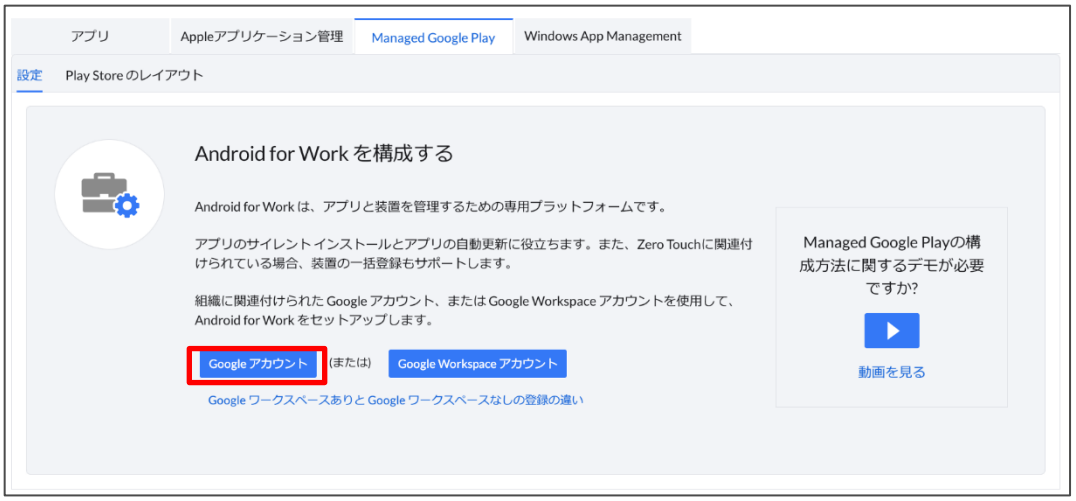
6. サーバートークンのアップロードが完了すると、トークンの詳細がコンソール上に表示されるようになり、ABM で購入されたアプリケーションがリポジトリに自動的に追加されます。


(C) ZOHO Japan Corporation. All rights reserved.

## Managed Google Play と同期

Google Workspace のアカウント、または Google のアカウントを用いて、Managed Google Play を構成することができます。本節では Google のアカウントを用いて設定を行う方法について説明します。

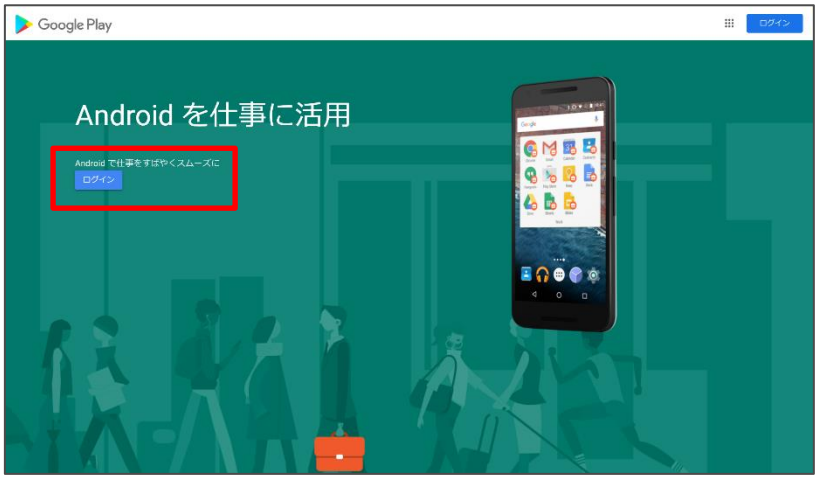
1. 「Google アカウント」→「今すぐ設定する」を選択します。



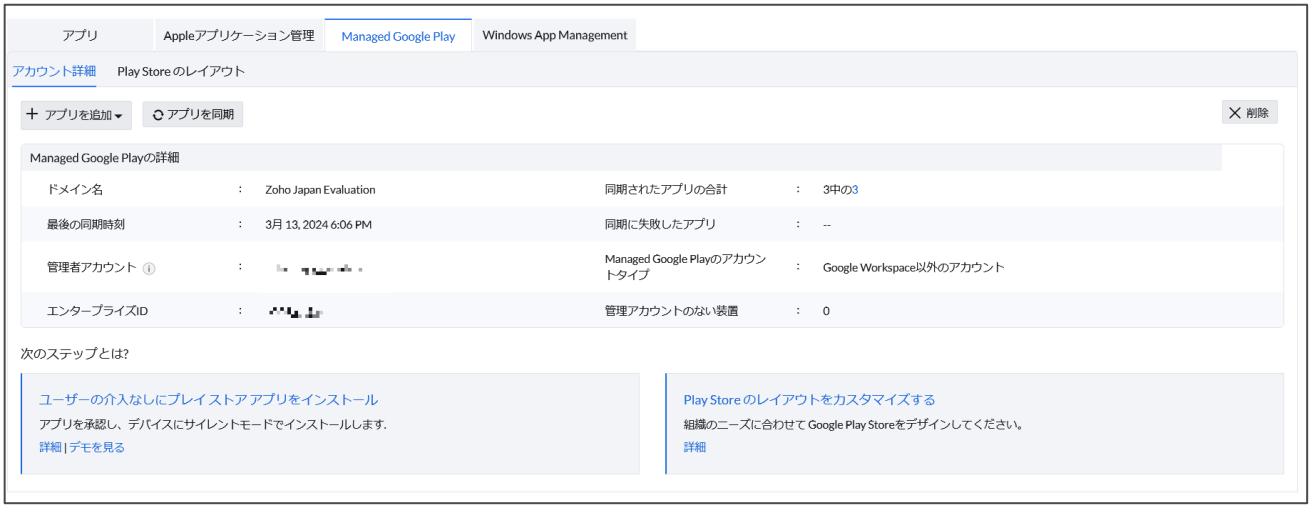


2. 外部サイト（Google Play）に移動します。画面の指示に従い、組織名、連絡先の情報を入力します。

(C) ZOHO Japan Corporation. All rights reserved.




3. 設定完了後、Managed Google Play と同期されます。




(C) ZOHO Japan Corporation. All rights reserved.

## 5 - 2 リポジトリの関連付け

リポジトリに追加したアプリケーションはグループまたはユーザーに配布することができます。アプリケーションの配布方法には以下の 2 種類あります。

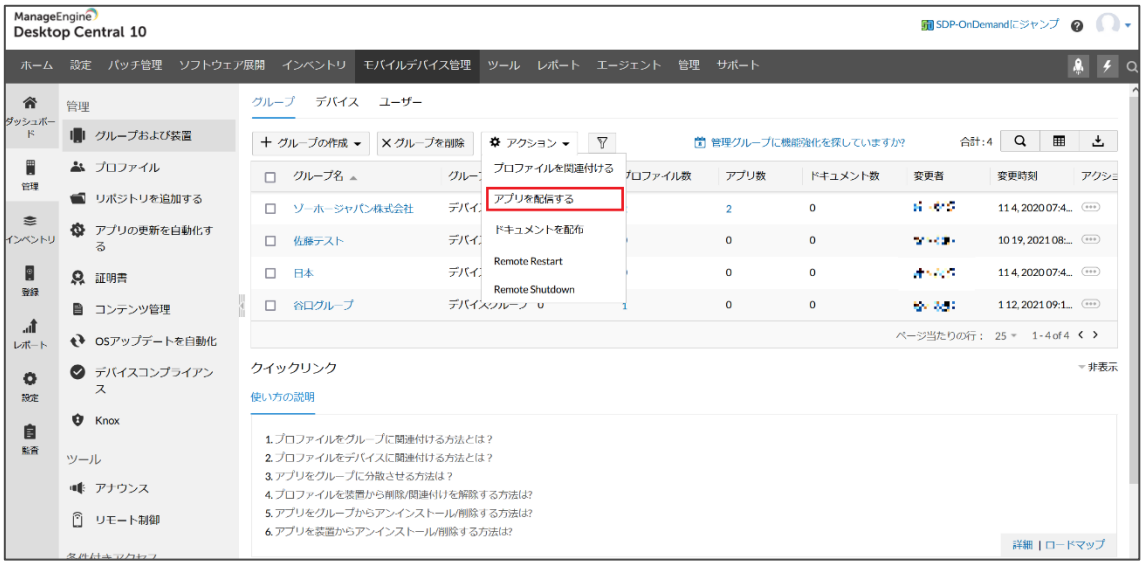
1. 端末の ManageEngine MDM アプリケーションにリストを公開し、ユーザーがそこにアクセスしてインストールする方法
2. ユーザーの操作を必要としないサイレントインストール

   サイレントインストールは、

   - 監視モードの端末に対して Apple Business Manager（ABM）から追加したアプリケーションを配布する場合（iOS）
   - デバイスオーナーの端末に対し Managed Google Play から追加したアプリケーションを配布する場合（Android）に有効です。

### 配布方法

1. 「管理」→「グループおよび装置」から「グループ」または「デバイス」をクリックします。
2. アプリケーションを配布するグループまたは端末名の、左にあるチェックボックスにチェックを入れ「アクション」から「アプリを配信する」を選択します。

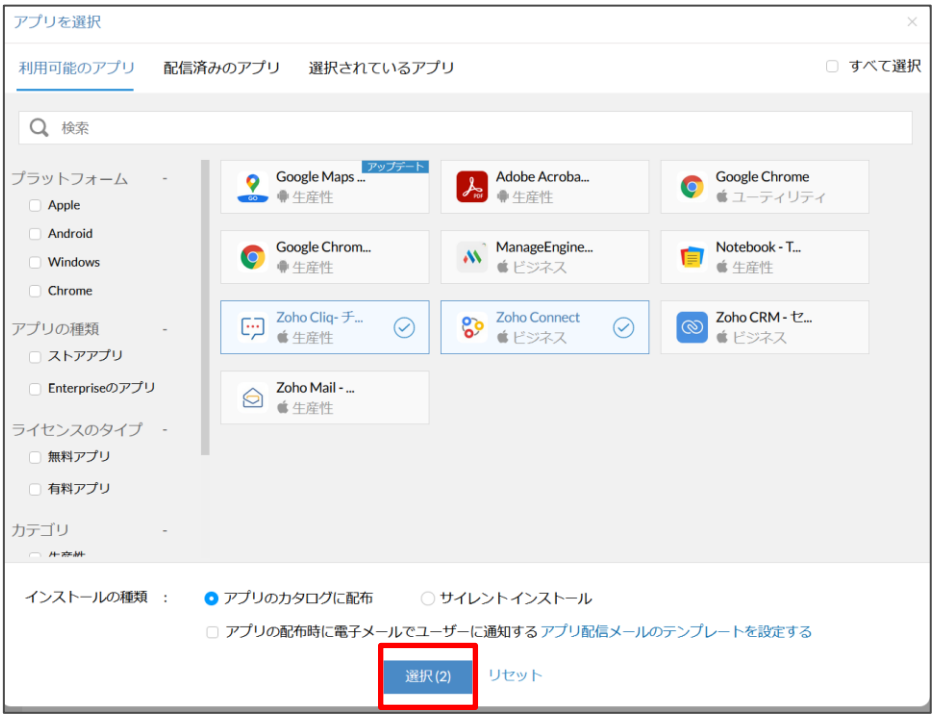



(C) ZOHO Japan Corporation. All rights reserved.

3. 配布するアプリ選択します。
4. インストールのオプションを選択します。
   - インストールの種類
     - ➢ カタログに配布

       アプリケーションを端末の ManageEngine MDM アプリケーションに表示し、ユーザーがそこにアクセスしてインストールします。
     - ➢ サイレントインストール

       Full device Management の端末に対し、サイレントインストールを実施します。端末が Workspace Management の場合は、プッシュインストール時に Apple store/Google アカウントのログインが必要です。
   - アプリの配布時に電子メールでユーザーに通知する
5. 設定完了後「選択」をクリックします。




以上で、端末が通信可能になると配信が実行されます。

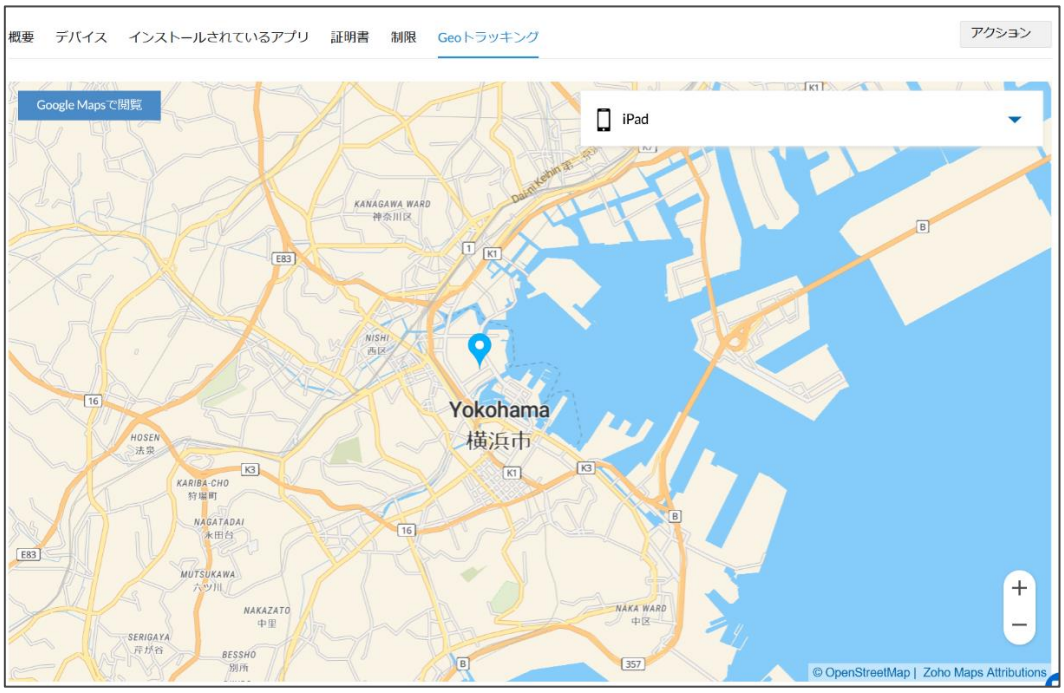
(C) ZOHO Japan Corporation. All rights reserved.

# 6 デバイスの位置情報とセキュリティ

本章では、デバイスの物理的な安全を保つための機能や、万が一端末を紛失したときに役立つ機能を紹介します。
位置情報機能を利用するためには、ManageEngine MDM アプリケーションに位置情報を常に許可する必要があります。

## 6 - 1 ジオトラッキング機能

IT 管理者はジオトラッキング機能によって管理デバイスの物理的な位置を知ることができます。本機能を利用するためには端末に ManageEngine MDM アプリケーションをインストールし、位置情報サービスを常に許可する必要があります。管理端末の位置情報は、「インベントリ」→「デバイス」→デバイス名を選択→「Geo トラッキング」から確認することができます。




## 6 - 2 紛失モード

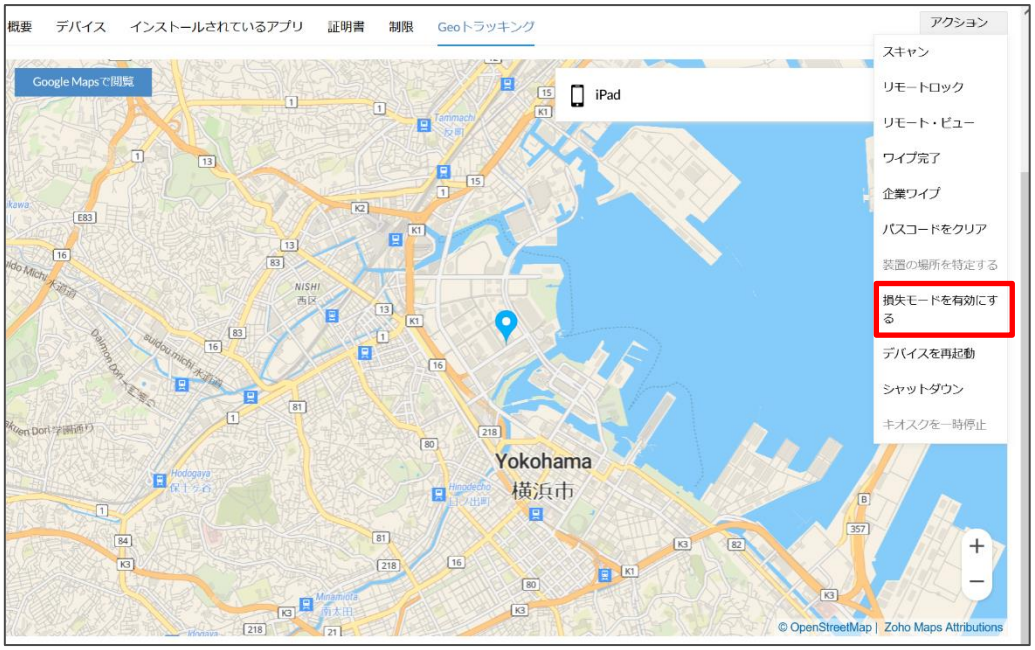
モバイルデバイスを紛失した際に**紛失モード**に設定することでリモートロックをかけ、スクリーン上にメッセージ、連絡を希望する電話番号、電話ボタンを表示することができます。

紛失モードの設定方法

iOS の画面を用いて説明しますが Android も設定方法は同様です。

1. 「インベントリ」→「デバイス」からデバイス名を選択します。
2. 「アクション」から「紛失モードを有効にする」を選択します。

(C) ZOHO Japan Corporation. All rights reserved.




3. 紛失モードに関する設定を行います。画面に表示する連絡先と、メッセージを入力して「次へ」をクリックします。

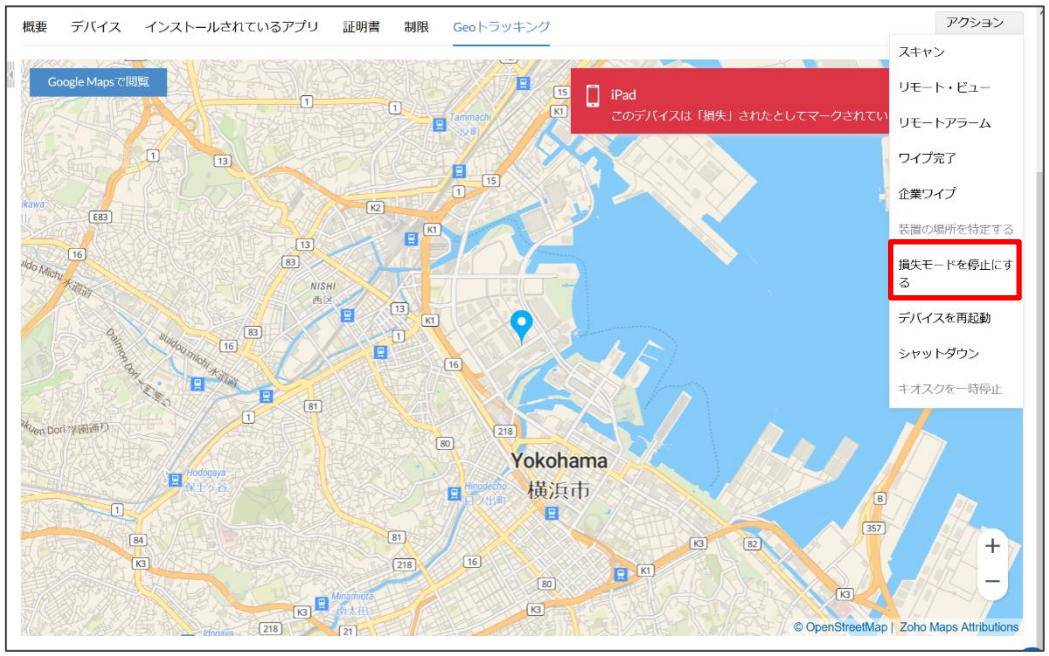

4. 紛失を社内で管理する番号がある場合はチケット ID を入力し、メッセージにメッセージを入力します。メッセージは監査ログに反映されます。入力後「探す」をクリックします。


(C) ZOHO Japan Corporation. All rights reserved.

5. 端末と通信が可能になると、紛失モードが有効になり、端末にロックがかかります。

紛失モードの解除方法

1. 「インベントリ」→「デバイス」から紛失モードのデバイスを選択します。
2. 「アクション」から「紛失モードを停止にする」を選択します。




## 6 - 3 リモートワイプ

端末の紛失時にデータ保護のためにデバイスのデータを遠隔から削除（ワイプ）することが可能です。ワイプには以下の 2 種類があります。なおデバイスポリシーによって機能が制限される場合がございます。

企業ワイプ

「インベントリ」→「デバイス」→デバイス名を選択→「アクション」から「企業ワイプ」を実行します。
企業ワイプでは MDM を利用して配布したアプリケーションやプロファイルのみを削除します。

完全ワイプ（「ワイプ完了」と表記されている箇所がございます）

「インベントリ」→「デバイス」→デバイス名を選択→「アクション」から「完全ワイプ（ワイプ完了）」を実行します。
完全ワイプでは端末のデータを完全に削除し、初期化します。
＊iPhone のアクティベーションロックが有効な場合、初期化後に登録してある Apple ID でログインが必要になります。そのため初期化時には、端末の Apple ID を予め調査したうえでご使用ください。

(C) ZOHO Japan Corporation. All rights reserved.


## 6 - 4　ジオフェンシング機能

ジオフェンシングは位置情報を判定基準として、特定のアクションを端末に実行する機能です。ジオフェンシングを利用する手順は以下の通りです。

まずフェンスリポジトリからジオフェンスを作成します。ジオフェンスは地球表面上の任意の 1 点を中心とした円の領域です（半径 1m から 500km まで設定可能）。つぎにフェンスポリシーから、ジオフェンスを基準にしたコンプライアンスルールを定義し、ルールに合致する端末に対する操作を決定します。最後にフェンスポリシーをグループまたは装置に関連付けします。

### フェンスリポジトリ

ジオフェンスの作成方法は以下の通りです。

1. 「管理」→「フェンスリポジトリ」→「フェンスを作成」を選択します。


(C)　ZOHO Japan Corporation. All rights reserved.

2. フェンスの設定項目

- 緯度と経度

  ジオフェンスの中心点を指定します。直接、数値を入力するか、検索窓から指定します。

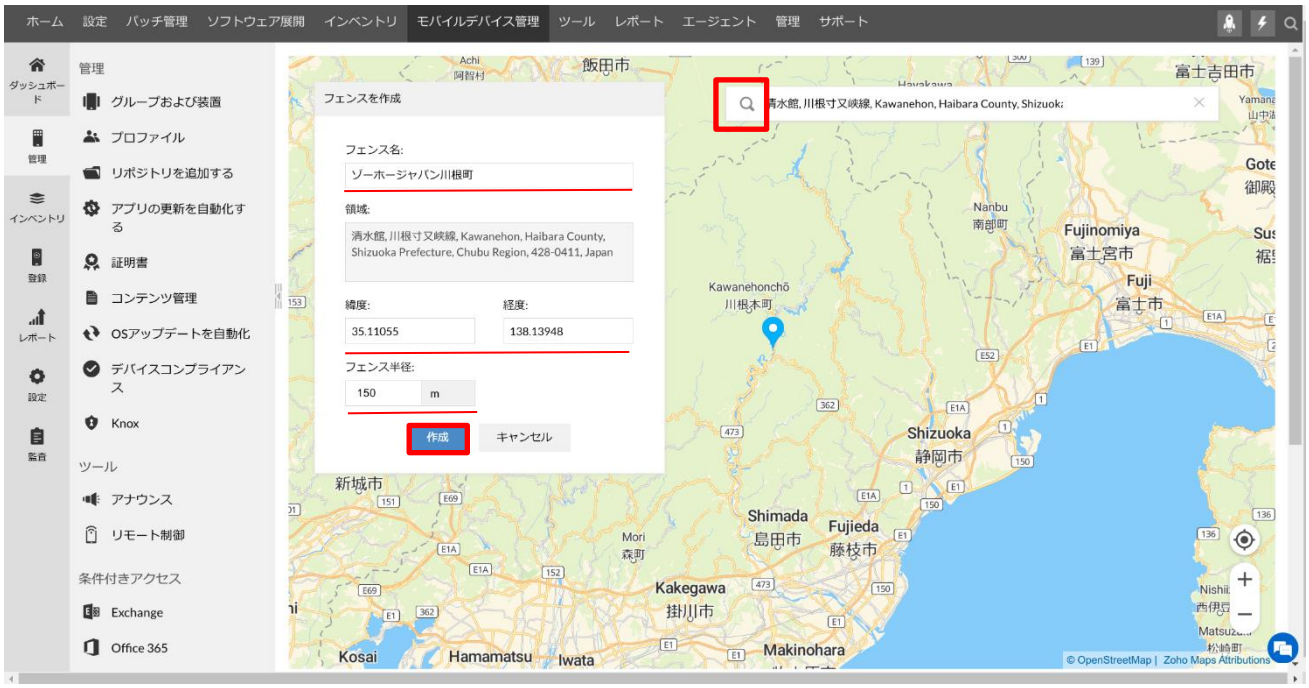
- フェンス半径

  中心点からフェンス半径を半径とした円の領域がジオフェンスになります。

- フェンス名

  フェンスの名前を設定します。

3. 設定完了後「作成」をクリックします。




以上でジオフェンスの作成が完了します。

(C) ZOHO Japan Corporation. All rights reserved.

フェンスポリシー

フェンスポリシーではジオフェンスを用いてコンプライアンスルールを定義し、それに合致する端末（非準拠装置と呼びます）に対する操作を決定します。

1. 「管理」→「フェンスポリシー」から「ポリシーを作成する」をクリックします。
2. ジオフェンスを用いて、コンプライアンスルールを定義します。
   - 次の場合、装置は非準拠とみなされます

     事前に定義したジオフェンスを選択します。
   - 条件の選択

     「Within（次の～以内に）」または「以内にない」を選択します。「Within（次の～以内に）」の場合ジオフェンスに端末が存在するとき、「以内にない」の場合ジオフェンスに端末が存在しないときに、非準拠装置となりアクションが実行されます。


(C) ZOHO Japan Corporation. All rights reserved.

3. 非準拠装置に対してトリガーされるアクションを定義しますから非準拠装置に対するアクションを決定します。

頻度を選択でアクションを実行するタイミングを「今すぐ」または「一日の後」から選択します。実行できるアクションの種類は頻度の設定によって差異があります（下表）。つぎにアクションタイプを選択してくださいとアクションを選択から実行するアクションを決定してください。

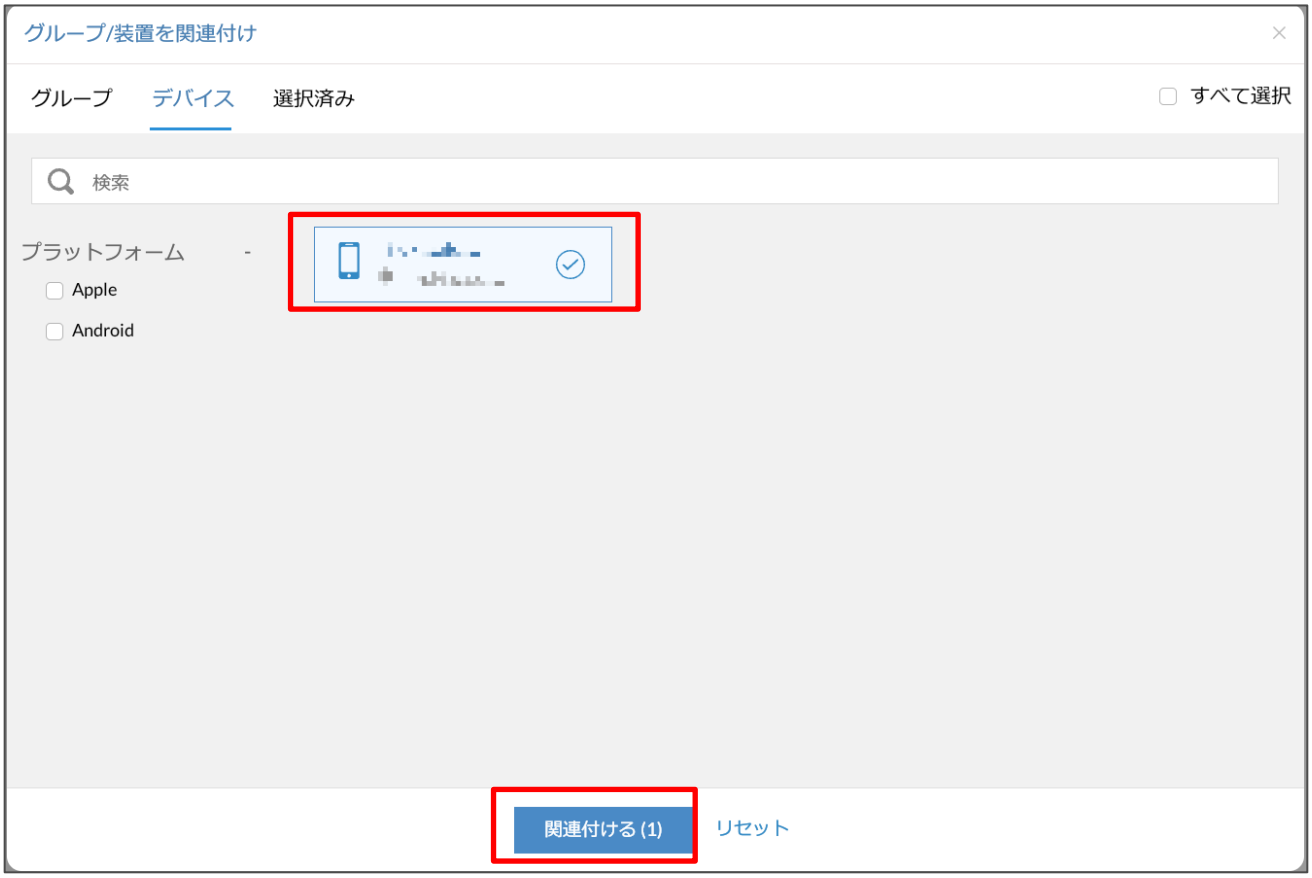
| 頻度 ＼アクション | メールを管理者に送る | 紛失モード | 完全ワイプ（ワイプ完了）<br>Complete wipe | ワイプ＋SD カード完了<br>Complete wipe + SD card |
|---|---|---|---|---|
| 今すぐ | ○ | ○ | × | × |
| 一日の後 | ○ | ○ | ○ | ○ |


## フェンスポリシーの関連付け

1. 「管理」→「フェンスポリシー」→作成済みのポリシー右上の ボタンから「グループ/装置を関連付け」をクリックします。


(C) ZOHO Japan Corporation. All rights reserved.

2. フェンスポリシーを関連付けるグループまたは装置を選択します。




以上でフェンスポリシーの関連付けが完了します。

## 7 製品のお問い合わせ先

ManageEngine Endpoint Central Cloud に関するご質問、ご購入の相談は下記までお問い合わせください。

製品提供元

ゾーホージャパン株式会社
神奈川県横浜市西区みなとみらい 3-6-1 みなとみらいセンタービル 13 階
Tel: 045-319-4612（ManageEngine 営業担当）
Web サイト https://www.manageengine.jp/products/Endpoint_Central/mobile-device-management.html
E-mail: jp-mesales@zohocorp.com

©ZOHO Japan Corporation. All rights reserved