

# 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

## 内容

---

1 はじめに.....	4
1 - 1 本ガイドの目的.....	4
1 - 2 MDM のサポート OS .....	4
2 モバイルデバイス管理タブについて .....	5
2 - 1 管理タブの概要.....	5
2 - 2 MDM タブにアクセス可能なユーザー .....	6
3 登録 .....	8
3 - 1 プラットフォーム共通の登録方法 .....	9
製品ユーザーまたは招待による登録 .....	9
自己登録 .....	12
3 - 2 iOS の登録方法 .....	13
APNs 証明書の登録.....	13
Apple Business Manager/Apple School Manager を利用した登録.....	15
Apple Configurator による登録.....	20
監視モード (Supervised mode) .....	25
3 - 3 Android の登録方法 .....	26
EMM トークン .....	26
管理タイプ .....	28
3 - 4 登録設定 .....	29
3 - 5 デバイスピリシー.....	30
3 - 6 ユーザーの再割り当て .....	31
4 プロファイル .....	32
プロファイルの作成.....	32
プロファイルの関連付け .....	33
5 アプリケーション .....	34
5 - 1 リポジトリへ追加 .....	34
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 .....	34
Apple Business Manager (ABM) と同期 .....	40
Managed Google Play と同期 .....	43
5 - 2 リポジトリの関連付け .....	45
配布方法 .....	45
6 デバイスの位置情報とセキュリティ .....	47

6 - 1 ジオトラッキング機能 .....	47
6 - 2 紛失モード .....	47
6 - 3 リモートワイプ .....	49
6 - 4 ジオフェンシング機能 .....	50
フェンスリポジトリ .....	50
フェンスポリシー .....	52
フェンスポリシーの関連付け .....	53
7 製品のお問い合わせ先 .....	54

**■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。

## 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

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](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。

## 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。

## 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。



The screenshot shows the 'User Management' section of the Endpoint Central interface. On the left, there is a sidebar with various navigation options. The main area displays a table of users with columns for 'User Name', 'Email', 'Phone Number', 'Role Name', 'Status', and 'Actions'. A red box highlights the 'Add User' button at the top left of the table area.

「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：



The screenshot shows the 'Add User' wizard. It consists of two main steps: 'Step 1: User Information' and 'Step 2: Scope Definition'. In Step 1, fields for 'Email\*', 'User Name\*', 'Role\*', and 'Phone Number' are shown. In Step 2, under 'Managed Devices', the 'All Devices' radio button is selected. At the bottom of Step 2, a red box highlights the 'Add User' button.

- 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。

- 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

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。

特定の役割を持つ製品へのアクセスが必要なユーザーを含めます。			
ユーザー	役割	安全な認証	
+ 役割の追加			合計: 5 <input type="button" value="検索"/>
名前	説明	作成者	アクション
Administrator	には完全なアクセス権限があります	System	<input type="button" value="..."/>
Auditor	にはレポートへのアクセス権限があります	System	<input type="button" value="..."/>
Guest	には読み取りのみのアクセス権限があります	System	<input type="button" value="..."/>
IT Asset Manager	には資産管理モジュールへのアクセス権限...	System	<input type="button" value="..."/>
Technician	には制限されたアクセス権限があります	System	<input type="button" value="..."/>

ページ当たりの行: 25 1-5 of 5 < >

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。

ステップ1: 役割を定義する

役割の名称:

説明: 特殊文字: 「<>[]」は許可されていません

手順2: MDMコントロールを選択

Configure permissions to access and manage different modules. [Learn More.](#)

モジュール名	フルコントロール	書き込む	読み取り	アクセスなし
登録	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
プロファイル管理	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
アプリケーション管理	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
コンテンツ管理	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Group Management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
イベント	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
OSアップデート管理	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
リモート制御	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

フルコントロール	書き込む	読み取り	アクセスなし
モジュール内での、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。

### 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](https://www.manageengine.jp/support/kb/Desktop_Central_Cloud/?p=1689)

### 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

- 「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。

デバイス名	要求時間	登録時間	状態	備考	アクション	登録元
iPhone	2021/10/25 10:25	2021/10/25 10:25	登録済み	デバイスが正常に登録されました。	招待!	
Android	2021/10/32 3:25	2021/10/32 3:25	登録済み	このデバイスは非アクティブです。	招待!	
Windows Phone	2020/11/11 11:9	2020/11/11 11:9	登録済み	このデバイスは非アクティブです。	招待!	

- (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）。



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

## (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ピ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

## 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。

Integrate your directory from Microsoft Active-Directory, Office365(Azure), Okta, G-Suite.  
Automate deployment of directory based services and replicate your directory structure in MDM for ease of management with [Directory Integration](#).

**Self Enrollment Settings**

自己登録を使用してデバイスを登録すると、パーソナルスペースに対する制御をゼロにして企業空間のみを管理できます。このメソッドで登録済みの装置は、デフォルトでは、個人用装置と見なされます。

認証モード : Zoho認証

次の事項に対する自己登録を許可する : すべてのグループ

Restricted Platforms :

ユーザー毎の許可された装置個数 ? : 無制限

E-mail notification when a device is enrolled through Self Enrollment :

Apple User Enrollment : 無効

グループの自動割り当て

Devices that don't match the below criteria will be marked as **unassigned** and will have to be manually added to respective groups. [Learn more](#)

**プラットフォーム**

Apple :

Android :

Windows :



Scan the QR code to Enroll the BYOD devices.

または

Access the URL from devices to be enrolled.  
<https://znode...>



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。

### 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。



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。

APNsをAppleポータルに作成してください

APNs証明書をMDMサーバーにアップロード

ヘルプ | トラブルシューティングのヒント

APNsの作成に使用する本社Apple ID\*: [Redacted]

組織名\*: ゾーホージャパン

APN有効期限のメール通知\*: [Redacted]

複数のメールアドレスはコンマで区切ってください

前へ **アップロード**

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。

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。

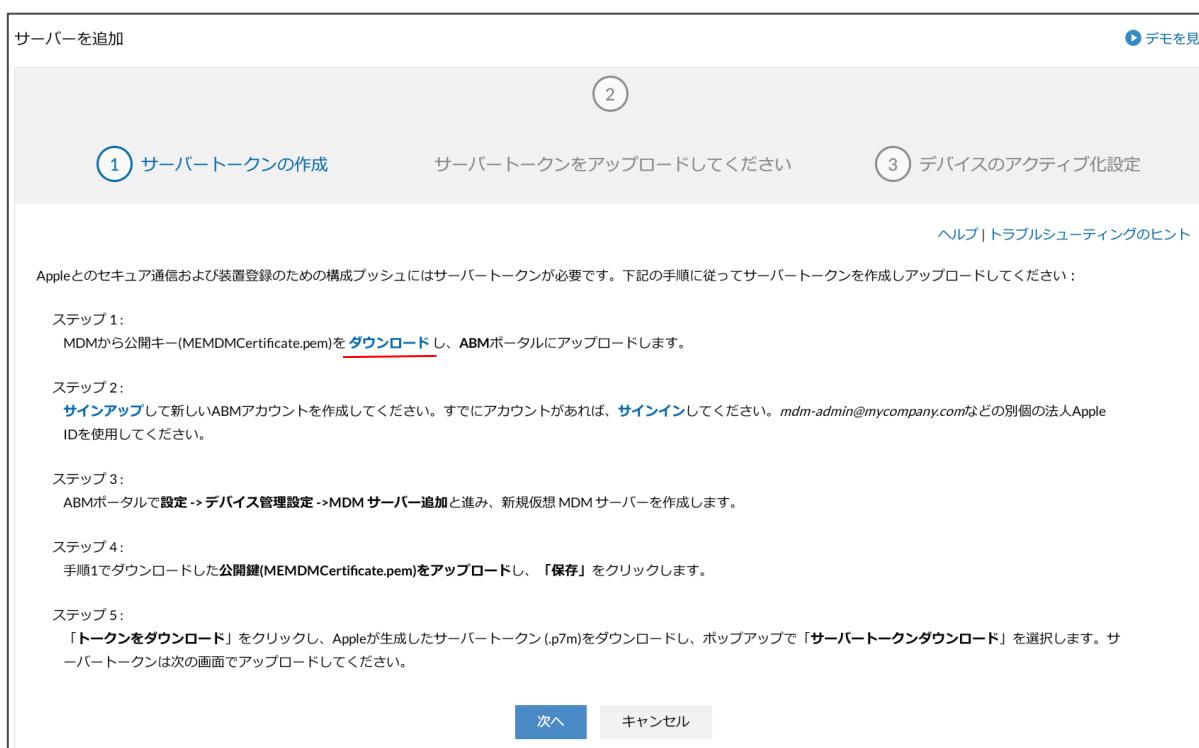
以下、本書では ABM を利用した場合について設定方法を説明します。ASM の場合も手順は同様ですので、必要に応じて ABM を ASM に読み替えてください。

### MDM サーバーと ABM の連携方法

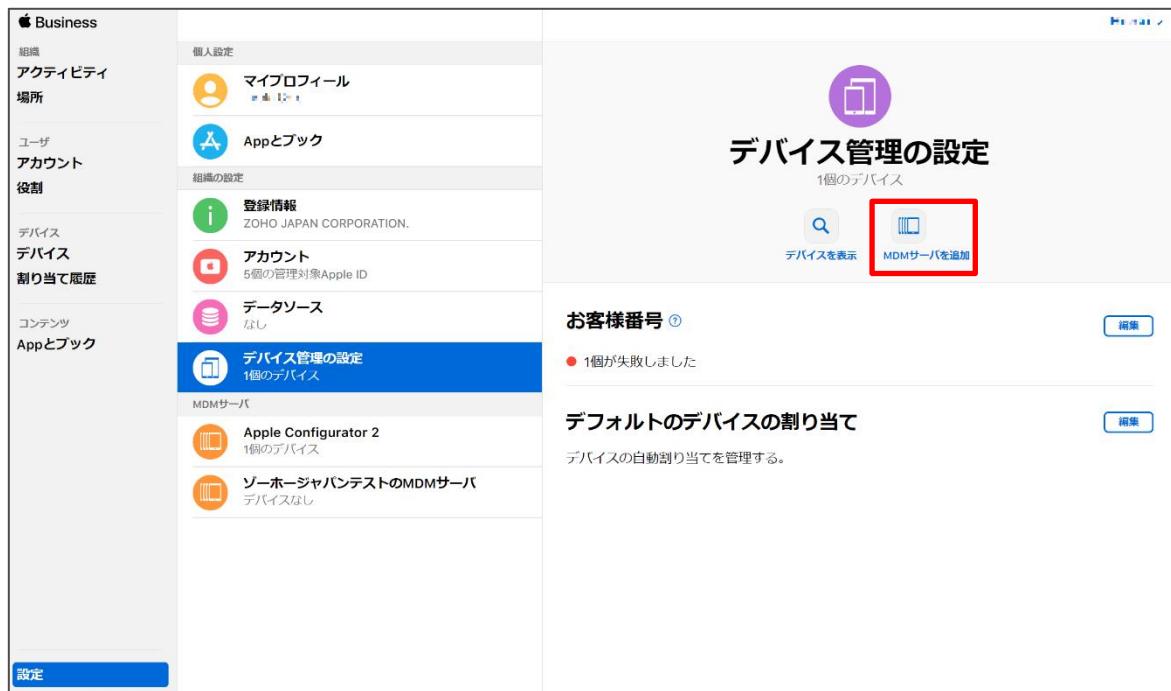
- 「登録」→「Apple 登録(ABM/ASM)」→「装置を法人用に登録」を選択します。



- 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。



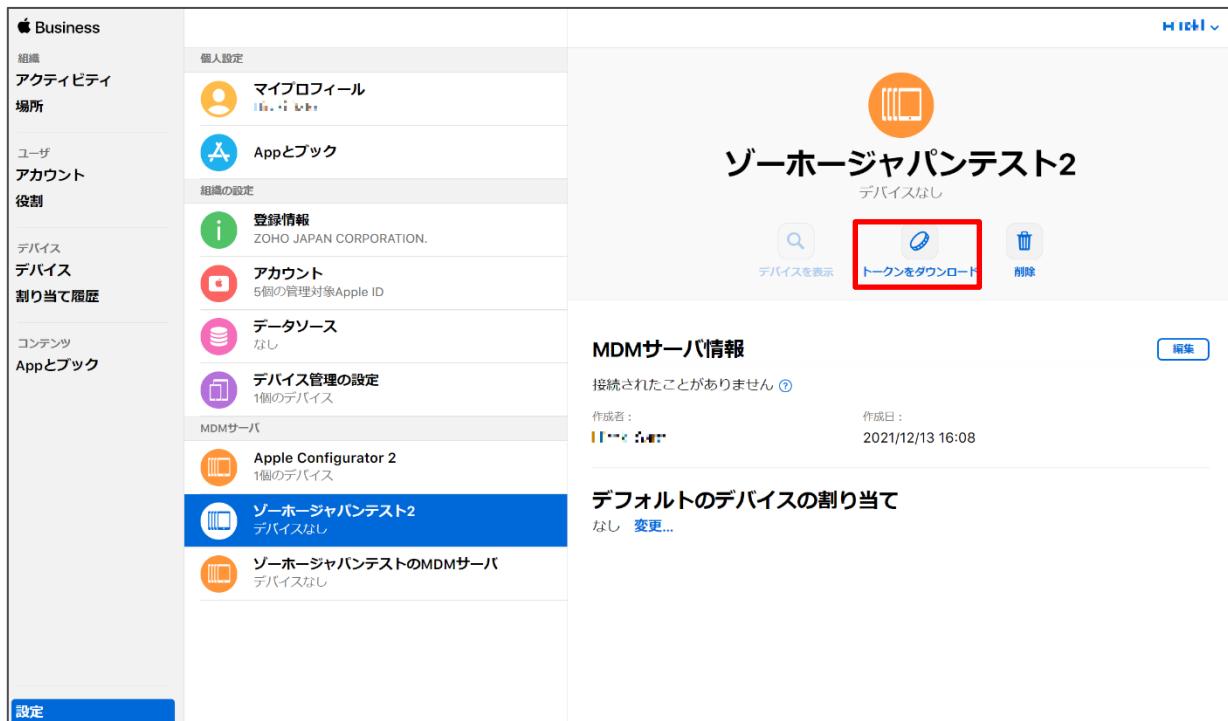
3. ABM ポータルにログインし、「設定」→「デバイス管理の設定」→「MDM サーバーの追加」をクリックします。



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。



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。



Apple Business

組織  
アクティビティ  
場所

ユーザ  
アカウント  
役割

デバイス  
デバイス  
割り当て履歴

コンテンツ  
Appとブック

設定

個人設定  
マイプロフィール

Appとブック

組織の設定  
登録情報  
ZOHO JAPAN CORPORATION.

アカウント  
5個の管理対象Apple ID

データソース  
なし

デバイスマネジメント  
1個のデバイス

MDMサーバ  
Apple Configurator 2  
ゾーホージャパンテスト2  
ゾーホージャパンテストのMDMサーバ

ゾーホージャパンテスト2  
デバイスなし

ゾーホージャパンテストのMDMサーバ  
デバイスなし

ゾーホージャパンテスト2  
デバイスなし

デバイスなし

MDMサーバ情報  
接続されたことがありません  
作成者：  
作成日：  
2021/12/13 16:08

デフォルトのデバイスの割り当て  
なし [変更...](#)

デバイスなし

トークンをダウンロード



① サーバートークンの作成

② サーバートークンをアップロードしてください

③ デバイスのアクティブ化設定

ヘルプ | ブラウザのヒント

Appleとのセキュア通信および装置登録のための構成プロファイルにはサーバートークンが必要です。下記の手順に従ってサーバートークンを作成しアップロードしてください：

ステップ1：  
MDMから公開キー(MEMDMCertificate.pem)を [ダウンロード](#) し、ABMポータルにアップロードします。

ステップ2：  
サインアップして新しいABMアカウントを作成してください。すでにアカウントがあれば、サインインしてください。[mdm-admin@mycompany.com](mailto:mdm-admin@mycompany.com)などの別の法人Apple IDを使用してください。

ステップ3：  
ABMポータルで設定 -> デバイスマネジメント -> MDM サーバー追加と進み、新規仮想 MDM サーバーを作成します。

ステップ4：  
手順1でダウンロードした公開鍵(MEMDMCertificate.pem)をアップロードし、「保存」をクリックします。

ステップ5：  
「トークンをダウンロード」をクリックし、Appleが生成したサーバートークン(.p7m)をダウンロードし、ポップアップで「サーバートークンダウンロード」を選択します。サーバートークンは次の画面でアップロードしてください。

次へ

キャンセル

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

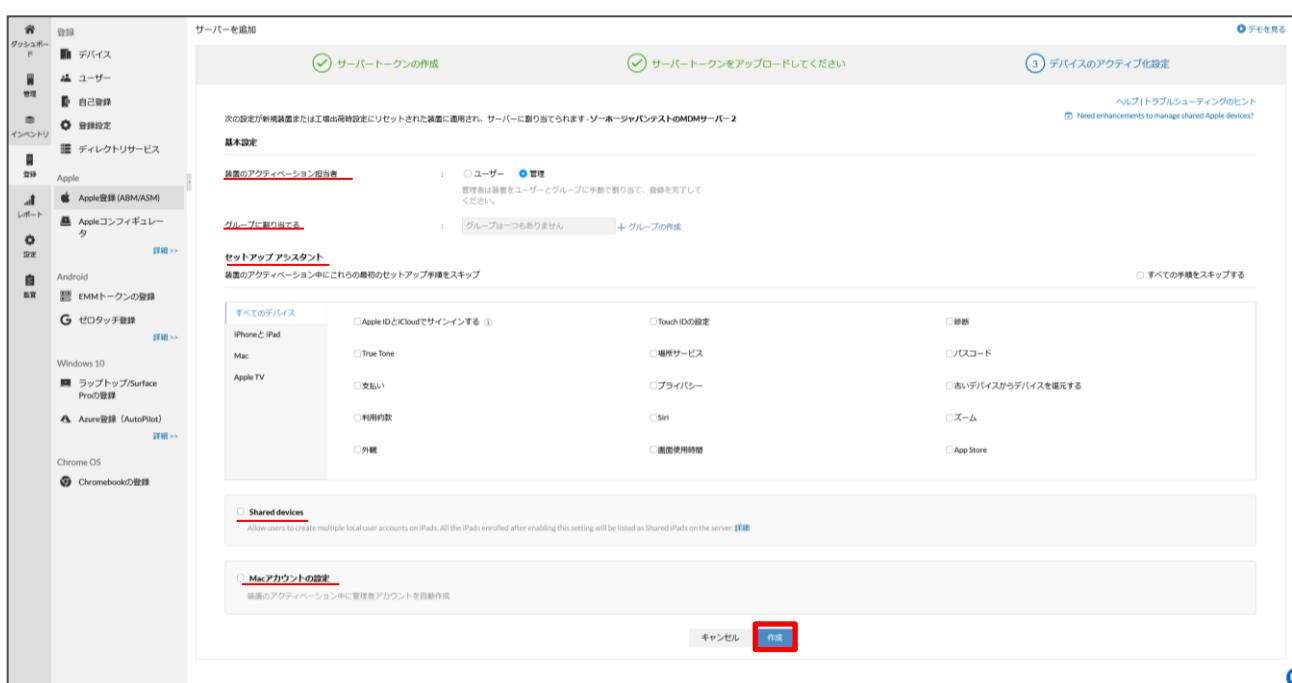
「ユーザー」または「管理」（=製品ユーザー）を選択します。

- 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。



- 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。

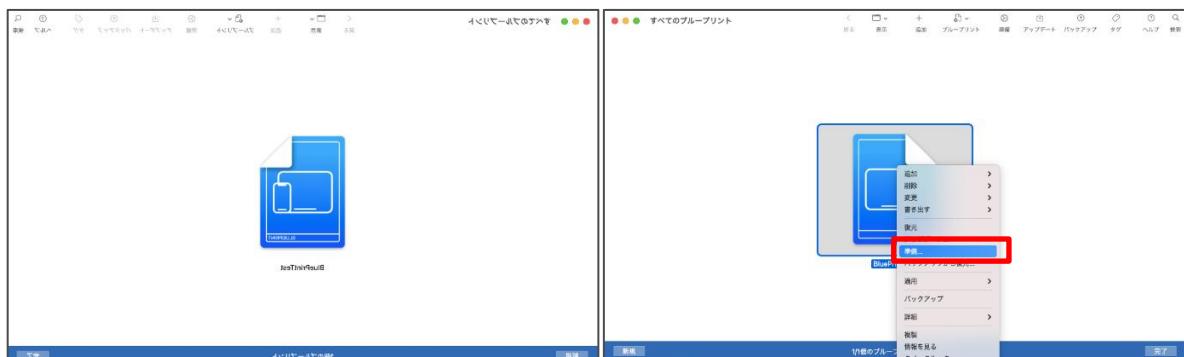
## Apple Configurator による登録

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。

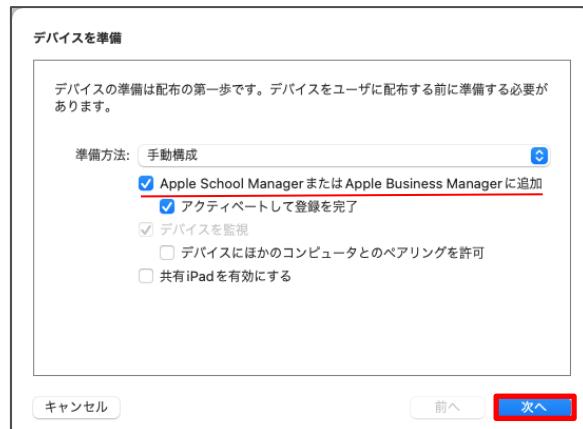
1. App Store から Apple Configurator 2 をダウンロードします。
2. 自動的に Wi-Fi に接続するプロファイルを必要に応じて作成します（このプロファイルは端末の初期化後に必要に応じて利用します）。「ファイル」→「新規プロファイル」をクリックして、左メニューから Wi-Fi を選択し、SSID や、セキュリティの種類、パスワードなど必要な情報を入力してください。入力後、「ファイル」→「保存」からプロファイルを保存します。



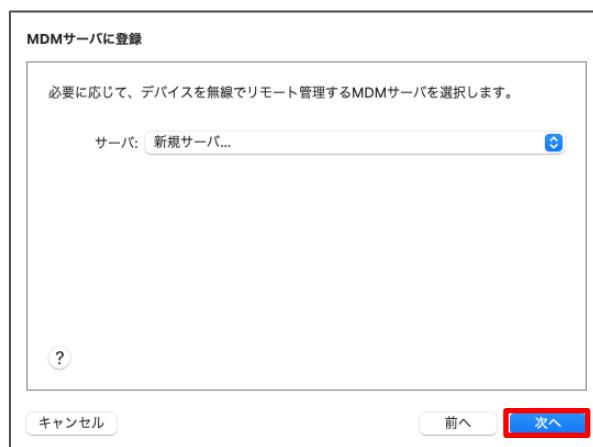
3. 「ファイル」→「新規ブループリント」をクリックし、新しいブループリントを作成します。その後、右クリックを押し、「準備」をクリックします。



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。



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。

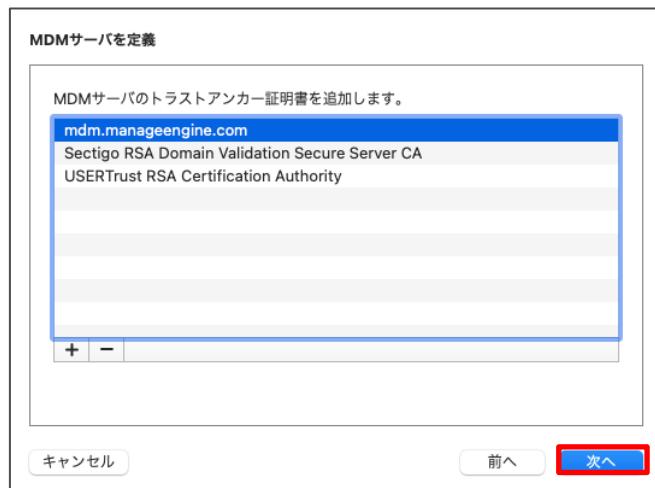


6. サーバー名を入力します。URL は、コンソール画面の「モバイルデバイス管理」タブ→「登録」→「Apple コンフィギュレーター」に表示されている URL を入力してください。





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。

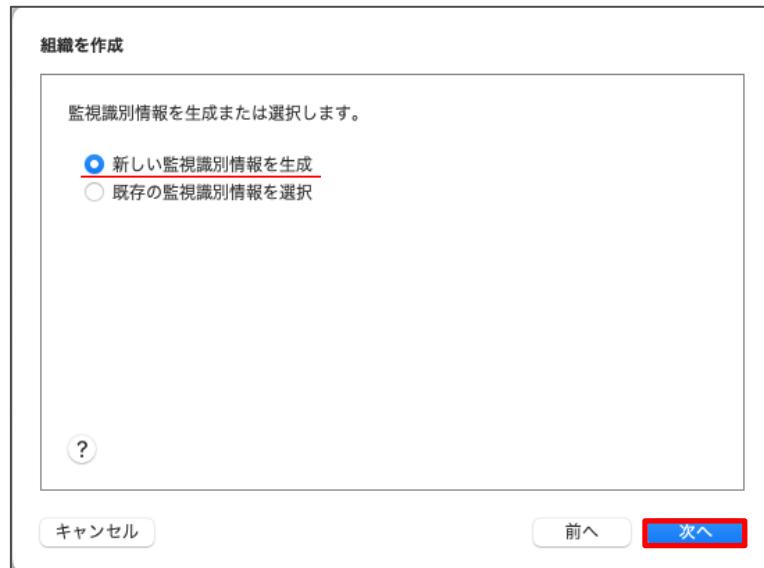


8. ABM のアカウント情報を入力します。



9. 組織に関する詳細を入力し、「次へ」をクリックします。

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。



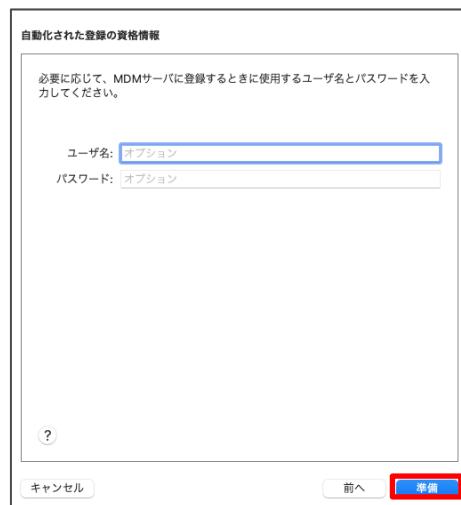
11. 「iOS 設定アシスタントを構成」でデバイスの初期化時に、ユーザーが設定を行う項目を選択します。



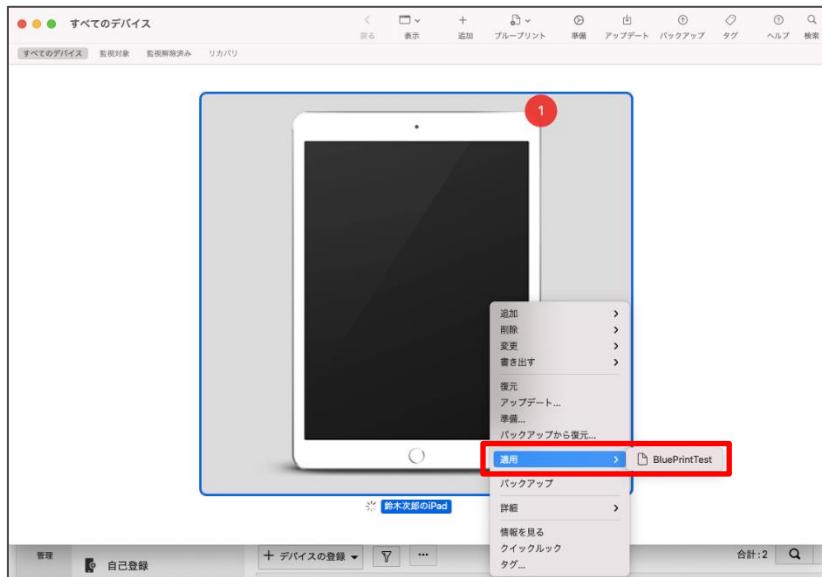
12. デバイスが登録を完了するためには、ABM および MDM サーバーとの通信が必要です。「ネットワークプロファイルを選択」で必要に応じて、ステップ 1 で作成した Wi-Fi の設定プロファイルを選択し、「次へ」をクリックします。



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。



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。

## 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。



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。



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。

## 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

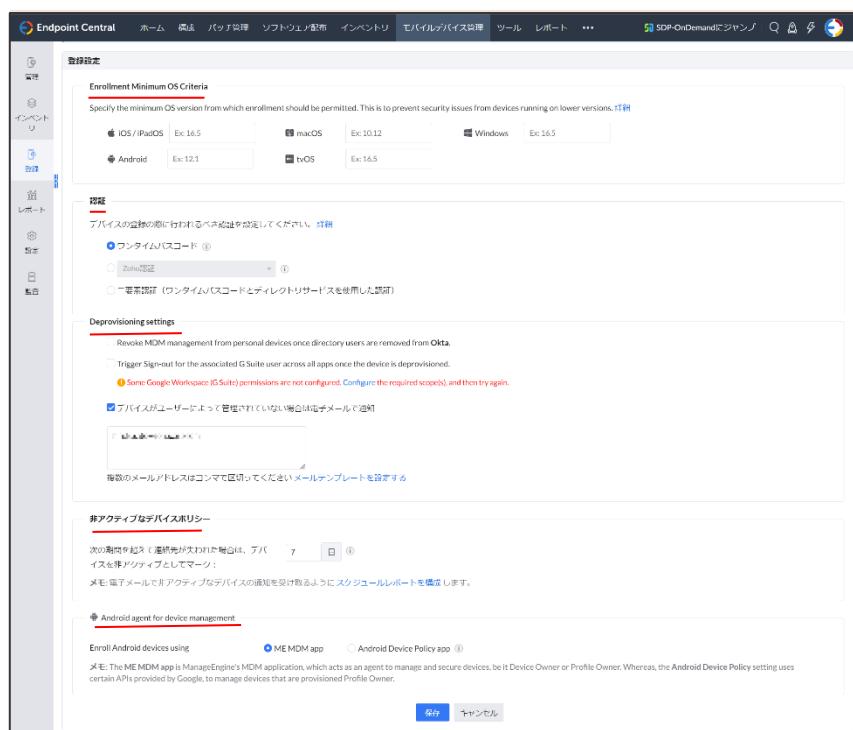
登録デバイスのプロビジョニング解除に関する設定です。Okta からユーザーが削除された際のデバイスのプロビジョニング解除と、ManageEngine MDM の削除（Android）または MDM プロファイルの削除（iOS）を行った際の管理者への通知を設定できます。

- 非アクティブなデバイスピリシー

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

Android管理に使用するアプリケーションを選択します。



## 3 - 5 デバイスピリシー

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。



Androidデバイスを登録

登録するデバイス :  自分で  ユーザー招待を通じて

ユーザー\* : 

所有者\* :  個人  企業

グループに割り当てる : Select [+ グループの作成](#)

[次へ](#) [キャンセル](#)

## 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、これをデバイスピ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。



従業員が所有している装置に対するデフォルト設定 変更

**デバイスデータ**

- IMEI : 収集して表示
- シリアル番号 : 収集して表示
- 電話番号 : 回収しない
- Mac Address  ⓘ : 回収しない
- デバイス名 : 回収しない
- User Installed certificates  ⓘ : 回収しない  ⓘ
- ユーザーがインストールしたアプリ : 回収しない
- 地政学的場所 : 回収しない
- 装置の状態レポート  ⓘ  ⓘ  ⓘ : 回収しない
- 最近のユーザー報告  ⓘ  ⓘ  ⓘ : 回収しない

**リモートコマンド**

- ワイプ完了  ⓘ : 無効
- リモートビュー/コントロール : 無効
- バグレポート  ⓘ : 無効
- Reset Device Passcode  ⓘ : 無効

**ポリシー表示**

- ユーザーに表示可能 : はい

本社が所有している装置に対するデフォルト設定

**デバイスデータ**

- IMEI : 収集して表示
- シリアル番号 : 収集して表示
- 電話番号 : 回収しない
- Mac Address  ⓘ : 回収しない
- デバイス名 : 回収しない
- User Installed certificates  ⓘ : 回収しない  ⓘ
- ユーザーがインストールしたアプリ : 回収しない
- 地政学的場所 : 回収しない
- 装置の状態レポート  ⓘ  ⓘ  ⓘ : 回収しない
- 最近のユーザー報告  ⓘ  ⓘ  ⓘ : 回収しない

**リモートコマンド**

- ワイプ完了  ⓘ : 有効  !
- リモートビュー/コントロール : ユーザーによってコントロールされている
- バグレポート  ⓘ : ユーザーによってコントロールされている
- Reset Device Passcode  ⓘ : 有効

**ポリシー表示**

- デバイスに表示 : デバイスに表示

## 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。

- 「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。

- 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

- ユーザーを設定後、「割り当て」をクリックします。

## 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)を選択します。

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。

<p><b>監視対象装置</b> 監視により、セキュリティと制御のレベルが向上するため、Appleデバイスの高度な管理が可能になります。<a href="#">もっと詳しく知る</a></p>	<p><b>完全な装置管理(装置所有者)</b> 装置の所有者としてAndroid 6.0 以降を実行している装置を登録すると、高度な設定と管理機能を堪能できます。<a href="#">詳細</a></p>
--	--

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

## 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。

- 「管理」→「グループおよび装置」に移動します。
- 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	デバイス	ユーザー
+ グループの作成	×	×
×	×	×
□ グループ名	グループ	プロファイルを関連付ける
□ デバイス	デバイス	アプリを配信する
□ デバイス	デバイス	コンテンツを配布する
□ デバイス	デバイス	リモート再起動
□ デバイス	デバイス	リモートシャットダウン
□ デバイス	デバイス	アプリデータをクリアする
□ デバイス	デバイスグループ	

グループに対してプロファイルを関連付ける場合

- 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を選択し、画面の「すべてをアップグレードする」をクリックします。

プロファイルバージョン	古いバージョンのデバイス	割当てグループ	連携デバイス
4	1	0	1

## 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。

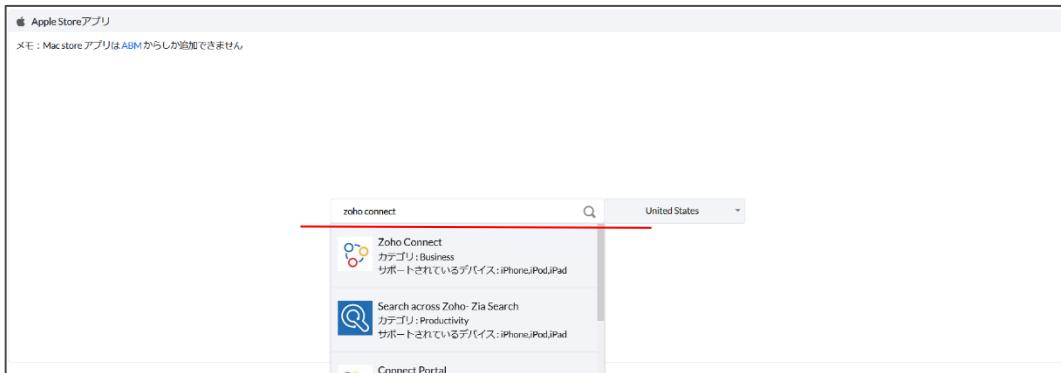
コンソール画面からストアにアクセスしアプリケーションを検索して追加する方法

1. 「管理」→「リポジトリを追加する」をクリックします。

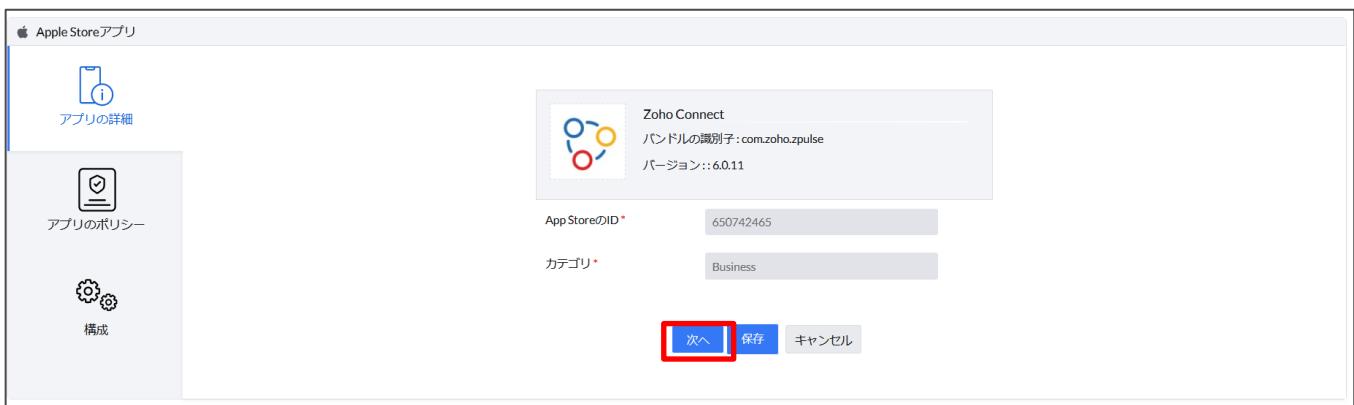
2. 「+アプリを追加する」から、「Apple Store アプリ」（iOS の場合）または「Play Store App」（Android の場合）を選択します。「Play Store App」（Android の場合）は、さらに Managed Google play を設定している場合とそうでない場合で、方法がやや異なります。

アプリ	プラットフォームの種類	アプリの種類	最新のバージョン	サポートされているデバイス	変更時刻	アクション	アプリのカテゴリ
Apple アプリ	Apple	Apple Store アプリ	24.02.01	iPhone,iPod,iPad	22 2024 05:52 午後	...	ビジネス
Apple Store アプリ	Apple	Apple Enterprise アプリ	24.02.30.0	スマートフォン、タブレット	22 2024 05:52 午後	...	BUSINESS
Android Apps	Android	Android ストアアプリ	6.2.5	スマートフォン、タブレット	2 2024 05:52 午後	...	PRODUCTIVITY
Play Store App	Android	Android ストアアプリ	1.0	Mac	26 2024 11:09 午後	...	ビジネス
Android Enterprise App	Apple	Apple Enterprise アプリ	1.0	スマートフォン	8 24, 2023 06:48 午後	...	生産性
Windows アプリ	Android	Android Enterprise App	1.0	スマートフォン	8 24, 2023 06:48 午後	...	生産性
Windows 企業アプリ	Apple	Apple Store アプリ	1.33.0	iPhone,iPod,iPad	8 21, 2023 12:55 午後	...	ゲーム
MSI アプリケーション	Android	Android ストアアプリ	2.4.24.1	スマートフォン、タブレット	12 1, 2021 06:31 午後	...	生産性
Chrome OS アプリ	Android	Android ストアアプリ	96.0.4664.45	スマートフォン、タブレット	12 1, 2021 06:31 午後	...	生産性
Chrome ネイティブ アプリ	Android	Android ストアアプリ	...	スマートフォン、タブレット	11 25, 2021 07:06 午後	...	生産性
Chrome カスタム アプリ	Android	Android ストアアプリ	...	スマートフォン、タブレット	11 25, 2021 07:06 午後	...	生産性

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。



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。

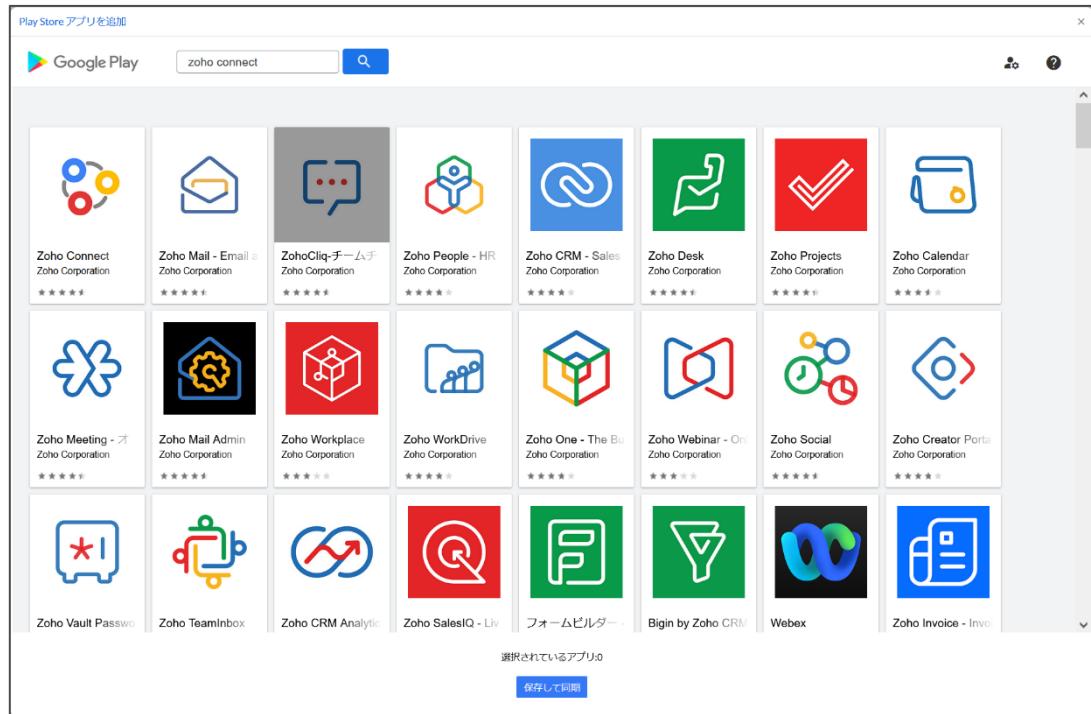
\*アプリの識別子の取得方法

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。

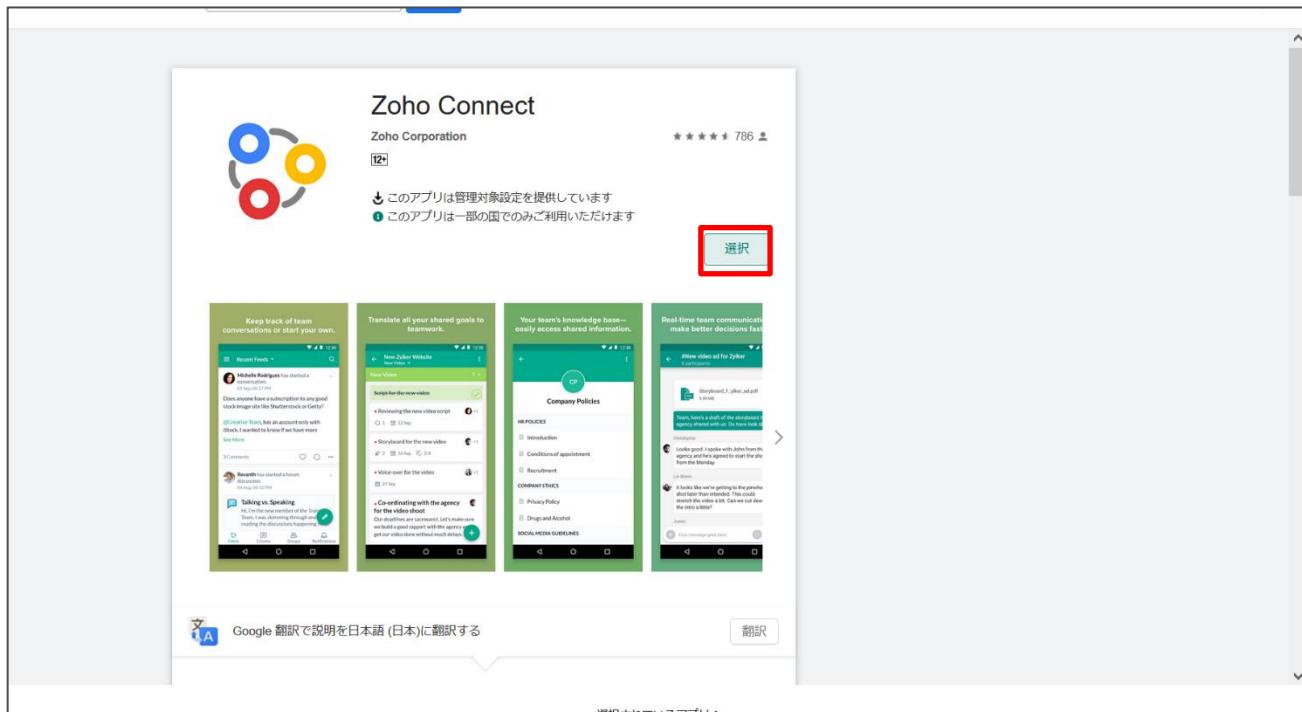
(例) Google Chrome の場合、識別子は’com.android.chrome’になります。



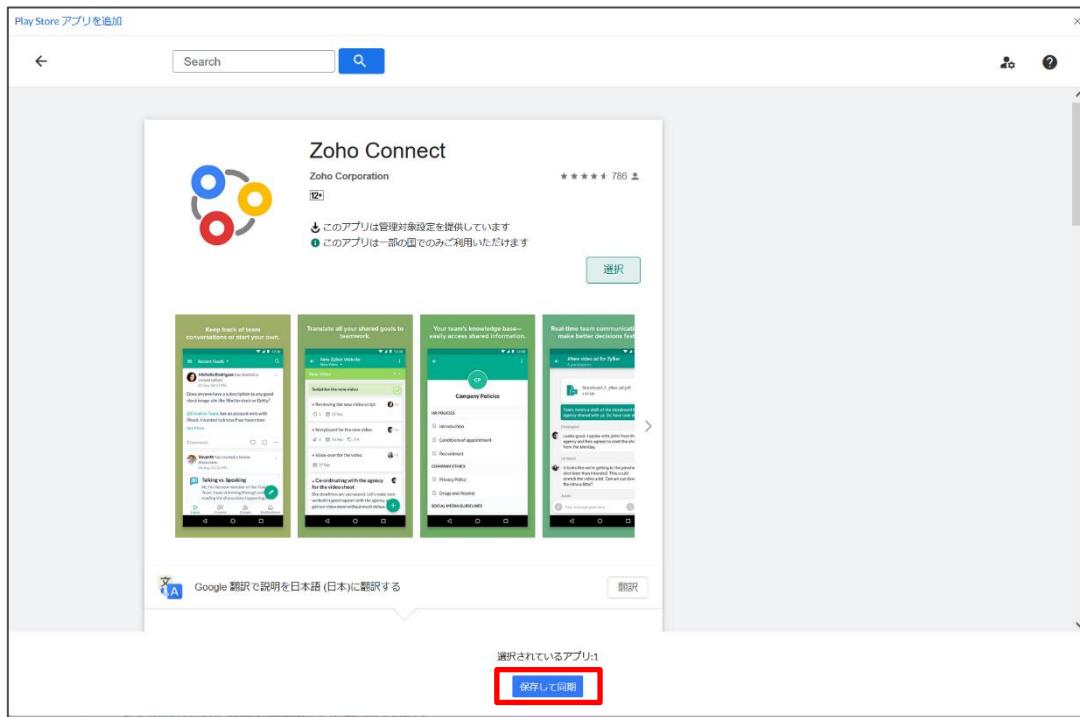
2-2-2 「Play Store App」(Android の場合)かつ Managed Google Playを設定済みの場合  
 「Play Store App」を選択し、アプリケーション名を検索窓に入力します。



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。



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。



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。

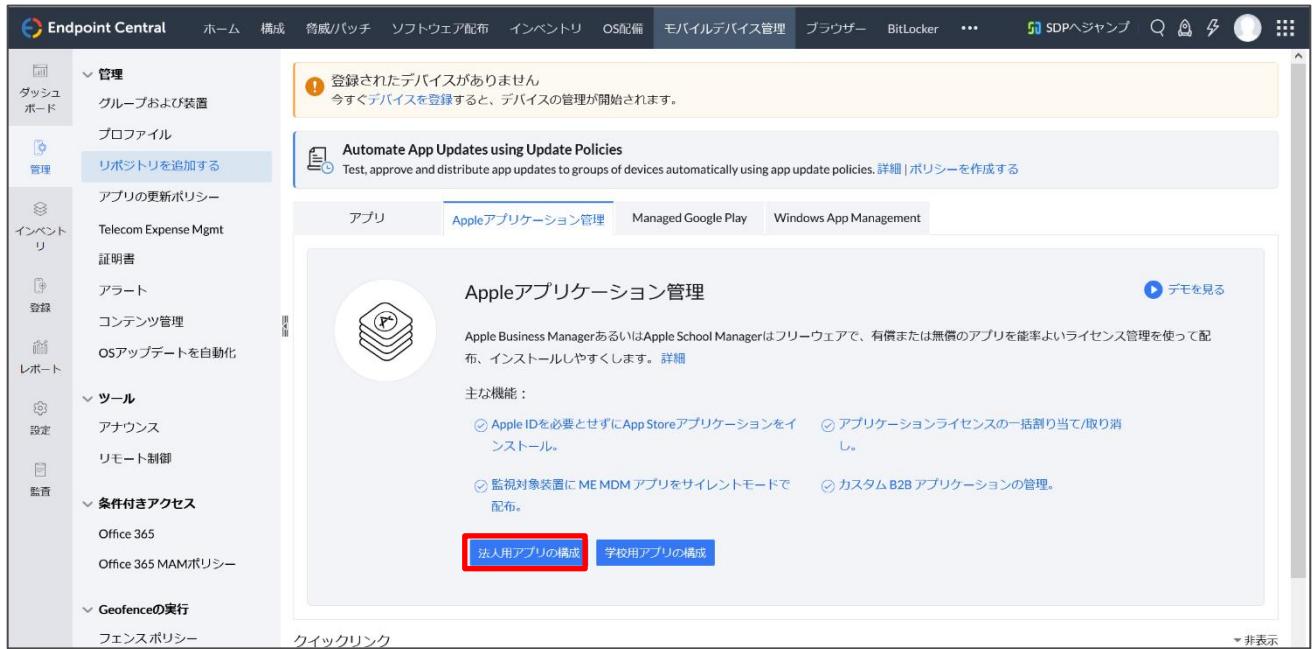
1. ABM ポータルにログインし、「環境設定」→「お支払いと請求」を表示します。
2. 右下の「コンテンツトークン」の「ダウンロード」をクリックして、サーバートークンをダウンロードします。



The screenshot shows the ABM portal interface. On the left, a sidebar lists various management categories. The main area is titled 'Billing and Invoicing' (お支払いと請求). It includes sections for 'Billing Methods' (お支払い方法), 'Store Credit' (Storeクレジット), and 'Content Token' (コンテンツトークン). The 'Content Token' section shows a list of tokens, with one entry for 'ZOHO JAPAN CORPORATION.' followed by a red box highlighting the 'Download' (ダウンロード) button.

3. Endpoint Central Cloud コンソールの「モバイルデバイスマネジメント」→「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。

## 4. 「法人用アプリの構成」(ABM の場合) をクリックします。



The screenshot shows the 'Apple Application Management' section. A red box highlights the '法人用アプリの構成' (Corporate App Configuration) button. The interface includes a sidebar with various management options like 'ダッシュボード', '管理', 'イベントリ', '登録', 'レポート', 'ツール', '条件付きアクセス', and 'Geofenceの実行'. The main content area displays information about Apple Business Manager and the 'Apple Application Management' tab is selected. A message at the top right says '登録されたデバイスがありません 今すぐデバイスを登録すると、デバイスの管理が開始されます。' (No devices are registered. Registering a device will start device management.)

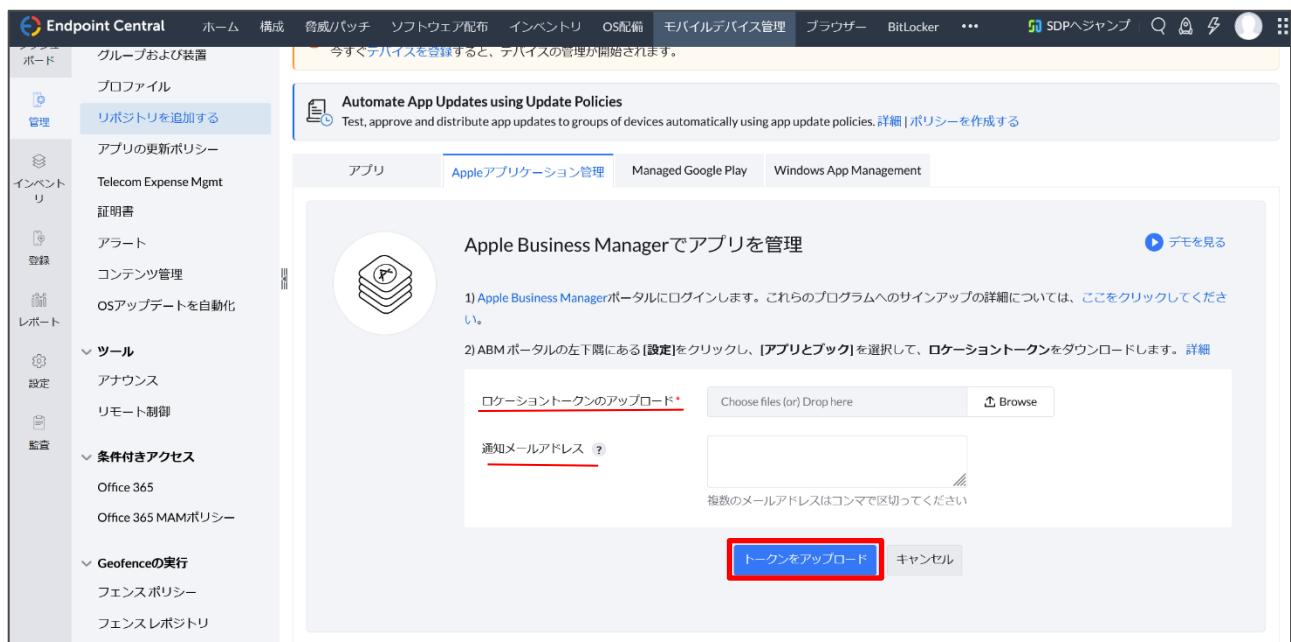
## 5. 画面から、サーバートークンをアップロードします。

● 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。



The screenshot shows the 'Apple Business Managerでアプリを管理' (Manage Apps via Apple Business Manager) section. A red box highlights the 'トークンをアップロード' (Upload Token) button. The interface includes a sidebar with various management options like 'ダッシュボード', '管理', 'イベントリ', '登録', 'レポート', 'ツール', '条件付きアクセス', and 'Geofenceの実行'. The main content area displays instructions for logging into the ABM portal and uploading the token. It also includes fields for 'ロケーショントークンのアップロード' (Upload Location Token) and '通知メールアドレス' (Notification Email Address). A note at the bottom says '複数のメールアドレスはコンマで区切ってください' (Please separate multiple email addresses with commas).

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。



The screenshot shows the ManageEngine Endpoint Central web interface. The left sidebar is collapsed, and the main content area is titled 'Locations Token'. A sub-section titled 'Locations Token Details' is expanded, showing a table with the following data:

場所名	同期されたアプリの合計
ZOHO JAPAN CORPORATION.	5

Below the table, there is a section titled 'Locations Token Details' with the following information:

ABM 組織名	追加された時間
ZOHO JAPAN CORPORATION.	7/24, 2023 02:15 午後

Further down, there is a section titled 'Locations Token Details' with the following information:

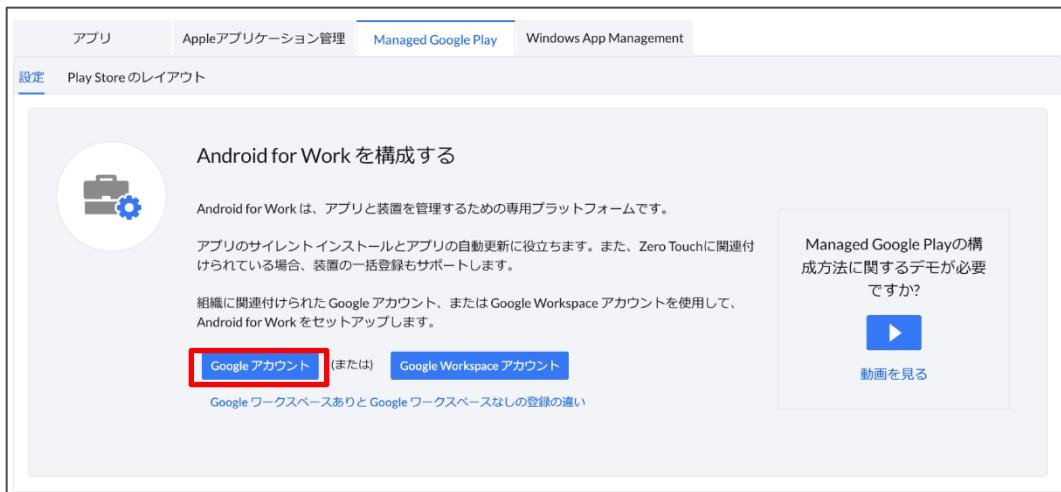
最終同期時刻	次の同期時刻
3/5, 2024 01:41 午後	3/5, 2024 06:06 午後

At the bottom of the expanded section, there is a link 'View Details'.

## 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。



3. 設定完了後、Managed Google Play と同期されます。

アプリ Appleアプリケーション管理 Managed Google Play Windows App Management

アカウント詳細 Play Store のレイアウト

+ アプリを追加 ▾ ⚙ アプリを同期 × 削除

Managed Google Playの詳細

ドメイン名	:	Zoho Japan Evaluation	同期されたアプリの合計	:	3中の3
最後の同期時刻	:	3月 13, 2024 6:06 PM	同期に失敗したアプリ	:	--
管理者アカウント ①	:	...@zoho.com	Managed Google Playのアカウントタイプ	:	Google Workspace以外のアカウント
エンタープライズID	:	...@zoho.com	管理アカウントのない装置	:	0

次のステップとは?

ユーザーの介入なしにプレイストアアプリをインストール  
アプリを承認し、デバイスにサイレントモードでインストールします。  
[詳細](#) [デモを見る](#)

Play Store のレイアウトをカスタマイズする  
組織のニーズに合わせて Google Play Storeをデザインしてください。  
[詳細](#)

## 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。

グループ名	グループ	アクション
ソーホージャパン株式会社	デバイス	アプリを配信する
佐藤テスト	デバイス	ドキュメントを配布
日本	デバイス	Remote Restart
谷口グループ	デバイス	Remote Shutdown

3. 配布するアプリを選択します。
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

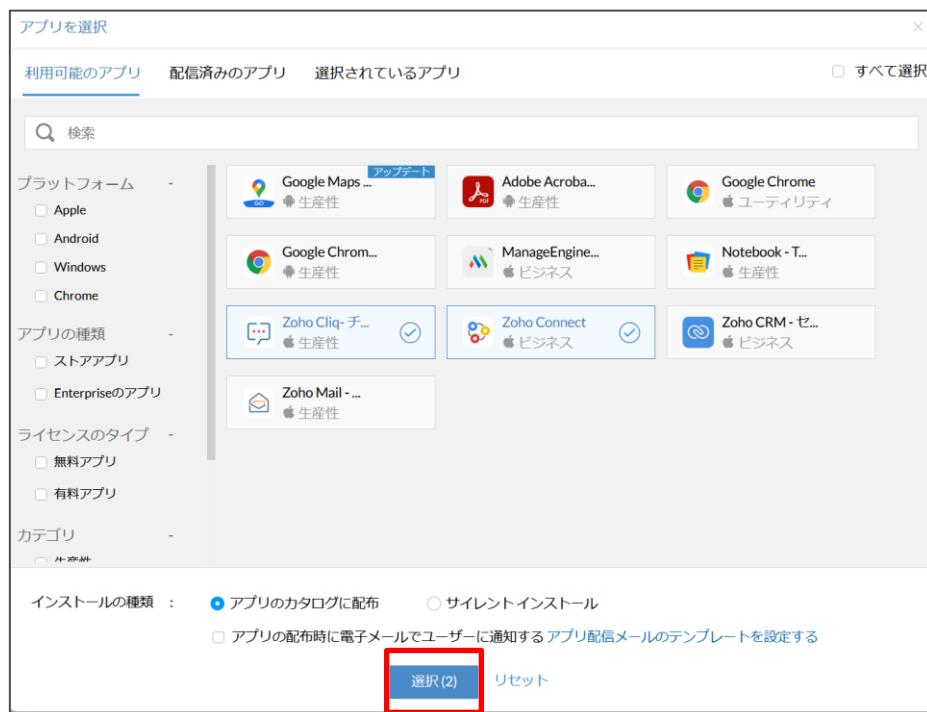
アプリケーションを端末の ManageEngine MDM アプリケーションに表示し、ユーザーがそこにアクセスしてインストールします。

- 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。

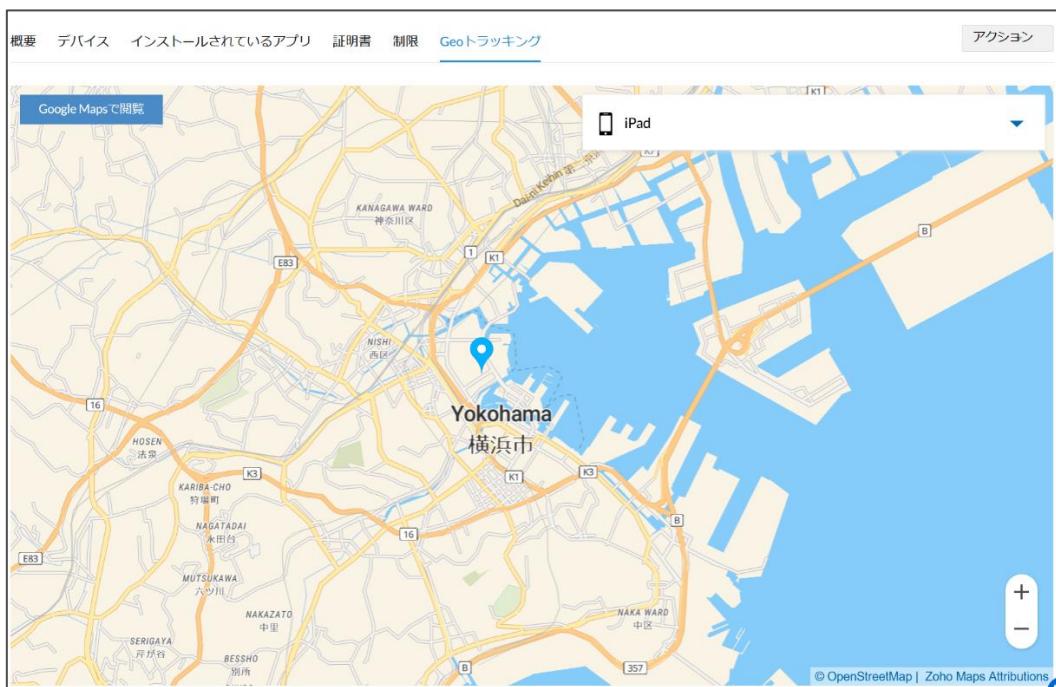
## 6 デバイスの位置情報とセキュリティ

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。



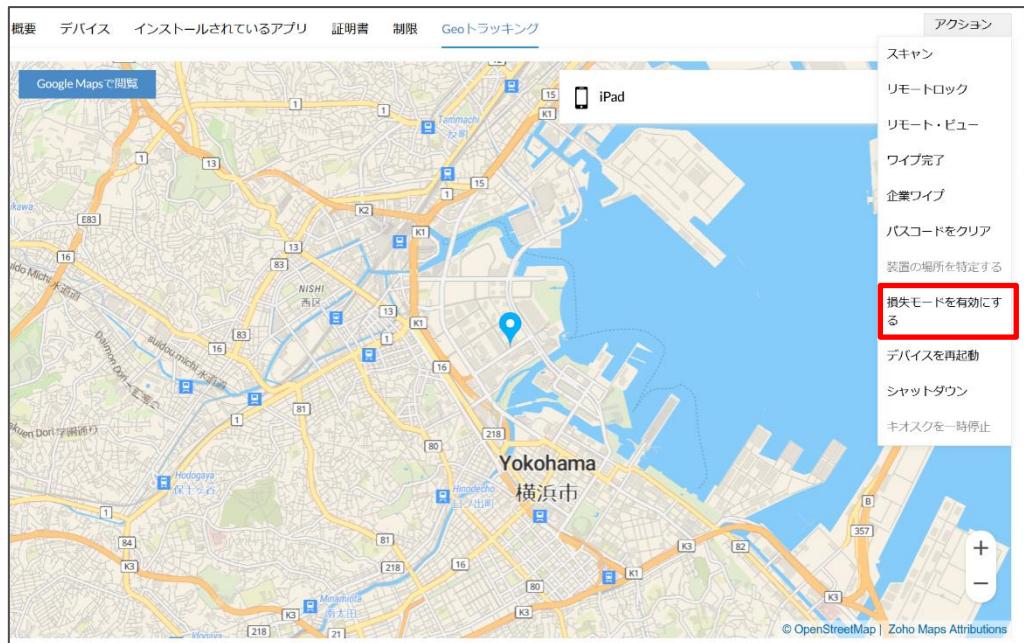
### 6-2 紛失モード

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。



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。



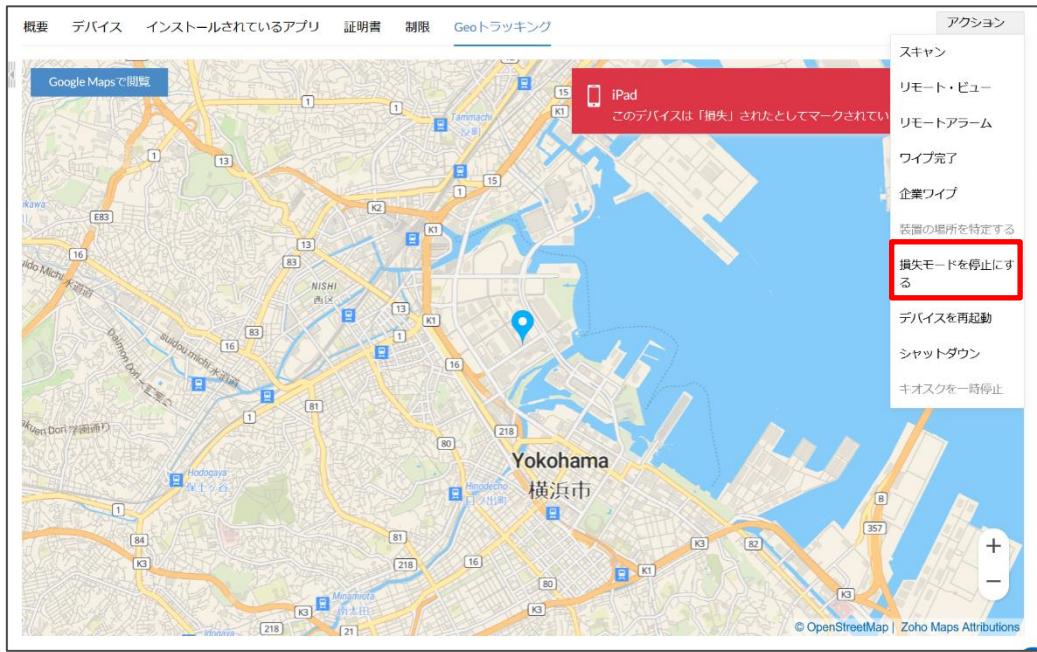
4. 紛失を社内で管理する番号がある場合はチケットIDを入力し、メッセージにメッセージを入力します。メッセージは監査ログに反映されます。入力後「探す」をクリックします。



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）することができます。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。

## 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）。つぎにフェンスピリシーから、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。最後にフェンスピ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。

## 2. フェンスの設定項目

● 緯度と経度

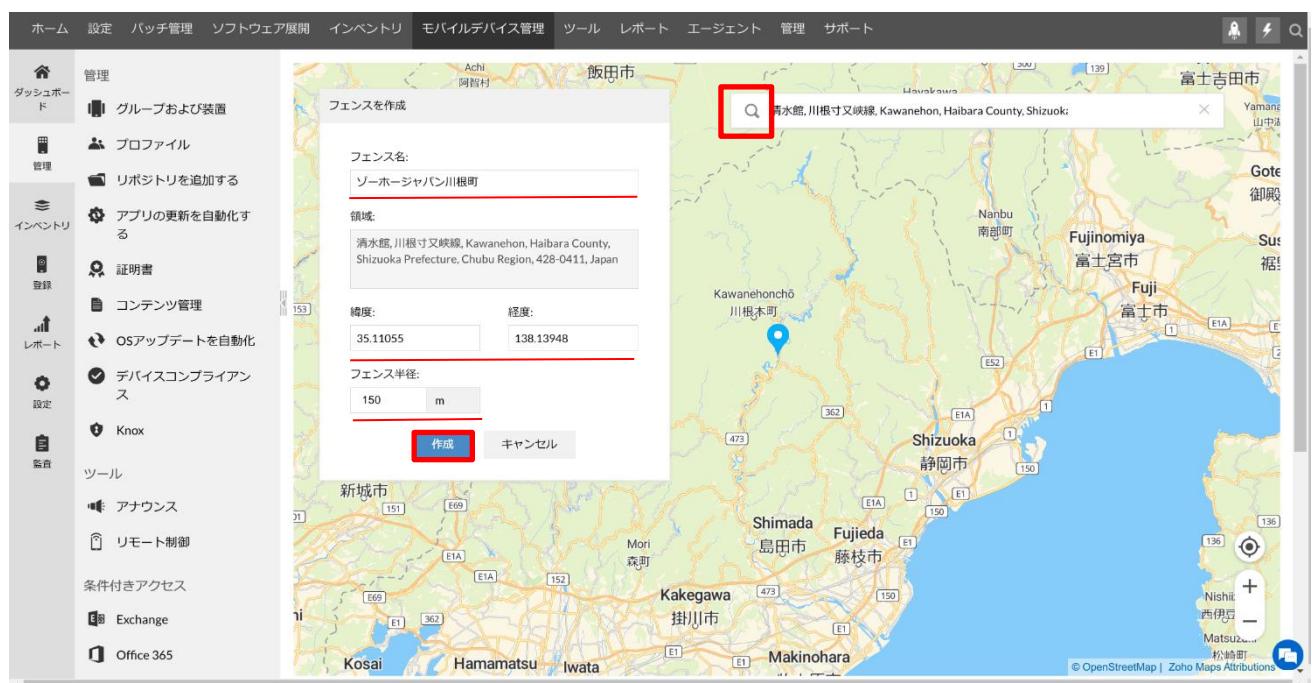
ジオフェンスの中心点を指定します。直接、数値を入力するか、検索窓から指定します。

● 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。

## 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。



マイポリシー

Geofence ポリシー

装置が特定の地理的領域の中にあることを識別し、この外にあればセキュリティコマンドを自動実行します。装置のプライバシー設定が装置の場所を取得するように構成

次の場合、装置は非準拠と見なされます：

デバイス 条件の選択 領域を選択してください フェンスを作成

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

頻度を選択 アクションタイプを選択して アクションを選択 +

ポリシーを作成する キャンセル

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	<u>紛失モード</u>	<u>完全ワイプ (ワイプ完了)</u> Complete wipe	ワイプ+SD カード完了 Complete wipe + SD card
今すぐ	○	○	×	×
一日の後	○	○	○	○

マイポリシー

Geofence ポリシー

装置が特定の地理的領域の中にあることを識別し、この外にあればセキュリティコマンドを自動実行します。装置のプライバシー設定が装置の場所を取得するように構成

次の場合、装置は非準拠と見なされます：

デバイス 条件の選択 領域を選択してください フェンスを作成

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

頻度を選択 アクションタイプを選択して アクションを選択 +

ポリシーを作成する キャンセル

#### 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。

フェンス ポリシー

川根町ポリシー

変更者: hiroki.saito

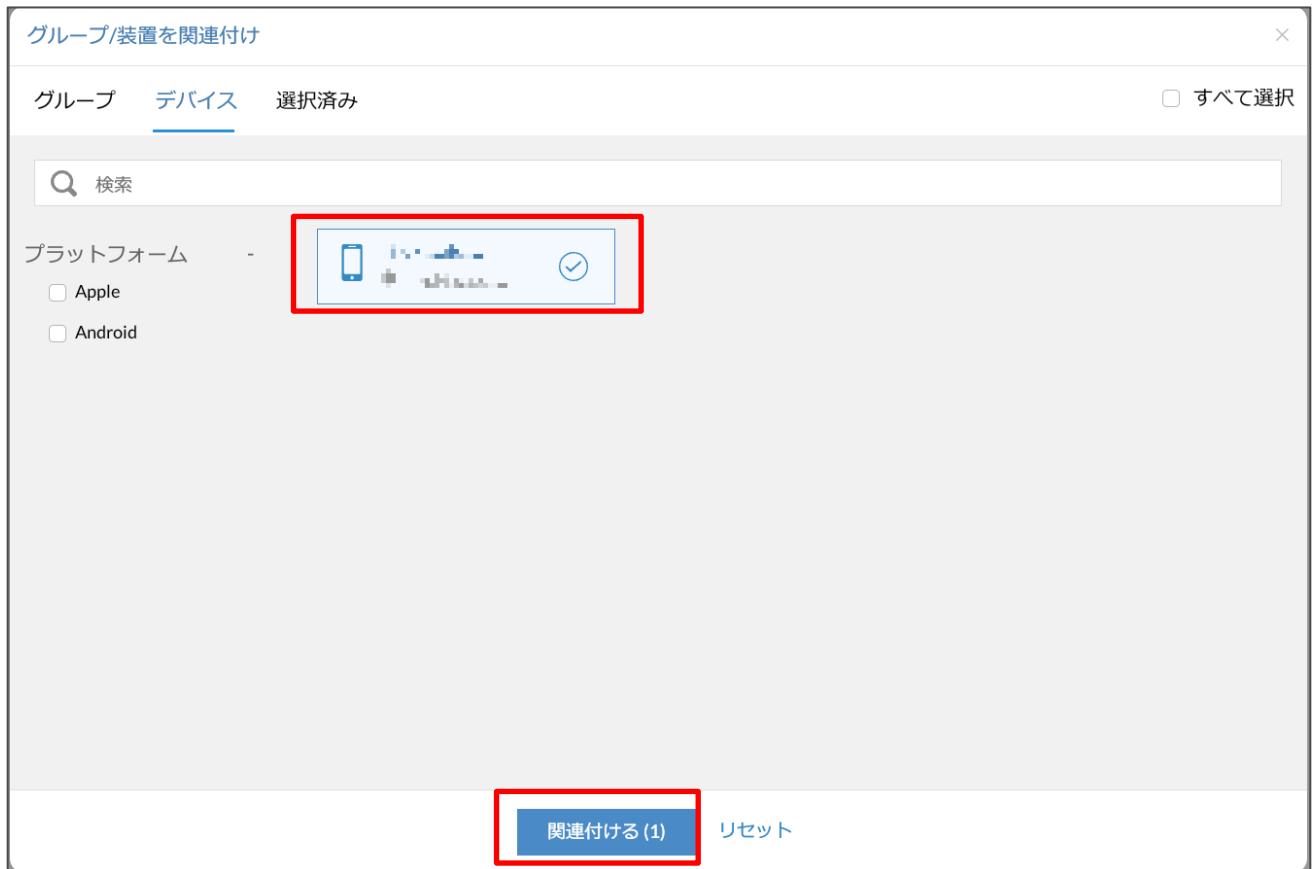
このポリシーに登録された装置: 0

グループ/装置を関連付け

変更 削除

装置監視用にコンプライアンスルールをさらに追加しますか? キャンセル ポリシーを作成する

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](https://www.manageengine.jp/products/Endpoint_Central/mobile-device-management.html)

E-mail: [jp-mesales@zohocorp.com](mailto:jp-mesales@zohocorp.com)



©ZOHO Japan Corporation. All rights reserved