
OPTiM

Optimal Biz iOS キットティングマニュアル

最終更新日 2024年7月15日
(Web サイト ver.9.21.0)
株式会社オプティム

はじめに

本マニュアルでは、Optimal Biz（以下、本製品と呼ぶ）の操作ほか、各機能の概要、画面の説明、設定操作について説明しています。

また、要点となる各種の内容を以下に記載しています。これらの内容をご理解の上、マニュアルをお読みください。

名称・呼称

本マニュアルに登場する特定の企業、人について、以下の定義で記載しています。

名称	説明
サービス企業	本製品を提供する企業。
管理者	本製品の管理サイト（機器の管理・運用を行う Web サイト）を運用する者。
端末使用者	本製品で管理している端末を使用する者。
システム管理者	企業の社内システム（サーバー・インフラなど）を管理する者。

注意・ポイントマーク

操作を行う場合に注意する点や、操作のポイントとなる点を示す場合は、以下のマークで記載しています。

マーク	説明
	データの破損や消失など、特に注意していただきたい内容を記載しています。
	操作のポイントや知っておくと便利な内容を記載しています。

記号

画面に表示されるボタンやメニュー、キーボードのキーなどを示す場合は、以下の記号で記載しています。

マーク	説明
[]	ボタン、メニュー、タブ、リンク、チェックボックス、ラジオボタンなどの名称を示しています。
「 」	画面名、機能名、項目名、マニュアル内の参照先などを示しています。
『 』	マニュアルや資料などの名称を示しています。
< >	キーボードなどのハードキー名称（スペースキーは〈スペース〉と表記）を示しています。

参照マーク

他のマニュアルや他のページへなどの参照を示す場合は、以下のマークで記載しています。

マーク	説明
	他のページや Web サイトへの参照を示しています。クリックすると該当箇所にジャンプします。
	セクション内の画面への参照を示しています。クリックすると該当の画面にジャンプします。
	他のマニュアルや資料への参照を示しています。

用語集

不明な用語は、以下を参照してください。

 [『よくあるご質問 \(FAQ\)』](#)

免責事項

- 本マニュアルは、ユーザー種別が [管理者] のユーザーを対象としています。[管理者] 以外のユーザー種別でログインした場合は、操作が制限されます。
- iPad OS の操作は iOS と同様です。差異がある場合は iPad OS 用の記載をしています。
- 画面上のバージョン表記は、実際の表示と異なる場合があります。
- 本マニュアルに記載されている Web サイトの URL は、予告なく変更される場合があります。
- OS のバージョンやブラウザにより、一部の画面や操作が異なる場合があります。本マニュアルでは、Google Chrome を例に説明しています。

登録商標

- Apple、iPad、iPadOS、iPhone、Mac、macOS は、米国およびその他の国で登録された Apple Inc.の商標です。
- iOS は、Apple Inc.の OS 名称です。
IOS は、Cisco Systems, Inc.またはその関連会社の米国およびその他の国における登録商標または商標であり、ライセンスに基づき使用されています。
- iPhone 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。
- App Store は、Apple Inc.のサービスマークです。
- Android、Google Chrome、Google Cloud、Google マップ、Google Play、Google Workspace は、Google LLC の商標です。
- Microsoft、Microsoft Edge は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
- Windows の正式名称は、Microsoft Windows Operating System です。Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
- その他記載の会社名、製品名は、各社の登録商標および商標です。

目次

1 iOS クライアントについて	5
1.1 概要	6
1.2 OS サポートポリシー	7
1.3 動作環境	8
2 キットティング方法を選択する	10
2.1 キットティング方法の概要と流れ	11
2.1.1 ADE とは	12
3 ライセンス認証を行う	13
3.1 MDM 構成プロファイルをインストールする	14
3.1.1 iOS 12.2 未満の場合	14
3.1.2 iOS 12.2 以上の場合	19
3.2 機器情報を登録する	25
4 ADE を利用してライセンス認証を行う	26
4.1 ADE を利用するための準備をする	27
4.1.1 ADE トークンを準備する	27
4.1.1.1 ADE トークンをダウンロードする	27
4.1.1.2 ADE トークンをアップロードする	34
4.1.2 ABM で端末をサーバーに割り当てる	36
4.1.3 ADE 定義プロファイルを作成する	41
4.1.4 ADE 定義プロファイルを適用する	46
4.2 端末のアクティベーションを行う	48
5 エージェントを認証する	50
5.1 エージェントをインストール／認証する	51
5.1.1 ポータルからインストール／認証する	51
5.1.1.1 iOS 13.0 以上の端末で位置情報の常に利用を許可する	55
5.1.2 App Store からインストール／認証する	57
5.1.3 アプリケーション配信を利用してインストール／自動認証する	60
5.1.3.1 アプリケーション配信でエージェントをインストールする	60
5.1.3.2 エージェントを自動認証する	68

1 iOS クライアントについて

1.1 概要

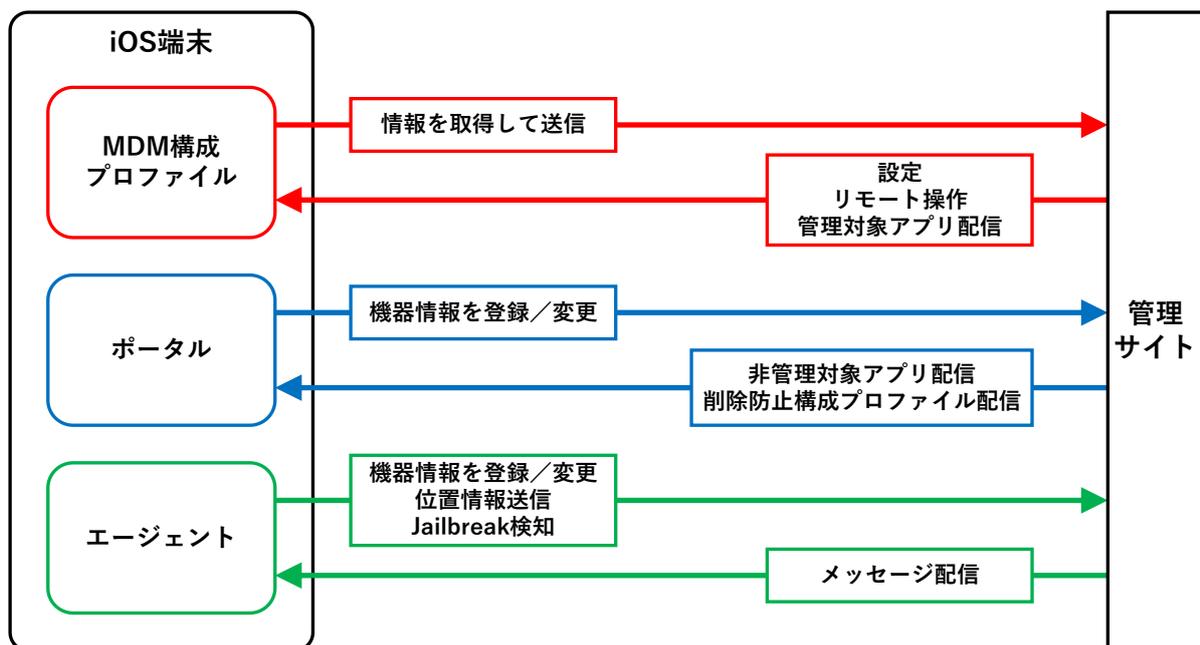
本製品は、専門の知識を必要とせず、機器の管理・運用を行うサポートサービスです。管理サイトから端末のリモートロックやリモートワイプ（初期化）ができます。iOS 端末にアプリ「Optimal Biz エージェント（以下、エージェントと呼ぶ）」をインストールすることもできます。

📄 管理サイトの操作については、以下を参照してください。

📖 『管理サイト リファレンスマニュアル』

本製品で行えること

本製品は、MDM 構成プロファイル、ポータル、エージェントを使用して、iOS 端末を管理します。



◆ MDM 構成プロファイル

MDM 構成プロファイルとは、iOS 端末の構成を制御するファイルです。

本製品を利用するには、MDM 構成プロファイルのライセンスを認証する必要があります。以下を参照して、MDM 構成プロファイルのライセンスを認証してください。

📄 「ライセンス認証を行う」 13 ページ

MDM 構成プロファイルで行えることは、以下のとおりです。

- 定期的に iOS 端末の情報を取得して、管理サイトに送信する。
- 定期的に管理サイトからの設定を取得して、iOS 端末に設定する。
- 管理サイトからリモート操作の指示を受けて、iOS 端末を操作する。
- 管理サイトから管理対象アプリが送信される。

📄 MDM 構成プロファイルについては、以下を参照してください。

📖 『iOS クライアント リファレンスマニュアル』の「MDM 構成プロファイルについて」

◆ポータル

ポータルとは、Web クリップです。アイコンをタップするとブラウザでポータルホーム画面が表示されます。

ポータルのアイコンは、MDM 構成プロファイルのライセンス認証を行うと、iOS 端末のホーム画面に表示されます。

管理サイトと同期するたびに、ポータルは再インストールされます。

ポータルで行えることは、以下のとおりです。

- 機器情報を登録／変更する。
- 管理サイトから非管理対象アプリが送信される。
- 管理サイトから削除防止構成プロファイルが送信される。

 ポータルの使用方法については、以下を参照してください。

 『iOS クライアント リファレンスマニュアル』の「ポータルの使用方法」

◆エージェント

エージェントとは、MDM 構成プロファイルのライセンス認証を行ったあと、App Store からインストール／認証して使用するアプリです。iOS 端末のホーム画面にエージェントのアイコンが表示されます。以下を参照して、エージェントのインストール／認証を行ってください。

 「エージェントを認証する」50 ページ

エージェントで行えることは、以下のとおりです。

- 機器情報を登録／変更する。
- 位置情報を送信する。
- Jailbreak を検知する。
- 管理サイトからメッセージが配信される。

 エージェントの使用方法は、以下を参照してください。

 『iOS クライアント リファレンスマニュアル』の「エージェントの使用方法」

1.2 OS サポートポリシー

本製品では、確実な製品の動作とセキュリティ機能の提供を目的として、以下の OS サポートポリシーを定めています。

- 本製品の最新対応 OS より 3 世代前の OS メジャーバージョンまでをサポート。
- 最新対応 OS 追加に伴い、サポート対象外となった OS バージョンについては、サポート期限が切れた日から 1 年間に限り、お問い合わせには可能な限り対応いたします。ただし、動作保証や不具合対応はいたしません。
-  定期的に下位の OS バージョンのサポートを終了します。サポート対象外となる OS や端末を利用している場合は、OS アップデートまたは機種の変更をしてください。

サポート対象	<ul style="list-style-type: none">● iOS 17.x : 最新対応 OS● iOS 16.x : 1 世代前● iOS 15.x : 2 世代前● iOS 14.x : 3 世代前 iOS 13.x のサポートは終了しました。お問い合わせには 2024 年 9 月 18 日まで可能な限り対応します。
--------	---

1.3 動作環境

 エージェントのリリース日から 180 日間は、180 日間にリリースされたすべてのエージェントがサポートされます。ただし、リリース日から 180 日を超えた場合は、180 日以降最初にリリースされたエージェントから 2 つ前のエージェントまでが、サポートの対象になります。

対応機種	
	iPhone 6s
	iPhone 6s Plus
	iPhone 7
	iPhone 7 Plus
	iPhone 8
	iPhone 8 Plus
	iPhone X
	iPhone XS
	iPhone XS Max
	iPhone XR
	iPhone SE
	iPhone SE (第 2 世代)
	iPhone SE (第 3 世代)
	iPhone 11
	iPhone 11 Pro
	iPhone 11 Pro Max
	iPhone 12
	iPhone 12 mini
	iPhone 12 Pro
	iPhone 12 Pro Max
	iPhone 13
	iPhone 13 mini
	iPhone 13 Pro
	iPhone 13 Pro Max
	iPhone 14
	iPhone 14 Plus
	iPhone 14 Pro
	iPhone 14 Pro Max
	iPhone 15
	iPhone 15 Plus
	iPhone 15 Pro
	iPhone 15 Pro Max
	iPad (第 5 世代)
	iPad (第 6 世代)
	iPad (第 7 世代)
	iPad (第 8 世代)
	iPad (第 9 世代)
	iPad (第 10 世代)
	iPad mini (第 4 世代)
	iPad mini (第 5 世代)
	iPad mini (第 6 世代)
	iPad Air (第 2 世代)
	iPad Air (第 3 世代)

	iPad Air (第 4 世代) iPad Air (第 5 世代) iPad Pro 9.7 インチ iPad Pro 10.5 インチ iPad Pro 11 インチ (第 1 世代) iPad Pro 11 インチ (第 2 世代) iPad Pro 11 インチ (第 3 世代) iPad Pro 11 インチ (第 4 世代) iPad Pro 12.9 インチ (第 1 世代) iPad Pro 12.9 インチ (第 2 世代) iPad Pro 12.9 インチ (第 3 世代) iPad Pro 12.9 インチ (第 4 世代) iPad Pro 12.9 インチ (第 5 世代) iPad Pro 12.9 インチ (第 6 世代) iPod touch (第 7 世代)
対応 OS	iOS 14.0 以上
ネットワーク接続	モバイルネットワークまたは Wi-Fi でインターネットへアクセスができること。 直接またはプロキシを介して管理サイトと HTTPS 通信 (443 番ポート) ができること。

2 キットティング方法を選択する



- あらかじめ Apple Push 証明書の登録が必要です。登録方法については、以下のマニュアルを参照してください。

 『Apple Push 証明書年次更新マニュアル』

2.1 キットティング方法の概要と流れ

iOS 端末のキットティングには、Automated Device Enrollment (ADE) の利用の有無により、2 種類の方法があります。利用している端末と運用ケースをご確認のうえ、適切なキットティング方法を選択してください。

 「ADE を利用する」で「監視対象モードに設定する (iOS 13 以上では必須)」を選んでキットティングした端末が、監視対象端末になります。

キットティング方法	説明
ADE を利用しない	<p>ABM または ASM に登録していない端末を ADE に紐づけずに、指定の URL からライセンス認証を行います。この方法には、以下のメリットがあります。</p> <ul style="list-style-type: none"> • キットティング時に端末の初期化が必要ありません。 <p>キットティング方法の詳細については、以下を参照してください。</p> <p> 「ライセンス認証を行う」13 ページ</p>
ADE を利用する	<p>ABM または ASM に登録済みの端末を ADE に紐づけてライセンス認証を行います。この方法には、以下のメリットがあります。</p> <ul style="list-style-type: none"> • キットティング前の機器情報を、あらかじめ「事前機器」として登録できます。 • アクティベーション時の端末操作を短縮できます。 <p>ADE の詳細については、以下を参照してください。</p> <p> 「ADE とは」12 ページ</p> <p>キットティング方法の詳細については、以下を参照してください。</p> <p> 「ADE を利用してライセンス認証を行う」26 ページ</p> <p> ADE を利用するには、メールアドレスと D-U-N-S ナンバー (企業識別コード) が必要です。D-U-N-S ナンバーについては、以下の Apple のサイトを確認してください。</p> <p> https://developer.apple.com/jp/support/D-U-N-S/</p> <p> キットティング時に端末の初期化が必要です。</p>

2.1.1 ADE とは

ADE とは、Apple Business Manager (ABM) によって提供されている端末管理のための機能です。ADE を利用することにより、企業や教育機関用に iOS 端末を導入する場合に、関連する作業を簡略化できます。ADE の設定は端末のアクティベーション時に Over-The-Air (無線通信経由) で反映されるため、従来端末に対して個別に行っていた煩雑な導入手順 (Apple Configurator を利用した有線接続によるアクティベーションや、プロファイルのインストール) が不要になります。

また、よりセキュアな端末管理ができる監視対象モードを利用したり、端末使用者が端末から MDM プロファイルを削除することを禁止したりすることもできます。

ABM について

ABM は、Apple が提供するシステム管理者を支援するためのポータルサイトです。システム管理者は ABM を MDM と連動させて利用することにより、端末のさまざまな値を設定したり、アプリを購入し、端末に配信したりすることができます。

また、ABM は旧来の Apple Deployment Programs (ADP) に代わる仕組みです。

ABM の詳細については、以下の Web サイトを参照してください。

 <https://support.apple.com/ja-jp/guide/apple-business-manager/welcome/1/web>

3 ライセンス認証を行う

3.1 MDM 構成プロファイルをインストールする

以下の手順で、MDM 構成プロファイルをインストールし、ライセンス認証を行います。

なお、iOS 12.2 未満／以上で操作が異なります。端末で使用している iOS のバージョンに応じて、以下のいずれかの方法を選択してください。

- iOS 12.2 未満の場合
- iOS 12.2 以上の場合

管理サイトの機器認証制御を利用している場合は、ライセンス認証を行う前に対象端末を設定に登録しておく必要があります。詳細については、管理者にお問い合わせください。

3.1.1 iOS 12.2 未満の場合

認証方式には2種類あります。以下いずれかの方式を選択してください。

- 認証コードによる認証
 - ユーザーID／メールアドレス、パスワードによる認証
- 以下の操作に使用できるブラウザは、Safari のみです。
- どちらの方法も、手順【6】以降は共通です。

認証コードによる認証

【1】 ホーム画面の [Safari] をタップします。

【2】 ライセンス認証画面の URL を入力します。

⇒ ライセンス認証画面が表示されます。

ライセンス認証画面の URL は、管理者にお問い合わせください。



お気に入り



プライバシーレポート

過去7日以内、0件のトラッカーによるプロファイリングが阻止されました

リーディングリスト

リーディングリストを使うと、Webページやリンクを集めてあとで読むことができます。*共有*ボタンをタップして現在のページを追加します。



【3】 [利用規約] をタップし、利用規約を確認します。

☑手順【5】で [送信] をタップすることにより、本規約に同意したものとみなします。

【4】 「企業コード」および「認証コード」を入力します。

☑企業コードは、管理者にお問い合わせください。

☑異なる入力項目が表示されている場合は、(A) [認証方式変更] をタップして画面を切り替えてください。

【5】 [送信] をタップします。

⇒ライセンス認証が開始されます。

ユーザーID/メールアドレス、パスワードによる認証

【1】 ホーム画面の [Safari] をタップします。

【2】 ライセンス認証画面の URL を入力します。

⇒ライセンス認証画面が表示されます。

☑ライセンス認証画面の URL は、管理者にお問い合わせください。



【3】 [利用規約] をタップし、利用規約を確認します。

☑手順【5】で [送信] をタップすることにより、本規約に同意したものとみなします。

【4】 「企業コード」、「ユーザーID またはメールアドレス」、および「パスワード」を入力します。

☑企業コード、ユーザーID/メールアドレス、パスワードは、管理者にお問い合わせください。

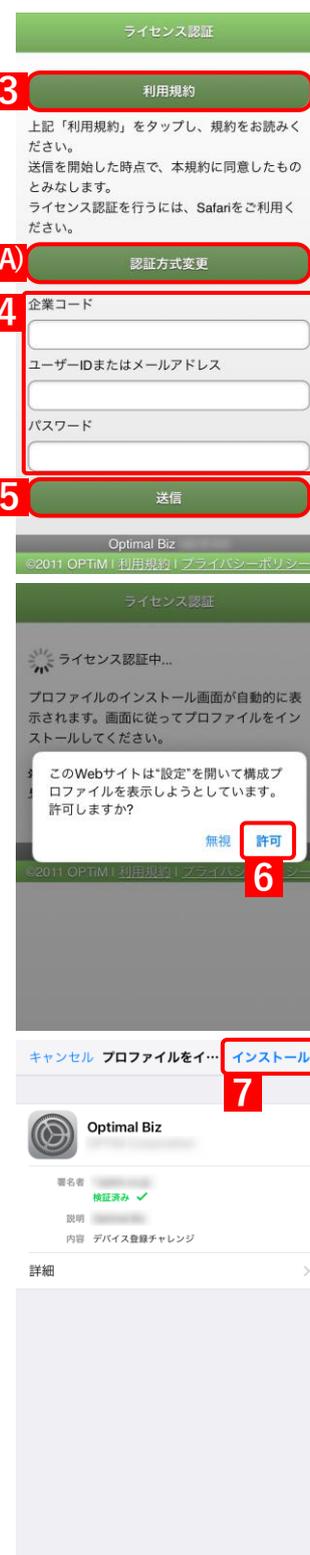
☑異なる入力項目が表示されている場合は、(A) [認証方式変更] をタップして画面を切り替えてください。

【5】 [送信] をタップします。

⇒ライセンス認証が開始されます。

【6】 [許可] をタップします。

【7】 [インストール] をタップします。



【8】 [インストール] をタップします。

⇒ インストールが開始され、リモート管理について確認を求められます。

☑️ パスコード入力画面が表示された場合は、端末のパスコードを入力してください。

【9】 [信頼] をタップします。

⇒ インストール完了画面に切り替わるまで、しばらくお待ちください。

【10】 [完了] をタップします。

⇒ ライセンス認証が開始されます。完了するまで、しばらくお待ちください。



【11】 続けて機器情報を登録する場合は、[次へ] をタップします。

⇒以降の手順については、以下を参照してください。

🏠 「機器情報を登録する」 25 ページ

☑️ 機器情報を登録しない場合は、ライセンス認証は完了です。引き続き以下を参照して、エージェントをインストール／認証してください。

🏠 「エージェントをインストール／認証する」 51 ページ

📝 機器情報は、あとから管理サイトで登録することもできます。



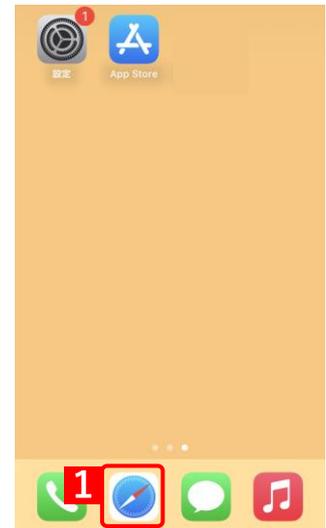
3.1.2 iOS 12.2 以上の場合

認証方式には2種類あります。以下いずれかの方式を選択してください。

- 認証コードによる認証
- ユーザーID/メールアドレス、パスワードによる認証
- ☑ 以下の操作に使用できるブラウザは、Safariのみです。
- ☑ どちらの方法も、手順【6】以降は共通です。

認証コードによる認証

【1】 ホーム画面の [Safari] をタップします。



【2】 ライセンス認証画面の URL を入力します。

⇒ ライセンス認証画面が表示されます。

☑ ライセンス認証画面の URL は、管理者にお問い合わせください。



【3】 [利用規約] をタップし、利用規約を確認します。

☑ 手順【5】で [送信] をタップすることにより、本規約に同意したものとみなします。

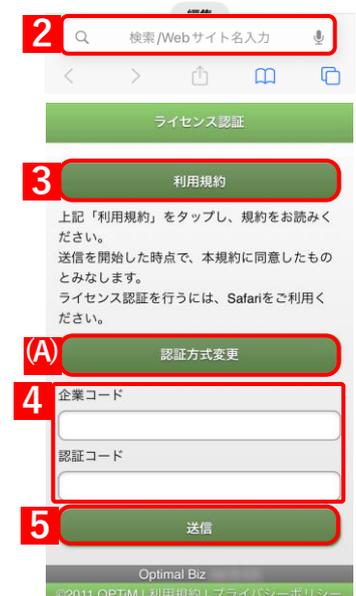
【4】 「企業コード」および「認証コード」を入力します。

☑ 企業コードは、管理者にお問い合わせください。

☑ 異なる入力項目が表示されている場合は、(A) [認証方式変更] をタップして画面を切り替えてください。

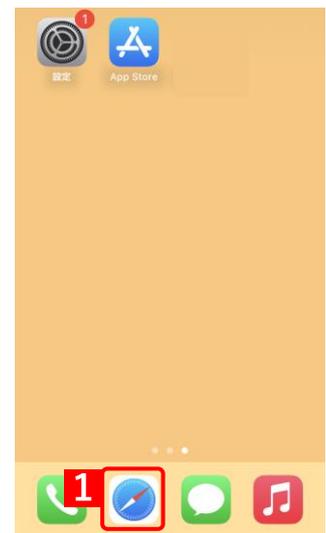
【5】 [送信] をタップします。

⇒ ライセンス認証が開始されます。



ユーザーID／メールアドレス、パスワードによる認証

【1】 ホーム画面の [Safari] をタップします。



【2】 ライセンス認証画面の URL を入力します。

⇒ ライセンス認証画面が表示されます。

☑ ライセンス認証画面の URL は、管理者にお問い合わせください。



【3】 [利用規約] をタップし、利用規約を確認します。

☑ 手順【5】で [送信] をタップすることにより、本規約に同意したものとみなします。

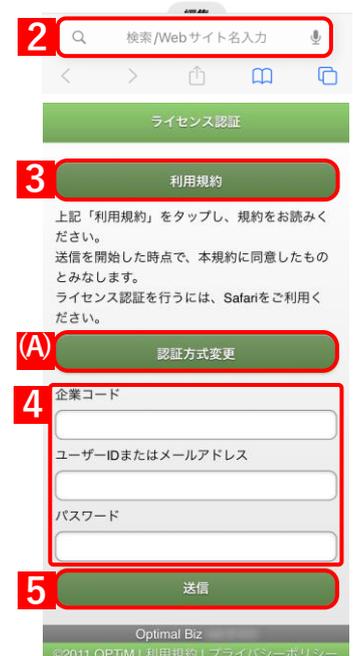
【4】 「企業コード」、「ユーザーID またはメールアドレス」、および「パスワード」を入力します。

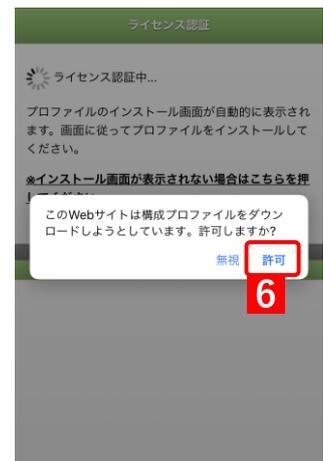
☑ 企業コード、ユーザーID／メールアドレス、パスワードは、管理者にお問い合わせください。

☑ 異なる入力項目が表示されている場合は、(A) [認証方式変更] をタップして画面を切り替えてください。

【5】 [送信] をタップします。

⇒ ライセンス認証が開始されます。



[6] 「許可」 をタップします。**[7] 「閉じる」 をタップします。**

⇒ プロファイルのダウンロードが完了します。

- ☑ iOS のバージョンにより「プロファイルがダウンロード済み」は、「プロファイルがダウンロードされました」など、表記が異なる場合があります。

**[8] ホーム画面の「設定」 をタップします。**

【9】 [プロフィールがダウンロード済み] をタップします。

🔗 iOS のバージョンにより [プロフィールがダウンロード済み] は、
[プロフィールがダウンロードされました] など、表記が異なる
場合があります。

【10】 [インストール] をタップします。

🔗 パスコード入力画面が表示された場合は、端末のパスコードを入
力してください。

【11】 [インストール] をタップします。



【12】 [インストール] をタップします。

⇒ インストールが開始され、リモート管理について確認を求められます。

**【13】 [信頼] をタップします。**

⇒ インストール完了画面に切り替わるまで、しばらくお待ちください。

**【14】 [完了] をタップします。**

📝 iOS 16.4 以上では、「デバイス ID 証明書」が「SCEP デバイス ID 証明書」と表示されます。



【15】 ホーム画面の [Safari] をタップします。

⇒ ライセンス認証が開始されます。完了するまで、しばらくお待ちください。

【16】 続けて機器情報を登録する場合は、[次へ] をタップします。

⇒ 以降の手順については、以下を参照してください。

📄 「機器情報を登録する」 25 ページ

☑️ 機器情報を登録しない場合は、ライセンス認証は完了です。引き続き以下を参照して、エージェントをインストール／認証してください。

📄 「エージェントをインストール／認証する」 51 ページ

📄 機器情報は、あとから管理サイトで登録することもできます。



3.2 機器情報を登録する

以下の手順で、機器情報を登録します。

- ☑ 管理サイトでポータルを表示に設定している場合、本画面が表示されます。ポータル表示の設定については、以下を参照してください。

🔍 『管理サイト リファレンスマニュアル』の「サービス環境設定」 - 「ポータル表示」

【1】必要に応じて、「機器情報登録」の設定を行います。

- ☑ 「機器情報登録」に表示される項目（「分類」、「自由入力項目」など）は、管理サイトの「入力項目のカスタマイズ」の設定により異なります。詳細については、以下のマニュアルの該当セクションを参照してください。

🔍 『管理サイト リファレンスマニュアル』の「機器」 - 「入力項目のカスタマイズ」

【2】[次へ] をタップします。

⇒ユーザー情報の登録が開始されます。完了するまで、しばらくお待ちください。

- ☑引き続き以下を参照して、エージェントをインストール／認証してください。

🔗 「エージェントをインストール／認証する」51 ページ

- ☑エージェント機能を契約していない場合は、これで端末のキックオフが完了します。以降の操作は不要です。



4 ADE を利用してライセンス認証を行う

4.1 ADE を利用するための準備をする

ADE を利用するための準備として、以下の一連の操作を行います。

4.1.1 ADE トークンを準備する

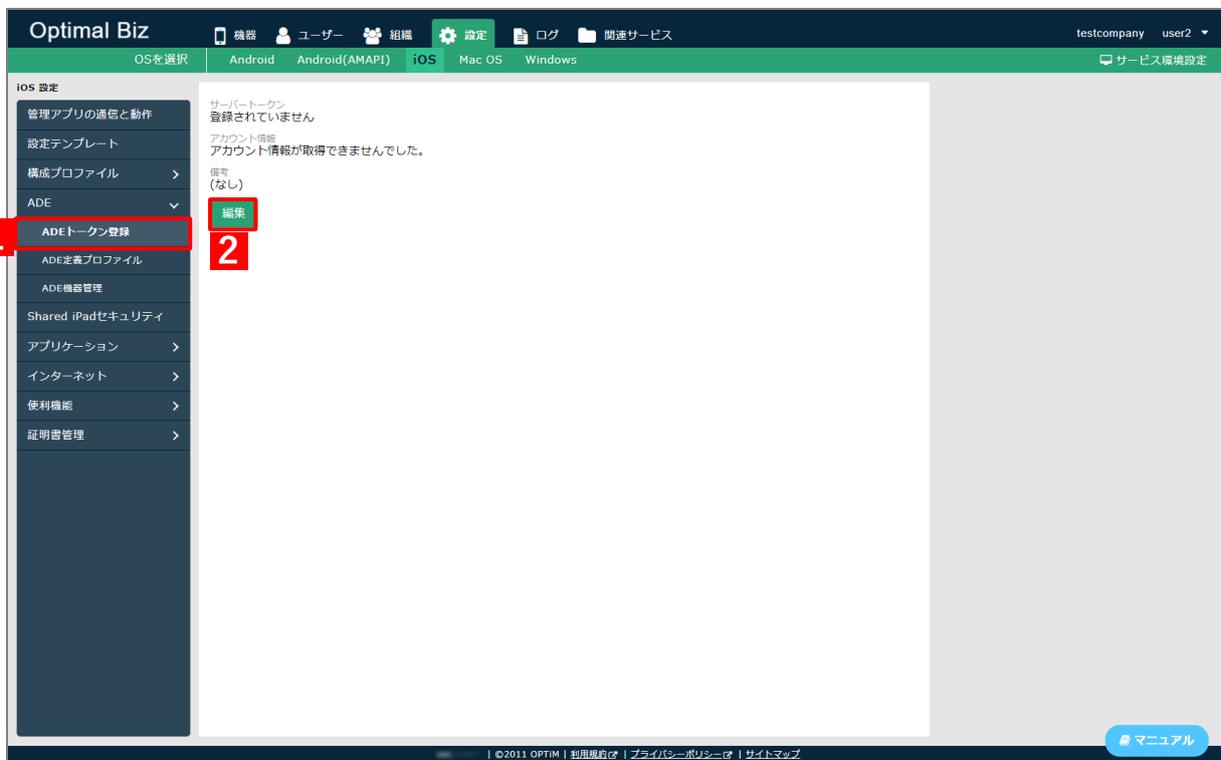
ADE トークンとは、ADE と管理サイトを紐づけるためのトークンです。これを ABM でダウンロードし、管理サイトにアップロードします。

 ADE トークンの準備は、初回のキitting時のみ必要な操作です。

4.1.1.1 ADE トークンをダウンロードする

以下の手順で、ABM から ADE トークンをダウンロードします。

- [1]** [設定] → [iOS] → [ADE] → [ADE トークン登録] をクリックします。
- [2]** [編集] をクリックします。



【3】 [ダウンロード] をクリックします。

⇒ 手順【15】で必要となる「サーバー公開鍵証明書 (PEM) ファイル」のダウンロードが開始されます。
任意の場所を指定して、ファイルを保存してください。

【4】 [<https://business.apple.com>] をクリックします。

⇒ABM のサイトが表示されます。以降の操作は、ABM のサイトで行います。

1. サーバー公開鍵証明書(PEM)ファイルの生成とダウンロード
サーバー公開鍵証明書(PEM)ファイルをダウンロードしてください。

3 **ダウンロード**

2. サーバートークンの取得
以下のリンクよりMDMサーバー登録用のサーバートークンを取得してください。サーバートークンはサーバー公開鍵証明書(PEM)をアップロードすることで取得できます。
Apple Business Manager: **4** <https://business.apple.com>
Apple School Manager: <https://school.apple.com>

※サーバートークンを定期的に更新する必要があります。有効期限が切れた場合、本製品はご利用いただけなくなります。

3. サーバートークンファイルの登録
2.より作成したサーバートークンファイルを指定してください。
[ファイルを選択] 選択されていません
備考 (※サーバートークン発行の際に使用されたApple IDを以下に記載することを推奨します。)

【5】 管理者用の「Apple ID」を入力します。**【6】 をクリックします。**

⇒ 「パスワード」入力欄が表示されます。

Business

所属する組織のデバイスやApp、アカウントを管理します。

5 **6**

Apple IDをブラウザに保存

[管理対象Apple IDまたはパスワードをお忘れですか？](#)
[まだApple Businessになっていませんか？今すぐ登録する。](#)

【7】 「パスワード」を入力します。

【8】  をクリックします。

⇒ 本人確認用の「確認コード」を受け取る電話番号を選択する画面が表示されます。



Apple Business

所属する組織のデバイスやApp、アカウントを管理します。

7 パスワード **8** 

Apple IDをブラウザに保存

[管理対象Apple IDまたはパスワードをお忘れですか？](#)

[まだApple Businessになっていませんか？今すぐ登録する。](#)

【9】 「確認コード」を受け取る電話番号を選択します。

⇒ 選択した電話番号の端末に「確認コード」がSMSで送信されます。

 複数の電話番号が登録されている場合は、選択肢が表示されます。



Apple Business

本人確認

9 

確認コードの送信先に使用する電話番号を選択してください。

[これらの電話番号にアクセスできませんか？](#)

【10】受信したメッセージを確認し、「確認コード」を入力します。

⇒6桁の入力が終わると、自動的に次の画面に進みます。

☑「確認コード」に誤りがあるとログインできず、手順【5】の「Apple ID」入力画面に戻ります。



☑「確認コード」の入力後に以下の画面が表示される場合があります。(A) [信頼する] をクリックすると、次回以降に同端末の同ブラウザからサインインするとき、「確認コード」の入力が不要になります。



【11】 「アカウント」 をクリックします。



【12】 [環境設定] をクリックします。



【13】 「MDM サーバ」の  をクリックします。



【14】 「MDM サーバ情報」の「MDM サーバ名」に、任意の名前を入力します。

【15】 「ファイルを選択…」をクリックし、手順【3】でダウンロードした「サーバー公開鍵証明書 (PEM ファイル)」を指定します。

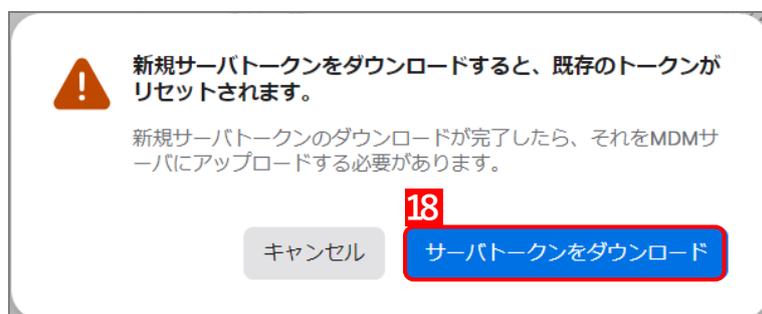
【16】 「保存」をクリックします。



【17】 [トークンをダウンロード] をクリックします。**【18】 [サーバトークンをダウンロード] をクリックします。**

⇒ ADE トークンのダウンロードが開始されます。任意の場所を指定して、ファイルを保存してください。

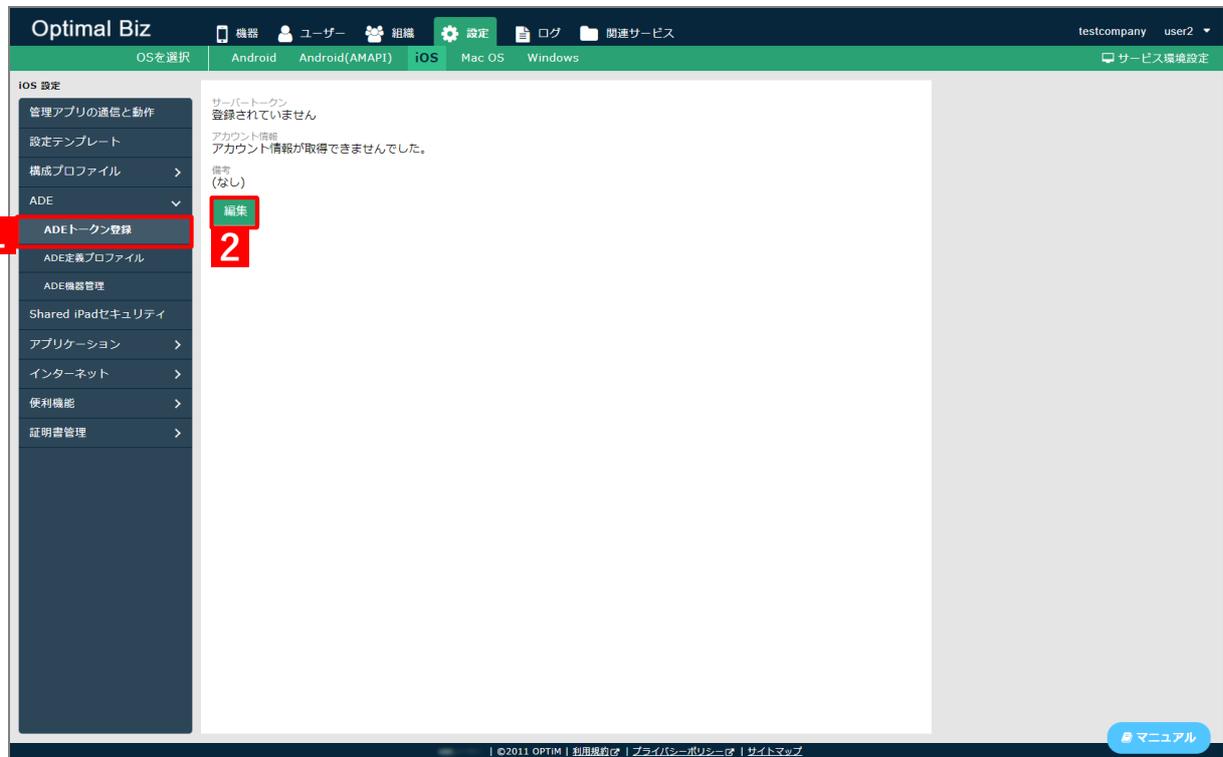
📌 ダウンロードした ADE トークンは、速やかに管理サイトにアップロードしてください。アップロードせずに長時間経過すると、管理サイトとの通信ができなくなることがあります。



4.1.1.2 ADE トークンをアップロードする

以下の手順で、ダウンロードした ADE トークンを管理サイトにアップロードします。

- [1] [設定] → [iOS] → [ADE] → [ADE トークン登録] をクリックします。
- [2] [編集] をクリックします。



- [3] [ファイルを選択] をクリックし、「ADE トークンをダウンロードする」でダウンロードした ADE トークンを指定します。
⇒ (A) 選択したファイル名が [ファイルを選択] の右側に表示されます。
- [4] 「備考」を入力します。
 ABM サインイン時の Apple ID、および ADE トークンの取得日の入力をお勧めします。
- [5] [保存] をクリックします。

1. サーバー公開鍵証明書(PEM)ファイルの生成とダウンロード

サーバー公開鍵証明書(PEM)ファイルをダウンロードしてください。

[ダウンロード](#)

2. サーバートークンの取得

以下のリンクよりMDMサーバー登録用のサーバートークンを取得してください。サーバートークンはサーバー公開鍵証明書(PEM)をアップロードすることで取得できます。

Apple Business Manager: <https://business.apple.com>
 Apple School Manager: <https://school.apple.com>

※サーバートークンを定期的に更新する必要があります。有効期限が切れた場合、本製品はご利用いただけなくなります。

3. サーバートークンファイルの登録

2.より作成したサ(A) トークンファイルを指定してください。

[3] .p7m

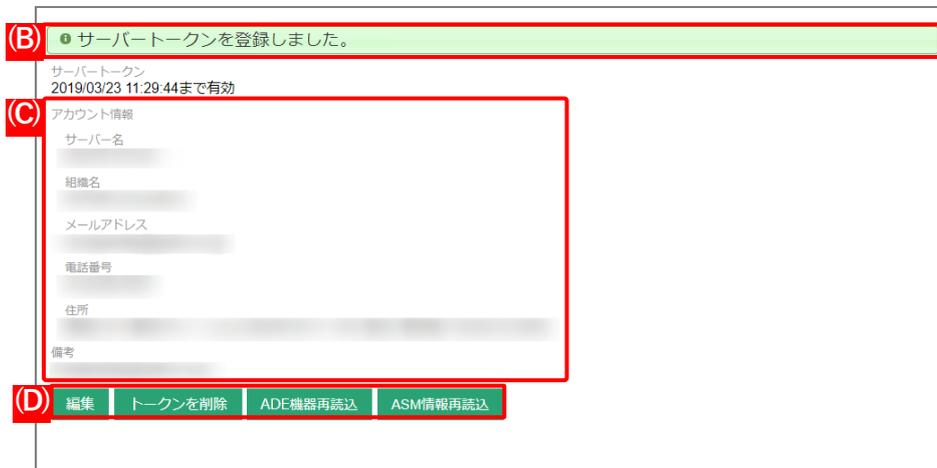
[4] 備考 (※サーバートークン発行の際に使用されたApple IDを以下に記載することを推奨します。)

[5]

⇒ (B) 「サーバトークンを登録しました。」と表示されます。(C) 「アカウント情報」に表示されている内容に誤りがないか確認してください。

✎ (D) の詳細については、以下のマニュアルの該当セクションを参照してください。

🔍 『管理サイト リファレンスマニュアル』の「設定-iOS」-「ADE」-「ADE トークン登録」-「画面 (登録後)」



4.1.2 ABM で端末をサーバーに割り当てる

以下の手順で、ADE を利用して管理する端末を ABM で特定のサーバーに割り当て、管理サイトに端末の情報を反映させます。

【1】 ABM のサイト (<https://business.apple.com/>) にアクセスします。

【2】 管理者用の「Apple ID」を入力します。

【3】  をクリックします。

⇒パスワードの入力欄が表示されます。



Apple Business

所属する組織のデバイスやApp、アカウントを管理します。

2 Apple ID **3** 

Apple IDをブラウザに保存

[管理対象Apple IDまたはパスワードをお忘れですか？](#)

[まだApple Businessになっていませんか？今すぐ登録する。](#)

【4】 「パスワード」を入力します。

【5】  をクリックします。

⇒本人確認用の「確認コード」を受け取る電話番号を選択する画面が表示されます。



Apple Business

所属する組織のデバイスやApp、アカウントを管理します。

4 パスワード **5** 

Apple IDをブラウザに保存

[管理対象Apple IDまたはパスワードをお忘れですか？](#)

[まだApple Businessになっていませんか？今すぐ登録する。](#)

【6】 「確認コード」を受け取る電話番号を選択します。

⇒ 選択した電話番号の端末に「確認コード」が SMS で送信されます。

☑ 複数の電話番号が登録されている場合は、選択肢が表示されます。

**【7】 受信したメッセージを確認し、「確認コード」を入力します。**

⇒ 6 桁の入力が終わると、自動的に次の画面に進みます。

☑ 「確認コード」に誤りがあるとログインできず、手順【2】の「Apple ID」入力画面に戻ります。



- ☑ 「確認コード」の入力後に以下の画面が表示される場合があります。(A) [信頼する] をクリックすると、次回以降に同端末の同ブラウザからサインインするとき、「確認コード」の入力が不要になります。



- [8]** [デバイス] をクリックします。

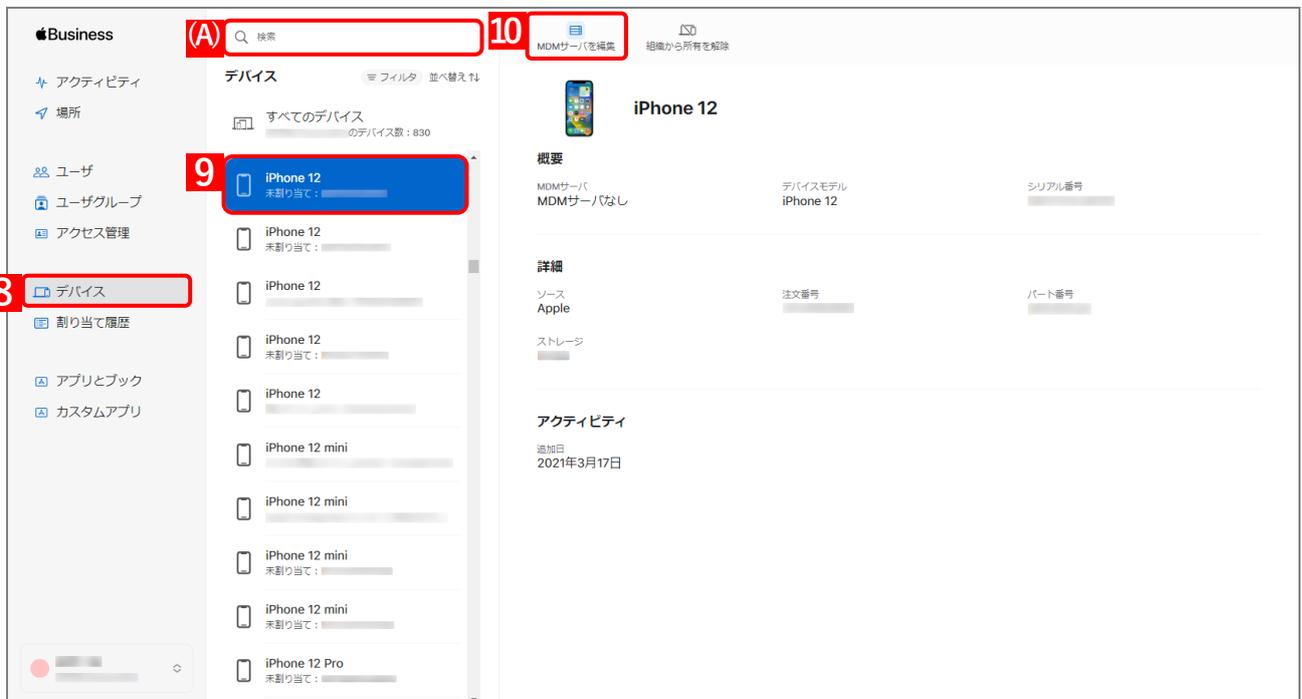
- [9]** 一覧から対象端末をクリックします。

☑ 対象端末が一覧に表示されていない場合は、Apple にお問い合わせください。

✎ (A) を利用して、一覧から端末を検索できます。

- [10]** [MDM サーバを編集] をクリックします。

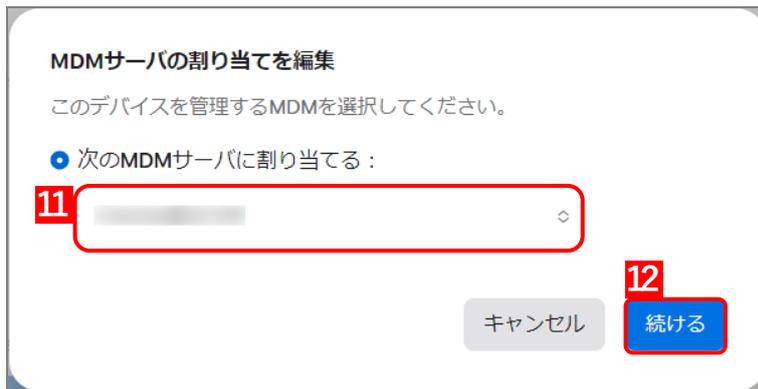
⇒ 「MDM サーバの割り当てを編集」画面が表示されます。



【11】 「ADE トークンをダウンロードする」の手順【14】で入力したサーバー名を選択します。

【12】 「続ける」をクリックします。

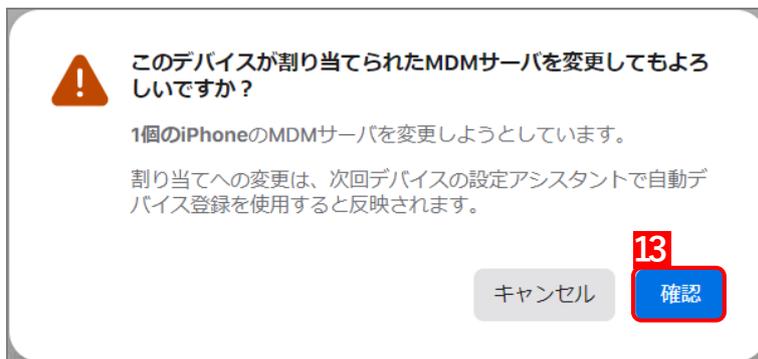
⇒確認画面が表示されます。



【13】 「確認」をクリックします。

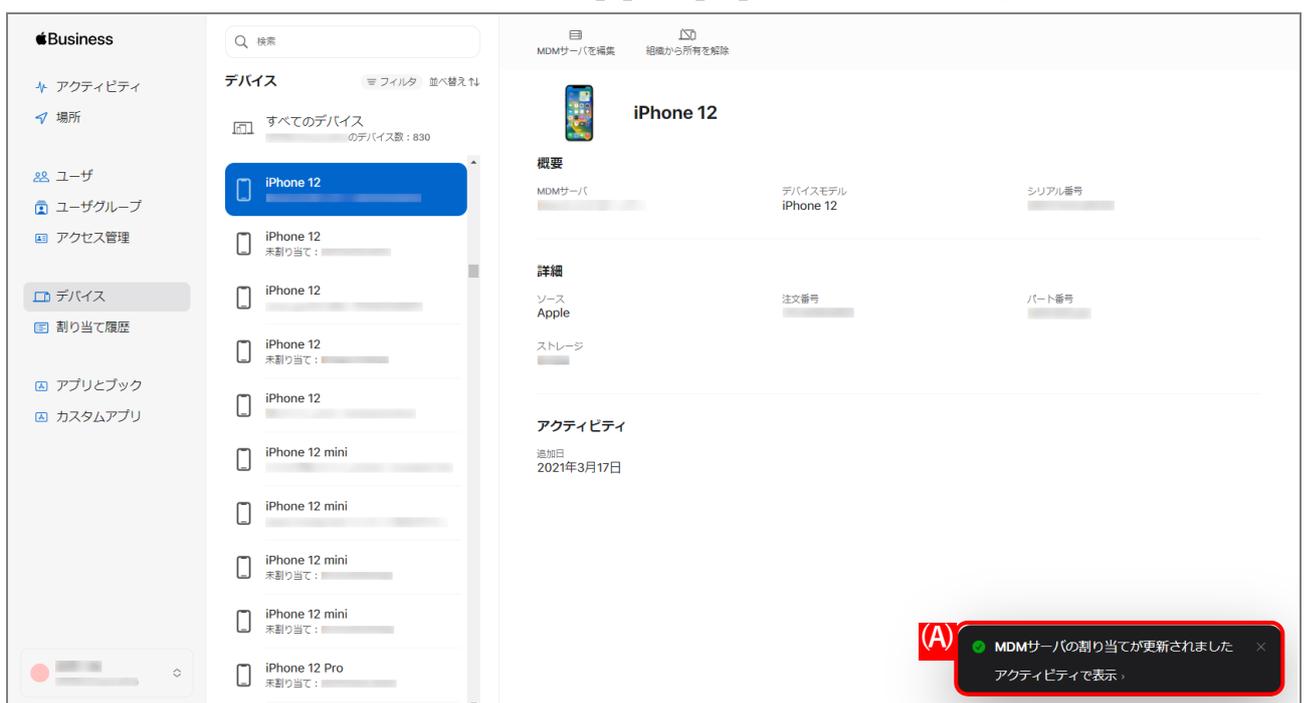
⇒対象端末の割り当てが開始されます。しばらくお待ちください。

❗本操作に失敗する場合は、対象端末で ADE を利用できない状態になっている可能性があります。詳細については、Apple または端末の購入元にお問い合わせください。



⇒割り当ての更新が完了すると、右下に (A) メッセージが表示されます。

割り当てたい端末が複数ある場合は、手順【8】～【13】を繰り返してください。



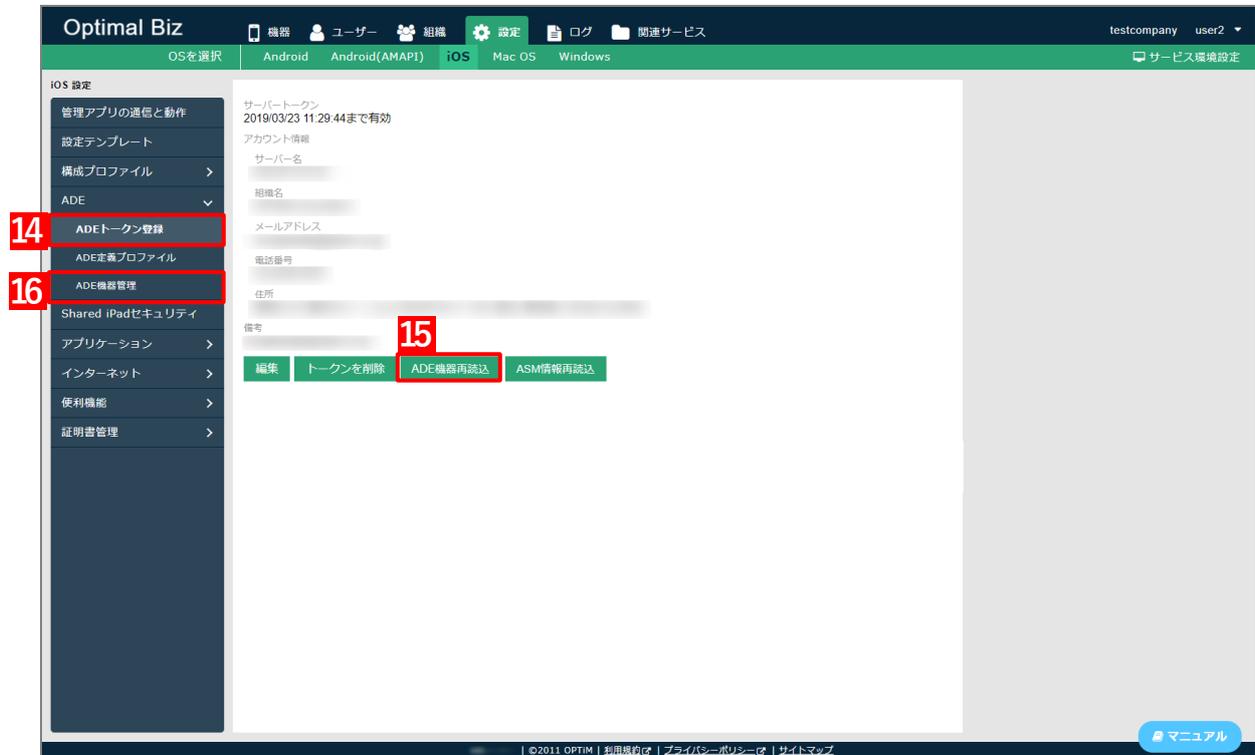
【14】 [設定] → [iOS] → [ADE] → [ADE トークン登録] をクリックします。

【15】 [ADE 機器再読込] をクリックします。

⇒ ボタンの表示が [ADE 機器再読込中...] に変わります。[ADE 機器再読込] に戻るまで、しばらくお待ちください。

☑️ しばらく経ってもボタンの表示が [ADE 機器再読込] に戻らない場合は、ブラウザでページを再読み込みしてください。

【16】 [ADE 機器管理] をクリックします。



⇒ 手順【13】で登録した端末の情報が、(A) 一覧に表示されます。

☑️ 端末の情報が正しく表示されていない場合は、(B) [ADE と同期] をクリックしてください。

☑️ 発売直後の端末は、「ADE 機器管理」画面のモデル名に「iPhone_U」と表示されることがあります。

📖 「ADE 機器管理」画面の詳細については、以下のマニュアルの該当セクションを参照してください。

🔍 『管理サイト リファレンスマニュアル』の「設定-iOS」-「ADE」-「ADE 機器管理」

機器情報		登録情報		ADE情報					
シリアル番号	モデル	ユーザー	組織	ADE状態	プロファイル(適用済)	プロファイル	端末反映日時	ADE登録日時	ステータス
<input type="checkbox"/>	iPhone 8			(なし)				2020/08/07 14:02:02	

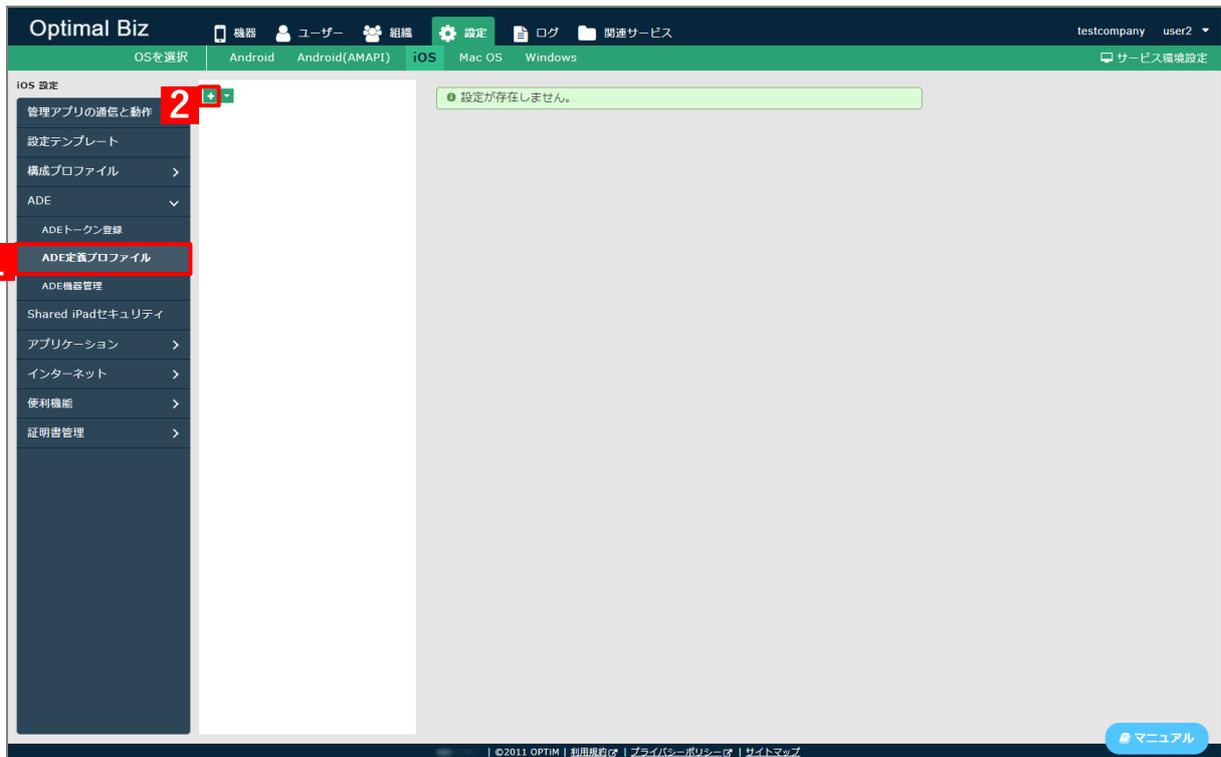
4.1.3 ADE 定義プロファイルを作成する

ADE 定義プロファイルとは、ADE を利用する端末に対して適用するさまざまな設定をまとめたものです。以下の手順で、ADE 定義プロファイルを作成します。

✍️ ADE 定義プロファイルは、端末のアクティベーション時に適用されます。そのため、ADE 定義プロファイルを変更した場合は、再度端末のアクティベーションを行う必要があります。

[1] [設定] → [iOS] → [ADE] → [ADE 定義プロファイル] をクリックします。

[2] **+** をクリックします。



[3] ADE 定義プロファイルの設定を行います。

 詳細については、以下を参照してください。

 「ADE 定義プロファイルの設定項目について」43 ページ

[4] [保存] をクリックします。


新規作成

設定

設定 - 編集

3 プロファイル名

認証設定

企業コードと認証コードの入力を必須とする

サポート設定

部署名

電話番号

メールアドレス

MDM設定

MDM登録を必須とする

※iOS13以降では必ずMDM登録されます。

監視対象モードに設定する

※iOS13以降では必ず監視対象モードになります。

MDM登録の削除を禁止する

Shared iPadに設定する

Shared iPadユーザー最大数

Shared iPad最大ユーザーストレージ容量

MB

※端末の状態により、設定値に近似したストレージ容量が
端末に設定される場合があります。
設定値が小さい場合には端末のデフォルト値が設定される
場合があります。

Macとのペアリングを許可する

※iOS13以降ではこの項目の設定は非推奨になります。
制限を行う場合は構成プロファイルアップロード - iOS制限設定の
「Apple Configurator 2 以外のホストとのペアリングを許可」
を使用してください。

セットアップアシスタントの省略する手順

パスコードを省略する

位置情報サービスを有効にしない

バックアップからの復元を有効にしない

Apple IDでのサインインを有効にしない

利用規約の表示を省略する

指紋認証の設定を省略する

Apple Payの設定を省略する

Zoom設定を省略する

Siriを有効にしない

診断情報を自動的に送信しない

True Toneの設定を省略する

データとプライバシーの設定を省略する

デバイスの復元に「Androidから移行」を表示しない

ホームボタン感度の設定を省略する

iMessageとFaceTimeの設定を省略する

機能の使い方の説明を省略する

スクリーンタイムの設定を省略する

OSの自動アップデートを有効にしない

ようこそ画面を省略する

外観モードの設定を省略する

アップデート完了表示を省略する

モバイル通信設定を省略する

4
保存

◆ADE 定義プロファイルの設定項目について

名称	説明
プロファイル名	ADE 定義プロファイルの名前を入力します。
認証設定	<ul style="list-style-type: none"> ●企業コードと認証コードの入力を必須とする 端末使用者に企業コードと認証コードを入力するよう要求します。 チェックが入っていない場合は、ADE による自動設定が行われます。 ●サポート設定 <ul style="list-style-type: none"> ・部署名 ADE 定義プロファイルに含める部署名を入力します。 ・電話番号 ADE 定義プロファイルに含める電話番号を入力します。 ・メールアドレス ADE 定義プロファイルに含めるメールアドレスを入力します。 <p><input checked="" type="checkbox"/> 「部署名」はアクティベーション中の iOS 端末にのみ表示され、アクティベーション完了後に確認することはできません。</p>
MDM 設定	<ul style="list-style-type: none"> ●MDM 登録を必須とする iOS 端末のアクティベーション時に、MDM 構成プロファイルのインストールが必須になります。 <input checked="" type="checkbox"/> iOS 13.0 以上の端末では、チェックを入れなくても必ず MDM 構成プロファイルのインストール（ライセンス認証）が行われます。 ●監視対象モードに設定する MDM 構成プロファイルにより、iOS 端末が「監視対象」になります。これにより、AirDrop、iMessage、Apple Books などの許可設定や Web フィルタリングなどの幅広い設定を適用して管理できるようになります。 <input checked="" type="checkbox"/> iOS 13.0 以上の端末では、チェックを入れなくても必ず監視対象モードになります。 ・MDM 登録の削除を禁止する 端末利用者による MDM 構成プロファイルの削除を禁止します。 <input checked="" type="checkbox"/> 「監視対象モードに設定する」にチェックが入っていない場合は、本設定にチェックを入れることはできません。 <input checked="" type="checkbox"/> この設定を有効にしたとき、以下の状態になると MDM サーバーとの通信および再認証ができなくなります。その場合、再度端末を管理できるようにするには、端末を初期化する必要があります。 <ul style="list-style-type: none"> ・管理サイトで端末が削除されている。 ・MDM 構成プロファイルが同期不可になっている。 初期化を禁止している場合は、端末を工場出荷時の状態に戻す必要があります。この方法については、Apple へお問い合わせください。 <input checked="" type="checkbox"/> 誤った HTTP プロキシ設定が端末にインストールされている場合は、通信ができなくなる可能性があります。 ・Shared iPad に設定する 端末を Shared iPad（共有 iPad）に設定します。 <input checked="" type="checkbox"/> 「MDM 登録を必須とする」と「監視対象モードに設定する」の両方にチェックが入っていない場合は、本設定にチェックを入れることはできません。 <input checked="" type="checkbox"/> 「Shared iPad ユーザー最大数」は、本製品の仕様では 50,000 です。ただし、端末の仕様により 50,000 以下になることがあります。 <input checked="" type="checkbox"/> 「Shared iPad 最大ユーザーストレージ容量」は、本製品の仕様で 1 メガバイト以上で設定します。端末の状態によっては設定値に近いストレージ容量が設定される場合があります。また、設定値が小さいと端末のデフォルト値が設定される場合があります。 ●Mac とのペアリングを許可する iOS 端末と Mac OS 端末とのペアリングができるようになります。 <input checked="" type="checkbox"/> iOS 13.0 以上の端末では、本設定は非推奨です。「構成プロファイルアップロード」 - 「iOS 制限設定」 - 「機能の制限」の「Apple Configurator 2 以外のホストとのペアリングを許可(監視対象のみ)」を使用してください。詳

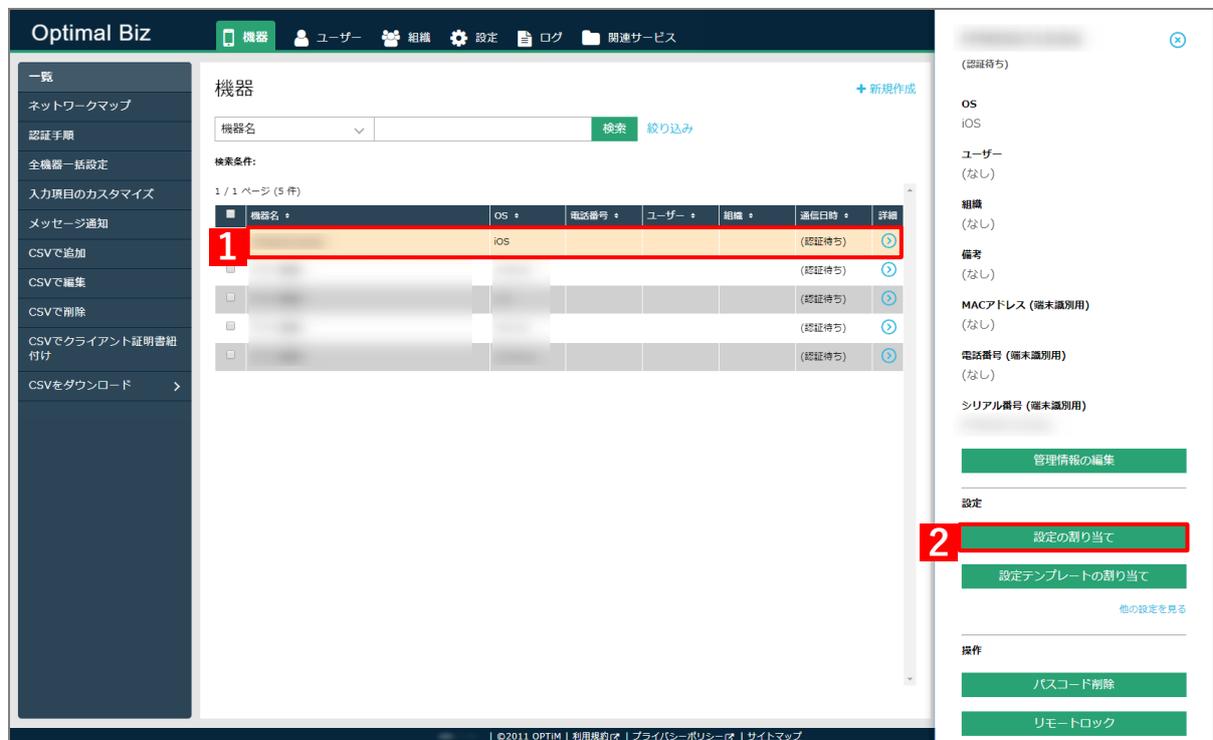
名称	説明
	<p>細については、以下のマニュアルの該当セクションを参照してください。</p> <p> 『管理サイト リファレンスマニュアル』の「設定-iOS」 - 「構成プロファイル」 - 「構成プロファイルアップロード」 - 「[iOS 制限設定] タブ」 - 「画面 (機能の制限)」</p> <p><input checked="" type="checkbox"/> 本設定にチェックが入っていない場合は、Apple の仕様により Windows 端末に接続できません。</p>
<p>セットアップアシスタントの省略する手順</p>	<ul style="list-style-type: none"> ● パスコードを省略する アクティベーション時のパスコード設定が省略されます。 <input checked="" type="checkbox"/> パスコード設定を省略する場合は、「Apple Pay の設定を省略する」、および「指紋認証の設定を省略する」を有効にしてください。 <input checked="" type="checkbox"/> iCloud から復元する場合は、パスコード設定は省略されません。 ● 位置情報サービスを有効にしない 位置情報サービスが自動的に無効になります。設定画面もスキップされます。 <input checked="" type="checkbox"/> 設定画面をスキップするには、アクティベーション時に Wi-Fi 接続を使用してください。モバイルデータ通信を使用している場合は、設定画面が表示されることがあります。 ● バックアップからの復元を有効にしない バックアップからの復元が自動的に無効になります。設定画面もスキップされます。 <input checked="" type="checkbox"/> 設定画面をスキップするには、アクティベーション時に Wi-Fi 接続を使用してください。モバイルデータ通信を使用している場合は、設定画面が表示されることがあります。 ● Apple ID でのサインインを有効にしない Apple ID でのサインインが自動的に無効になります。設定画面もスキップされます。 ● 利用規約の表示を省略する アクティベーション時の利用規約表示が省略されます。 ● 指紋認証の設定を省略する アクティベーション時の指紋認証設定が省略されます。 <input checked="" type="checkbox"/> 指紋認証設定を省略する場合は、「Apple Pay の設定を省略する」も有効にしてください。 <input checked="" type="checkbox"/> iCloud から復元する場合は、指紋認証設定は省略されません。 ● Apple Pay の設定を省略する アクティベーション時の Apple Pay 設定が省略されます。 ● Zoom 設定を省略する アクティベーション時の Zoom 設定が省略されます。 ● Siri を有効にしない Siri が自動的に無効になります。設定画面もスキップされます。 ● 診断情報を自動的に送信しない 診断情報の自動送付が無効になります。設定画面もスキップされます。 <input checked="" type="checkbox"/> アクティベーション時に「App とデータ」画面で「Android からデータを移行」を選択した場合、設定画面はスキップされません。 ● True Tone の設定を省略する True Tone の設定が自動的に有効になります。設定画面もスキップされます。 ● データとプライバシーの設定を省略する データとプライバシーの設定が自動的に有効になります。設定画面もスキップされます。 ● デバイスの復元に「Android から移行」を表示しない バックアップから復元画面で、「Android から移行」が表示されず、選択できなくなります。 ● ホームボタン感度の設定を省略する ホームボタン感度の設定が省略されます。 ● iMessage と Face Time の設定を省略する iMessage と Face Time の設定が省略されます。 ● 機能の使い方の説明を省略する

名称	説明
	<p>機能の使い方の説明が省略されます。</p> <ul style="list-style-type: none">●スクリーンタイムの設定を省略する スクリーンタイムの設定が省略されます。●OS の自動アップデートを有効にしない OS の自動アップデートの設定が省略されます。 <input checked="" type="checkbox"/>自動アップデートの設定は、端末により異なります。●ようこそ画面を省略する ようこそ画面が省略されます。●外観モードの設定を省略する 外観モードの設定が省略されます。●アップデート完了表示を省略する ソフトウェアのアップデートが完了したとき、完了表示が省略されます。●モバイル通信設定を省略する モバイル通信設定が省略されます。

4.1.4 ADE 定義プロファイルを適用する

作成した ADE 定義プロファイルを端末または組織に割り当て、「ADE 機器管理」画面で ADE と同期を行います。その後、端末のアクティベーションを行うと ADE 定義プロファイルの設定が端末に適用されます。

- [1]** 「機器」 → 「一覧」 → 一覧から対象端末をクリックします。
- [2]** 「設定」の「設定の割り当て」をクリックします。

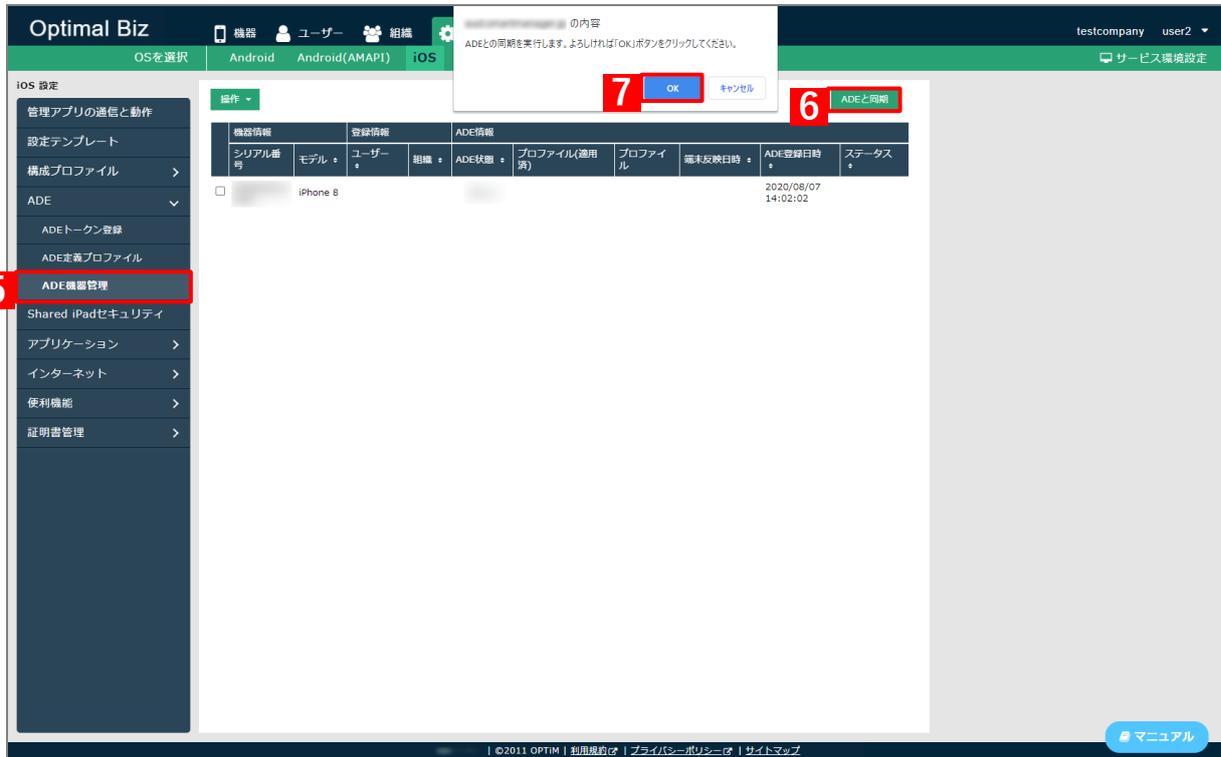


- [3]** 「ADE 定義プロファイル」のプルダウンメニューから、ADE 定義プロファイルを指定します。
 組織に割り当てる場合は、[組織] → [一覧] → 対象組織 → [iOS] タブの編集画面で、「ADE 定義プロファイル」のプルダウンメニューから、ADE 定義プロファイルを指定します。
- [4]** 「保存」をクリックします。



- [5] [設定] → [iOS] → [ADE] → [ADE 機器管理] をクリックします。
- [6] [ADE と同期] をクリックします。
- [7] [OK] をクリックします。

⇒ADE との同期が完了します。引き続き、端末のアクティベーションを行います。



◆ 「ADE 状態」 の表示について

「ADE 機器管理」 画面には ADE 定義プロファイルの状況に応じて、以下のとおり「ADE 状態」が表示されます。

- ✍️ 端末との同期が完了すると、適用されている ADE 定義プロファイル名が「ADE 定義プロファイル (適用済)」に表示され、「ADE 状態」が「適用済」に移行します。

ADE情報		
ADE状態 ↓	プロファイル(適用済)	プロファイル
適用済	ADE定義プロファイル 2	ADE定義プロ ファイル2

ADE 状態	説明
(なし)	ADE 定義プロファイルが適用されていない状態です。 ❌この状態の場合は、アクティベーション時に ADE 定義プロファイルは適用されません。
適用済	ADE に ADE 定義プロファイルが登録されている状態です。次回のアクティベーション時に ADE 定義プロファイルが適用され、「端末反映済」に移行します。
削除済	ADE から ADE 定義プロファイルが削除されている状態です。 ❌この状態の場合は、アクティベーション時に ADE 定義プロファイルは適用されません。 ✍️この状態から「適用済」に戻すには、ADE 定義プロファイルを再度適用し、[ADE と同期] をクリックします。
端末反映済	ADE に登録されている ADE 定義プロファイルが、すでに端末に適用されている状態です ❌この状態でアクティベーションを行うと、該当の ADE 定義プロファイルが毎回適用されます。

4.2 端末のアクティベーションを行う

以下の手順で、端末のアクティベーションを行うことにより、ライセンス認証が完了します。

【1】 端末を起動し、画面の指示に従って操作を進めます。

- 画面の指示は、端末に適用される ADE 定義プロファイルの設定によって異なります（「セットアップアシスタントの省略する手順」でチェックを入れた設定項目は、アクティベーション時に省略されます）。

なお、ADE 定義プロファイルは、以下の「Wi-Fi ネットワークを選択」画面でネットワーク接続の方法を選択したあとに適用されます。



こんにちは

ホームを押して開く



- 端末をパソコンに接続している場合に、「Wi-Fi ネットワークを選択」画面に表示される (A) [Mac または PC へ接続] は、タップしないでください。



[2] 「ようこそ iPhone へ」の画面が表示されたら、[さあ、はじめよう!] をタップします。

⇒ 端末のアクティベーション、およびライセンス認証が完了します。

- ☑ 引き続き以下を参照して、エージェントをインストール/認証してください。

🔗 「エージェントをインストール/認証する」51 ページ

- ☑ エージェント機能を契約していない場合は、これで端末のキッティングが完了します。以降の操作は不要です。

ようこそiPhoneへ



5 エージェントを認証する



注意

- 該当の端末とは異なるアクティベーションコードでも認証されますので注意してください。
 - ☑ 異なるアクティベーションコードで認証してしまった場合は、エージェントのアンインストールと再インストールが必要です。
-

5.1 エージェントをインストール／認証する

エージェントをインストール／認証するには、3種類の方法があります。管理サイトおよび端末の設定に応じて、適切な方法を選択してください。

- ポータルからインストール／認証する

端末にポータルと App Store をどちらも表示している設定の場合は、本方法を選択してください。

- App Store からインストール／認証する

App Store のみ表示している設定の場合は、本方法を選択してください。

- アプリケーション配信を利用してインストール／自動認証する

ポータルと App Store をどちらも非表示にしている設定の場合は、本方法を選択してください。

🔗 エージェントをインストール／認証するには、あらかじめ以下のどちらかのライセンス認証を行う必要があります。

🔗 「MDM 構成プロファイルをインストールする」14 ページ

🔗 「ADE を利用してライセンス認証を行う」26 ページ

🔗 ポータルの表示／非表示および App Store の非表示は、管理サイトで設定できます。詳細については、以下のマニュアルの該当セクションを参照してください。

🔗 『管理サイト リファレンスマニュアル』の「サービス環境設定」－「ポータル表示」

🔗 『管理サイト リファレンスマニュアル』の「設定-iOS」－「構成プロファイル」－「構成プロファイルアップロード」

5.1.1 ポータルからインストール／認証する

以下の手順で、ポータルからエージェントをインストール／認証します。

[1] ホーム画面の [ポータル] をタップします。

⇒ ブラウザー (Safari) が起動し、ポータルが表示されます。



【2】 [エージェントを認証する] をタップします。



【3】 [App Store からインストール] タップします。



【4】 [OK] をタップします。

⇒ App Store でエージェントのページが表示されます。

パスワードを求められた場合は、該当 Apple ID のパスワードを入力してください。

【5】 [入手] をタップします。

⇒ エージェントのインストールが開始されます。端末のホーム画面に、[Optimal Biz] のアイコンが表示されるまでお待ちください。



【6】ポータルに戻り、[起動して認証] をタップします。

⇒ エージェントの認証が開始されます。

☑ ライセンス認証を行っていない場合は、このあと表示される画面に従ってライセンス認証を行ってください。

☑ iOS 13.0 以上の端末の場合は、以降の手順が異なります。以下を参照してください。

🔗 「iOS 13.0 以上の端末で位置情報の常に利用を許可する」55ページ

【7】「OK」をタップします。

【8】[常に許可] をタップします。

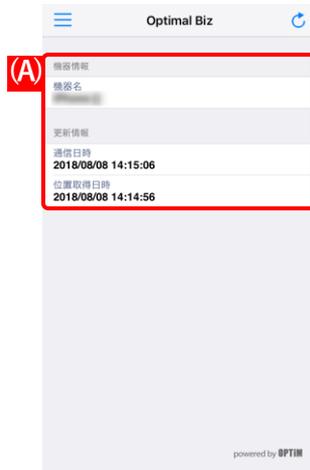
☑ 位置情報を「常に許可」に設定していないと、エージェントの機能が使用できないことがあります。



【9】 「許可」 をタップします。

- ☑ 本操作は、初回起動時のみ求められます。
- ☑ 「許可」 をタップしないと、端末が管理サイトからメッセージを受信したときに、通知が表示されません。

⇒ (A) 「機器情報」 および 「更新情報」 が表示されたら、エージェントの認証は完了です。



5.1.1.1 iOS 13.0 以上の端末で位置情報の常に利用を許可する

iOS 13.0 以上の端末でエージェントを認証する場合は、位置情報の利用について許可を求める画面で「常に許可」に設定できません。そのため、以下の手順で位置情報の利用を常に許可する設定にします。

- ☑ 本操作を行わないと、端末から正しい位置情報の取得や送信ができません。
- ☑ 位置情報を「常に許可」に設定していないと、エージェントの機能が使用できないことがあります。

【1】 [App の使用中は許可] をタップします。

⇒ 位置情報サービスの権限について許可を求められます。



【2】 [許可] をタップします。

- ☑ 本操作は、初回起動時のみ求められます。
- ☑ [許可] をタップしないと、端末が管理サイトからメッセージを受信したときに、通知が表示されません。

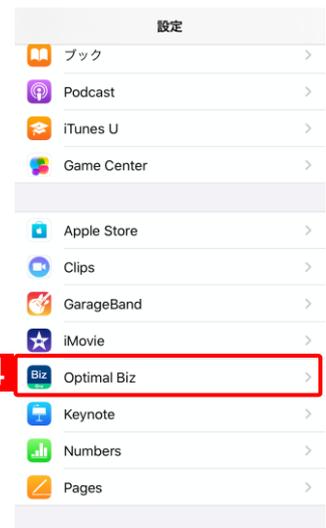


【3】 [はい] をタップします。



【4】 端末の「設定」画面から、[Optimal Biz] をタップします。

📌 「設定」の異なる階層が表示されている場合は、最初の階層を表示してください。

**【5】** [位置情報] をタップします。**【6】** [常に] をタップし、チェックを入れます。

5.1.2 App Store からインストール／認証する

以下の手順で、App Store からエージェントをインストール／認証します。

🔗 Apple の仕様により、App Store の操作は変更されることがあります。

【1】 ホーム画面の [App Store] をタップします。

⇒ App Store が表示されます。



【2】 「Optimal Biz」と入力し、検索します。

⇒ 検索結果が表示されます。

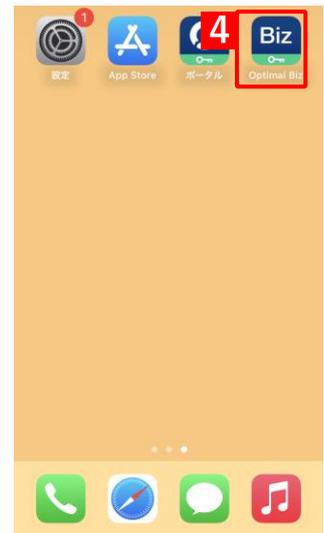


【3】 エージェントの [入手] をタップします。

⇒ エージェントのインストールが開始されます。端末のホーム画面に、[Optimal Biz] のアイコンが表示されるまでお待ちください。

【4】 ホーム画面の [Optimal Biz] をタップします。

⇒ エージェントが起動し、プライバシーポリシーの画面が表示されます。

**【5】 [同意する] をタップします。**

☑ 本操作は、エージェントのインストールおよびアップデート後の初回起動時のみ求められます。

**【6】 「OK」 をタップします。**

☑ 本操作は、エージェントのインストールおよびアップデート後の初回起動時のみ求められます。



【7】 「企業コード」、「アクティベーションコード」、および「URL」を入力します。

- ☑ 企業コード、アクティベーションコード、URL は管理者にお問い合わせください。

【8】 [送信] をタップします。

⇒ エージェントの認証が開始されます。

- ☑ ライセンス認証を行っていない場合は、このあと表示される画面に従ってライセンス認証を行ってください。
- ☑ iOS 13.0 以上の端末の場合は、以降の手順が異なります。以下を参照してください。

🔗 「iOS 13.0 以上の端末で位置情報の常に利用を許可する」55 ページ

【9】 [常に許可] をタップします。

- ☑ 位置情報を「常に許可」に設定していないと、エージェントの機能が使用できないことがあります。

【10】 [許可] をタップします。

- ☑ 本操作は、初回起動時のみ求められます。
- ☑ [許可] 以外をタップした場合は、管理サイトからメッセージを受信したときに、端末に通知が表示されません。

⇒ (A) 「機器情報」および「更新情報」が表示されたら、エージェントの認証は完了です。



5.1.3 アプリケーション配信を利用してインストール／自動認証する

端末上にポータルと App Store をどちらも非表示にしている設定の場合は、管理サイトのアプリケーション配信機能と App Configuration 機能を利用することにより、エージェントをインストール／自動認証できます。

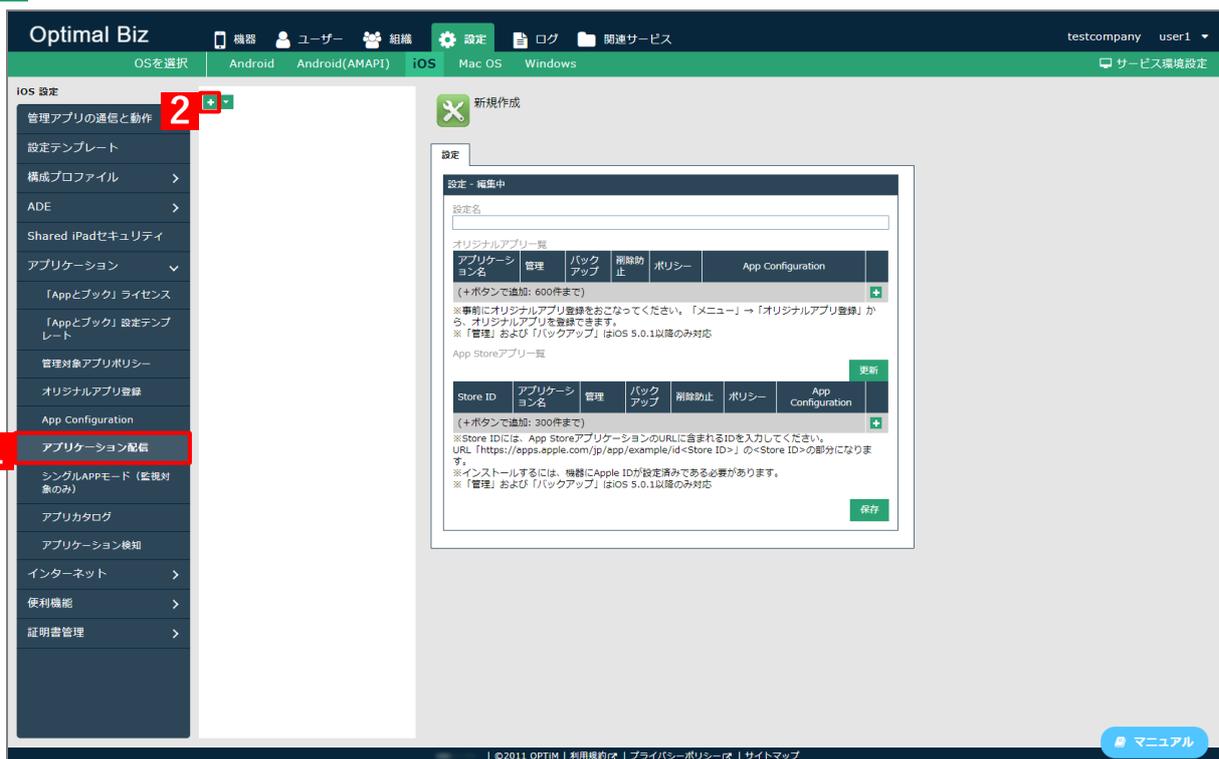
📌 機能および操作の詳細については、以下のマニュアルの該当セクションを参照してください。

- 🔍 『管理サイト リファレンスマニュアル』の「設定-iOS」-「アプリケーション」-「アプリケーション配信」
- 🔍 『管理サイト リファレンスマニュアル』の「設定-iOS」-「アプリケーション」-「App Configuration」
- 🔍 『管理サイト リファレンスマニュアル』の「機器」-「一覧」-「機器の設定」-「(設定-iOS) 設定の割り当て」

5.1.3.1 アプリケーション配信でエージェントをインストールする

以下の手順で、エージェントを端末に配信するための設定（アプリケーション配信設定）と、エージェントを自動認証するための設定（App Configuration 設定）を作成します。

- [1]** [設定] → [iOS] → [アプリケーション] → [アプリケーション配信] をクリックします。
- [2]** **+** をクリックします。



- [3]** 「設定名」に任意の設定名を入力します。
- [4]** 「App Store アプリ一覧」の **+** をクリックします。

新規作成

設定

設定 - 編集集中

設定名

オリジナルアプリ一覧

アプリケーション名	管理	バックアップ	削除防止	ポリシー	App Configuration
(+ ボタンで追加: 600件まで)					

※事前にオリジナルアプリ登録をおこなってください。「メニュー」→「オリジナルアプリ登録」から、オリジナルアプリを登録できます。
※「管理」および「バックアップ」はiOS 5.0.1以降のみ対応

App Storeアプリ一覧

Store ID	アプリケーション名	管理	バックアップ	削除防止	ポリシー	App Configuration
(+ ボタンで追加: 300件まで)						

※Store IDには、App StoreアプリケーションのURLに含まれるIDを入力してください。
URL「https://apps.apple.com/jp/app/example/id<Store ID>」の<Store ID>の部分になります。
※インストールするには、機器にApple IDが設定済みである必要があります。
※「管理」および「バックアップ」はiOS 5.0.1以降のみ対応

更新

保存

- [5]** 「Store ID」に「484555006」（エージェントのStore ID）を入力します。
- [6]** 「管理」の「有効」にチェックを入れます。
- [7]** [保存] をクリックします。

⇒アプリケーション配信設定が作成されます。

新規作成

設定

設定 - 編集集中

設定名

オリジナルアプリ一覧

アプリケーション名	管理	バックアップ	削除防止	ポリシー	App Configuration
(+ ボタンで追加: 600件まで)					

※事前にオリジナルアプリ登録をおこなってください。「メニュー」→「オリジナルアプリ登録」から、オリジナルアプリを登録できます。
※「管理」および「バックアップ」はiOS 5.0.1以降のみ対応

App Storeアプリ一覧

Store ID	アプリケーション名	管理	バックアップ	削除防止	ポリシー	App Configuration
484555006	---	<input checked="" type="checkbox"/> 有効 <input type="checkbox"/> 許可	<input type="checkbox"/> 有効	管理対象アプリポリシーがありません。	新規追加	App Configurationがありません。
(+ ボタンで追加: 300件まで)						

※Store IDには、App StoreアプリケーションのURLに含まれるIDを入力してください。
URL「https://apps.apple.com/jp/app/example/id<Store ID>」の<Store ID>の部分になります。
※インストールするには、機器にApple IDが設定済みである必要があります。
※「管理」および「バックアップ」はiOS 5.0.1以降のみ対応

更新

保存

- [8] [設定] → [iOS] → [アプリケーション] → [App Configuration] をクリックします。
[9] **+** をクリックします。

Optimal Biz

OSを選択 | Android | Android(AMAPI) | **iOS** | Mac OS | Windows | testcompany user1

サービス環境設定

iOS 設定

管理アプリの通信と動作 **9** **+**

設定テンプレート

構成プロファイル >

ADE >

Shared iPadセキュリティ

アプリケーション ▾

「Appとブック」ライセンス

「Appとブック」設定テンプレート

管理対象アプリポリシー

オリジナルアプリ登録

8 App Configuration

アプリケーション配信

シングルAPPモード (監視対象のみ)

アプリカタログ

アプリケーション検知

インターネット >

便利機能 >

証明書管理 >

新規作成

設定 - 編集中

設定名

アプリケーションタイプ

●オリジナルアプリ ○App Storeアプリ

アプリケーション名

設定値

Key	Type	Value
(+ボタンで追加: 100件まで)		

保存

マニュアル

©2011 OPTIM | 利用規約 | プライバシーポリシー | サイトマップ

- 【10】** 「設定名」に任意の設定名を入力します。
- 【11】** 「アプリケーションタイプ」の「App Store アプリ」を選択します。
- 【12】** 「アプリケーション名」のプルダウンメニューから、「Optimal Biz」を指定します。
- 【13】** 「設定値」の **+** をクリックして設定項目を追加し、各項目に (A) 企業コード、(B) 管理サイト URL、および (C) アクティベーションコードを設定します。
- (A) 企業コードの「Key」および「Value」に、それぞれ以下の値を入力してください。
 - Key : company_code
 - Value : (特定の企業コード) または%COMPANY_CODE%
 - (B) 管理サイト URL の「Key」および「Value」に、それぞれ以下の値を入力してください。
 - Key : server_url
 - Value : https://biz3.optim.co.jp/または%SERVER_URL%
 - (C) アクティベーションコードの「Key」および「Value」に、それぞれ以下の値を入力してください。
 - Key : activation_code
 - Value : %MDM_ACTIVATION_CODE%
 - (A) 企業コード、(B) 管理サイト URL、および (C) アクティベーションコードとともに、「Type」は「String」を選択してください。
- 【14】** 「保存」をクリックします。
⇒ App Configuration 設定が作成されます。

新規作成

設定

設定 - 編集

10 設定名

アプリケーションタイプ
○オリジナルアプリ App Storeアプリ 11

アプリケーション名

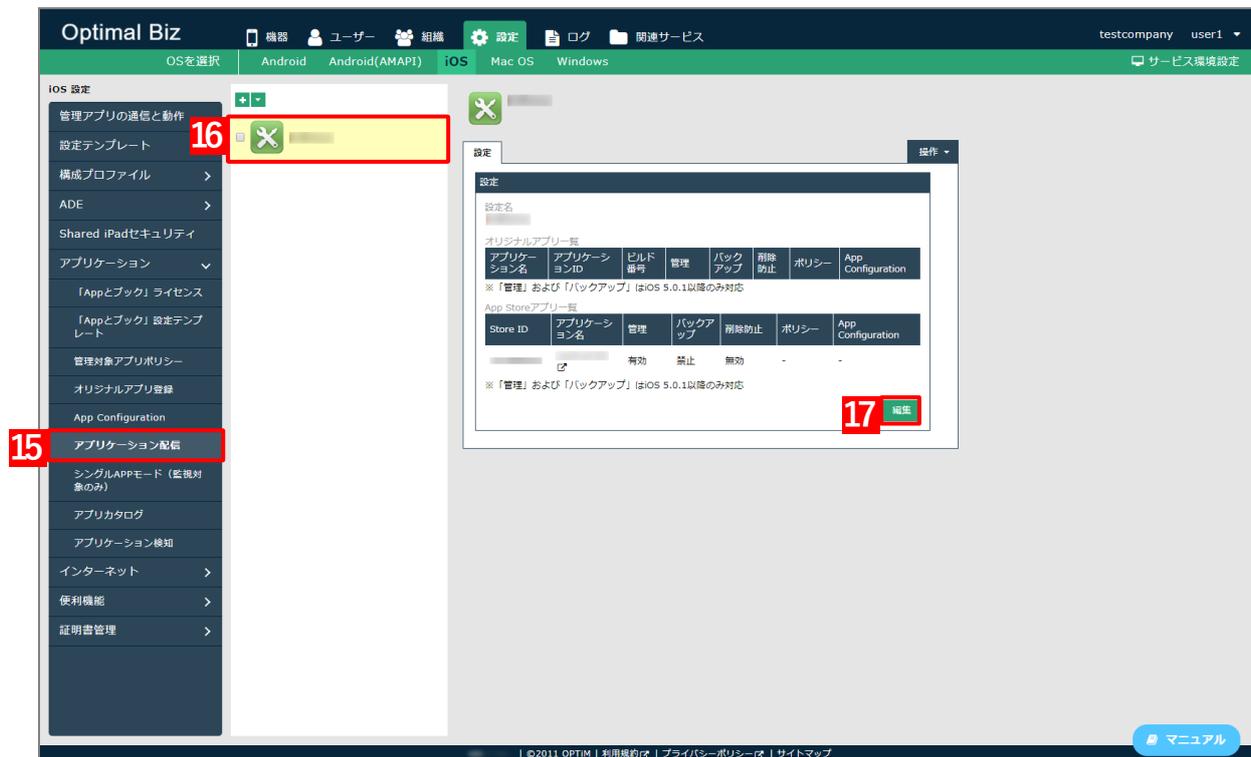
12

Key	Type	Value
(A) company_code	String	
(B) server_url	String	
(C) activation_code	String	%MDM_ACTIVATION_CODE%

(+ボタンで追加: 100件まで) 13

14 保存

- [15]** [設定] → [iOS] → [アプリケーション] → [アプリケーション配信] をクリックします。
[16] 一覧から、手順【7】で作成したアプリケーション配信設定をクリックします。
[17] [編集] をクリックします。



- [18]** 「App Configuration」のプルダウンメニューから、手順【10】で設定した設定名を指定します。
[19] [保存] をクリックします。



【20】 [機器] → [一覧] → 一覧から対象端末をクリックします。

【21】 「設定」の「設定の割り当て」をクリックします。

The screenshot shows the Optimal Biz interface. On the left is a navigation menu with options like '一覧', 'ネットワークマップ', '認証手順', etc. The main area displays a table of devices under the heading '機器'. The first row is highlighted with a red box and labeled '20'. The table has columns for '機器名', 'OS', '電話番号', 'ユーザー', '組織', '通信日時', and '詳細'. On the right sidebar, under the '設定' section, the '設定の割り当て' button is highlighted with a red box and labeled '21'. Other buttons in the sidebar include '管理情報の編集', '設定テンプレートの割り当て', 'パスワード削除', 'リモートロック', and 'ログ'.

【22】 「アプリケーション配信」の「編集」をクリックします。

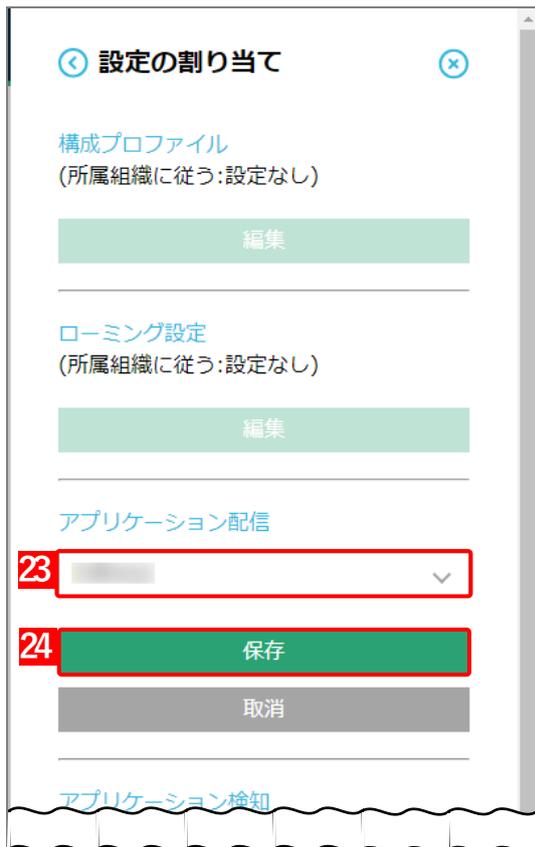
The screenshot shows a dialog box titled '設定の割り当て' (Assign Settings). It contains three sections, each with a green '編集' (Edit) button:

- 構成プロファイル (構成組織に依る: 設定なし)
- ローミング設定 (所属組織に依る: 設定なし)
- アプリケーション配信 (所属組織に依る: 設定なし)

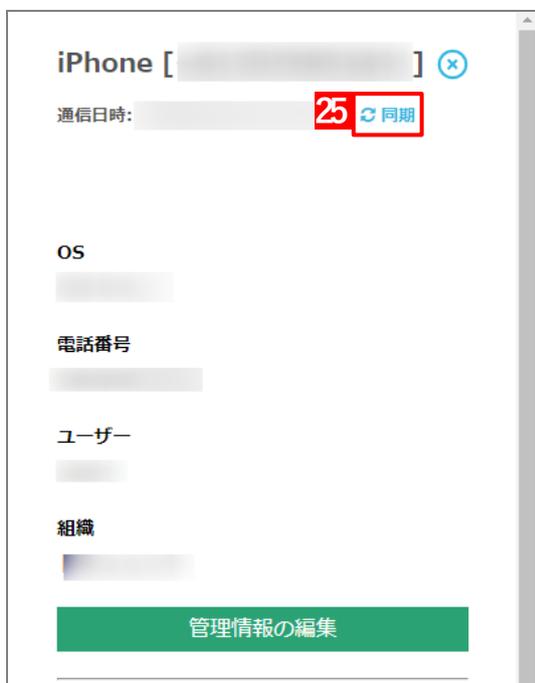
 The '編集' button for 'アプリケーション配信' is highlighted with a red box and labeled '22'. Below these sections is a section for 'アプリケーション検知'.

【23】 「アプリケーション配信」のプルダウンメニューから、手順【3】で設定した設定名を指定します。

【24】 「保存」をクリックします。



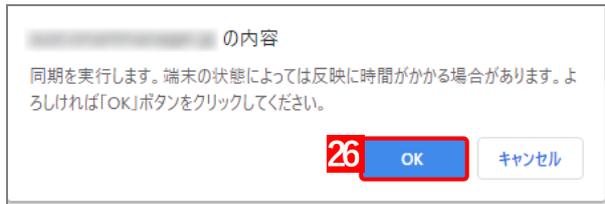
【25】 「同期」をクリックします。



【26】 [OK] をクリックします。

⇒ 端末にエージェントがインストールされます。端末のホーム画面に、[Optimal Biz] のアイコンが表示されるまでお待ちください。

📌 エージェントが端末にインストールされるまでに、多少時間がかかることがあります。



5.1.3.2 エージェントを自動認証する

以下の手順で、端末にインストールされたエージェントを自動認証します。

[1] ホーム画面の [Optimal Biz] をタップします。

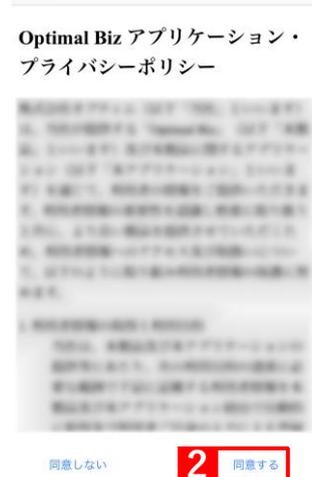
⇒ エージェントが起動し、プライバシーポリシーの画面が表示されます。



[2] [同意する] をタップします。

📌 iOS 13.0 以上の端末の場合は、以降の手順が異なります。以下を参照してください。

📄 「iOS 13.0 以上の端末で位置情報の常に利用を許可する」55 ページ

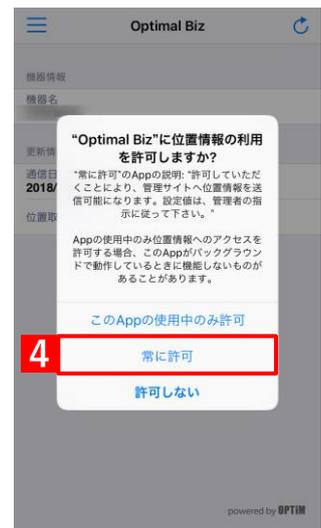


[3] 「OK」 をタップします。



【4】 [常に許可] をタップします。

- 📌 位置情報を「常に許可」に設定していないと、エージェントの機能が使用できないことがあります。



【5】 [許可] をタップします。

- 📌 [許可] をタップしないと、端末が管理サイトからメッセージを受信したときに、通知が表示されません。

⇒ (A)「機器情報」および「更新情報」が表示されたら、エージェントの認証は完了です。

