OPTiM

Optimal Biz
iOS Kitting Manual

Last update date October 16, 2022
(Website ver.9.13.1)
OPTiM Corporation

Getting Started

Purpose of this manual

This manual explains operation of iPhone/iPad device.

How to read this manual

The meanings of symbols and marks used in the explanation of this manual, the types of screens used in manuals, and notes are as follows.

This manual explains iOS device operations. For operations in the management site, refer to the following manual.

<Management Site Reference Manual>

This manual refers to the iPad OS as "iOS".

◆ About the symbol ·mark

The marks and symbols used in the manual are as follows.

Symbols / Mark	Description
[]	Represents menu name, button name, and link name.
" "	Represents the name you want to emphasize, such as tab name, function name, item name, reference destination in the manual.
< >	Represents the manual name or the document name.
⇒	Represents the result of the operation.
	Represents the manual or document to be referenced.
	Represents the reference in the manual and the link to the website.
	Explains what to watch out for.
	Explains points of handling and operation and what is convenient to know.
Operation	In the explanation of the screen, describes the menu operation for displaying the corresponding screen. Ex) **Operation** [Settings]→[ios]→[Applications]→[Application Distribution]→

◆ About the screen

- In this manual, the user type is for "administrator". When logging in to the management site other than the user type "administrator", editing and browsing are restricted according to the user type. For details, refer to the following.

  "User" – "List" – "Create a user"<Management Site Reference Manual>

- The version notation on the screen may differ from the actual one.
- Some screens and operations may differ depending on the OS version of Windows and the browser to be used. In this manual, we explain using the screen displayed in Google Chrome.

About website URL

URLs of websites other than our company described in the manual are subject to change without notice.

About trademark

●iOS and iPad are trademarks of Apple Inc.

●Company names and product names mentioned are trademarks and registered trademarks of each company.

Table of contents

1 About iOS client

This chapter describes the following items.

1.1 Overview

Optimal Biz (hereinafter referred to as this product) is a service that allows you to manage and operate your iOS devices without specialized knowledge. You can remotely lock or remotely wipe (factory reset) iOS devices from the Optimal Biz management site.

You must register an Apple Push certificate before you use this service. For information on registration, refer to the following manual.

<Apple Push Certificate Annual Update Manual>

For device management using Automated Device Enrollment (ADE) provided by Apple, refer to the following manual.

< Automated Device Enrollment (ADE) Operation Manual>

1.2 OS support policy

In this product, OS support policy was established with the aim of ensuring product operation and security functions. We will end support of lower OS version on a regular basis, so customers who use OS and devices that are not subject to support will be requested to update OS or change model.

This OS support policy also covers Optimal Biz Browser and app catalog.

Support policy	Example of support
●Support from the latest supported OS of this product to OS major version three generations ago. ●With the addition of the latest supported OS, as for the OS version that became out of support, we respond to inquiries as much as possible only for one year from the date the support period expires as transition period. Operation guarantee and trouble correspondence are not performed.	●iOS 15.x：Latest supported OS ●iOS 14.x：One generation ago ●iOS 13.x：Two generations ago ●iOS 12.x：Three generations ago iOS 11.x is no longer supported. We will try our best to respond to your inquiries until September 21, 2022.

1.3 System Requirement

iOS client system requirement is as follows.

Supported Devices	iPhone 5s iPhone 6 iPhone 6 Plus 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 (2nd generation) iPhone 11 iPhone 11 Pro iPhone 11 Pro Max iPhone 12 iPhone 12 Pro iPhone 12 mini iPhone 12 Pro Max iPad (5th generation) iPad (6th generation) iPad (7th generation) iPad (8th generation) iPad mini (2nd generation) iPad mini (3rd generation) iPad mini (4th generation) iPad mini (5th generation) iPad Air (1st generation) iPad Air (2nd generation) iPad Air (3rd generation) iPad Air (4rd generation) iPad Pro 9.7-inch model iPad Pro 10.5-inch model iPad Pro 11-inch model iPad Pro 12.9-inch model iPod touch (6th generation)
Supported OS	iOS 12.0 or later
Network Connection	Connected to the internet via Mobile network or Wi-Fi. Available to communicate HTTPS (port 443) to the management site with/without proxy.

Support for agent: Optimal Biz supports the agent for 180 days after release. Also supported are two newest generations of released agents.

2 Selecting a kitting method

This chapter describes the following items.

Attention

- You must register the Apple Push certificate before you use this service. For information on registration, refer to the following manual.

  <Apple Push Certificate Annual Update Manual>

2.1 Overview and flow of kitting methods

There are two methods for kitting iOS devices depending on whether or not you use Automated Device Enrollment (ADE). Review your devices and operation cases and select an appropriate kitting method.

Under "using ADE", select "Set to supervised mode (required for iOS 13 or higher)" to set the kitted device as a supervised device.

Kitting method	Description
Not using ADE	Perform license authentication of a device not registered to ABM or ASM from a specified URL without connecting to ADE. This method provides the following benefits. ・You do not have to factory reset a device before kitting. For details on kitting methods, refer to the following. "License authentication" Page 11
Using ADE	Perform license authentication a device not registered to ABM or ASM by connecting to ADE. This method provides the following benefits. ・Pre-kitting devices can be registered as pre-kitting devices. ・Device operation during activation can be reduced. For more information on ADE, refer to the following. "About ADE" Page 10 For details on kitting methods, refer to the following. "Using ADE for license authentication" Page 24 To use ADE, you need an Apple Customer Number and a D-U-N-S number (company identification code). For more information regarding the D-U-N-S number, contact a D-U-N-S number management company. You do not have to factory reset a device before kitting.

2.1.1 About ADE

ADE is a device management feature provided by Apple Business Manager (ABM). ADE simplifies tasks when you introduce iOS devices into a company or educational institution. Because ADE settings are reflected over-the-air during device activation, they eliminate cumbersome introduction steps that were previously carried out for each device, such as wired activation using Apple Configurator and profile installation.

You can also use a supervision mode for more secure device management, and prevent users from removing MDM profiles from their devices.

About ABM

ABM is a portal site provided by Apple for assisting system administrators. By integrating ADM with MDM, system administrators can configure various values in devices, and purchase apps and distribute them to devices.

ABM replaces the old Apple Deployment Programs (ADP).

For more information on ABM, refer to the following.

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

3 License authentication

This chapter describes the following items.

3.1 Installing an MDM configuration profile

Use the following steps to install an MDM configuration profile and perform license authentication.

Steps are different for devices below iOS 12.2 and devices with iOS 12.2 and later. Choose one of the following methods depending on the device's iOS version.

- For devices under iOS 12.2
- For devices with iOS 12.2 and later

If you are using device authentication control in the management site, you must register a target device in the setting before license authentication. For more information, contact your administrator.

3.1.1 For devices under iOS 12.2

There are two authentication methods. Select one of the following methods.

- ●Authentication with an authentication code
- ●Authentication by user ID/email address and password

Safari is the only browser you can use for the following procedure.

Steps after 0 are the same in both methods.

Authentication with an authentication code

【1】 Tap [Safari] on the home screen.

【2】 Enter the URL of the Activation screen.

⇒The Activation screen appears.

Contact your administrator for the URL of the Activation screen.

【3】 Tap [Terms of Service] and read the content.

If you tap [Submit] in step 【5】, it is considered that you have agreed to the terms of service.

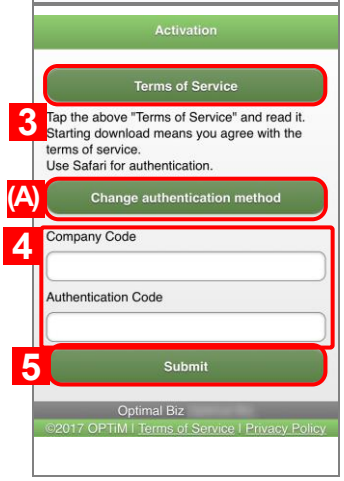
【4】 Enter "Company Code" and "Authentication Code".

Contact your administrator for your company code.

If you see different entries, tap [Change authentication method] (A) to change the screen.

【5】 Tap [Submit].

⇒License authentication will start.



Authentication by user ID/email address and password

【1】 Tap [Safari] on the home screen.

【2】 Enter the URL of the Activation screen.

⇒The Activation screen appears.

Contact your administrator for the URL of the Activation screen.

【3】 Tap [Terms of Service] and read the content.

If you tap [Submit] in step 【5】 , it is considered that you have agreed to the terms of service.

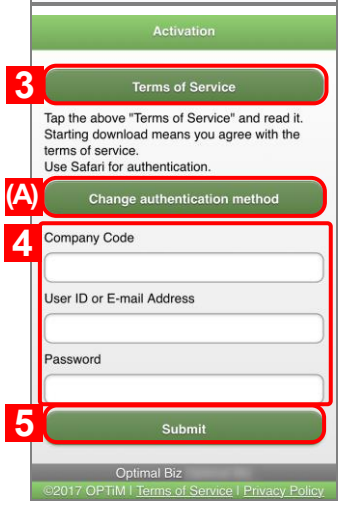
【4】 Enter the "Company Code", "User ID or E-mail Address", and "Password".

Contact your administrator for your company code, user ID/email address, and password.

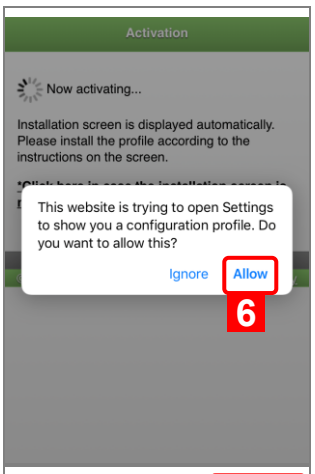
If you see different entries, tap [Change authentication method] (A) to change the screen.

【5】 Tap [Submit].

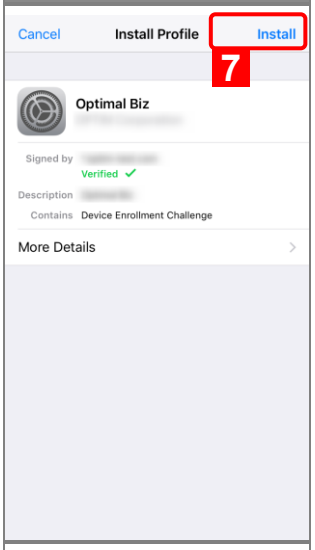
⇒License authentication will start.



【6】 Tap [Allow].



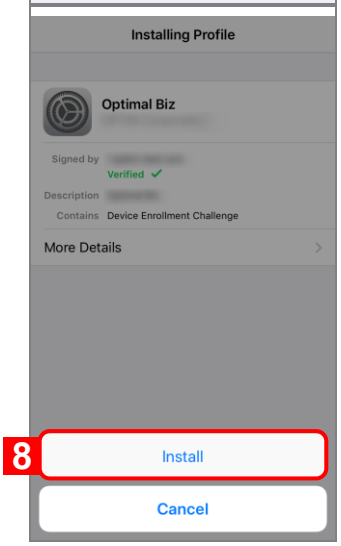
【7】 Tap [Install].



【8】 Tap [Install].

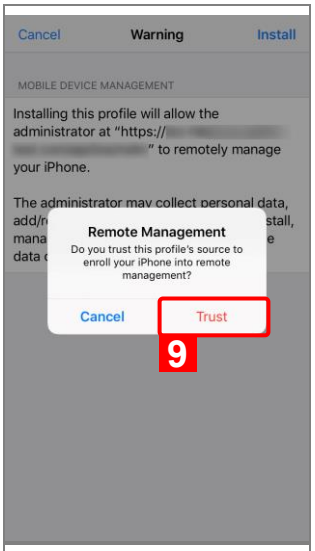
⇒Installation will start, and you will be asked to confirm remote management.

If a passcode entry screen appears, enter the passcode of the device.



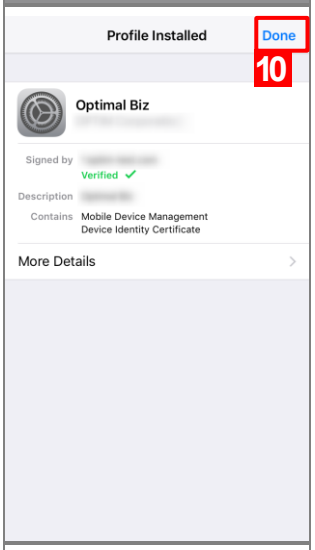
【9】Tap [Trust].

⇒Wait for a while until the installation completion screen appears.



【10】Tap [Done].

⇒License authentication will start. Wait for a while until it completes.



【11】To register additional device information, tap [Next].

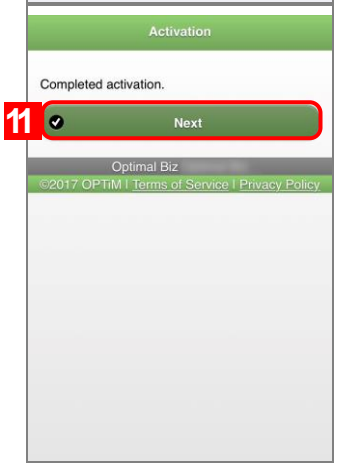
⇒For the rest of the procedure, refer to the following.

☞"Registering device information" Page 23

If you do not register device information anymore, license authentication is complete. Refer to the following and install/authenticate the agent.

☞"Installing and authenticating the agent" Page 51

You can register device information later in the management site.



3.1.2 For devices with iOS 12.2 and later

There are two authentication methods. Select one of the following methods.

- ●Authentication with an authentication code
- ●Authentication by user ID/email address and password

Safari is the only browser you can use for the following procedure.

Steps after 12 are the same in both methods.

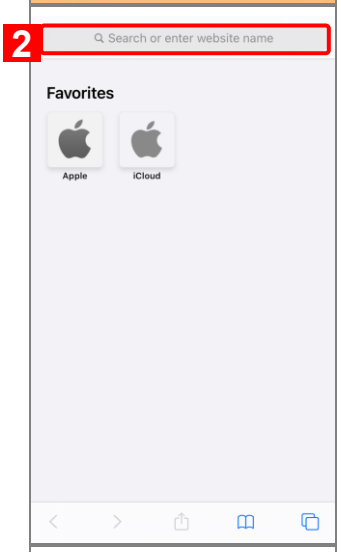
Authentication with an authentication code

【1】 Tap [Safari] on the home screen.

【2】 Enter the URL of the Activation screen.

⇒The Activation screen appears.

Contact your administrator for the URL of the Activation screen.



【3】 Tap [Terms of Service] and read the content.

If you tap [Submit] in step 【5】, it is considered that you have agreed to the terms of service.

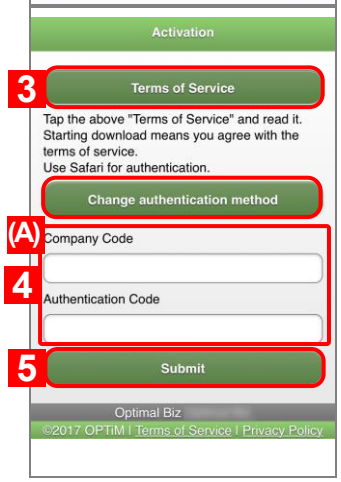
【4】 Enter "Company Code" and "Authentication Code".

Contact your administrator for your company code.

If you see different entries, tap [Change authentication method] (A) to change the screen.

【5】 Tap [Submit].

⇒License authentication will start.



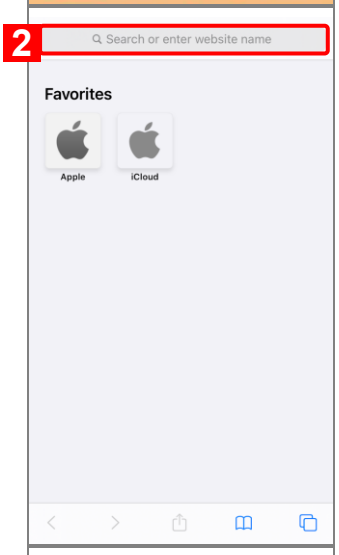
Authentication by user ID/email address and password

【1】 Tap [Safari] on the home screen.

【2】 Enter the URL of the Activation screen.

⇒The Activation screen appears.

Contact your administrator for the URL of the Activation screen.



【3】 Tap [Terms of Service] and read the content.

If you tap [Submit] in step 【5】 , it is considered that you have agreed to the terms of service.

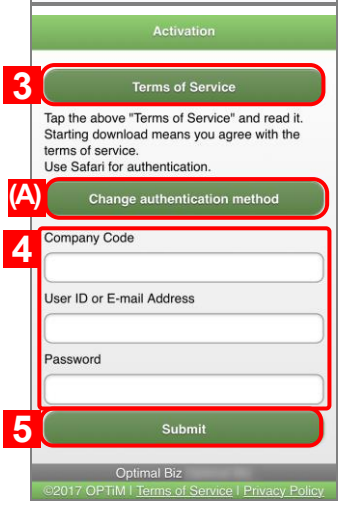
【4】 Enter the "Company Code", "User ID or E-mail Address", and "Password".

Contact your administrator for your company code, user ID/email address, and password.

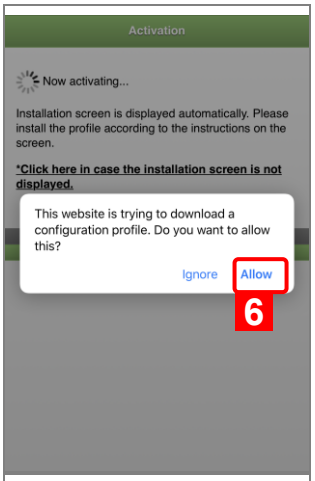
If you see different entries, tap [Change authentication method] (A) to change the screen.

【5】 Tap [Submit].

⇒License authentication will start.

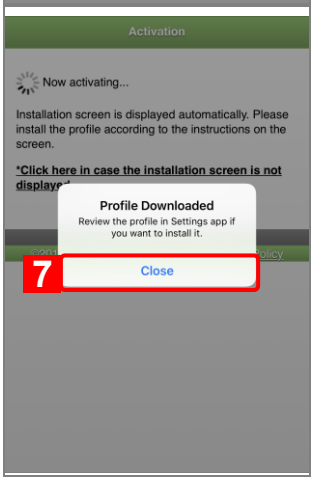


【6】**Tap [Allow].**

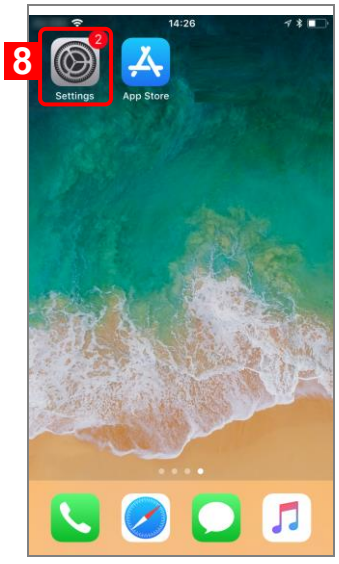


【7】**Tap [Close].**

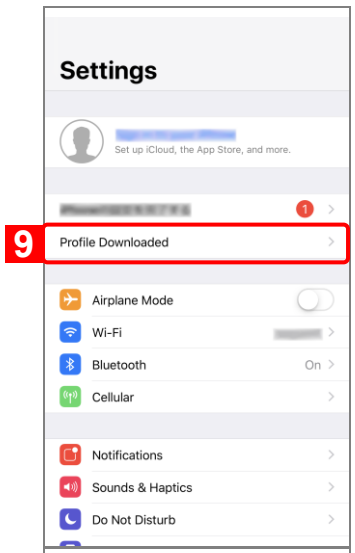
⇒The profile has been downloaded.



【8】**Tap [Settings] on the home screen.**

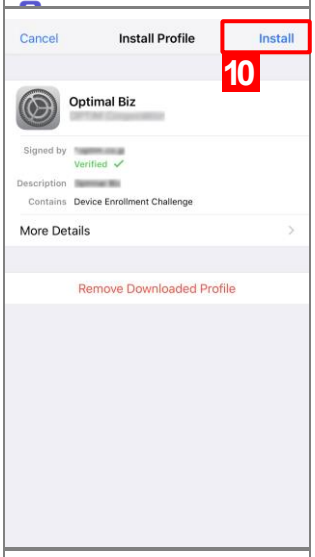


【9】Tap [Profile Downloaded].

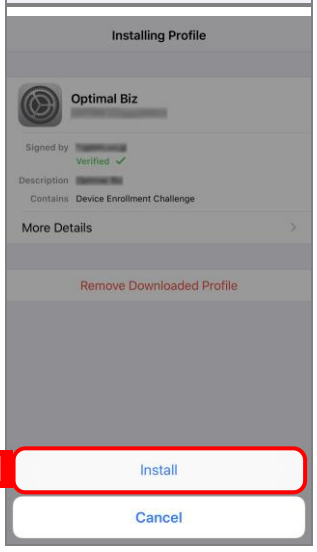


【10】Tap [Install].

If a passcode entry screen appears, enter the passcode of the device.

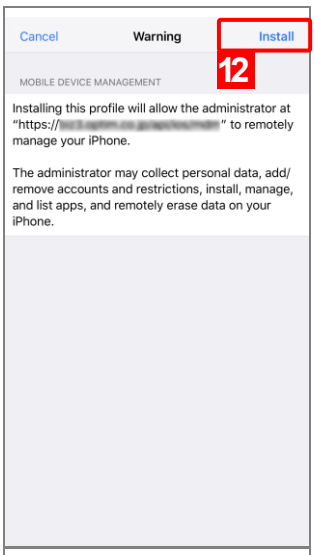


【11】Tap [Install].



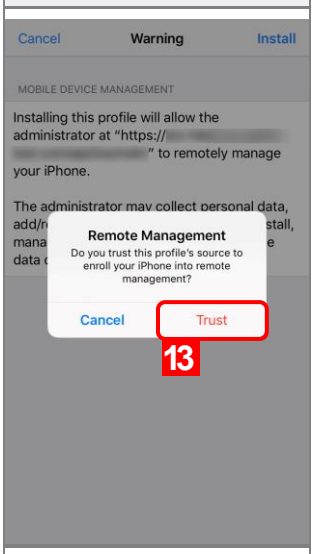
【12】Tap [Install].

⇒Installation will start, and you will be asked to confirm remote management.

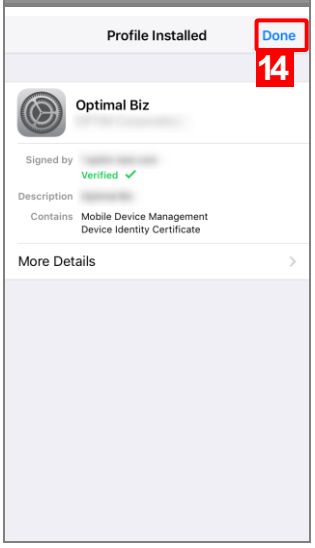


【13】Tap [Trust].

⇒Wait for a while until the installation completion screen appears.



【14】Tap [Done].



【15】Tap [Safari] on the home screen.

⇒License authentication will start. Wait for a while until it completes.

【16】To register additional device information, tap [Next].

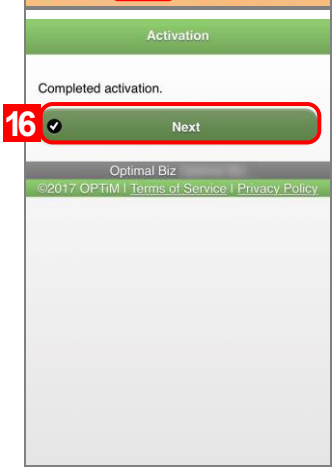
⇒For the rest of the procedure, refer to the following.

☞"Registering device information" Page 23

If you do not register device information anymore, license authentication is complete. Refer to the following and install/authenticate the agent.

☞"Installing and authenticating the agent" Page 51

You can register device information later in the management site.



3.2 Registering device information

Use the following steps to register device information.

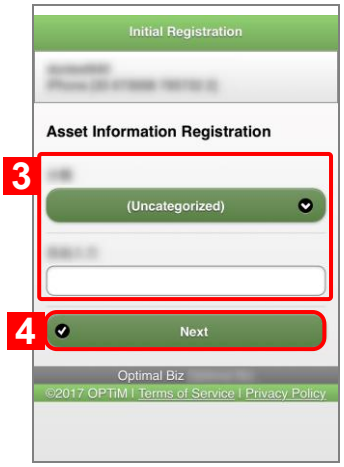
This screen does not appear if "Hide" is selected for "Portal for iOS" in "Portal Display" in the management site. For more information, refer to the relevant section of the manual below.

"Service Environment Setting" - "Portal Display" in <Management Site Reference Manual>

【1】 If necessary, configure the "Asset Information Registration" setting.

Items displayed in "Asset Information Registration" (such as classification and free entry items) depend on the "Customizing Input Items" in the management site. For more information, refer to the relevant section of the manual below.

"Assets" - "Customizing Input Items" in <Management Site Reference Manual>



【2】 Tap [Next].

⇒The device information will be registered. Wait for a while until it completes.

Refer to the following and install/authenticate the agent.

"Installing and authenticating the agent" Page 51

If you have not subscribed for the agent function, this completes device kitting. No further actions are required.

4 Using ADE for license authentication

This chapter describes the following items.

4.1 Getting ready for using ADE

Perform the following procedures to prepare to use ADE.

4.1.1 Preparing an ADE token

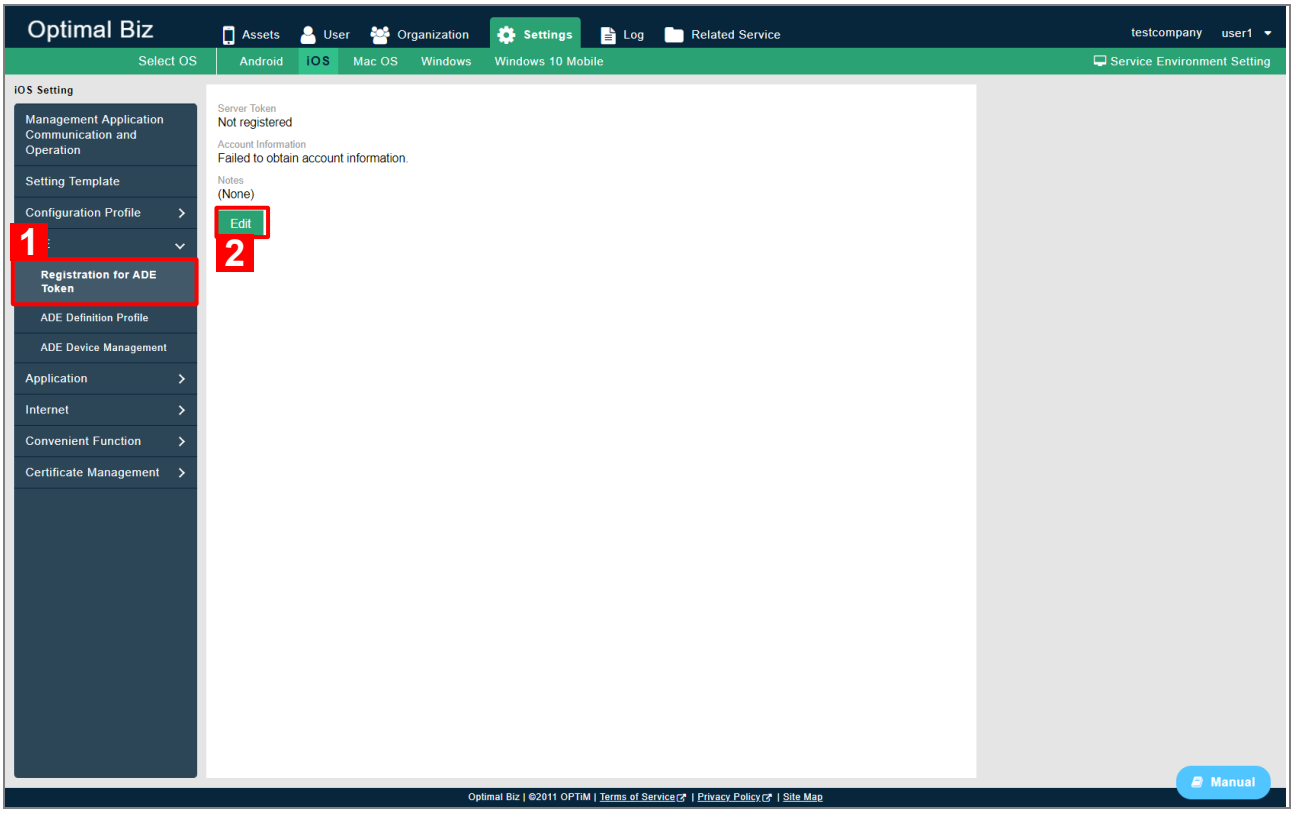
An ADE token is a token for connecting ADE and the management site. Download an ADE token from ABM and upload it to the management site.

Preparing an ADE token is only necessary for the first kitting.

4.1.1.1 Downloading an ADE token

Use the following steps to download an ADE token from ABM.

【1】 Click [Settings]→[iOS]→[ADE]→[Registration for ADE Token].
【2】 Click [Edit].

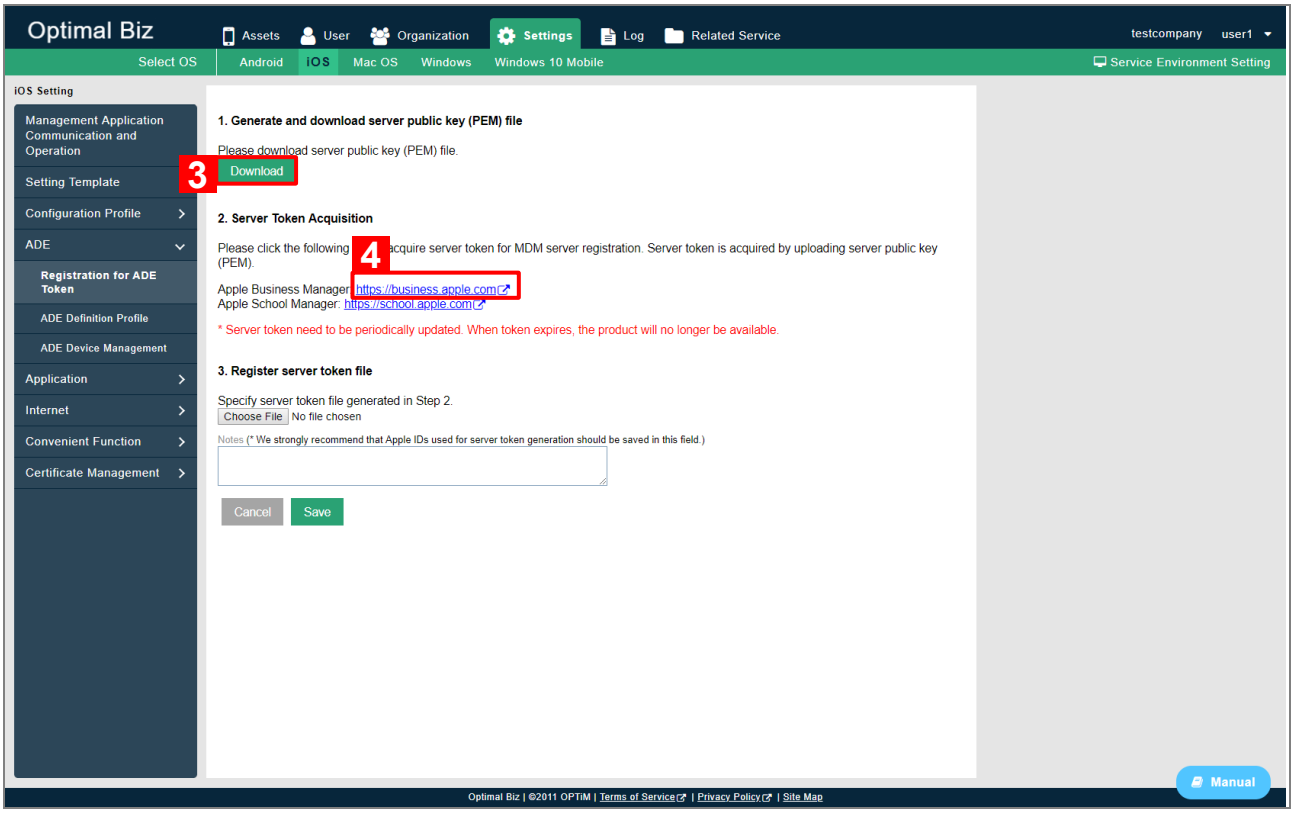


【3】 Click [Download].

⇒A server public key (PEM) file will be downloaded. Specify a location to save the file.

【4】 Click "Apple Business Manager: https://business.apple.com".

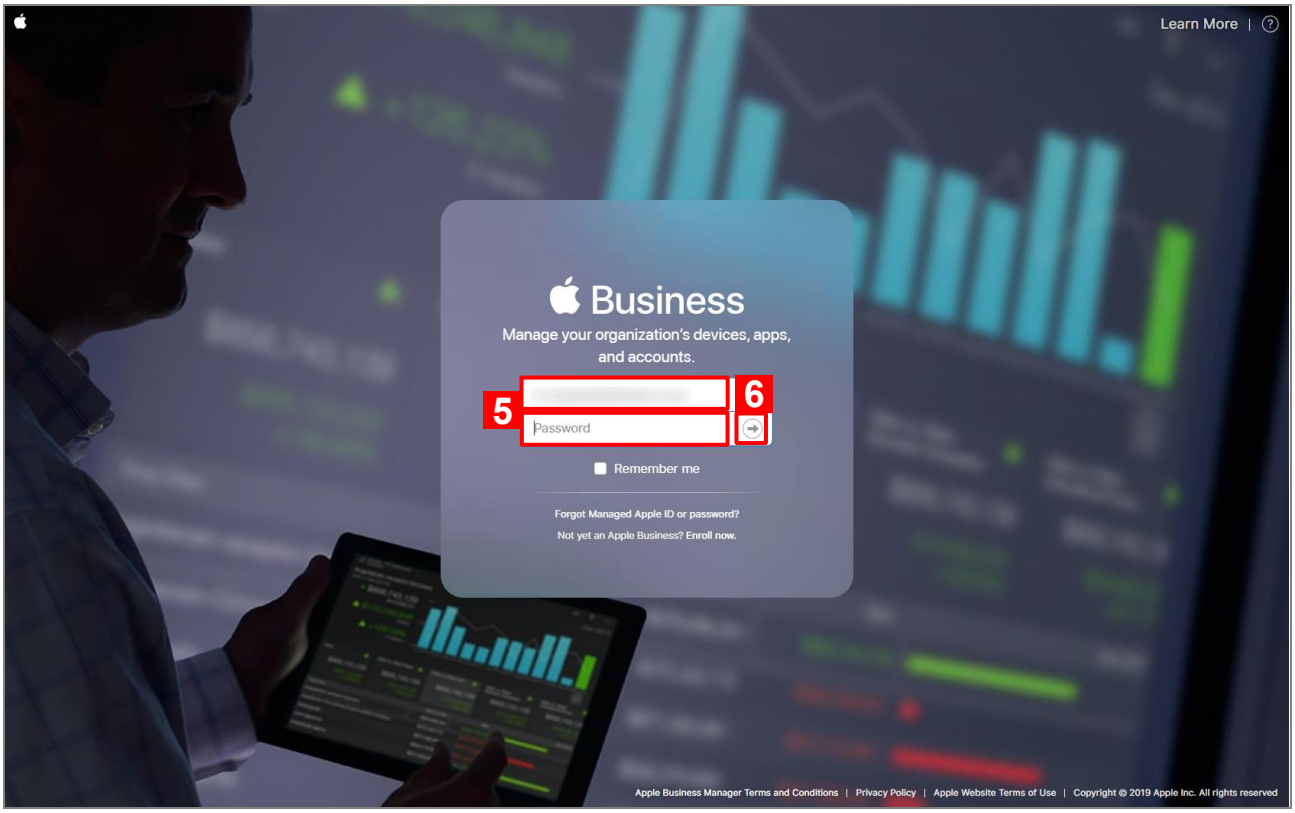
⇒The ABM website will be displayed. The rest of the operation is performed on the ABM website.



【5】 Enter an "Apple ID" and "Password" that have been approved by Apple.

【6】 Click  **.**

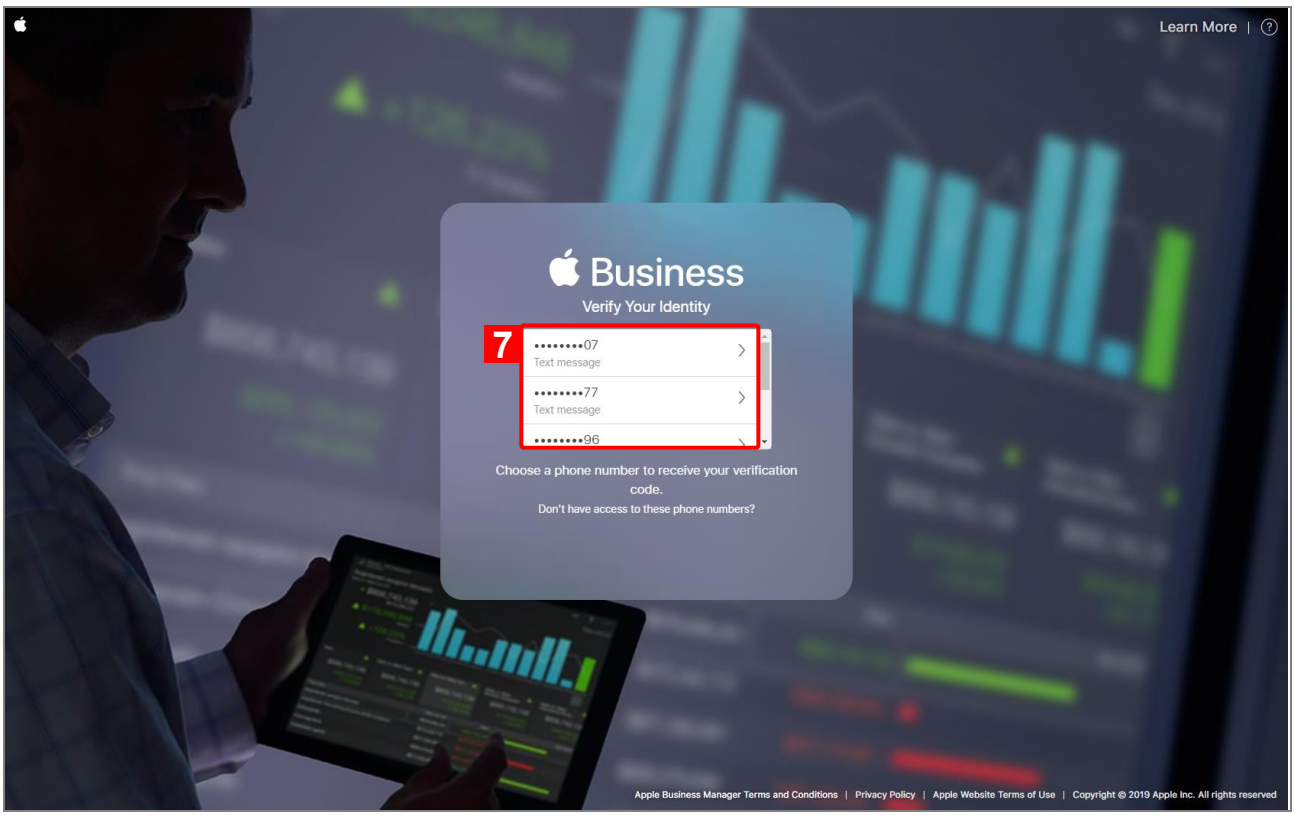
⇒An identification screen will appear.



【7】Select a phone number to receive a verification code.

The e-mail address set in the Apple ID will receive the verification code.

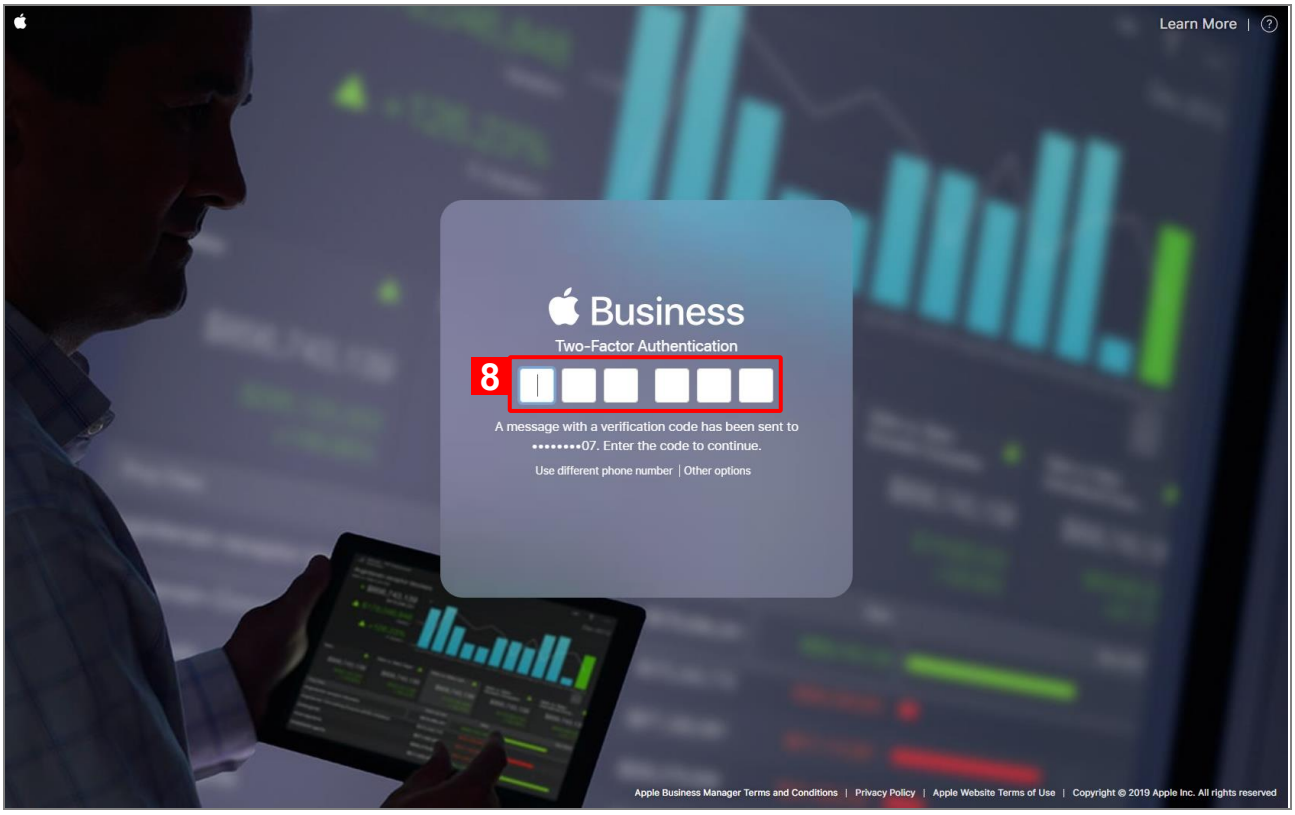
Make a choice if multiple phone numbers have been registered.



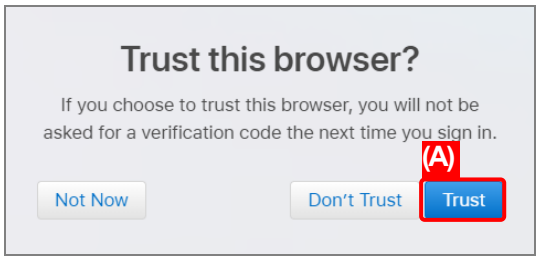
【8】Enter the verification code.

⇒If you enter the 6-digit number, the next screen will appear automatically.

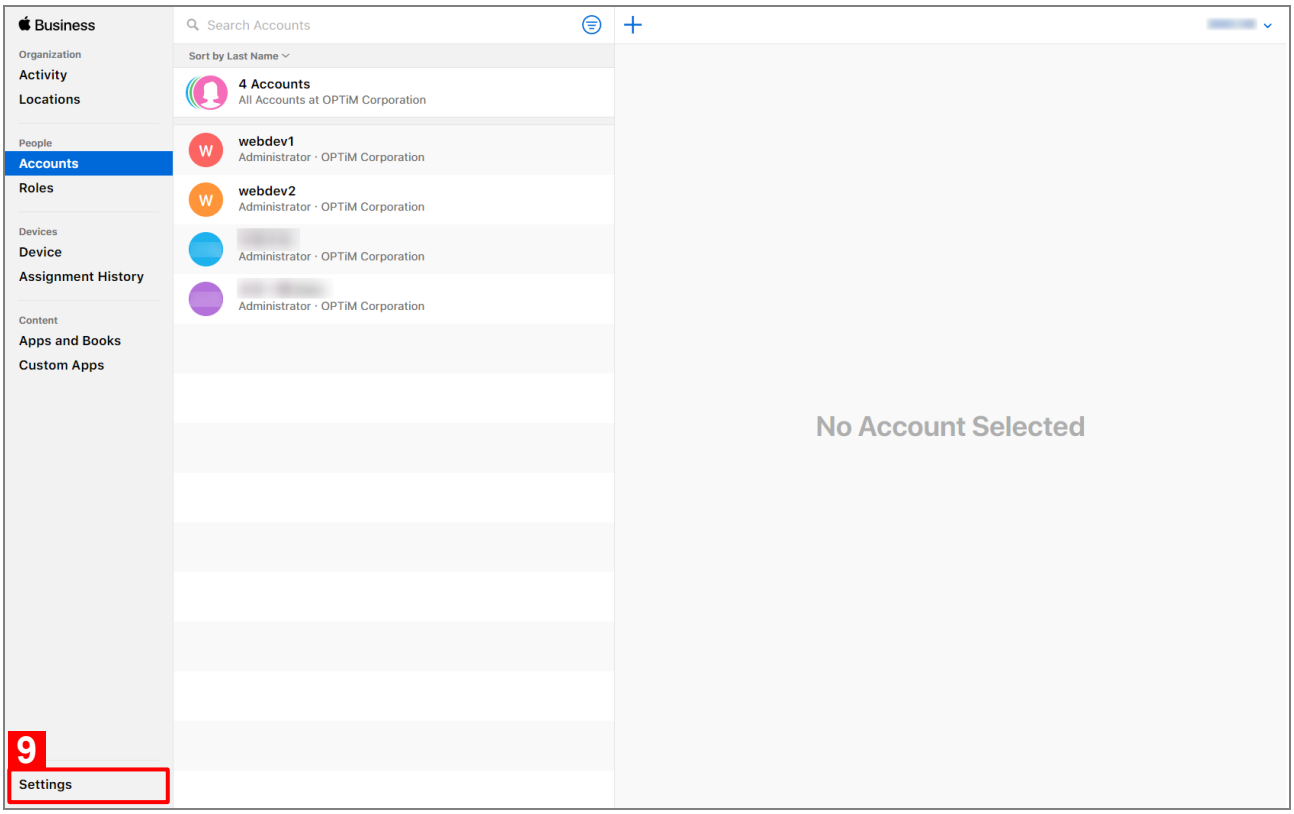
If you entered an incorrect verification code, the screen in step 【5】 will appear. Retry the step.



After entering a verification code, the following dialog may appear. If you click [Trust] (A) on this screen, you do not have to enter the verification code the next time you sign in from the same device and browser. Make an appropriate choice based on your situation.

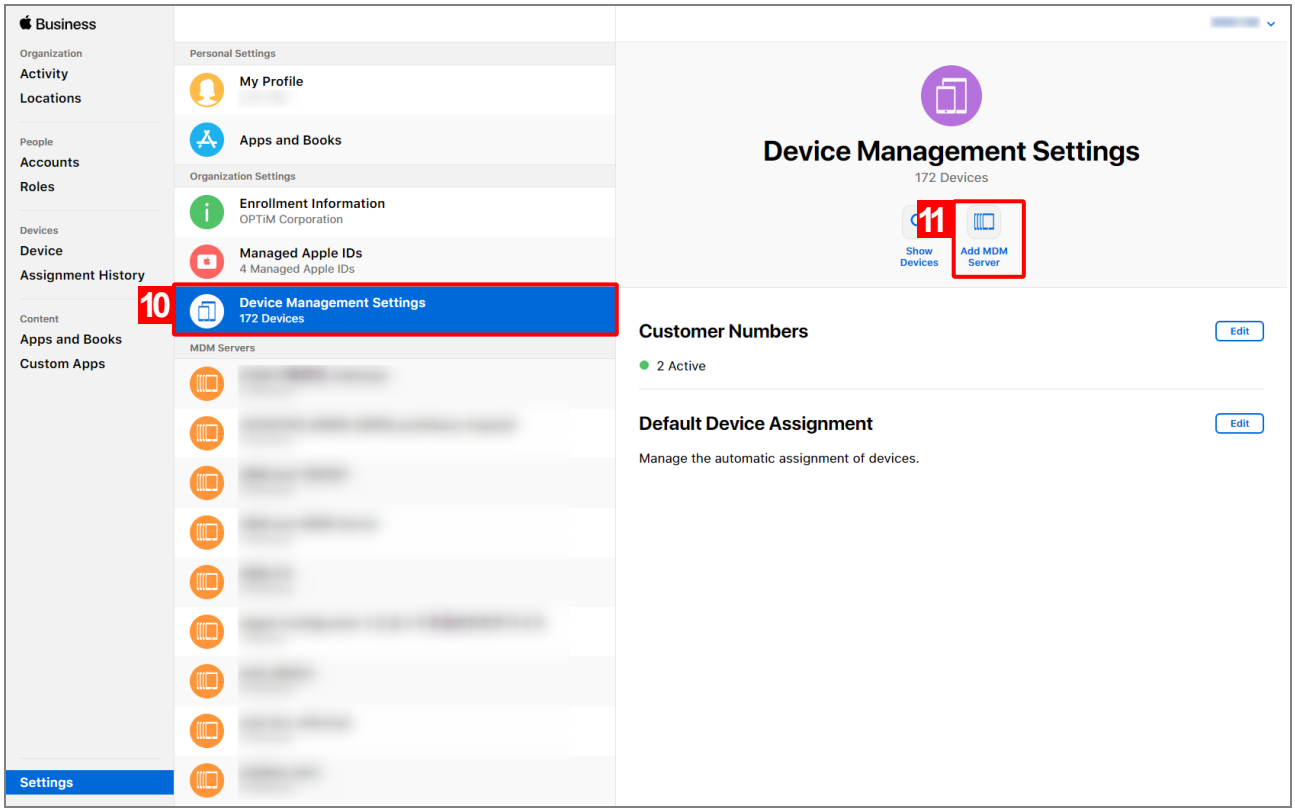


【9】Click "Settings".



【10】 Click "Device Management Settings".

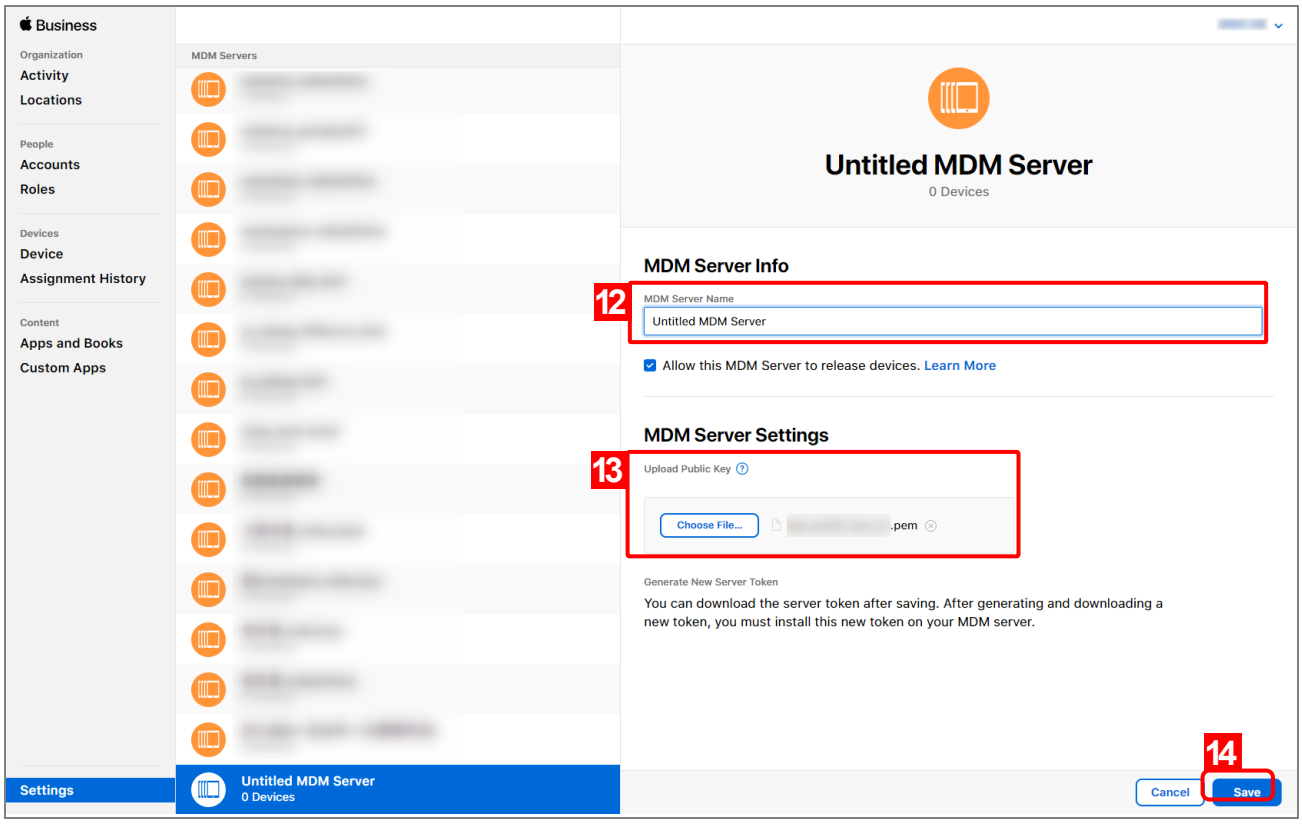
【11】 Click [Add MDM Server].



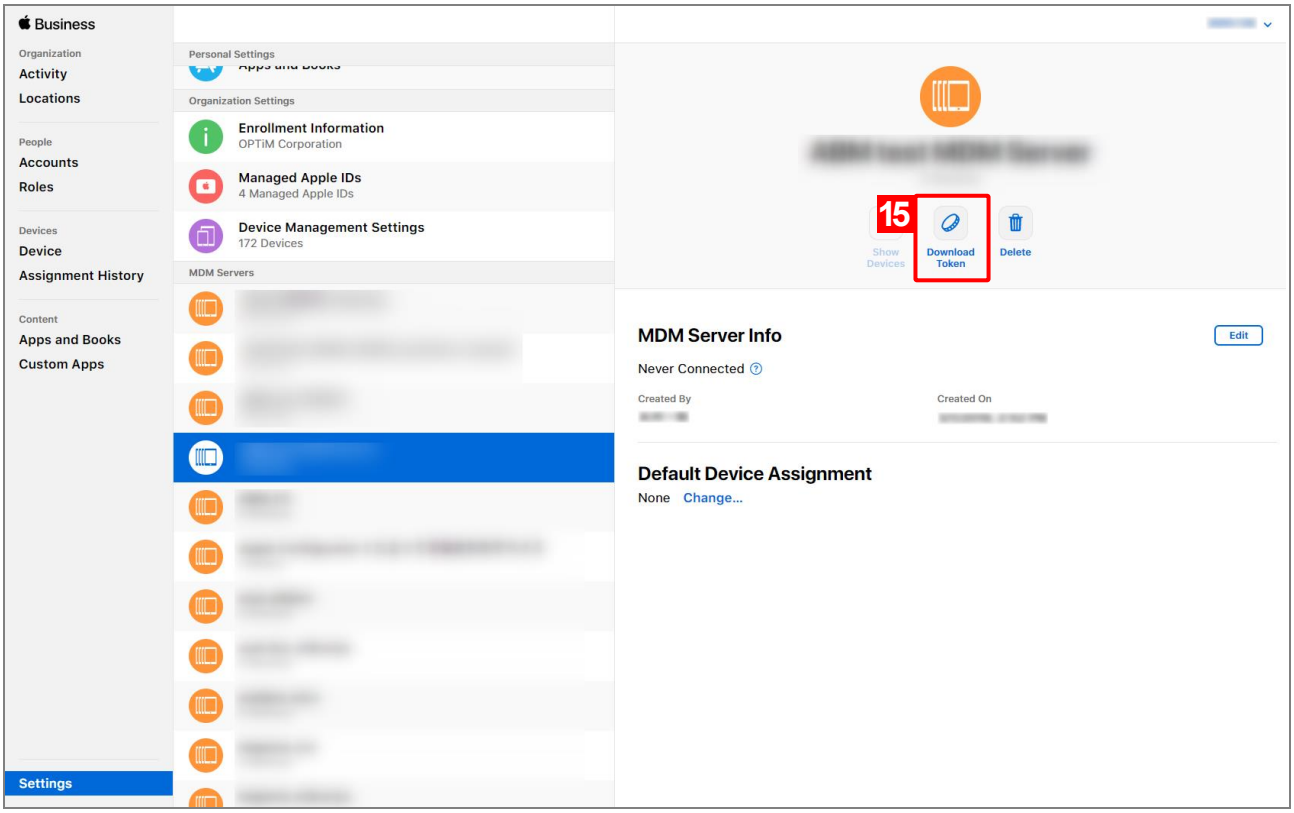
【12】 Enter an arbitrary name in "MDM Server Name" under "MDM Server Info".

【13】 Click [Choose File...] under "Upload Public Key", and specify the server public key (PEM) file you downloaded in step 【3】.

【14】 Click [Save].



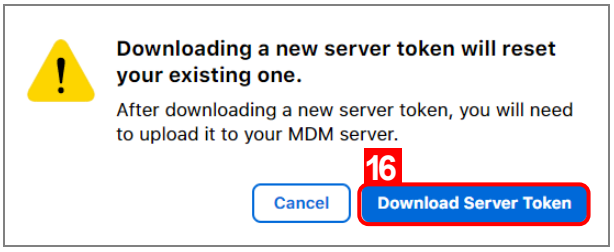
【15】Click [Download Token].



【16】Click [Download Server Token].

⇒The ADE token will be downloaded. Specify a location to save the file.

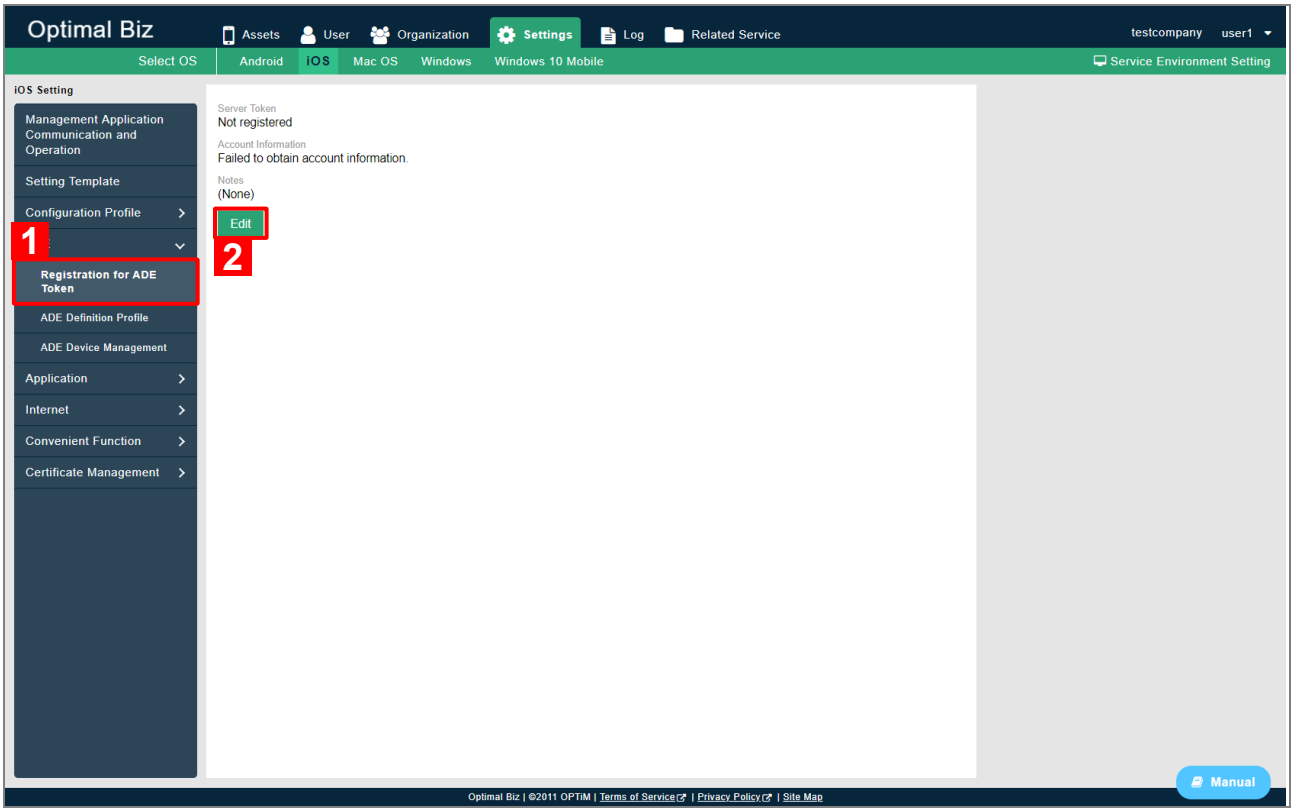
Upload the downloaded ADE token to the management site as soon as you can. If you do not upload it for a long period of time, you may not be able to communicate with the management site.



4.1.1.2 Uploading an ADE token to Optimal Biz

Use the following steps to upload the downloaded ADE token to the management site.

【1】Click [Settings]→[iOS]→[ADE]→[Registration for ADE Token].
【2】Click [Edit].



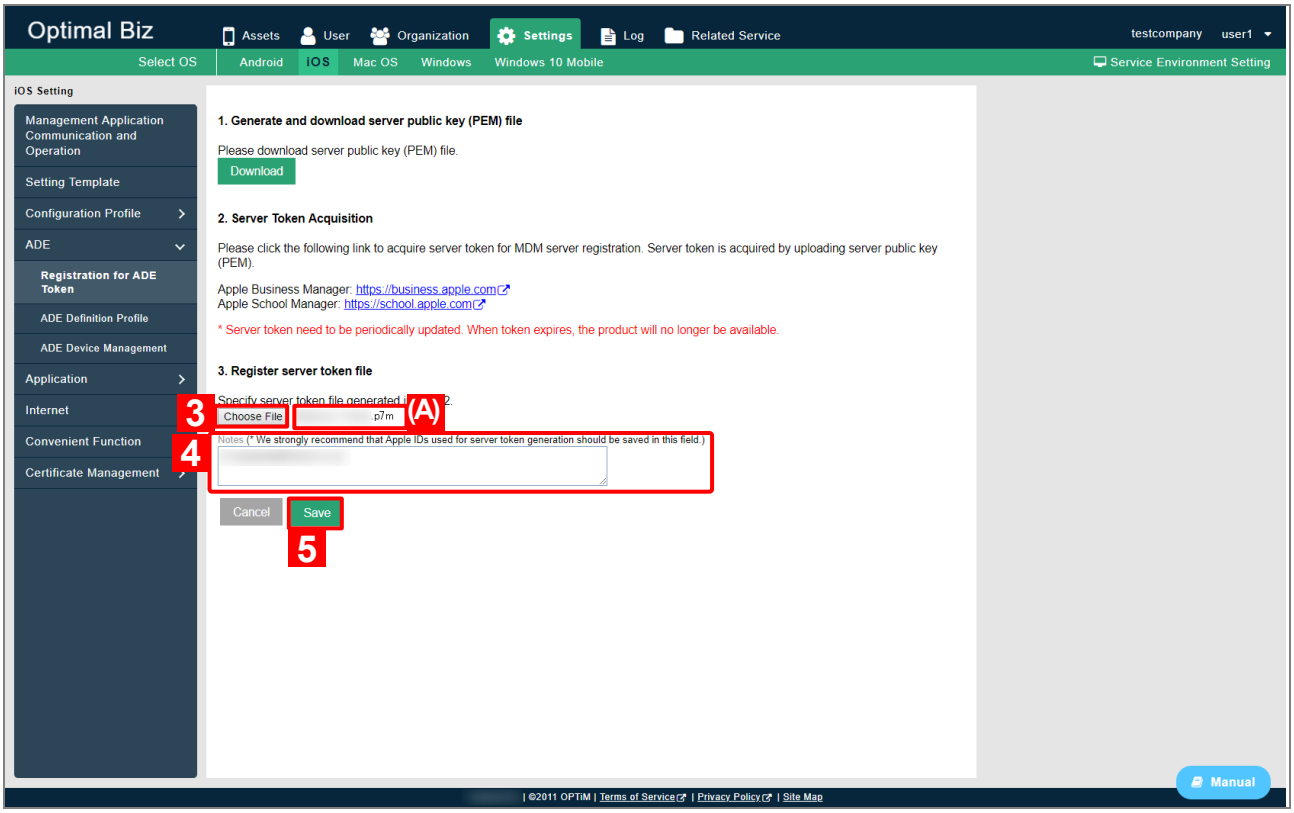
【3】Click [Choose File], and specify the ADE token you downloaded in "Downloading an ADE token".

⇒The selected file's name appears to the right of [Choose File] (A).

【4】Fill in "Notes".

We recommend that you enter your Apple ID for signing in to ABM or the date when you acquired the ADE token.

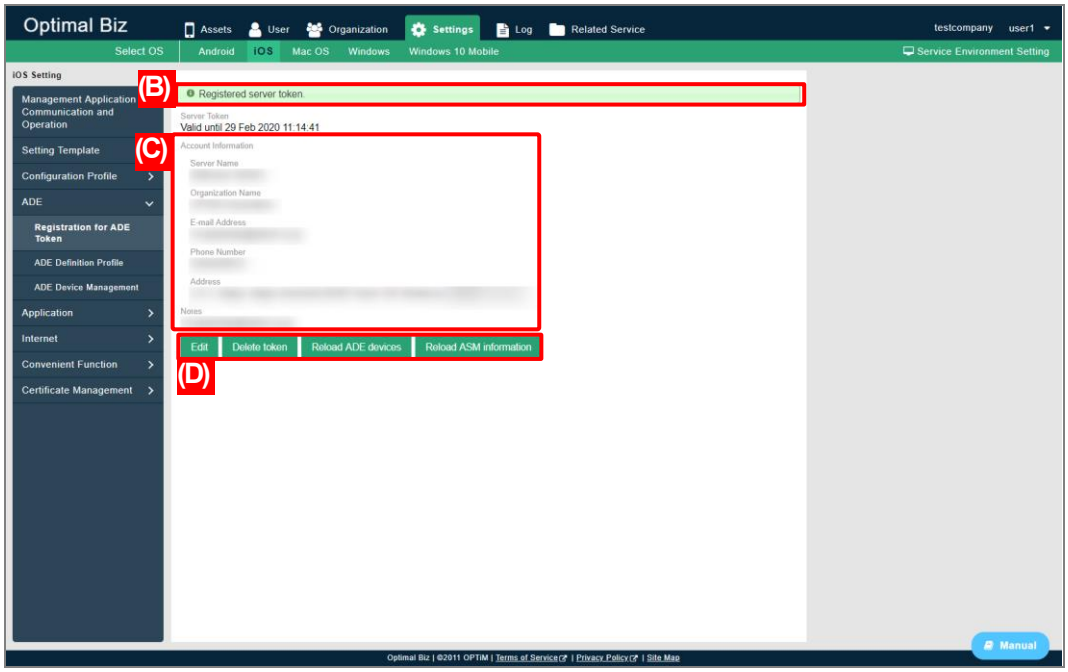
【5】Click [Save].



⇒The message "Registered server token" (B) will appear. Ensure that the content in "Account Information" (C) does not contain any errors.

For more information on (D), refer to the relevant section of the manual below.

"Settings – iOS" - "ADE" - "Registration for ADE Token" - "Screen (after registration)" in <Management Site Reference Manual>



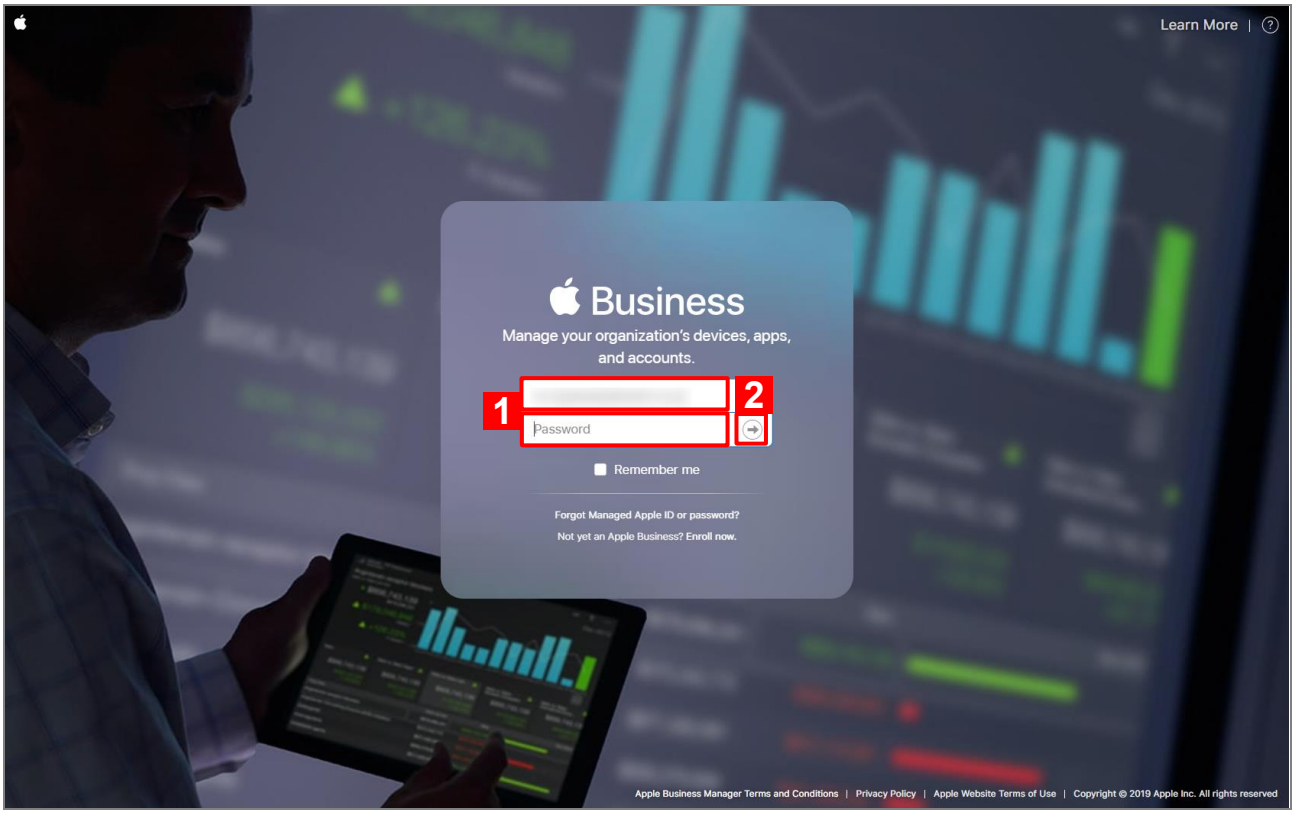
4.1.2 Allocating a device to a server using ABM

Use the following steps to allocate a managed device to a server by using ADE, and propagate the device information to the management site.

【1】 Go to the ABM website at https://business.apple.com/ and enter an "Apple ID" and "Password" that have been approved by Apple.

【2】 Click .

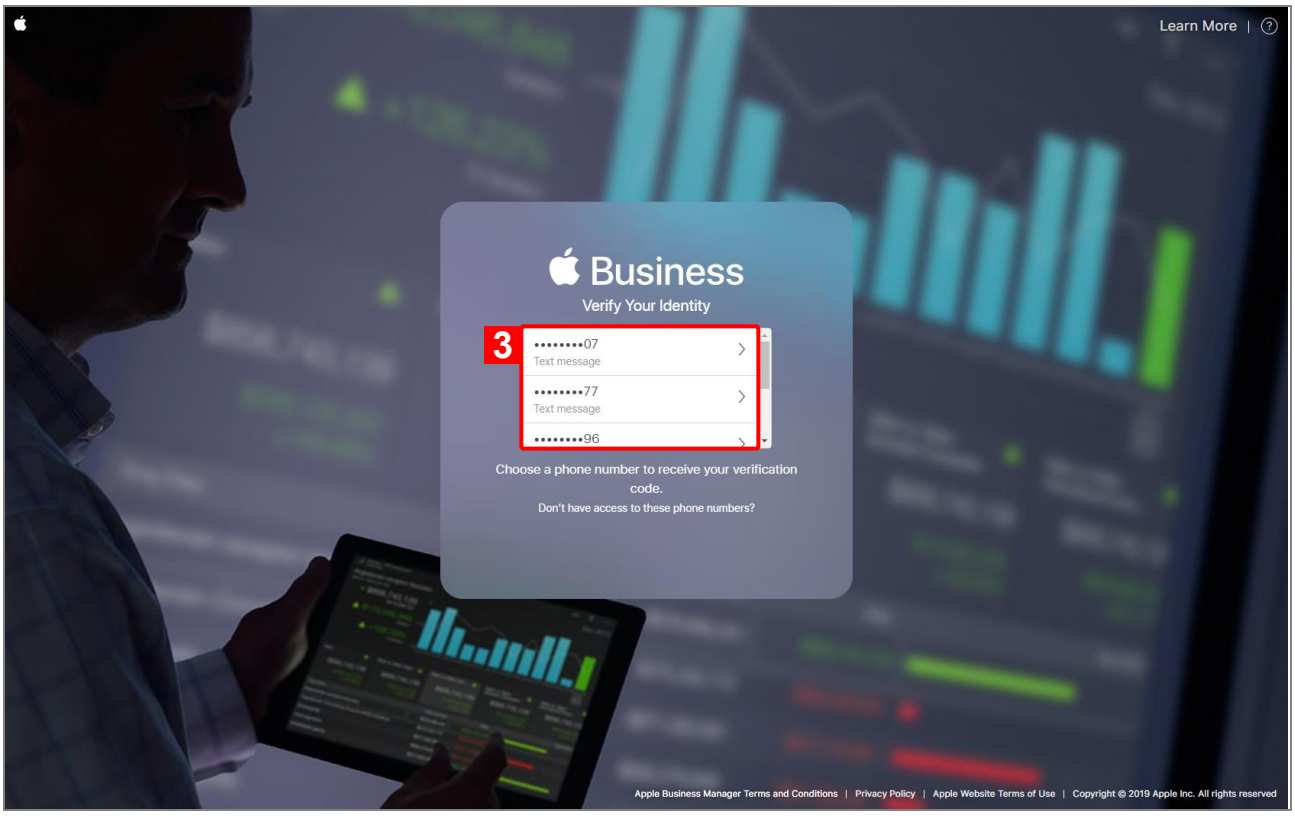
⇒An identification screen will appear.



【3】Select a phone number to receive a verification code.

The e-mail address set in the Apple ID will receive the verification code.

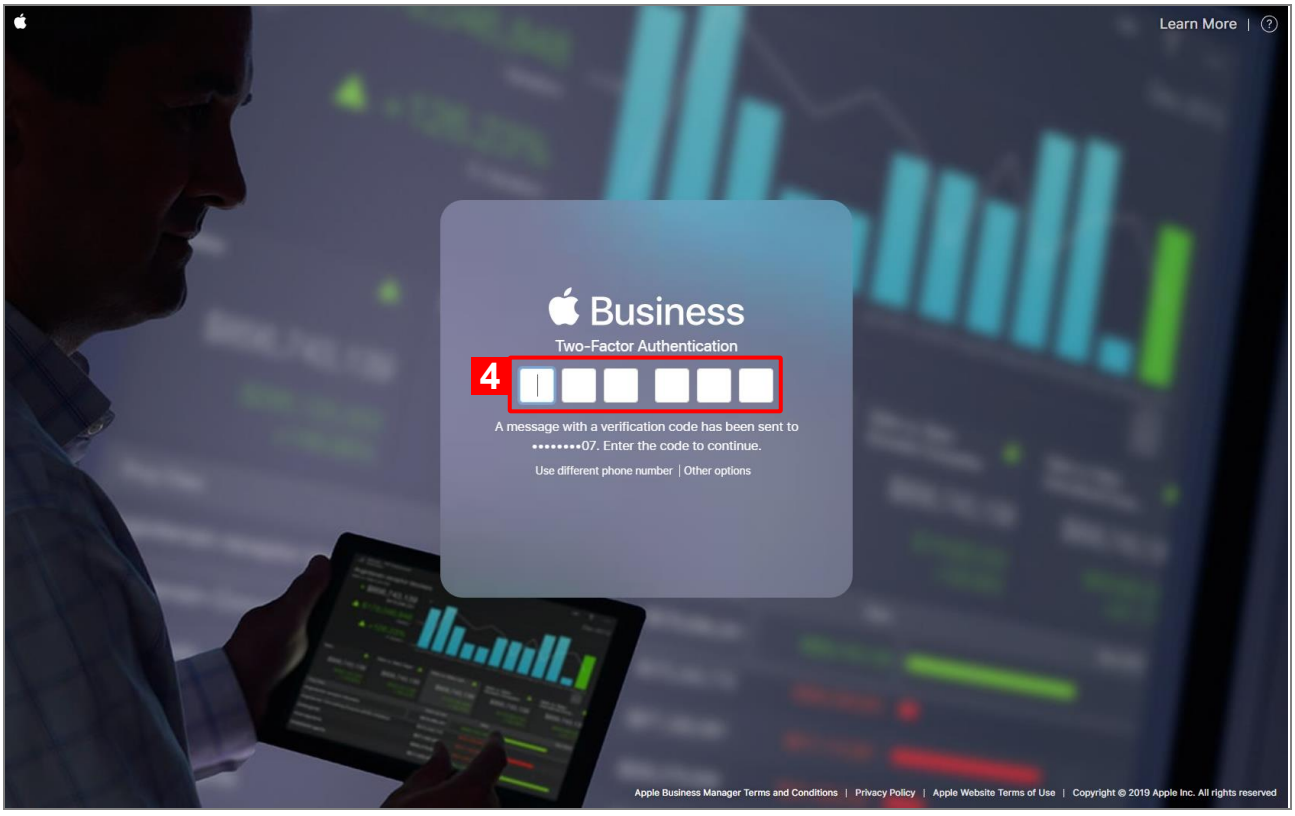
Make a choice if multiple phone numbers have been registered.



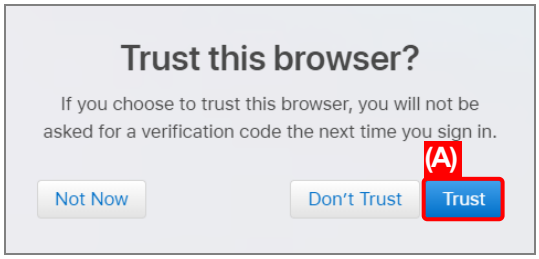
【4】Enter the verification code.

⇒If you enter the 6-digit number, the next screen will appear automatically.

If you entered an incorrect verification code, the screen in step 【1】 will appear.Retry the step.



After entering a verification code, the following dialog may appear. If you click [Trust] (A) on this screen, you do not have to enter the verification code the next time you sign in from the same device and browser. Make an appropriate choice based on your situation.



【5】 Click [Devices] in "Devices".

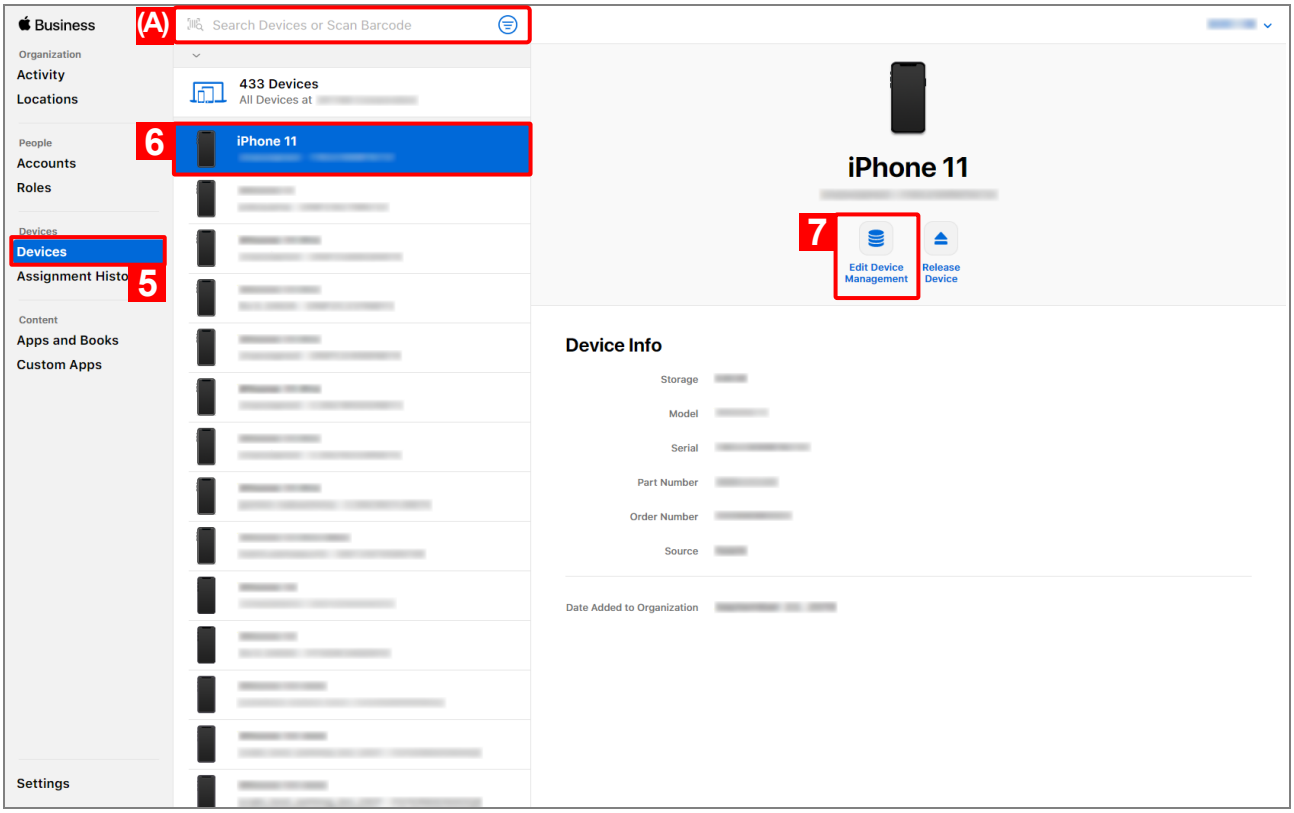
【6】 Click a target device from the list.

If a target device is not listed, contact Apple.

You can use (A) to search for a device from the list.

【7】 Click [Edit Device Management].

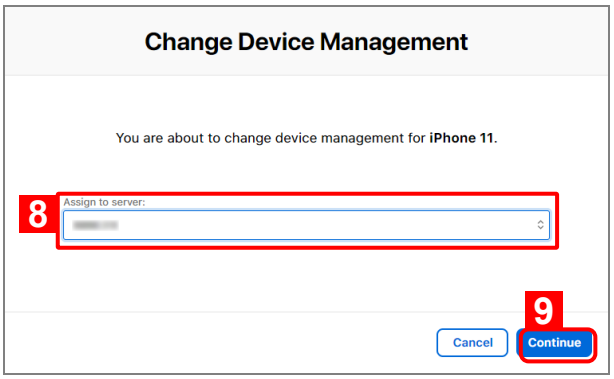
⇒The "Change Device Management" screen will appear.



【8】 In "Assign to server:", select the server name that you entered in step 【12】 of "Downloading an ADE token".

【9】 Click [Continue].

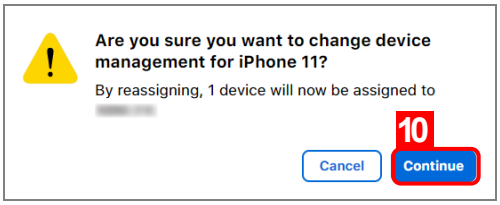
⇒A confirmation screen will appear.



【10】 Click [Continue].

⇒The target device will be allocated. Wait for a while.

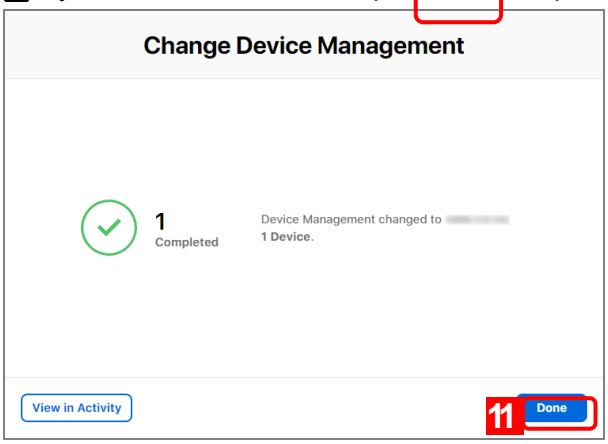
If this operation fails, it is possible that ADE cannot be used on the target device. For more information, contact Apple or the device's vendor.



【11】 Click [Done].

The following steps are performed in the management site.

If you want to allocate multiple devices, repeat steps 【5】 to 【11】.



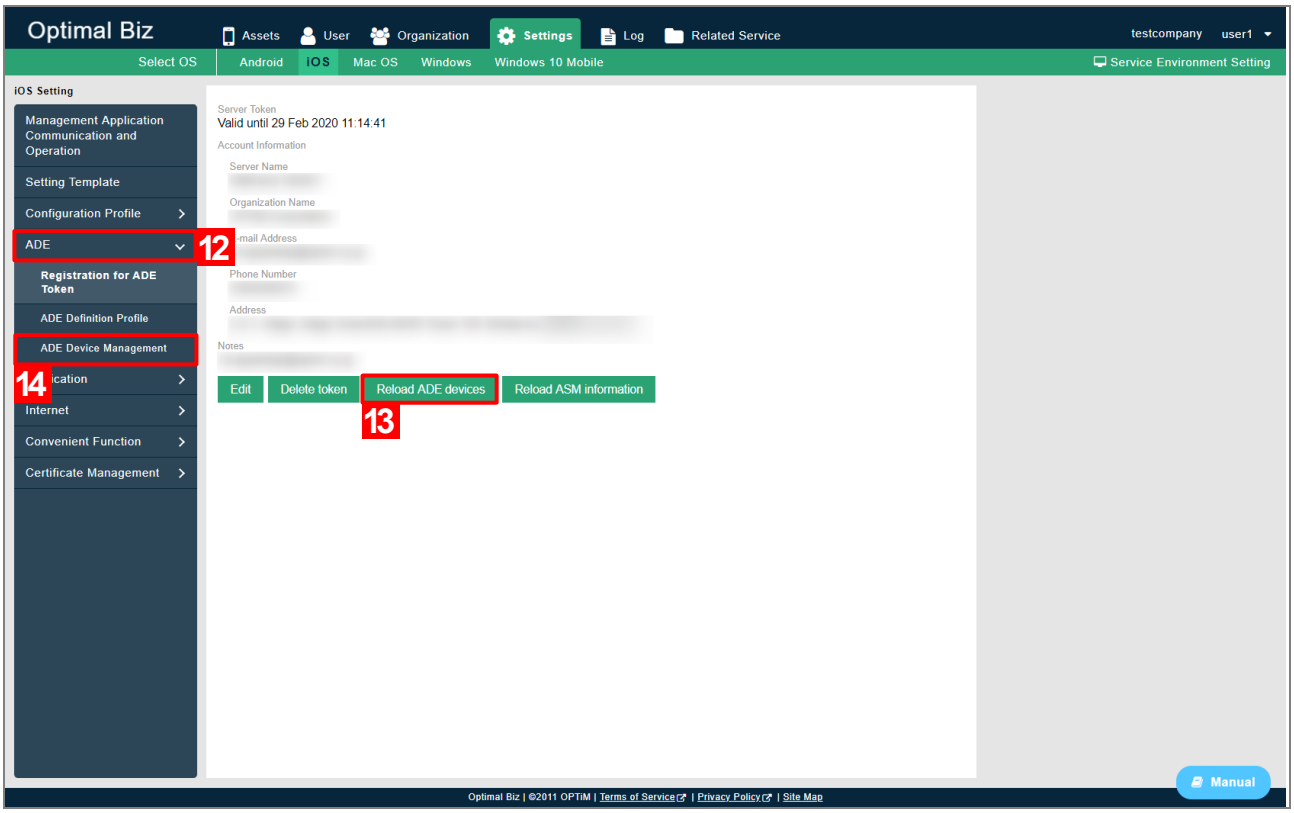
【12】 Click [Settings]→[iOS]→[ADE]→[Registration for ADE Token].

【13】 Click [Reload ADE devices].

⇒The button changes to [Reloading ADE devices...]. Wait for a while until it changes back to [Reload ADE devices].

If the button does not change back to [Reload ADE devices] after a while, reload the page on the browser.

【14】 Click [ADE Device Management].



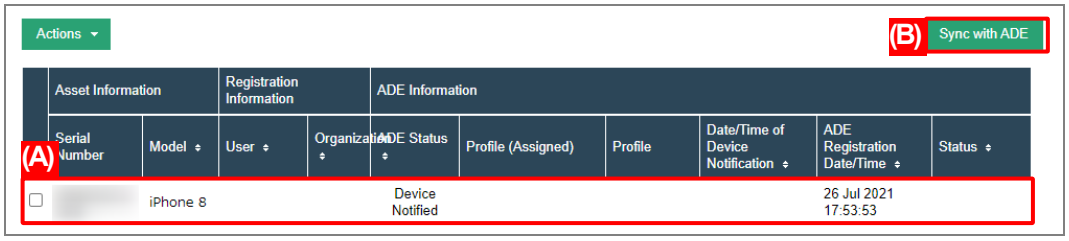
⇒The device information you registered in step 【11】 will appear in the list (A).

If the device information is not displayed correctly, click [Sync with ADE].

A device that has just been released may appear as "iPhone_U" in "Model" of the "ADE Device Management" screen.

For more information on "ADE Device Management", refer to the relevant section of the manual below.

"Settings - iOS " - " ADE " - " ADE Device Management" in <Management Site Reference Manual>



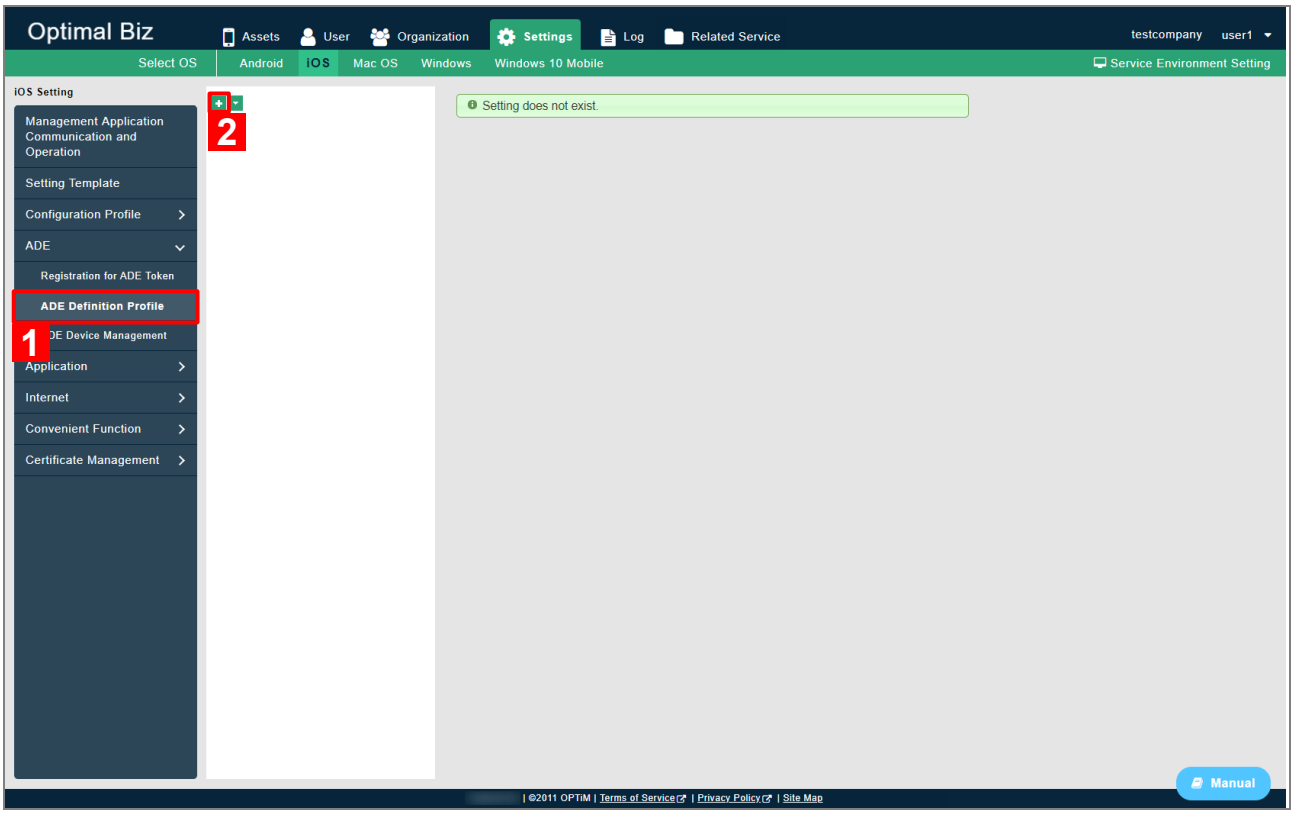
4.1.3 Creating an ADE definition profile

An ADE definition profile is a collection of various settings that is assigned to devices that use ADE. Use the following steps to create an ADE definition profile.

An ADE definition profile is assigned during device activation. If you change the ADE definition profile, you must activate the device again.

【1】 Click [Settings]→[iOS]→[ADE]→[ADE Definition Profile].

【2】 Click .

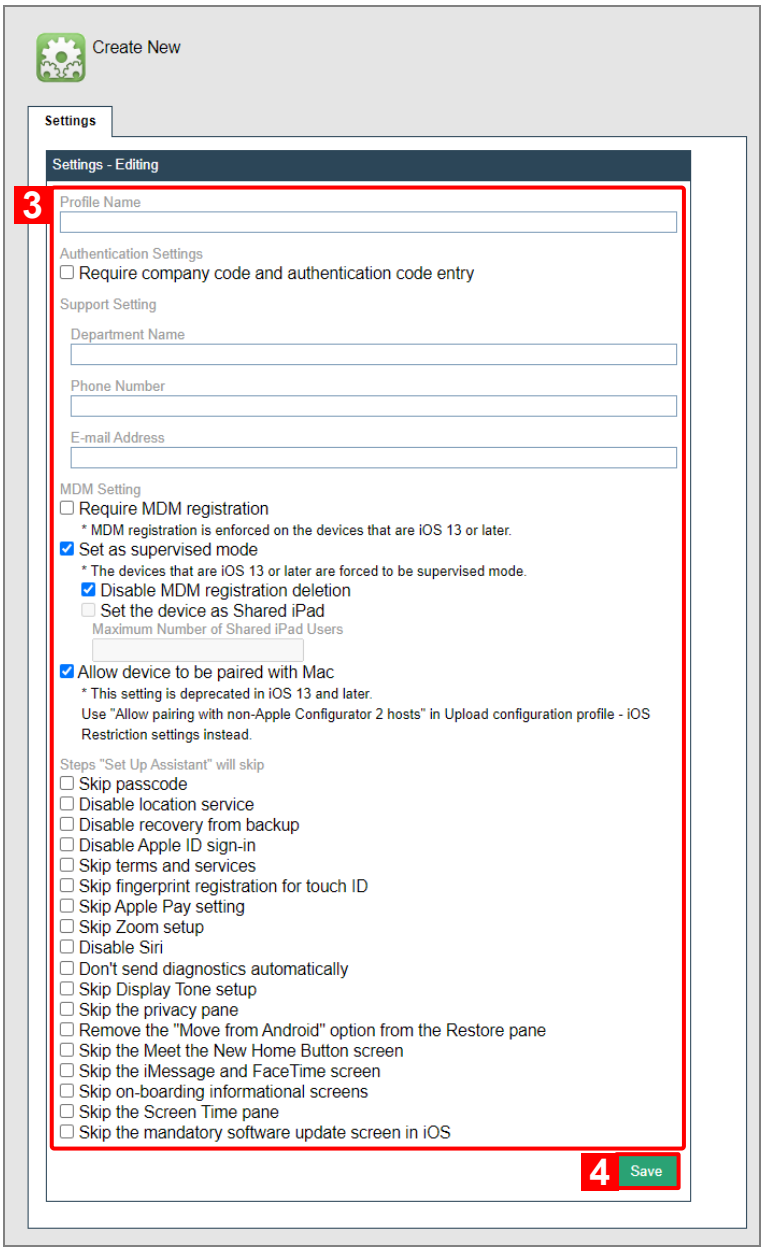


【3】Configure the ADE definition profile.

For more information, refer to the following.

☞"Setting items of an ADE definition profile" Page 41

【4】Click [Save].



◆ Setting items of an ADE definition profile

Name	Description
Profile Name	Enter a name of an ADE definition profile.
Authentication Settings	●Require company code and authentication code entry Require a user to enter a company code and authentication code. If this is not selected, ADE will perform automatic settings. ●Support Setting ・Department Name Enter a department name you want to include in the ADE definition profile. ・Phone Number Enter a phone number you want to include in the ADE definition profile. ・Email Address Enter an email address you want to include in the ADE definition profile. "Department Name" is only visible on an iOS device during activation, and cannot be seen after activation is complete.
MDM Setting	●Require MDM registration Require a user to install an MDM configuration profile during iOS device activation. On iOS 13 devices or higher, MDM configuration profile will always be installed (activated) without checking it. ●Set as supervised mode Set the iOS device as supervised mode using an MDM configuration profile. This allows a user to apply and manage a wide range of settings, including AirDrop, iMessage, iBooks Store, and web filtering. Devices that are on iOS 13.0 and later will always be on supervised mode even if you do not select this. ・Disable MDM registration deletion Prevent a device user from deleting the MDM configuration profile. If you do not select "Set as supervised mode", you cannot select this setting. If this setting is enabled, the following conditions prevent communication and re-authentication with the MDM server. To manage the device again, you must initialize it. ・The device has been deleted in the management site. ・The MDM configuration profile cannot be synced. If initialization is prohibited, the device must be restored to its factory default state. Contact Apple to learn how to do this. If a wrong HTTP proxy setting is installed on the device, communication may fail. ・Set the device as Shared iPad Set the device as Shared iPad. "Set the device as Shared iPad" only appears if "Education (Apple School Manager)" is used. You cannot select this setting unless you select both "Require MDM registration" and "Set as supervised mode". "Maximum Number of Shared iPad Users" is 50,000 for this product. However, it can be lower than 50,000 depending on the device. ●Allow device to be paired with Mac. Allow paring between an iOS device and a Mac OS device. This setting is not recommended for terminals with iOS13 or higher. Use "Allow Pairing with Hosts other than Apple Configurator 2 (Supervised only)" in "Configuration Profile Upload" - "iOS Restrictions settings" - "Functionality restrictions".

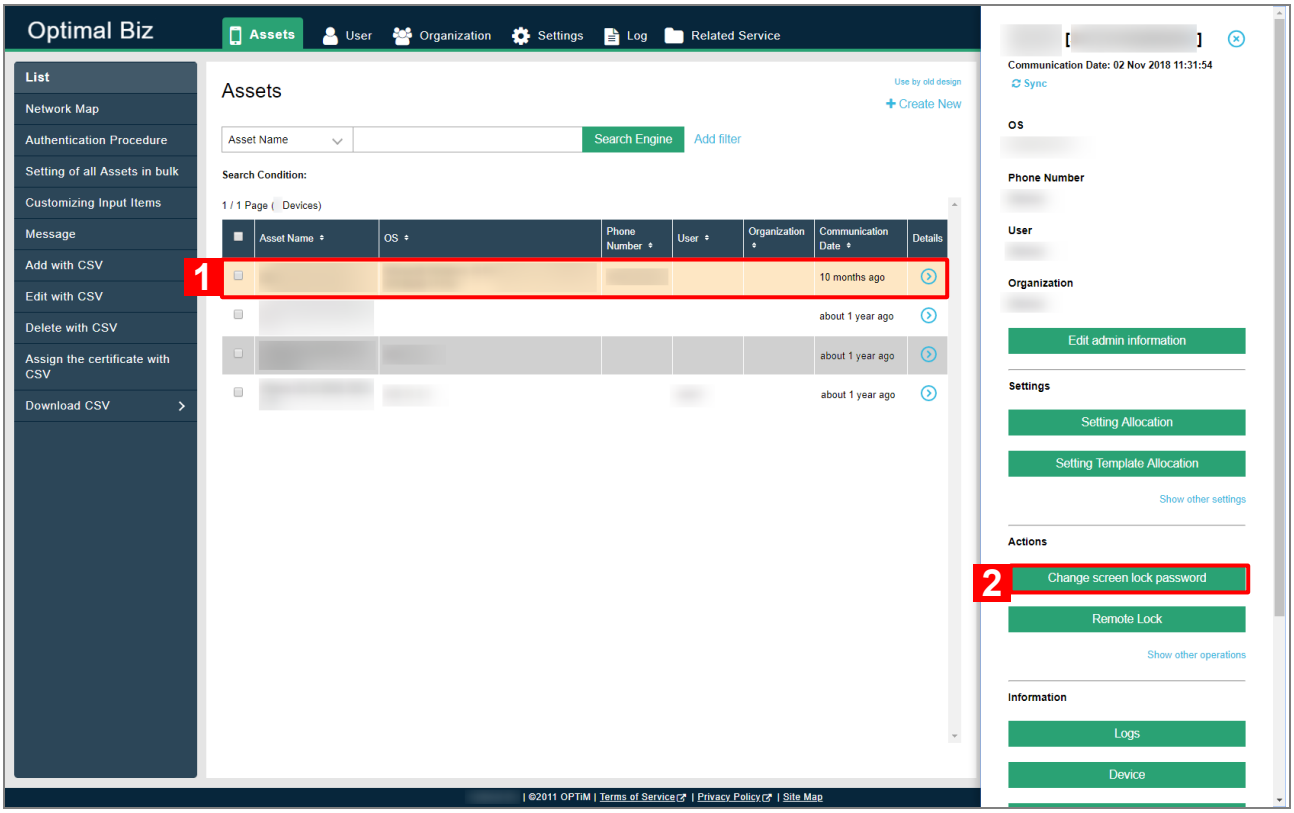
Name	Description
	For more information, refer to the relevant section of the manual below. "Editing [Functionality restrictions] on [iOS Restrictions settings] tab" in <Management Site Reference Manual> If this setting is not selected, you cannot connect to a Windows device, as designed by Apple.
Steps "Set Up Assistant" will skip	●Skip passcode Setting a passcode will be skipped during activation. If you want to skip setting a passcode, enable "Skip Apple Pay setting" and "Skip fingerprint registration for touch ID". Setting a passcode is not skipped when restoring from iCloud. ●Disable location service Location service will be automatically disabled. The setup screen will also be skipped. To skip the setup screen, use a Wi-Fi network during activation. If you are using a cellular network, the setup screen may appear. ●Disable recovery from backup Recovery from backup will be automatically disabled. The setup screen will also be skipped. To skip the setup screen, use a Wi-Fi network during activation. If you are using a cellular network, the setup screen may appear. ●Disable Apple ID sign-in Apple ID sign-in will be automatically disabled. The setup screen will also be skipped. ●Skip terms and services Terms and services will be skipped during activation. ●Skip fingerprint registration for touch ID Fingerprint registration will be skipped during activation. If you want to skip fingerprint registration, enable "Skip Apple Pay setting" too. Fingerprint registration is not skipped when restoring from iCloud. ●Skip Apple Pay setting up Apple Pay will be skipped during activation. ●Skip Zoom setup Setting up Zoom will be skipped during activation. ●Disable Siri Siri will be automatically disabled. The setup screen will also be skipped. ●Don't send diagnostics automatically Diagnostics will not be sent automatically. The setup screen will also be skipped. If you select "Move Data from Android" on the "Apps & Data" screen during activation, the setup screen will not be skipped. ●Skip Display Tone setup The Skip Display Tone setup will be automatically enabled. The setup screen will also be skipped. ●Skip the privacy pane The privacy pane will be automatically enabled. The setup screen will also be skipped. ●Remove the "Move from Android" option from the Restore pane The "Move Data from Android" option will not appear and cannot be selected on the recovery from backup screen. ●Skip the Meet the New Home Button screen The Meet the New Home Button screen will be skipped. ●Skip iMessage and FaceTime screen

Name	Description
	The iMessage and FaceTime screen will be skipped. ●Skip on-boarding informational screens On-boarding informational screens will be skipped. ●Skip the Screen Time pane The Screen Time pane will be skipped. ●Skip the mandatory software update screen in iOS Setting of auto update of OS is omitted. The settings for auto update vary by device.

4.1.4 Assigning an ADE definition profile

You can allocate an ADE definition profile setting to a device by allocating a created ADE definition profile to a device or an organization, syncing with ADE on the "ADE Device Management" screen, and activating the device.

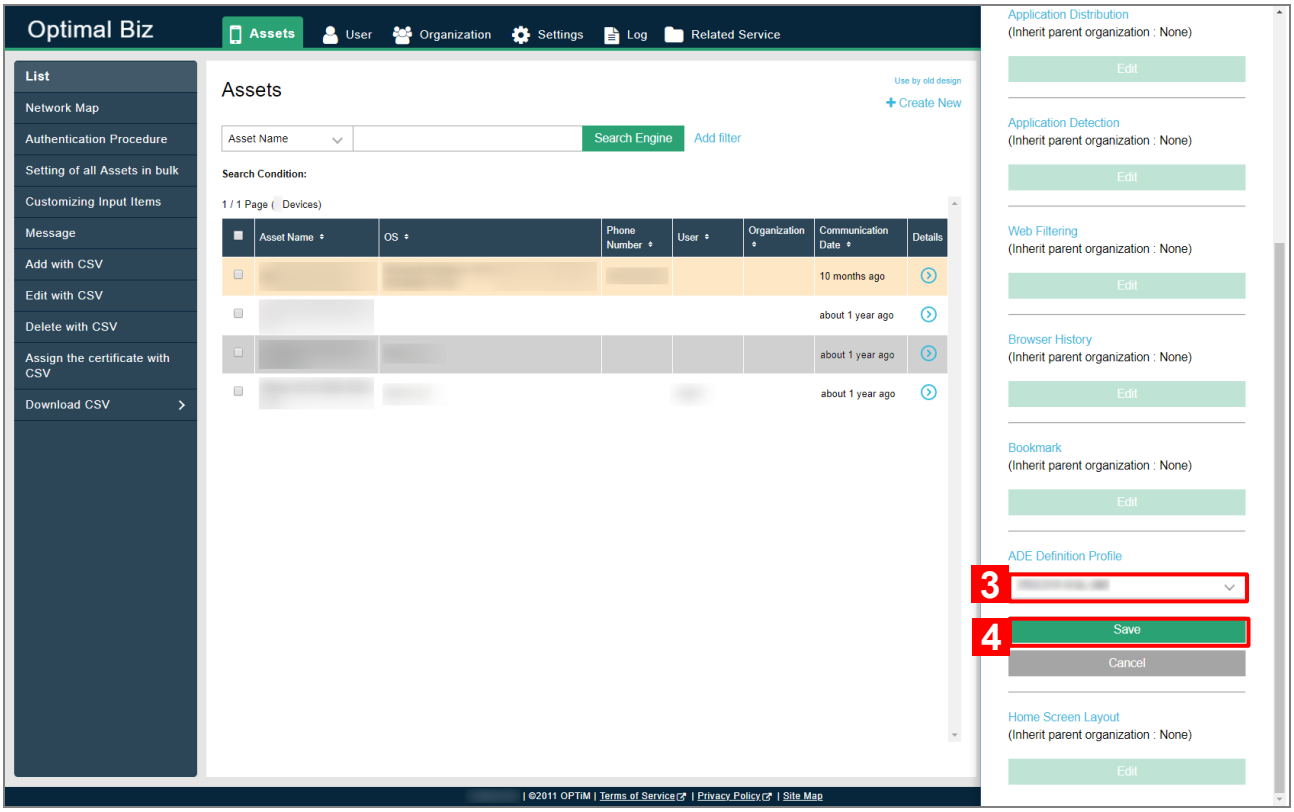
【1】Go to [Assets]→[List], and select a target device from the list.
【2】Click [Setting Allocation] in "Settings".



【3】Specify an ADE definition profile from the "ADE Definition Profile" pull-down menu.

To allocate an ADE definition profile to an organization, go to [Organization]→[List]→a target organization→the edit screen in the [iOS] tab, and specify an ADE definition profile from the "ADE Definition Profile" pull-down menu.

【4】Click [Save].

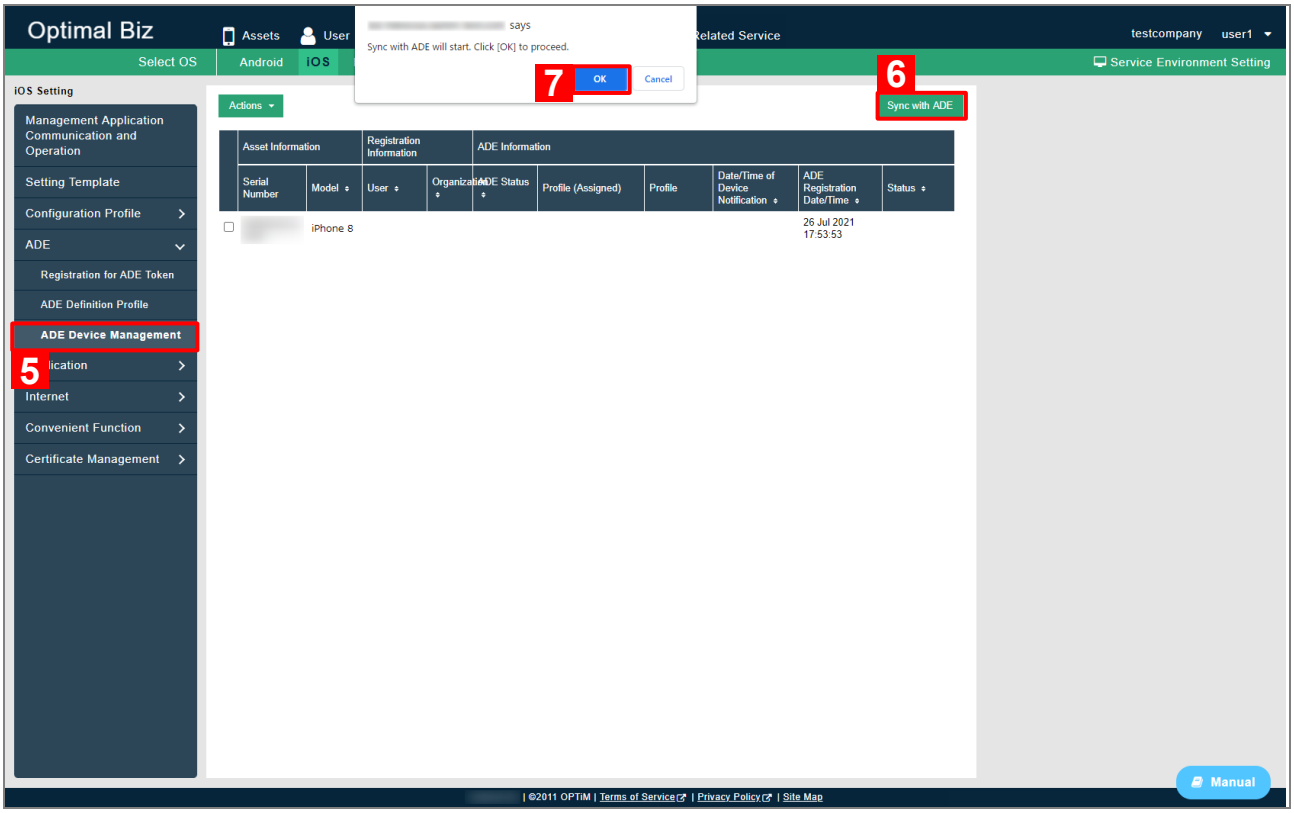


【5】Click [Settings]→[iOS]→[ADE]→[ADE Device Management].

【6】Click [Sync with ADE].

【7】Click [OK].

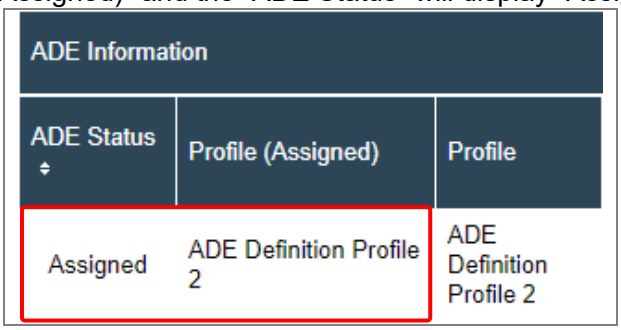
⇒Sync with ADE will complete. Proceed to activate a device.



◆ About "ADE Status"

The "ADE Device Management" screen displays "ADE status" as shown below depending on the status of an ADE definition profile.

When the sync with a device is complete, the name of an assigned ADE definition profile is displayed in "Profile (Assigned)" and the "ADE Status" will display "Assigned".



ADE Status	Description
(None)	The ADE definition profile has not been assigned. With this status, the ADE definition profile will not be assigned during activation.
Assigned	An ADE definition profile has been assigned to ADE. The ADE definition profile will be assigned during the next activation, and the Status will change to "Device Notified".
Removed	The ADE definition profile has been removed from ADE. With this status, the ADE definition profile will not be assigned during activation. To return this status to "Assigned", assign the ADE definition profile again and click [Sync with ADE].
Device Notified	The ADE definition profile registered in ADE has already been assigned to a device. The ADE definition profile is assigned every time when activation is performed with this status.

4.2 Activating a device

Use the procedure below to activate the device and complete license authentication.

【1】 Start a device and follow the on-screen instructions.

The on-screen instructions depend on the settings in the ADE definition profile to be assigned to a device (Items selected in "Steps "Set Up Assistant" will skip" will be skipped during activation).
Note that the ADE definition profile will be assigned after you select a network connection in the "Choose a Wi-Fi Network" screen.

If the device is connected to a computer, do not tap [Connect to Mac or PC] (A) on the "Choose a Wi-Fi Network" screen.

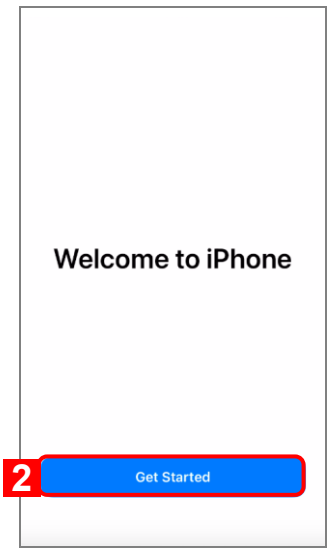
【2】 When the "Welcome to iPhone" screen appears, Tap [Get Started].

⇒Activation and license authentication for the device is complete.

Continue to refer to the following to install/authenticate the agents.

☞"Installing and authenticating the agent" Page 51

If you have not subscribed for the agent function, this completes device kitting. No further actions are required.



5 Authenticating the agent

This chapter describes the following item.

Attention

- The agent will be activated even with an activation code that are not for the relevant device.
  - If you happen to activate the agent with a wrong activation code, you need to uninstall and reinstall the agent.

5.1 Installing and authenticating the agent

There are three ways to install and authenticate the agent. Choose an appropriate method depending on the management site and device settings.

- ●Installation and authentication from Portal
  Select this method if both Portal and App Store are displayed on the device.
- ●Installation and authentication from App Store
  Select this if only App Store are displayed on the device.
- ●Installation and automatic authentication using Application Distribution
  Select this method if both Portal and App Store are hidden.

To install/activate the agent, you need to perform one of the following license authentication in advance.

☞"Installing an MDM configuration profile" Page 12
☞"Using ADE for license authentication" Page 24

You can display/hide Portal and hide the App Store from the management site. For more information, refer to the relevant section of the manual below.

"Service Environment Setting" - "Portal Display" in <Management Site Reference Manual>

"iOS " - "Upload Configuration Profile" in <Management Site Reference Manual>

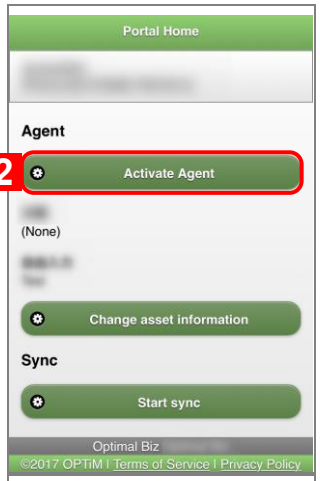
5.1.1 Installation and authentication from Portal

Use the following steps to install and authenticate the agent from Portal.

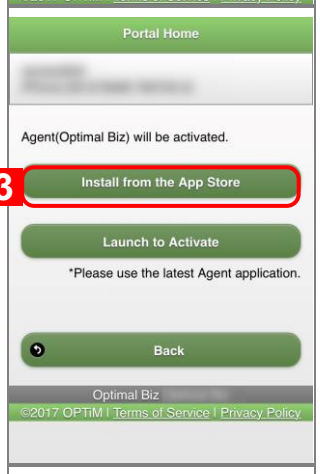
【1】Tap [Portal] on the home screen.

⇒The browser (Safari) opens and displays Portal.

【2】 **Tap [Activate Agent].**



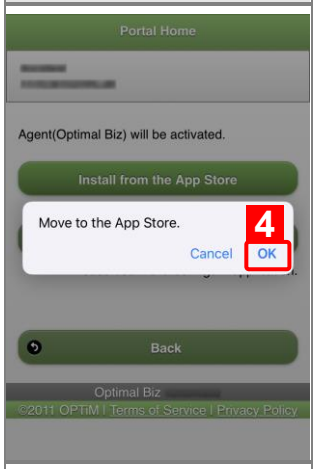
【3】 **Tap [Install from the App Store].**



【4】 **Tap [OK].**

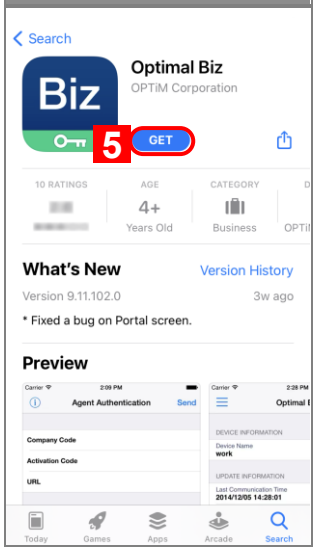
⇒The "Optimal Biz" page of the App Store will be displayed.

If you are prompted to enter a password, enter the password for the Apple ID.



【5】 **Tap [GET].**

⇒The agent (Optimal Biz) will be installed. Wait until the [Optimal Biz] icon appears on the device's home screen.



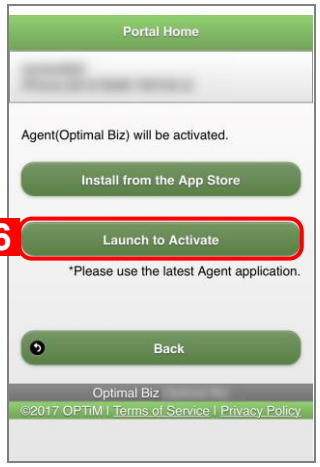
【6】Return to Portal and tap [Launch to Activate].

⇒The agent will be activated.

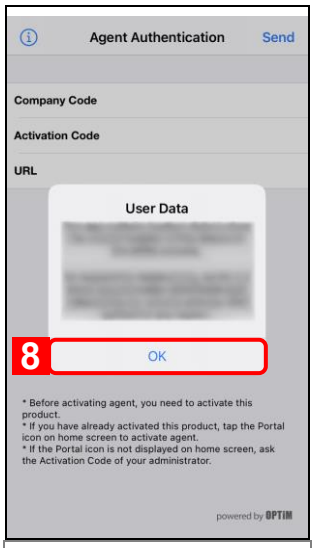
If you have not performed license authentication, follow the instructions that will be displayed on the screen and perform license authentication.

The following steps differ if the device is on iOS 13.0 and later. Refer to the following.

☞"Always allowing location access on devices with iOS 13.0 and later" Page 55

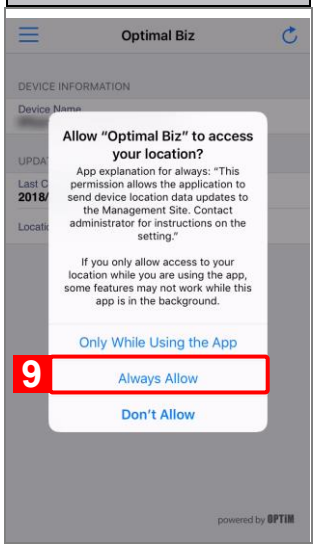


【7】Tap "OK".

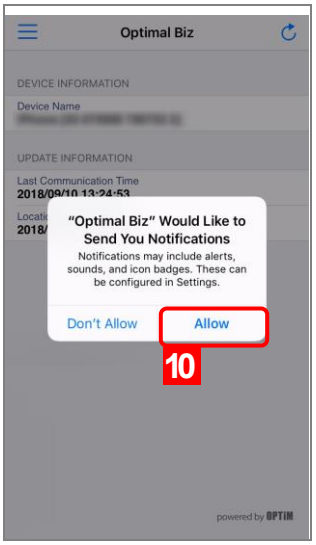


【8】Tap [Always Allow].

If you do not set [Always Allow] for your location information, the agent functions may not be available.



【9】 Tap [Allow].



This step is only required on the first launch.

If you do not tap [Allow], no notification appears when the device receives a message from the management site.

⇒When "Device Information" and "Update Information" (A) are displayed, the agent has been authenticated.

5.1.1.1 Always allowing location access on devices with iOS 13.0 and later

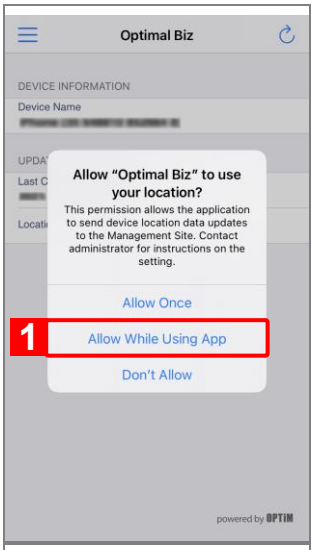
When you authenticate the agent on devices with iOS 13.0 and later, you cannot select "Always Allow" when you are asked to allow Optimal Biz to access your location. Use the following steps to always allow location access.

Without these steps, the device cannot retrieve or send correct location information.

If you do not set [Always Allow] for your location information, the agent functions may not be available.

【1】 Tap [Allow While Using App].

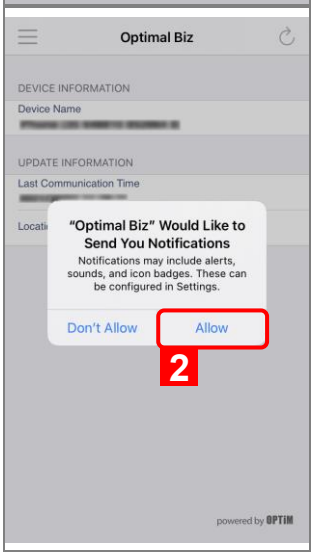
⇒You will be asked to allow location service.



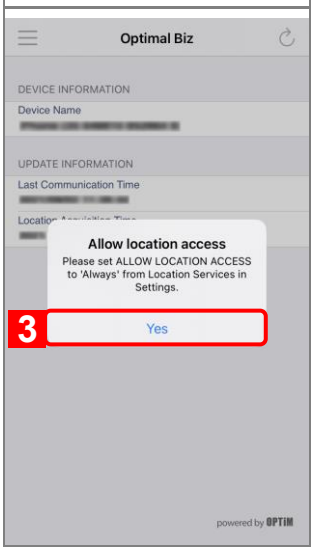
【2】 Tap [Allow].

This step is only required on the first launch.

If you do not tap [Allow], no notification appears when the device receives a message from the management site.

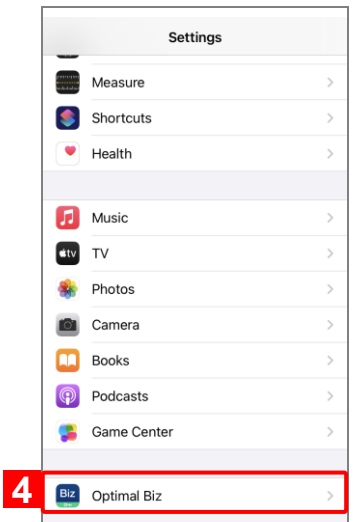


【3】 Tap [Yes].

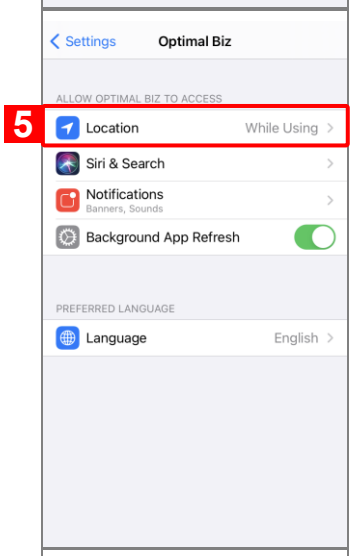


【4】 Tap [Optimal Biz] on the "Settings" screen of the device.

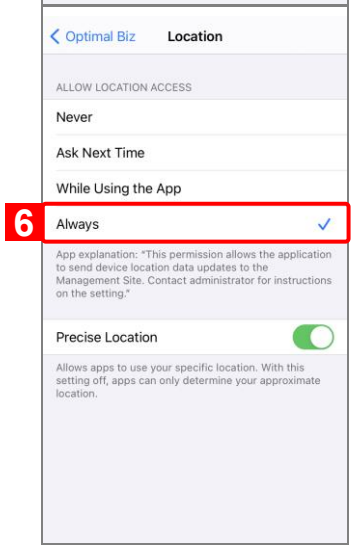
If you see a different hierarchy of "Settings", display the first hierarchy.



【5】 Tap [Location].



【6】 Tap [Always] to enable it.



5.1.2 Installation and authentication from App Store

Use the following steps to install and authenticate the agent from the App Store.

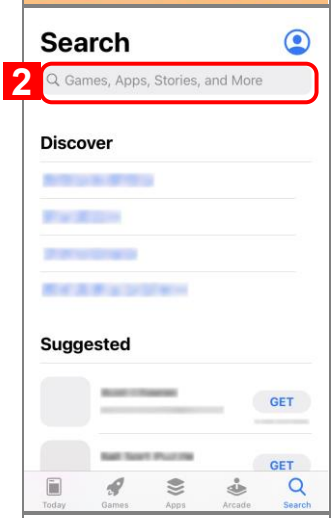
Operations to perform on the App Store are subject to change by Apple.

【1】 Tap [App Store] on the home screen.

⇒The App Store will be displayed.

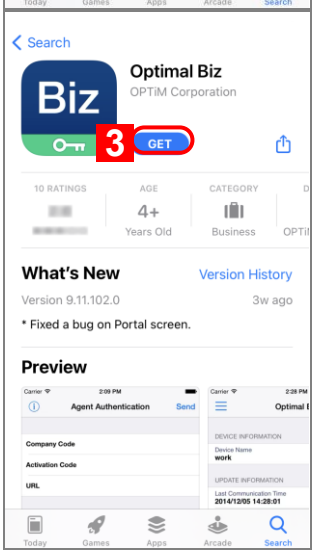
【2】 Type and search for " Optimal Biz ".

⇒The "Optimal Biz" page will be displayed.



【3】 Tap [GET].

⇒The agent (Optimal Biz) will be installed. Wait until the [Optimal Biz] icon appears on the device's home screen.



【4】 Tap [Optimal Biz] on the home screen.

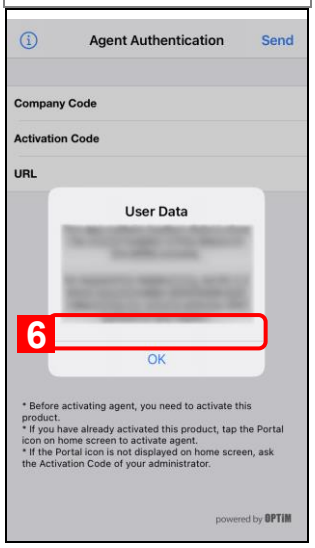
⇒The agent will be launched and the Privacy Policy screen will be displayed.

【5】 Tap [Accept].

This step is only required on the first launch after installing or updating the agent.

【6】 Tap "OK".

This step is only required on the first launch after installing or updating the agent.



【7】Enter "Company Code", "Activation Code", and "URL".

Contact your administrator for your company code, activation code, and URL.

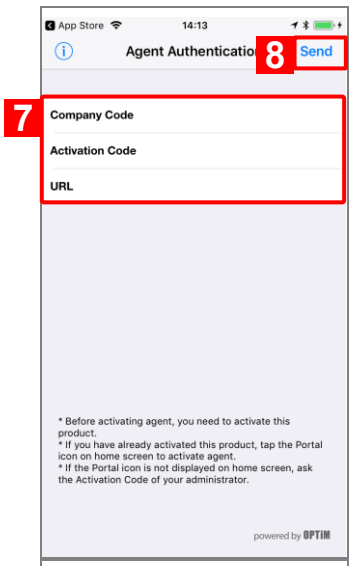
【8】Tap [Send].

⇒The agent will be activated.

If you have not performed license authentication, follow the instructions that will be displayed on the screen and perform license authentication.

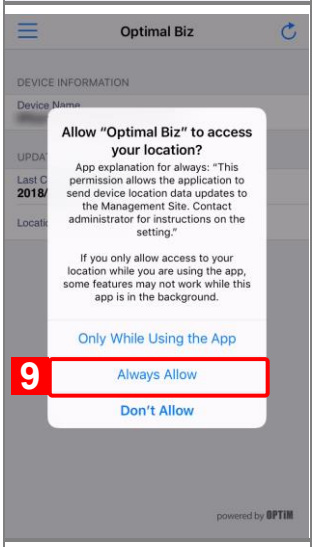
The following steps differ if the device is on iOS 13.0 and later. Refer to the following.

☞"Always allowing location access on devices with iOS 13.0 and later" Page 55



【9】Tap [Always Allow].

If you do not set [Always Allow] for your location information, the agent functions may not be available.

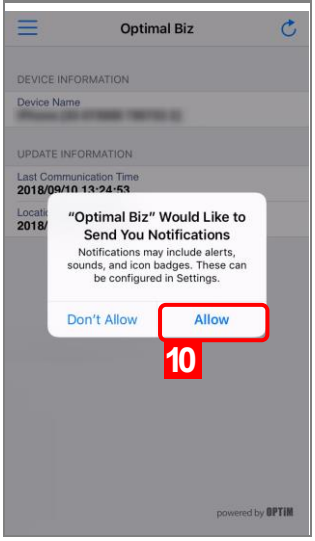


【10】Tap [Allow].

This step is only required on the first launch.

If you do not tap [Allow], no notification appears when the device receives a message from the management site.

⇒When "Device Information" and "Update Information" (A) are displayed, the agent has been authenticated.



5.1.3 Installation and automatic authentication using Application Distribution

If you hide Portal and the App Store on the device, you can install / automatically authenticate the agent by using the Application Distribution function and App Configuration function of the management site.

For more information on the functions and operations, refer to the relevant section of the manual below.

"Settings – iOS" - "Application" - "Application Distribution" in <Management Site Reference Manual>

"Settings – iOS " - "Application" - "App Configuration" in <Management Site Reference Manual>

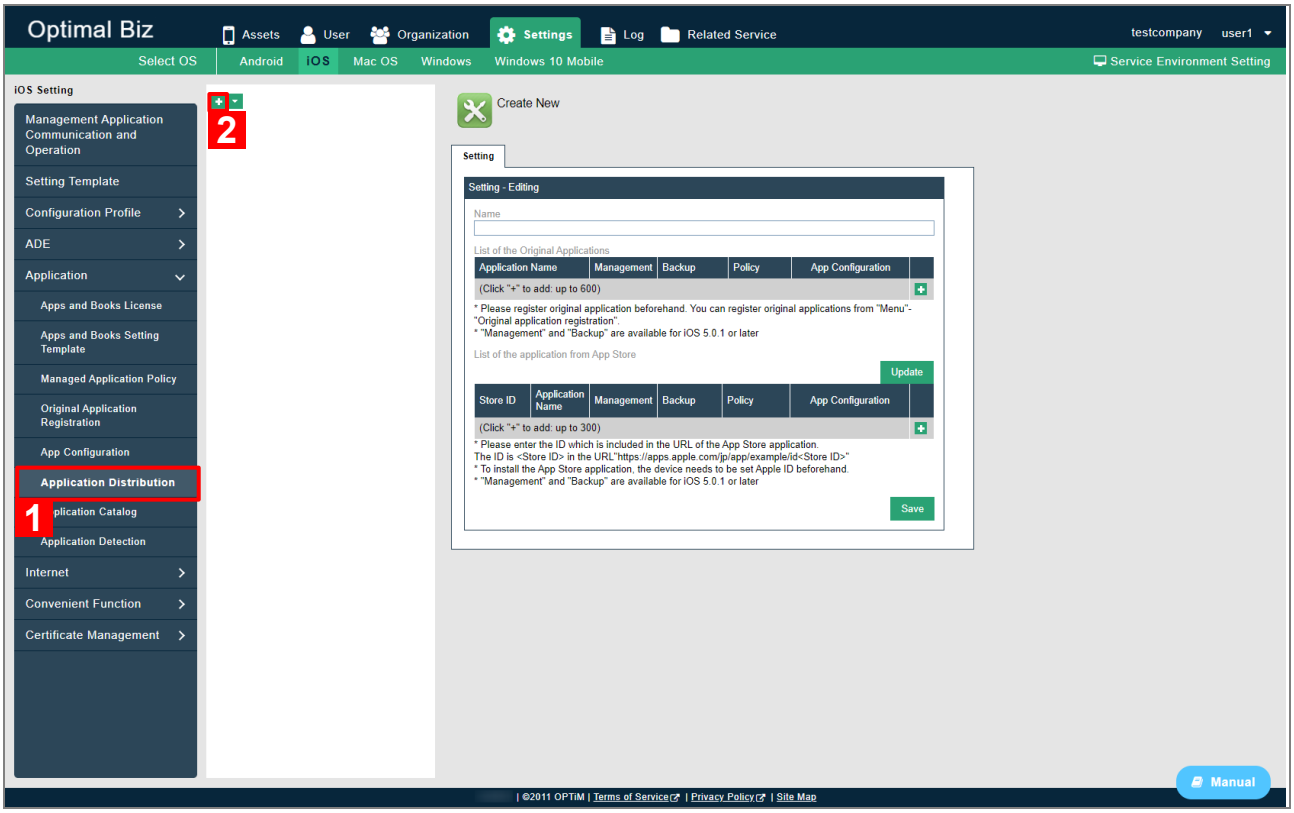
"Asset" - "List" - "Settings of assets" - "(Setting – iOS) Settings Allocation" in <Management Site Reference Manual>

5.1.3.1 Installing the agent through application distribution

Use the following steps to create a setting for distributing the agent to a device (Application Distribution setting) and setting for automatically authenticating the agent (App Configuration setting).

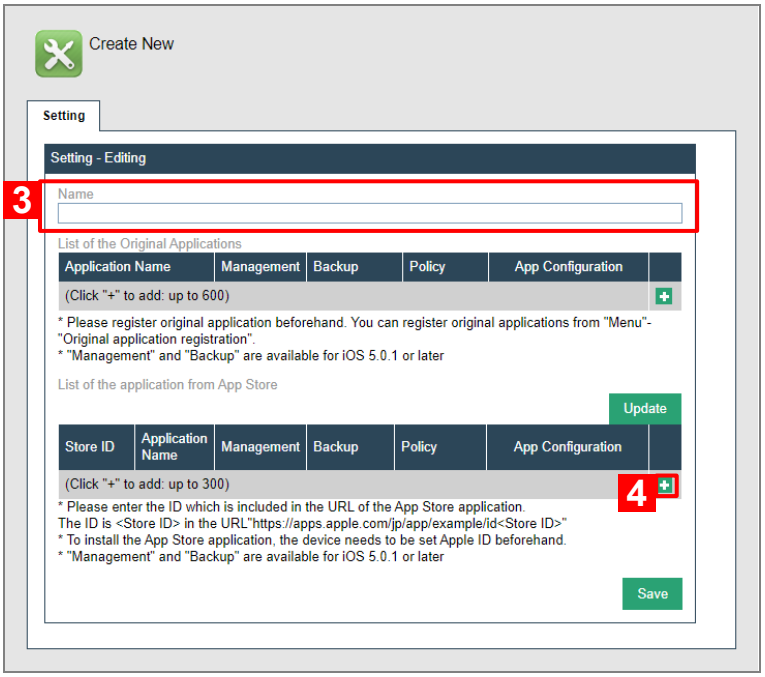
【1】 Click [Settings]→[iOS]→[Application]→[Application Distribution].

【2】 Click ＋.



【3】Enter a setting name in "Name".

【4】Click ＋ in "List of the application from App Store".

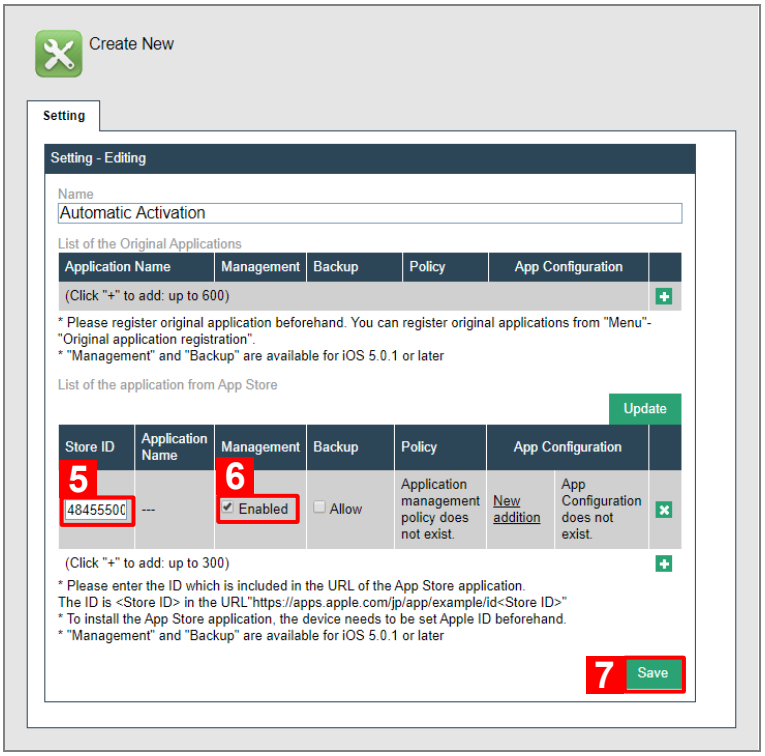


【5】Enter "484555006" (the Store ID of the agent (Optimal Biz)) in "Store ID".

【6】Select "Enabled" in "Management".

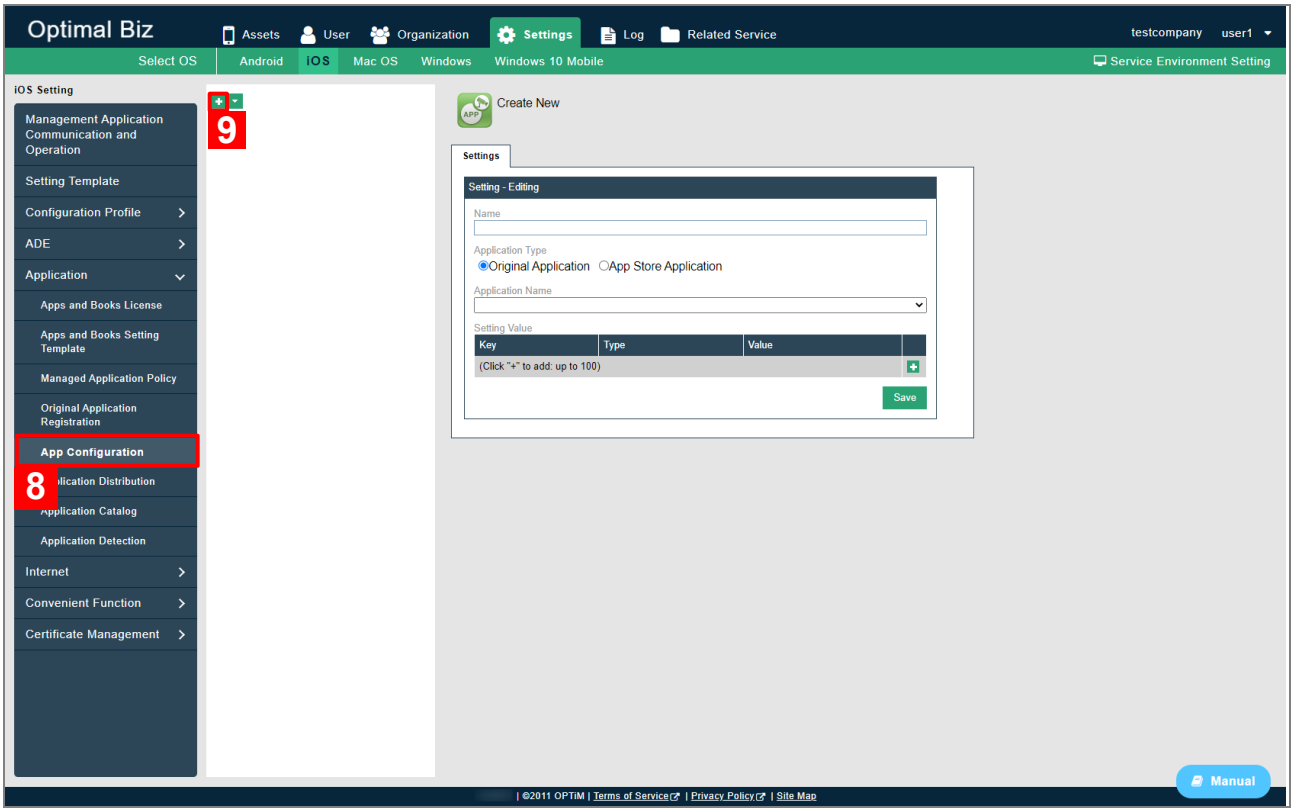
【7】Click [Save].

⇒An application distribution setting will be created.



【8】 Click [Settings]→[iOS]→[Application]→[App Configuration].

【9】 Click ＋.



【10】Enter a setting name in "Name".

【11】Select "App Store Application" in "Application Type".

【12】Specify "Optimal Biz" from the Application Name" pull-down menu.

【13】Click ＋ in Setting Value to add a setting item and configure a company code (A), management site URL (B), and an activation code (C) in each item.

Enter the following values in "Key" and "Value" of the company code (A).

- Key: company_code
- Value: (a specific company code)

Enter the following values in "Key" and "Value" of the management site URL (B).

- Key: server_url
- Value: https://biz3.optim.co.jp/

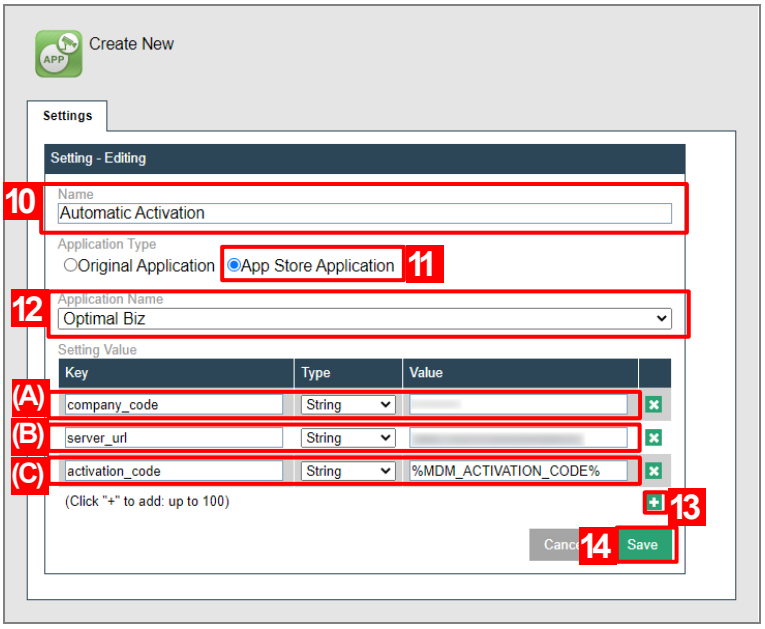
Enter the following values in "Key" and "Value" of the activation code (C).

- Key: activation_code
- Value: %MDM_ACTIVATION_CODE%

Specify "String" for "Type" of the company code (A), management site URL (B), and activation code (C).

【14】Click [Save].

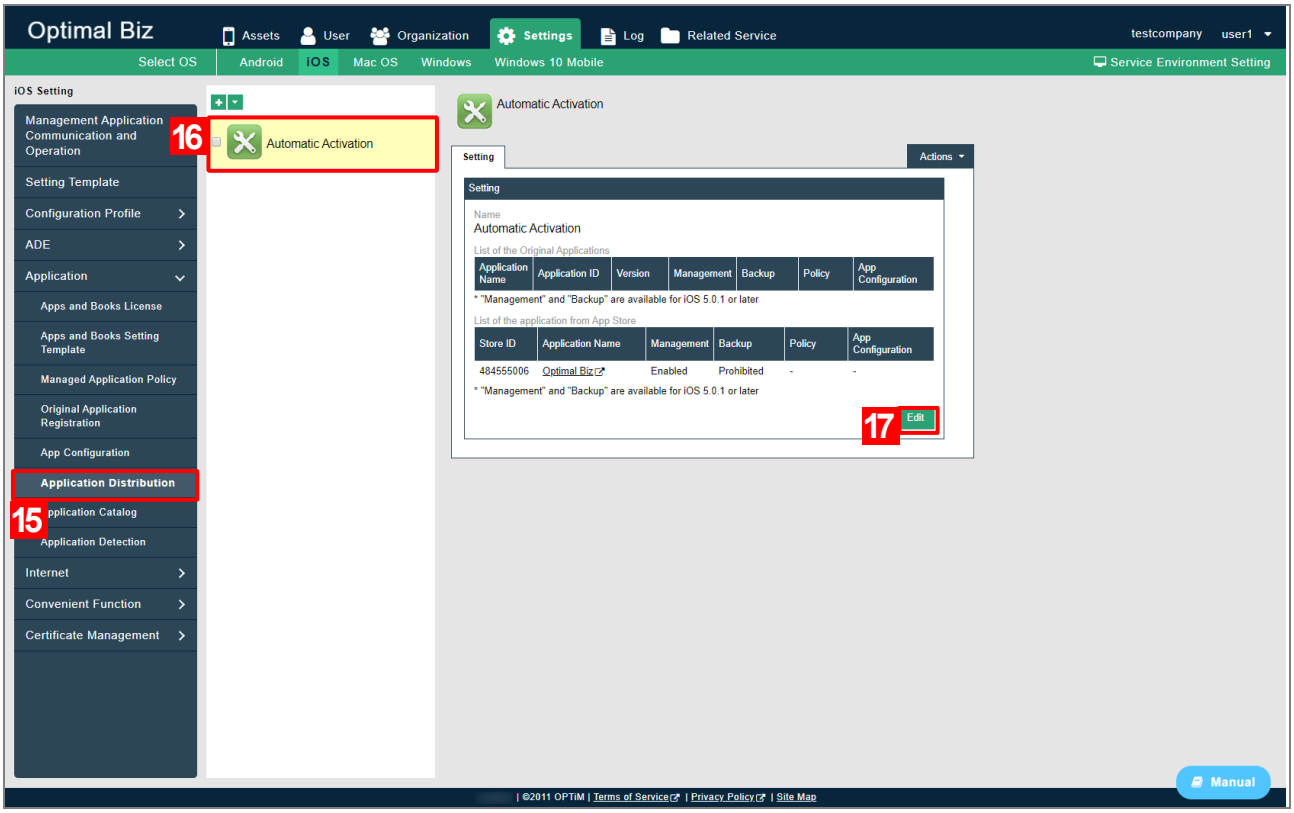
⇒The App Configuration setting will be created.



【15】 Click [Settings]→[iOS]→[Application]→[Application Distribution].

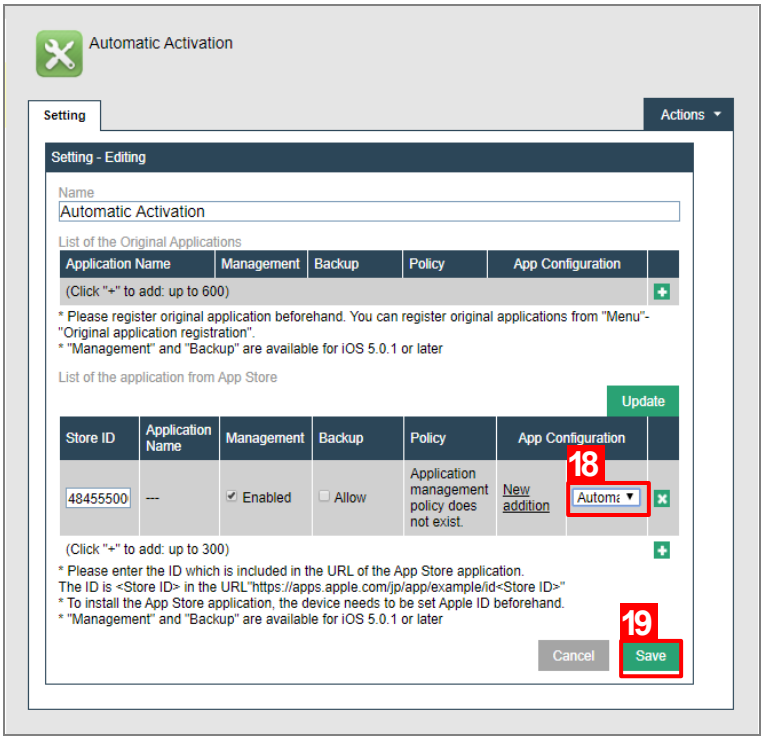
【16】 Click the application distribution setting you created in step 【7】 from the list.

【17】 Click [Edit].



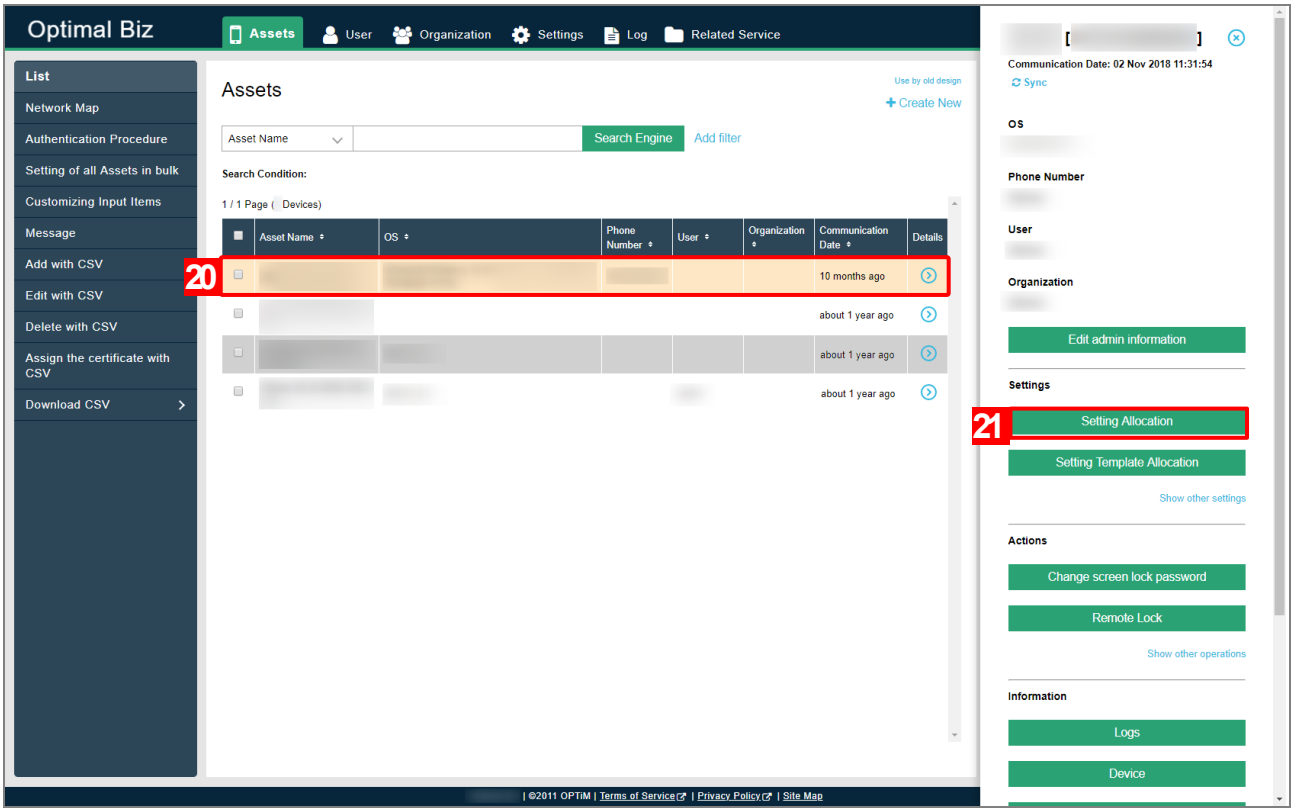
【18】 From the "App Configuration" pull-down menu, specify the name of the setting you configured in step 【10】.

【19】 Click [Save].

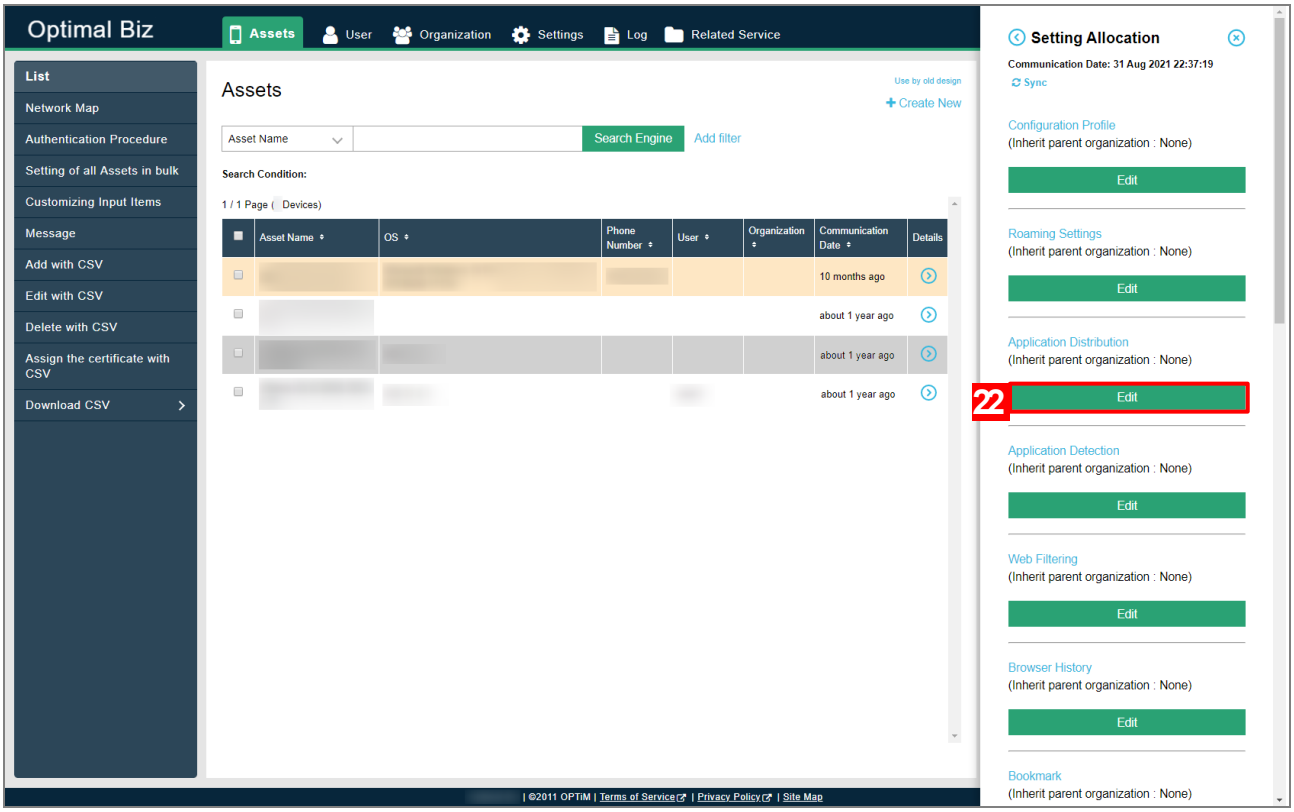


【20】 Go to [Assets]→[List], and select a target device from the list.

【21】 Click [Setting Allocation] in "Settings".

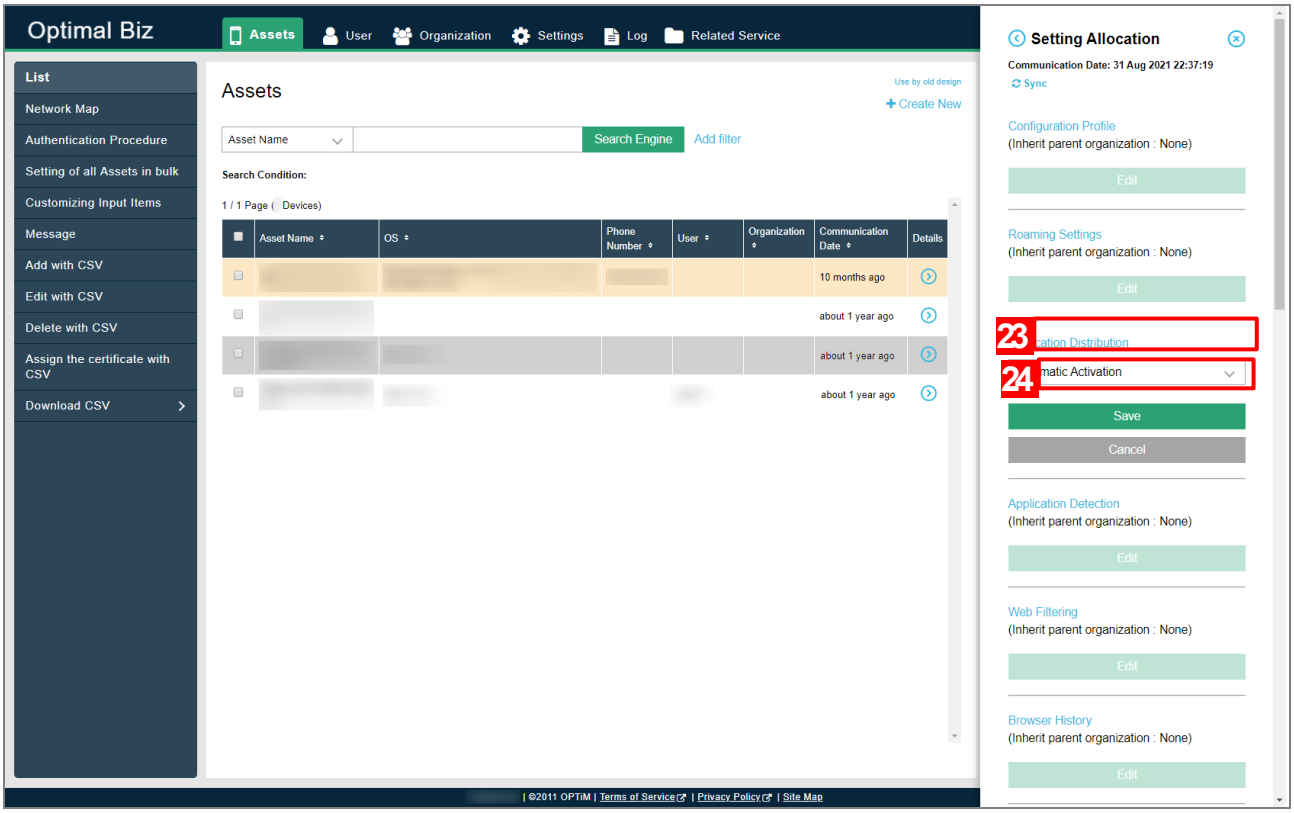


【22】 Click [Edit] in "Application Distribution".



【23】 **From the "Application Distribution" pull-down menu, specify the name of the setting you configured in step 【3】.**

【24】 **Click [Save].**

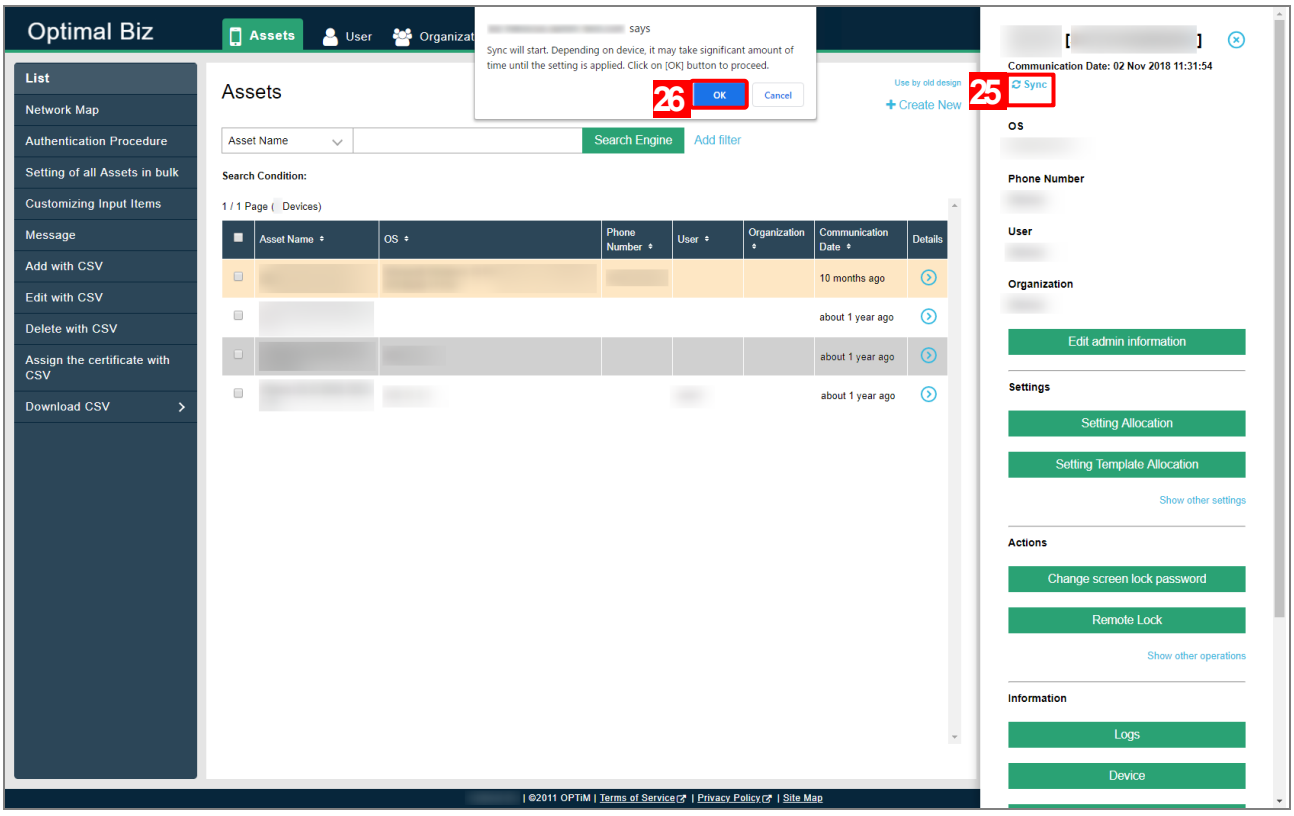


【25】 **Click [Sync].**

【26】 **Click [OK].**

⇒The agent (Optimal Biz) will be installed on the device. Wait until the [Optimal Biz] icon appears on the device's home screen.

It may take a while until the agent are installed on the devices.



5.1.3.2 Automatically authenticating the agent

Perform the following steps to automatically authenticate the agent installed on the device.

【1】Tap [Optimal Biz] on the home screen.

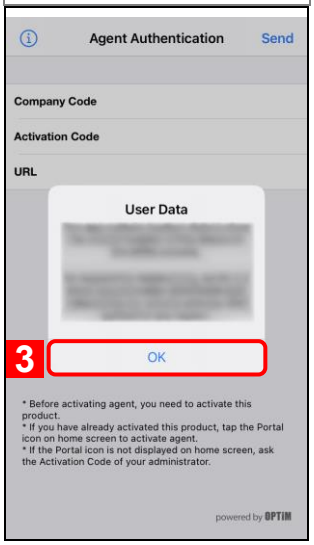
⇒The agent will be launched and the Privacy Policy screen will be displayed.

【2】Tap [Accept].

The following steps differ if the device is on iOS 13.0 and later. Refer to the following.

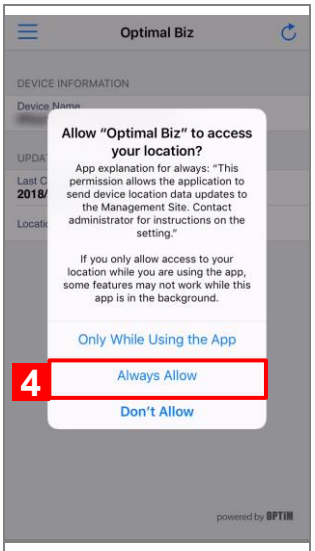
☞"Always allowing location access on devices with iOS 13.0 and later" Page 55

【3】Tap "OK".



【4】 Tap [Always Allow].

If you do not set [Always Allow] for your location information, the agent functions may not be available.



【5】 Tap [Allow].

If you do not tap [Allow], no notification appears when the device receives a message from the management site.

⇒When "Device Information" and "Update Information" (A) are displayed, the agent has been authenticated.