
OPTiM


Optimal Biz Android Kitting Manual

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

Getting Started

Purpose of this manual

This manual explains the kitting operation for Android.







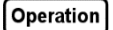

 To perform a kitting operation, the Android device must be in the factory default state (default setting screen).

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.


◆ 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.
	In the explanation of the screen, describes the menu operation for displaying the corresponding screen. Ex)  [Settings]→[Android]→[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

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

Table of contents

1 About Android client.....	5
1.1 Overview	6
1.2 OS support policy	6
1.3 System Requirement	7
2 Selecting kitting methods	8
2.1 Overview of each kitting method	9
3 Integrating Android Enterprise with a Google account Google	11
3.1 Registering a Google account.....	12
3.2 Creating a user	18
3.3 Kitting with the afw identifier.....	20
3.3.1 For less than Android 12	20
3.3.2 For Android 12 or later	26
3.4 Performing license authentication.....	34
3.4.1 Authenticating by a user ID	34
3.4.2 Authenticating by a company code / authentication code	36
3.5 Allocating a user to your device	38
4 Integrating with Android Enterprise by a Google Workspace (formerly G Suite) account.....	40
4.1 Issuing a token.....	41
4.2 Registering a Google Workspace (formerly G Suite) account.....	48
4.3 Creating a user.....	50
4.3.1 Registering a Google Workspace (formerly G Suite) account to an existing user	52
4.4 Kitting by a Google Workspace (formerly G Suite) account.....	54
4.4.1 For less than Android 12	54
4.4.2 For Android 12 or later	61
4.5 Performing license authentication.....	69
4.5.1 Authenticating by a user ID	69
4.5.2 Authenticating by a company code / authentication code	71
5 Performing Android Enterprise integration by using zero-touch enrollment with a Google account	73
5.1 Registering a Google account.....	74
5.2 Performing authentication settings of Google API.....	80
5.2.1 Registering your e-mail address as a Google account.....	80
5.2.2 Logging in to the zero-touch portal	83
5.2.3 Accepting the terms of service	84
5.2.4 Downloading API settings and a JSON file.....	86
5.2.5 Uploading a JSON file.....	100
5.3 Creating a user.....	105
5.4 Performing kitting with zero-touch registration (using a Google account)	107
5.4.1 For less than Android 10	107
5.4.2 For Android 10 or later	112
5.5 Performing license authentication.....	121
5.5.1 Authenticating by a user ID	121
5.5.2 Authenticating by a company code / authentication code	123
5.6 Allocating a user to your device	125
5.7 Syncing with the zero-touch registration server.....	127

6 Integrating with Android Enterprise by a Google Workspace (formerly G Suite) account using zero-touch enrollment	128
6.1 Issuing a token.....	129
6.2 Registering a Google Workspace (formerly G Suite) account.....	136
6.3 Performing authentication settings of Google API.....	138
6.3.1 Registering your e-mail address as a Google account.....	138
6.3.2 Logging in to the zero-touch portal	141
6.3.3 Accepting the terms of service	142
6.3.4 Downloading API settings and a JSON file.....	144
6.3.5 Uploading a JSON file.....	158
6.4 Creating a user.....	163
6.4.1 Registering a Google Workspace (formerly G Suite) account to an existing user	165
6.5 Performing kitting with zero-touch enrollment (using a Google Workspace (formerly G Suite) account)	167
6.5.1 For less than Android 10	167
6.5.2 For Android 10 or later	174
6.6 Performing license authentication.....	185
6.6.1 Authenticating by a user ID	185
6.6.2 Authenticating by a company code / authentication code	187
6.7 Syncing with the zero-touch registration server.....	189
7 Other kitting methods.....	190
7.1 Performing kitting using a QR code	191
7.1.1 Displaying a QR code	191
7.1.2 Scanning a QR code into your device	192
7.1.2.1 For less than Android 10	192
7.1.2.2 For Android 10 or later.....	198
7.2 Performing kitting using NFC.....	206
7.2.1 Creating a configuration set.....	206
7.2.2 Setting a master device.....	207
7.2.3 Setting a subdevice.....	210
7.3 Performing license authentication.....	212
7.3.1 Authenticating by a user ID	212
7.3.2 Authenticating by a company code / authentication code	214
8 Changing the owner of your device	216
8.1 Factory resetting the device.....	217
8.1.1 Factory reset using remote wipe.....	217
8.1.2 Factory reset using the device reset function	217
8.1.3 Factory reset using the agent	217
8.2 Deleting device information.....	218
9 Changing integration settings between Optimal Biz - Google	219
9.1 Deleting your Google account.....	220
9.2 Re-registering your Google account	223
9.3 Deleting your Google Workspace (formerly G Suite) account	225
10 Legacy Android agent	228
10.1 Installing the legacy agent.....	229
10.2 Activating the legacy agent	231


1 About Android client

Describes the following items

Item	Page
Overview	6
OS support policy	6
System Requirement	7

1.1 Overview

Optimal Biz (hereinafter referred to as this product) is a support service that manages and operates Android devices without requiring expert knowledge. Remote lock and remote wipe (initialization) of Android devices can be performed from Optimal Biz management site (hereinafter referred to as the management site) .


 This manual is the operation manual of Android devices. For operation of the management site, refer to the following.

 <Management Site Reference 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.

Support policy	Example of support
<ul style="list-style-type: none"> ● 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. 	<ul style="list-style-type: none"> ● Android 12: Latest supported OS ● Android 11: One generation ago ● Android 10: Two generations ago ● Android 9: Three generations ago  Android 8.x is no longer supported. We will try our best to respond to your inquiries until October 23, 2022.


1.3 System Requirement

The system requirement of Android client is as follows.

Device	Android 9 or later  We support up to Android 8.x for the conventional version agent.  For details of the device, refer to the following.  <Android Support Device List>
Device memory	At least 200MB available disk space
SD Card	At least 5MB of available disk space (required when saving the downloaded installer on the SD Card)
Network Connection	Connected to the internet via 3G/LTE or Wi-Fi. Available to communicate HTTPS (port 443) to the management site with/without proxy.

 If you use the following functions or apps on your device, they may disrupt the agent's behavior and communication.

- Data saver
- Background data usage settings
- Airplane mode
- Battery optimization
- Battery-saving apps (Kyocera "Eco-Mode", HUAWEI "Device Management", etc.)

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

2 Selecting kitting methods

The kitting method will vary depending on the device you use and whether you use a Google Workspace (formerly G Suite) account. Refer to the following to select an appropriate method.

Item	Page
Item	Page



Attention


- To execute kitting, you must factory reset the device (initial setup screen).
- The legacy Android agent can be installed to Android 5.x or lower, but the agent is guaranteed to operate in Android 9 or later. For legacy agent, refer to the following.

👉 "Legacy Android agent" Page 228

2.1 Overview of each kitting method




There are six ways to perform kitting for Android agents. See the table below for the characteristics of each method.











- Afw identifier
- Google Workspace (formerly G Suite) account
- Zero-touch enrollment (using a Google account)
- Zero-touch enrollment (using a Google Workspace (formerly G Suite) account)
- QR code
- NFC

 Depending on the kitting method, you cannot change it to another method. Before you begin kitting, review the table below and carefully select an appropriate method.

 When using Android Enterprise regardless of the kitting methods, one user can own up to 10 devices. Do not link more than 10 devices to one user.

If you link more than 10 devices to one user, Google account distributed to the device will be disabled. You will not be able to browse Google Play or install apps that are used on your account.

Kitting method	Description
Afw identifier	<p>Enter the afw identifier "afw#biz3" in the Google account input field that appears when you activate your device. This is the most standard kitting method that requires few preliminary settings.</p> <p>For the kitting steps, refer to the following.</p> <p> "Integrating Android Enterprise with a Google account Google" Page 11</p> <p> If you have a Google Workspace (formerly G Suite) contract, do not select this option and make sure to perform kitting using one of the following methods.</p> <ul style="list-style-type: none"> • Google Workspace (formerly G Suite) account • Zero-touch enrollment (using a Google Workspace (formerly G Suite) account)
Google Workspace (formerly G Suite) account	<p>Enter your Google Workspace (formerly G Suite) in the Google account input field that appears when you activate your device. This method is to integrate Android Enterprise by using your Google Workspace (formerly G Suite) account. This method provides the following benefits.</p> <ul style="list-style-type: none"> • Because you use a Google Workspace (formerly G Suite) account, you do not have to create a Google account for administration. • You can use Google services from your device by using your Google Workspace (formerly G Suite) account. <p>For the kitting steps, refer to the following.</p> <p> "Integrating with Android Enterprise by a Google Workspace (formerly G Suite) account" Page 40</p>

Kitting method		Description
Zero-touch enrollment (using a Google account)		<p>You use a device that supports zero-touch enrollment to integrate Android Enterprise via your Google account and force the device to be under control of this product. This method provides the following benefits.</p> <ul style="list-style-type: none"> • Pre-kitting devices can be registered as pre-kitting devices. • Device operation during activation can be reduced. <p>For the kitting steps, refer to the following.</p> <p> "Performing Android Enterprise integration by using zero-touch enrollment with a Google account" Page 73</p> <p> For the details of zero-touch enrollment, refer to the following.</p> <p> https://www.android.com/intl/ja_jp/enterprise/management/zero-touch/</p>
Zero-touch enrollment (using a Google Workspace (formerly G Suite) account)		<p>You use a device that supports zero-touch enrollment to integrate Android Enterprise via your Google Workspace (formerly G Suite) account and force the device to be under control of this product. This method provides the following benefits.</p> <ul style="list-style-type: none"> • Pre-kitting devices can be registered as pre-kitting devices. • Device operation during activation can be reduced. • Because you use a Google Workspace (formerly G Suite) account, you do not have to create a Google account for administration. • You can use Google services from your device by using your Google Workspace (formerly G Suite) account. <p>For the kitting steps, refer to the following.</p> <p> "Integrating with Android Enterprise by a Google Workspace (formerly G Suite) account using zero-touch enrollment" Page 128</p> <p> For the details of zero-touch enrollment, refer to the following.</p> <p> https://www.android.com/intl/ja_jp/enterprise/management/zero-touch/</p>
Others	QR code	<p>Tap the initial setup screen six times to install a QR code scanner, and scan a specified QR code.</p> <p>For the kitting steps, refer to the following.</p> <p> "Performing kitting using a QR code" Page 191</p>
	NFC	<p>Hold the NFC-supported master device over a subdevice to install the agent.</p> <p>For the kitting steps, refer to the following.</p> <p> "Performing kitting using NFC" Page 206</p> <p> Available on NFC-supported devices with Android 6.0 to 9, but guaranteed to operate in Android 9 or later. For NFC-supported devices, refer to the following.</p> <p> <Android Support Device List></p>

3 Integrating Android Enterprise with a Google account Google


To use Android Enterprise, perform an integration setting between this product and Google via your Google account before kitting your device.

This chapter describes the following items.

Item	Page
Registering a Google account	12
Creating a user	18
Kitting with the afw identifier	20
Performing license authentication	34
Allocating a user to your device	38



Attention

- You must have a Google account that is not integrated with Android Enterprise.
- If you want to delete an integrated account or re-register a new account, refer to the following.
 "Changing integration settings between Optimal Biz - Google" Page 219
- The items marked with * above are required only for the first kitting.



Reference

- By setting up the "Application Distribution" function of Android Enterprise on the management site in advance, apps can be distributed to your device at the same time as license authentication after kitting is complete. For details of app distribution, refer to the following.

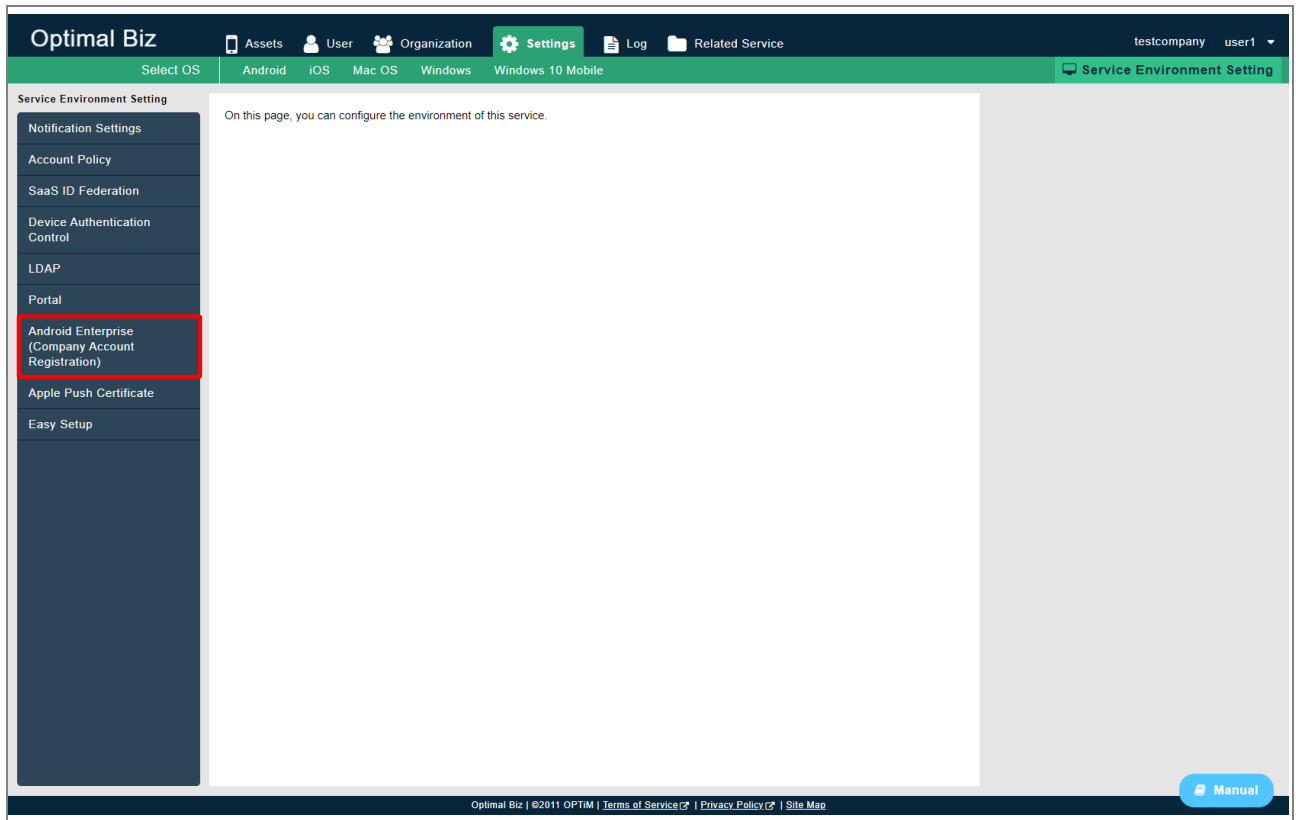


"Android Enterprise App distribution" in<Android Enterprise Manual>

3.1 Registering a Google account

Follow the steps below to register a Google account for integrating Android Enterprise with the management site.

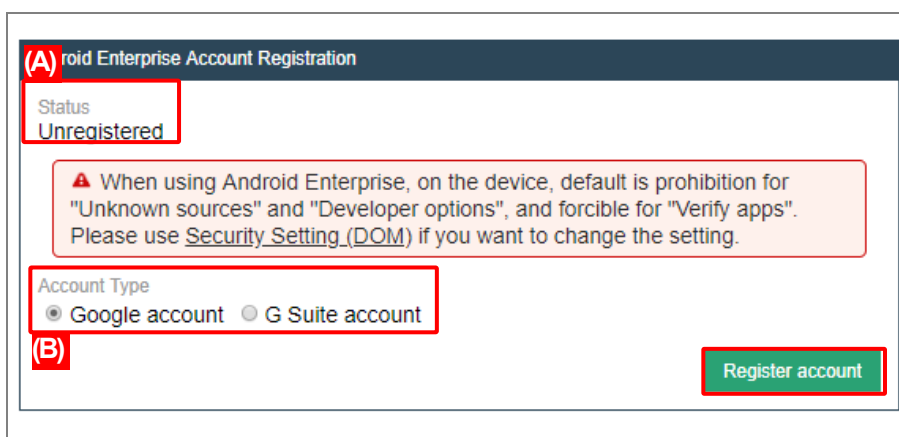
- [1] Click [Settings]→[Service Environment Setting]→[Android Enterprise (Company Account Registration)].**



- [2] The "Status" (A) shows "Unregistered".**
Google account" is selected in "Account Type" (B) by default. Click [Register account].

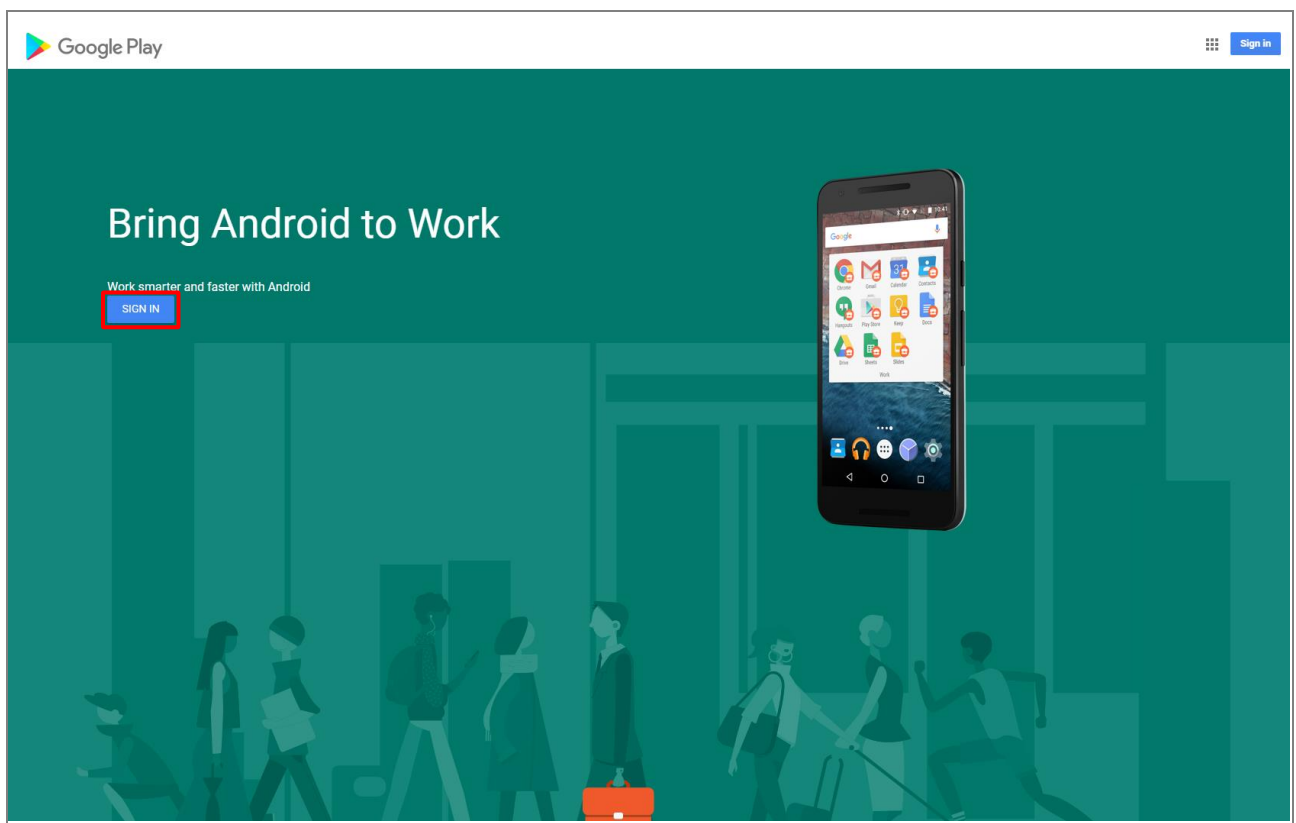
- ✓ After account registration is complete, the device's "Installation of unknown source apps" and "Developer options" will be set to "Prohibit" and "Force apps check" will be set to "Force". Create a configuration set that allows "Installation of unknown source apps" in "Security setting (DOM)", allocate it to your device, and perform a sync.

🔍 "Settings – Android" - "Device Owner Mode" - "Security setting (DOM)" in <Management Site Reference Manual>



[3] Google Play will be displayed. Click [SIGN IN].

 Depending on the browser you are using, Google Play may not work properly.

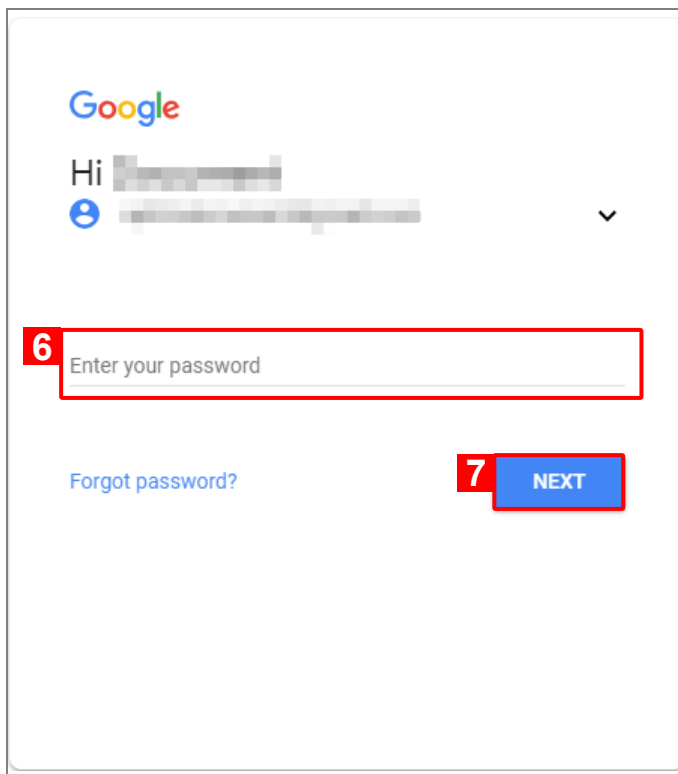


[4] Enter your company Google account.

[5] Click [NEXT].

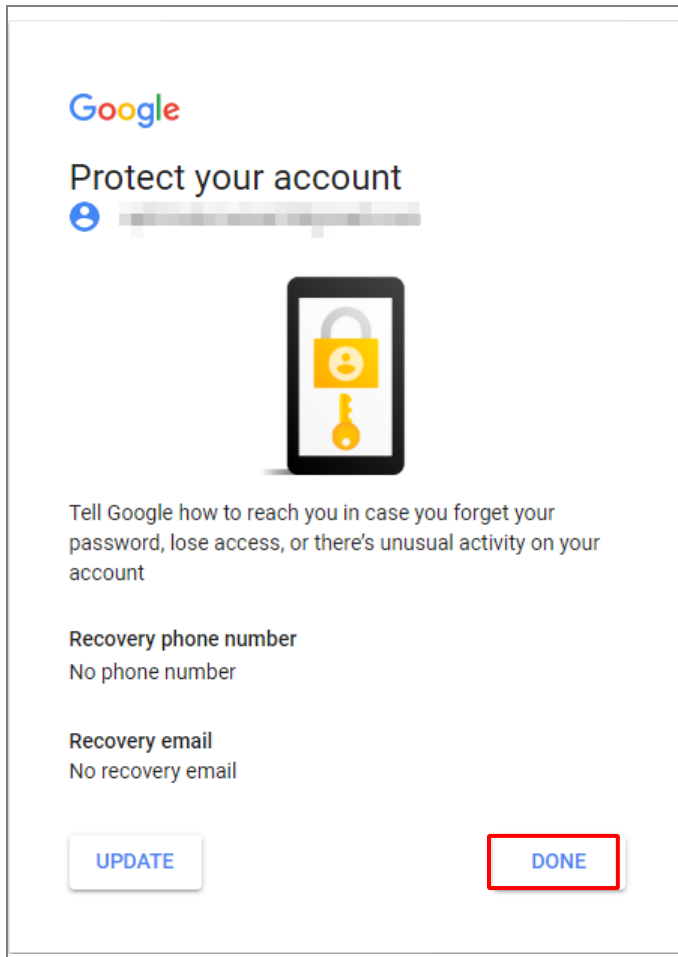
[6] Enter the password.

[7] Click [NEXT].



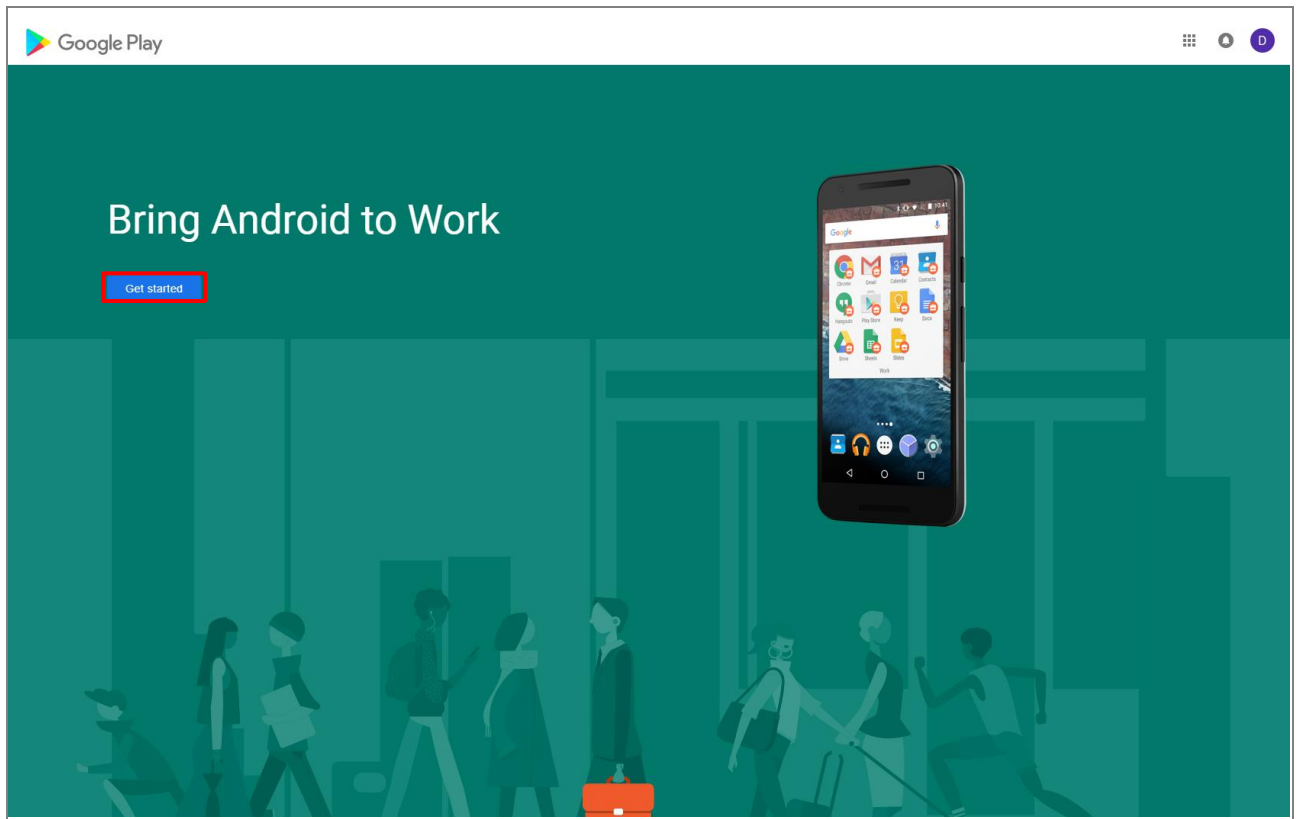
The image shows the Google login interface. At the top is the Google logo. Below it, the text "Hi" is followed by a blurred username and a blue profile icon. A red box labeled "6" highlights the password input field with the placeholder text "Enter your password". Below the input field is a link that says "Forgot password?". To the right of the input field is a blue button labeled "NEXT" with a red box labeled "7" highlighting it.

[8] Click [DONE].



The image shows the "Protect your account" screen. At the top is the Google logo. Below it, the text "Protect your account" is followed by a blurred username and a blue profile icon. In the center is an illustration of a smartphone with a yellow padlock icon on the screen. Below the illustration, the text reads: "Tell Google how to reach you in case you forget your password, lose access, or there's unusual activity on your account". Underneath, there are two sections: "Recovery phone number" with the text "No phone number" below it, and "Recovery email" with the text "No recovery email" below it. At the bottom, there are two buttons: "UPDATE" on the left and "DONE" on the right, which is highlighted with a red box.

[9] Click **[Get started]**.



[10] Enter "Business name".

[11] Click **[Next]**.

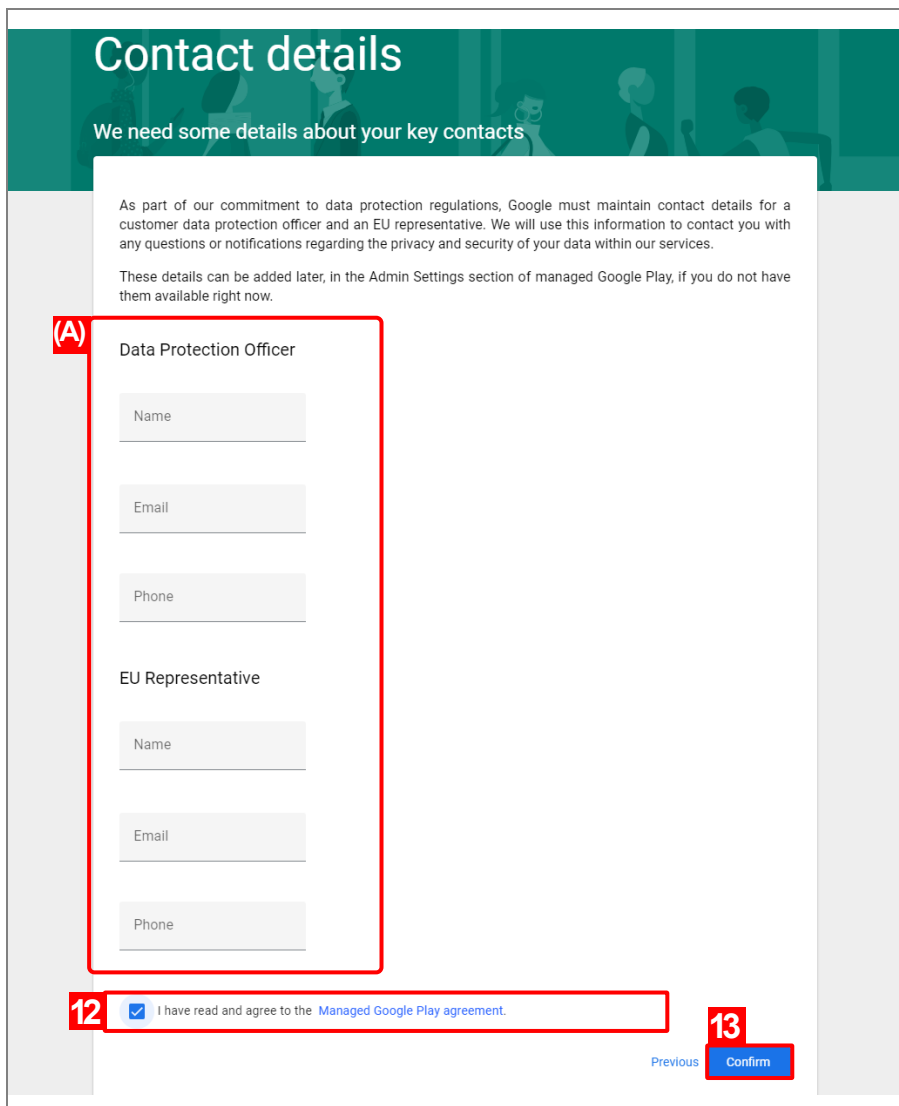
A screenshot of a setup screen titled 'Business name'. The subtitle reads 'We need some details about your business'. The screen contains two input fields. The first field is labeled 'Business name' and has a placeholder text 'Your answer' inside a light green box; this box is highlighted with a red rectangular box and a red '10' in a white box to its left. The second field is labeled 'Enterprise mobility management (EMM) provider' and has the text 'Optimal Biz' entered below it. At the bottom right of the form, there are two buttons: 'Previous' and 'Next'. The 'Next' button is highlighted with a red rectangular box and a red '11' in a white box to its left.

[12] Read the agreement and check the box.

[13] Click [Confirm].

- ☒ The Data Protection Officer and EU Representative (A) are optional. Enter them if required. For details of Data Protection Officer and EU Representative, refer to the following.

 <https://support.google.com/googleplay/work/answer/7681629>



Contact details

We need some details about your key contacts

As part of our commitment to data protection regulations, Google must maintain contact details for a customer data protection officer and an EU representative. We will use this information to contact you with any questions or notifications regarding the privacy and security of your data within our services.

These details can be added later, in the Admin Settings section of managed Google Play, if you do not have them available right now.

(A)

Data Protection Officer

Name

Email

Phone

EU Representative

Name

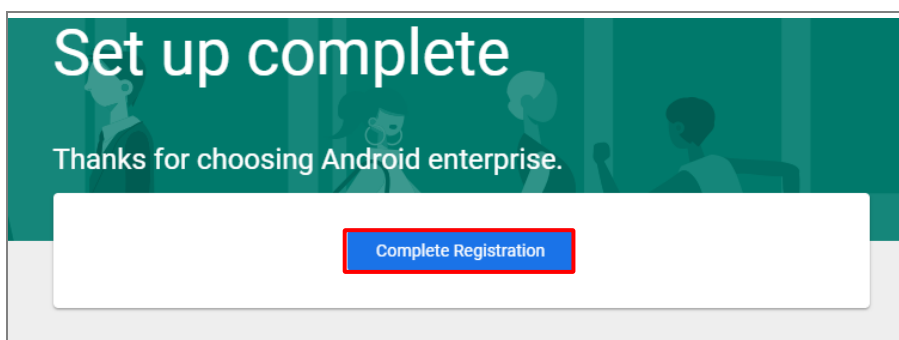
Email

Phone

12 ☒ I have read and agree to the [Managed Google Play agreement](#).

13 [Previous](#) [Confirm](#)

[14] Click [Complete Registration].



Set up complete

Thanks for choosing Android enterprise.

[Complete Registration](#)

- [15]** When you return to the management site, the "Status" (A) shows "Registered".
The email address registered for Google Play is displayed in "Account E-mail Address" (B).

The screenshot displays the 'Android Enterprise Account Registration' interface. At the top, a dark blue header contains the title. Below this, the 'Status' is listed as 'Registered', with a red box and label (A) highlighting it. A red-bordered warning box follows, containing a triangle icon and text about device settings. Under 'Account Type', 'Google account' is listed. The 'Account E-mail Address' field is highlighted with a red box and label (B). A green 'Delete account' button is located at the bottom right.

Android Enterprise Account Registration

(A) Status
Registered

⚠ When using Android Enterprise, on the device, default is prohibition for "Unknown sources" and "Developer options", and forcible for "Verify apps". Please use [Security Setting \(DOM\)](#) if you want to change the setting.

Account Type
Google account

(B) Account E-mail Address

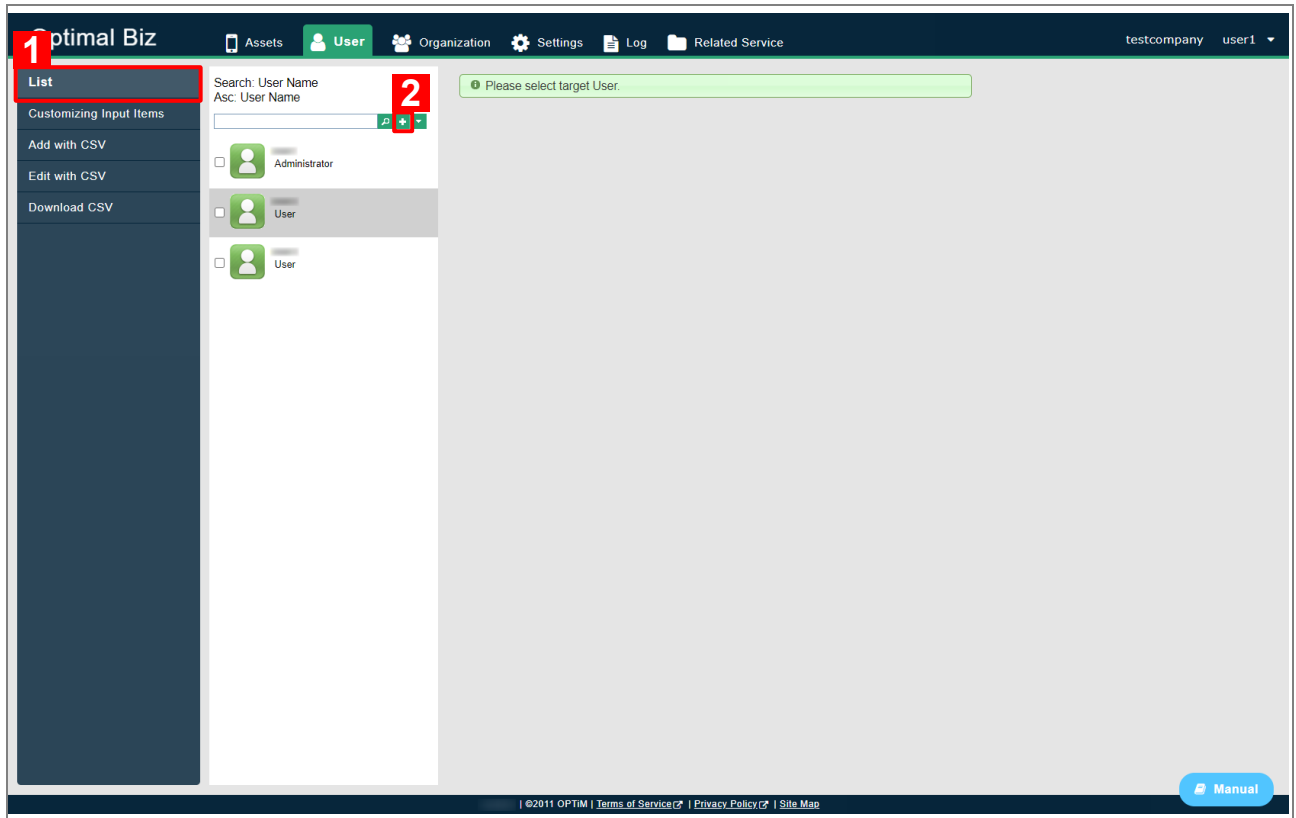
Delete account

3.2 Creating a user

Follow the steps below to create a user.

[1] Click [User]→[List].

[2] Click .



[3] Enter an arbitrary name in "Name".

✎ For details of other input and setting items, refer to the following.

✎ "User" - "List" - "Create a user" in <Management Site Reference Manual>

[4] Click [Save].

⇒ A user will be created.

The screenshot shows a web interface for managing users. At the top, there's a navigation bar with tabs: Admin, Apps and Books Setting, Access Control, Others, and Actions. Below this is a 'Management Information - Editing' form. The form is divided into two main sections: 'Management Information' on the left and 'Password' on the right. The 'Management Information' section includes fields for Name, Phonetic Name, Last Name, First Name, User ID, and E-mail Address. It also has a 'User Classification' section with radio buttons for Administrator, Operator, Reader, Lock/Wipe only, Login only, and User (selected). Below this are dropdown menus for Organization and Category. The 'Password' section has a 'Current Password' field with a green 'Edit' button. The 'Assets' section shows 'Number of Devices' as 0. The 'SaaS ID Federation' section shows 'Office 365' and 'G Suite' both set to '(None)'. At the bottom of the form, there's a 'Device Authentication Limit' section with radio buttons for No Restriction (selected), Restricted, and Prohibit authentication. A red box highlights the 'Name' field with a red '3' next to it. The 'Save' button is highlighted with a red '4' next to it.

3.3 Kitting with the afw identifier

Follow the steps below to perform kitting for your device with the afw identifier.

Note that the operation is different between Android versions earlier than 12 and versions 12 or later. Depending on the Android version of your device, choose one of the following methods.

● For less than Android 12

● For Android 12

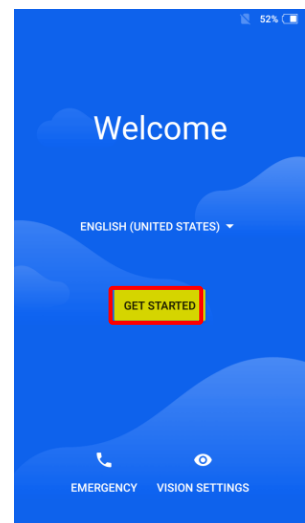
☑ When you are kitting Android 12 or later, kitting operation may not be able to complete if you have set Google Play Developer Services (com.google.android.gms) on the management site's "Application prohibition" blacklist and "Non-display application". Refer to the following to clear the setting in advance and then conduct kitting.

🔍 "Settings – Android" - "Application" - "Application prohibition" in <Management Site Reference Manual>

🔍 "Settings – Android" - "Device Owner Mode" - "Non-display application" in <Management Site Reference Manual>

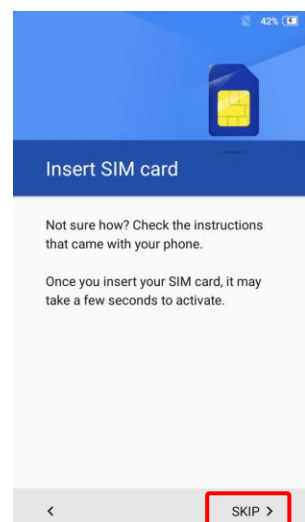
3.3.1 For less than Android 12

[1] Tap [GET STARTED].

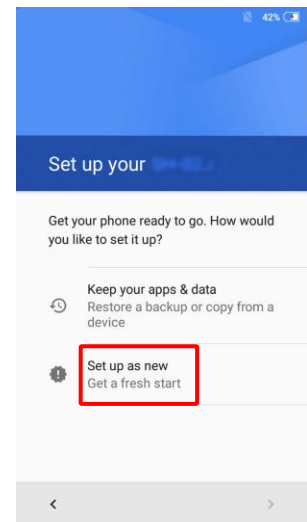


[2] Tap [SKIP].

☑ If a SIM card is already inserted, this screen does not appear.



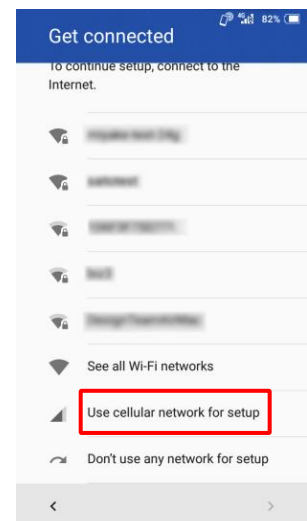
[3] Tap [Set up as new].



[4] Tap [Use cellular network for setup] or tap a Wi-Fi SSID to connect to Wi-Fi.

<<If you do not have a SIM>>

[Use cellular network for setup] will not be displayed, so connect to Wi-Fi.

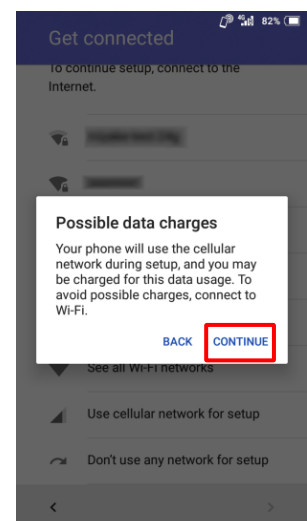


<<If you use a cellular network>>

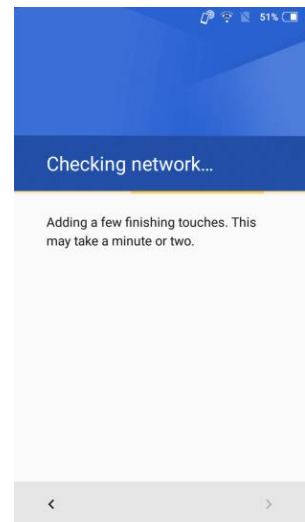
When a pop-up appears as shown on the screen on the right, tap [CONTINUE].

<<If you use a Wi-Fi connection>>

Continue with the next step.

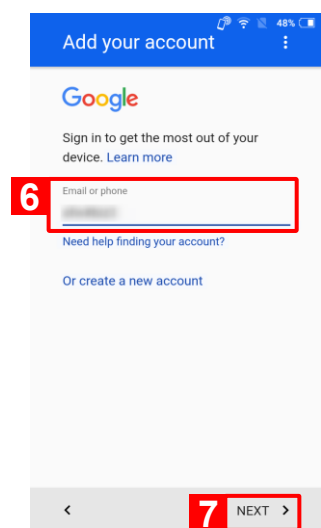


[5] Network connection starts.

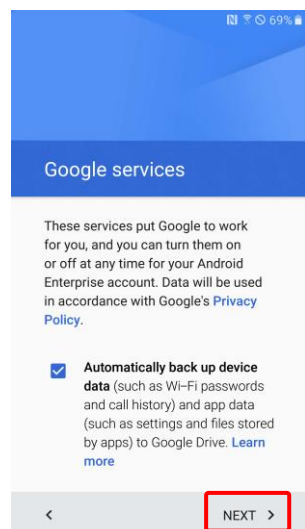


[6] Enter "afw#biz3" in "Email or phone".

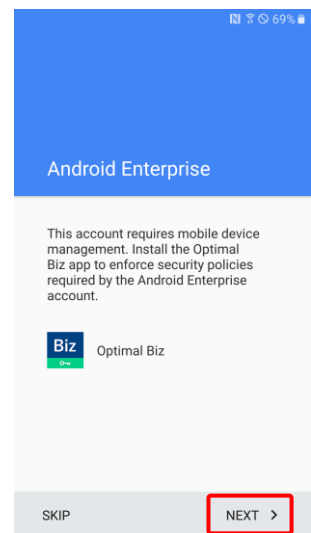
[7] Tap [NEXT].



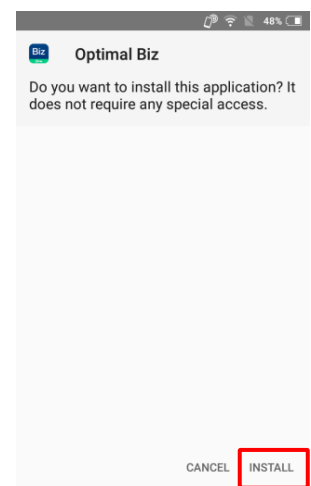
[8] Tap [NEXT].





[9] Tap [NEXT].

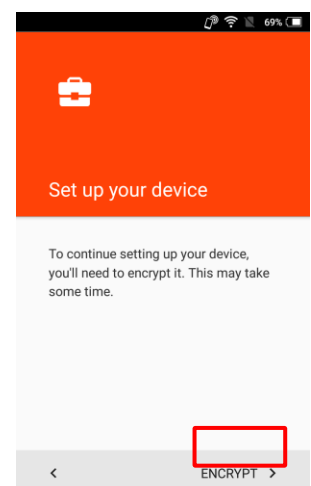


[10] Tap [INSTALL].

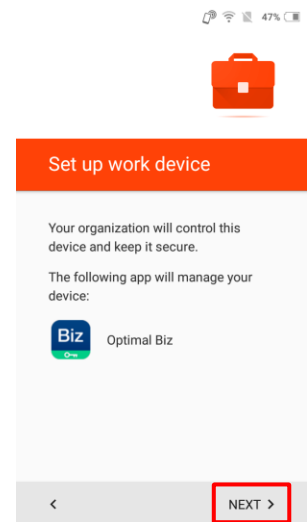


[11] Tap [ENCRYPT].

-  Without encryption, kitting may not be performed properly for the agent in some devices. Some devices do not display this screen.
-  Follow the on-screen instructions to perform encryption. Once encryption is complete, the device will reboot. On the network connection screen that appears after the reboot, select a network you want to use.

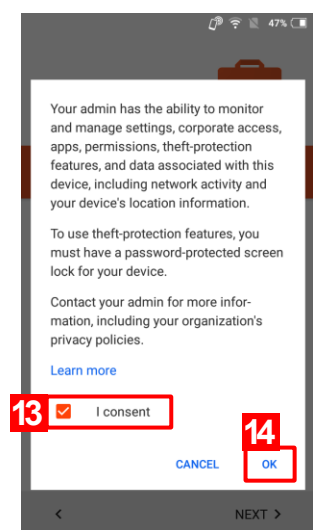


[12] Tap [NEXT].



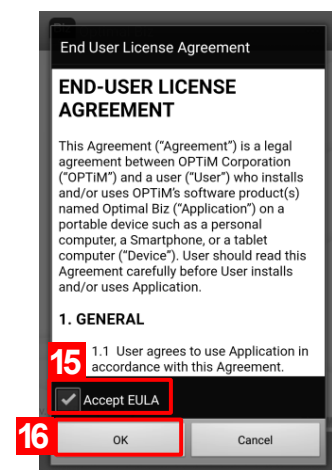
[13] Check "I consent".

[14] Tap [OK].



[15] Check "Accept EULA".

[16] Tap [OK].



[17] Read the user data policy, and tap [Privacy Policy].

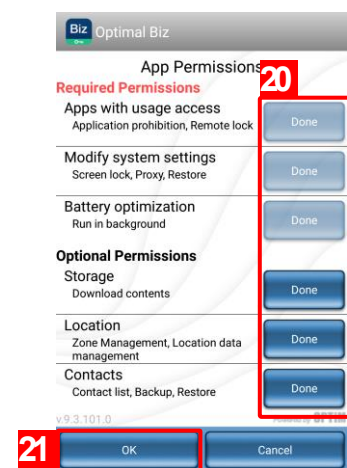
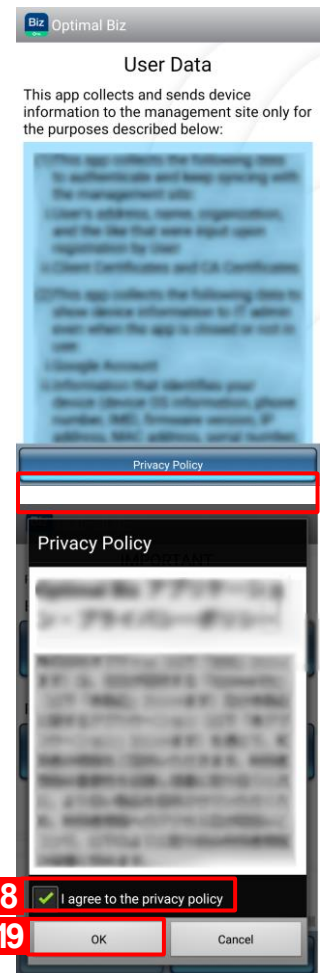
[18] Check "I agree to the privacy policy".

[19] Tap [OK].

[20] A screen that requests permission appears. Follow the on-screen instructions to set things up.

[21] Tap [OK].

⇒ The license authentication screen appears. Continue with the license authentication.

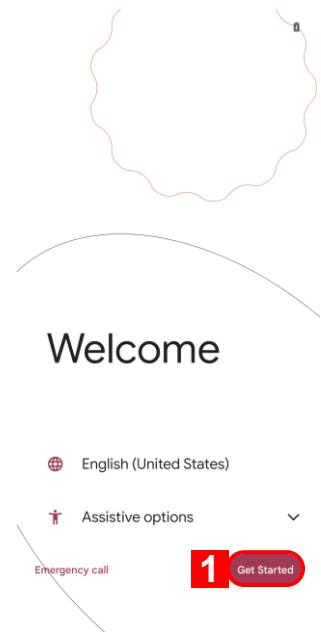
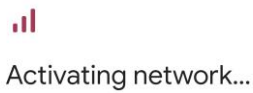


3.3.2 For Android 12 or later

[1] Tap [Get Started].

« If you are inserting SIM »

The following screen is displayed.



[2] Tap [Skip].



[3] Tap a Wi-Fi SSID to connect to Wi-Fi.

Android 12 or later cannot be kitted using mobile network. Be sure to connect to Wi-Fi.

⇒ Network connection starts.

**Connect to Wi-Fi**

Select a network



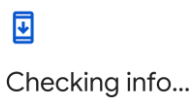
+ See all Wi-Fi networks

Use mobile network for setup

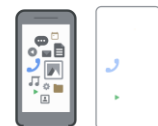
Set up offline

[4] Tap [Don't copy].

⇒ Checking information.

**Copy apps & data**

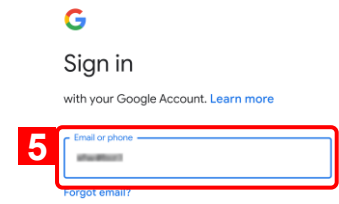
You can choose to transfer your apps, photos, contacts, Google Account, and more.



Next

[5] Enter "afw#biz3" in "Email or phone".

[6] Tap [Next].

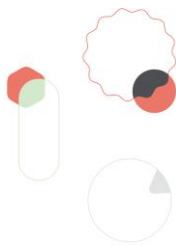


[7] Tap [Next].

⇒ Getting ready for work setup.



Getting ready for
work setup...



Create account

Skip

6 Next

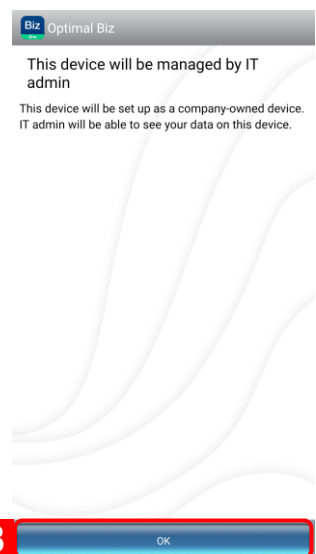


Your account is
managed

Your IT admin uses mobile device
management to enforce security policies

7 Next

[8] Tap [OK].



[9] Tap [Accept & Conetinue].

⇒ Setting up in the device.



Keep your work apps
at your fingertips



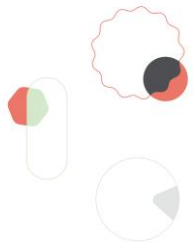
Setting up your device...

[10] Tap [Next].

⇒ Getting account information.



Getting account
info...

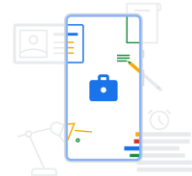
**[11] Tap [More].**

✎[More] is displayed several times on some devices. Tap [More]
until [Accept] is displayed.



Let's set up your
work device

[View terms](#)



9 Accept & continue



This device isn't
private

🔒 Your activity & data

Your IT admin may be able to see your data and activity on this device.

📄 App permissions

Your IT admin can set permissions for apps on this device, such as microphone, camera, and location permissions.

Cancel setup

10 Next



Google Services

Tap to learn more about each service, such as how to turn it on or off later. Data will be used according to Google's [Privacy Policy](#).

Location

📍 Use location ▾

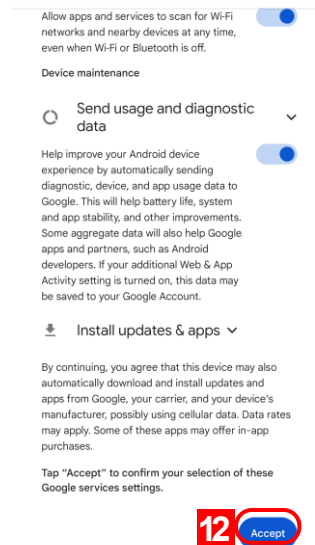
Allow apps and services with location permission to use your device's location. Google may collect location data periodically and use this data in an anonymous way to improve location accuracy and location-based services.

📍 Allow scanning ▾

Allow apps and services to scan for Wi-Fi

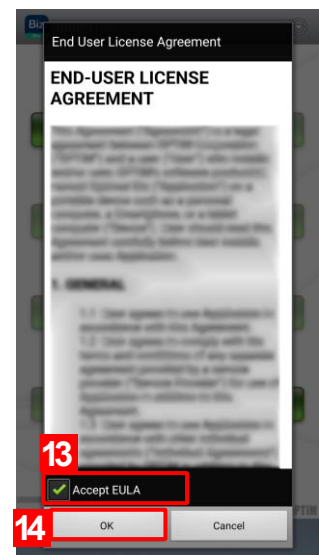
11 More

【12】 Tap [Accept].

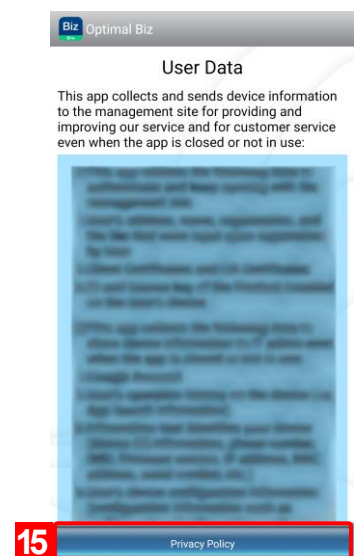


[13] Check "Accept EULA".

【14】 Tap [OK].

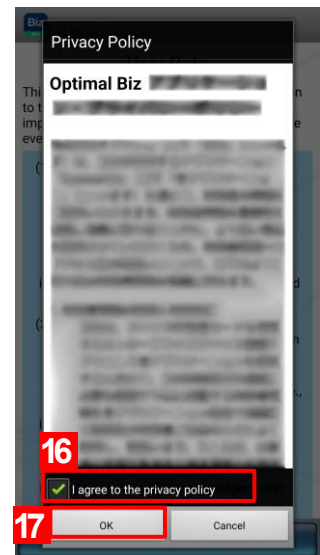


[15] Read the user data policy, and tap [Privacy Policy].

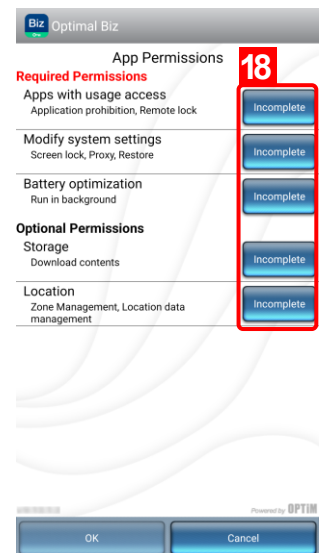


[16] Check "I agree to the privacy policy".

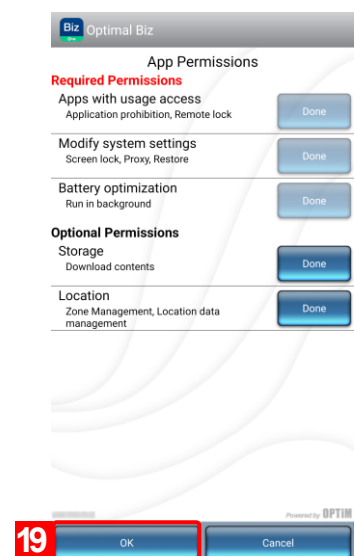
[17] Tap [OK].



[18] A screen that requests permission appears. Follow the on-screen instructions to set things up.



[19] Tap [OK].



[20] Enter a "company code" and "authentication code".

- ✎ Contact your administrator for your company code and authentication code.
- ✎ If you tap [Scan QR Code to fill out the Authentication information] (A) and scan a QR code for agent license activation, the "Company code", "Authentication code", and "URL" will be automatically entered. Contact your administrator for the QR code.

[21] Tap [Send].**[22] The license authentication completion screen appears. Tap [OK].**

« When portal settings are set to be displayed on Management Site »

After you tap [OK], initial registration screen appears.
Enter items as necessary.

- ✎ The user will link to the device if the initial registration has been made.
- ✎ If you do not need to register, you can either tap [Close] (A) or (B) the back button on the device to close the screen.
- ✎ If the user is already linked to the device, a message will appear and say that the user has been linked. Close the screen.

Biz Optimal Biz

Initial Registration (A) Close

ユーザー登録画面

User Registration

Employee Number

Last Name

First Name

Next

Optimal Biz ver. 1.0.0

©2011 OPTIM | Terms of Service | Privacy Policy

(B)

Biz Optimal Biz

Activation

20

Company Code

Authentication Code

URL

Authenticate by User ID and Password

(A) Scan QR Code to fill out the Authentication Information

21 Send

Powered by OPTIM

Biz Optimal Biz

The setting is completed.

Company Code: optima_1234567890

Authentication Code: 12345678901234567890

URL: https://www.optimalbiz.com/agent/1234567890

22 OK

Powered by OPTIM

[23] Tap [Skip].

⇒ Kitting is complete.

License authentication is also complete. Proceed to "Allocating a user to your device".

☞ "Allocating a user to your device" Page 38



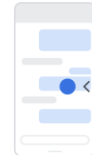
All set!

You're ready to start using your phone



Swipe to navigate
your phone

Learn gestures to go Home, go back, and
switch apps



Skip

Try it

System navigation settings

Swipe up to go Home



3.4 Performing license authentication

After kitting is complete, perform license authentication with your User ID or company code / authentication code.

✍ If you are using Android Enterprise, after you perform license authentication with the user ID registered from the management site, it will be integrated with Android Enterprise.

If you have not registered your user ID, the user ID can be integrated with Android Enterprise by performing a license authentication with a company code / authentication code, registering the user ID from the management site, and linking it with your device.

✍ Android 12 or later are license authenticated by kitting, so this operation is not necessary. Proceed to the next operation.

👉 "Allocating a user to your device" Page 38

3.4.1 Authenticating by a user ID

[1] Tap [Authenticate by User ID and Password].

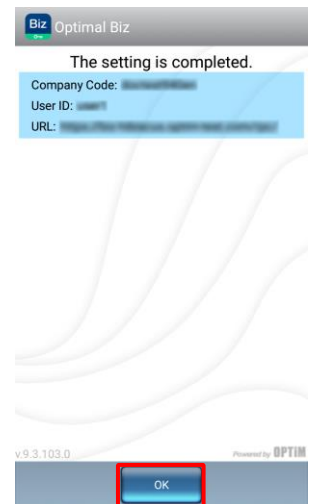
[2] Enter the "Company Code", "User ID or E-mail Address", and "Password".

✍ Contact your administrator for your company code, user ID, and password.

✍ You do not have to change the URL (A).

[3] Tap [Send].

- [4]** The license authentication completion screen appears. Tap [OK].



- [5]** The agent menu screen appears.

- ✓ After license authentication, users cannot interact with the agent screen until the initial synchronization is complete at the management site.



3.4.2 Authenticating by a company code / authentication code

✍ After license authentication is complete, allocate a user to the device on the management site.

🔍 "Asset" - "List" - "Asset management information" in <Management Site Reference Manual>

[1] Enter a "company code" and "authentication code".

✍ Contact your administrator for your company code and authentication code.

📄 If you tap [Scan QR Code to fill out the Authentication information] (A) and scan a QR code for agent license activation, the "Company code", "Authentication code", and "URL" will be automatically entered. Contact your administrator for the QR code.

[2] Tap [Send].

Optimal Biz
Activation
1 Company Code
Authentication Code
URL
E-mail Address
[Authenticate by User ID and Password](#)
(A) [Scan QR Code to fill out the Authentication Information](#)
v9.3.101.0
2 Send

[3] The license authentication completion screen appears. Tap [OK].

« When portal settings are set to be displayed on Management Site »

After you tap [OK], initial registration screen appears.
Enter items as necessary.

✍ The user will link to the device if the initial registration has been made.

✍ If you do not need to register, you can either tap [Close] (A) or (B) the back button on the device to close the screen.

✍ If the user is already linked to the device, a message will appear and say that the user has been linked. Close the screen.

Optimal Biz
The setting is completed.
Company Code:
User ID:
URL:
v9.3.103.0
OK

Optimal Biz
Initial Registration (A) Close
User Registration
Employee Number
Last Name
First Name
Next
Optimal Biz ver. 9.3.103.0
©2011 OPTIM | [Terms of Service](#) | [Privacy Policy](#)
(B)

[4] The agent menu screen appears.

- ✓ After license authentication, users cannot interact with the agent screen until the initial synchronization is complete at the management site.



3.5 Allocating a user to your device

Follow the steps below to allocate a user created in "Creating a user " to a device.

- [1] Go to [Assets]→[List], and select a target device from the list.**
- [2] Click [Edit admin information].**

The screenshot displays the 'Optimal Biz' web application interface. The top navigation bar includes 'Assets', 'User', 'Organization', 'Settings', 'Log', and 'Related Service'. The left sidebar contains a 'List' menu with options like 'Network Map', 'Authentication Procedure', and 'Download CSV'. The main content area is titled 'Assets' and features a search bar and a table of 14 devices. A red box labeled '1' highlights a row in the table. The right sidebar contains a form for 'Edit admin information' with fields for OS, Phone Number, User, Organization, and Note. A red box labeled '2' highlights the 'Edit admin information' button. Below the form are sections for 'Settings' (Setting Allocation, Setting Template Allocation) and 'Actions' (Change screen lock password, Remote Lock). The footer includes copyright information for ©2011 OPTIM.

Asset Name	OS	Phone Number	User	Organization	Communication Date	Details
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	about 2 years ago	[Details]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	27 days ago	[Details]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	19 days ago	[Details]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	about 4 years ago	[Details]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	about 1 month ago	[Details]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	about 1 hour ago	[Details]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	for over 2 years ago	[Details]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	almost 2 years ago	[Details]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	almost 2 years ago	[Details]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	about 1 year ago	[Details]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	for over a year ago	[Details]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	about 2 years ago	[Details]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	about 1 year ago	[Details]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	almost 2 years ago	[Details]

- [3]** Select "User" in "Division" and specify the user selected in "Creating a user" from the pull-down menu.
- [4]** Click [Save].

The screenshot shows the Optimal Biz interface. On the left is a sidebar with navigation options like 'List', 'Network Map', 'Authentication Procedure', etc. The main area is titled 'Assets' and contains a table with 14 devices. The table columns are: Asset Name, OS, Phone Number, User, Organization, Communication Date, and Details. A red box labeled '3' points to the 'Division' dropdown in the 'Management Information' panel on the right, which is currently set to 'User'. Another red box labeled '4' points to the 'Save' button in the same panel.

- [5]** Click [Sync].
- [6]** Click [OK].

⇒ The user will be allocated to the device.

This screenshot shows the same interface as the previous one, but with a modal dialog box open. The dialog box contains the text: 'Sync will start. Depending on device, it may take significant amount of time until the setting is applied. Click on [OK] button to proceed.' A red box labeled '6' highlights the 'OK' button in the dialog. Another red box labeled '5' highlights the 'Sync' button in the 'Management Information' panel on the right. The 'Sync' button is highlighted with a green border.

4 Integrating with Android Enterprise by a Google Workspace (formerly G Suite) account

To use Android Enterprise, perform integration setting between this product and Google by using a Google Workspace (formerly G Suite) account before performing kitting for the device. If you register your Google Workspace (formerly G Suite) account for integration setting, perform the setting on the Google Admin console and issue a token.

This chapter describes the following items.

Item	Page
Issuing a token *	41
Registering a Google Workspace (formerly G Suite) account *	48
Creating a user	50
Kitting by a Google Workspace (formerly G Suite) account	54
Performing license authentication	69



Attention

- You must have a Google Workspace (formerly G Suite) account for which the Android Enterprise integration setting has not been performed.
- If you have registered a Google Workspace (formerly G Suite) account for integration setting with Google, you may not be able to perform a forced (silent) installation. In that case, you must agree to the managed Google Play Store's terms of use. Log in to Google as a G Suite administrator from the following URL and accept the terms.

 <https://play.google.com/work/termsofservice>

For details of forced installation, refer to the following manual.



"App Distribution by <Android Enterprise Manual> " - "Application Distribution" - "If only specified apps can be installed" in Android Enterprise



"Using the managed Google Play store " - " Forced (silent) installation of apps" in <Android Enterprise Manual>

- The items marked with * above are required only for the first kitting.



Reference

- By setting up the "Application Distribution" function of Android Enterprise on the management site in advance, apps can be distributed to your device at the same time as license authentication after kitting is complete. For details of app distribution, refer to the following.




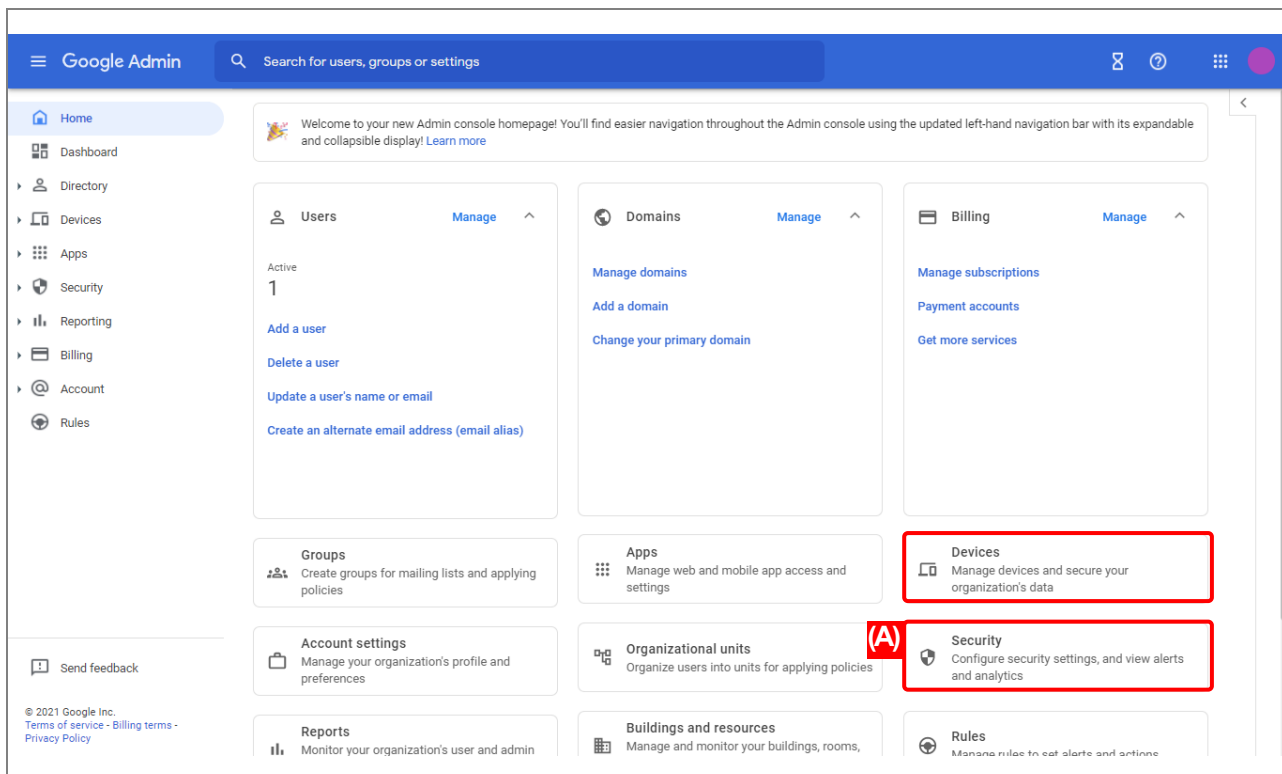
"Android Enterprise App distribution" in <Android Enterprise Manual>

4.1 Issuing a token

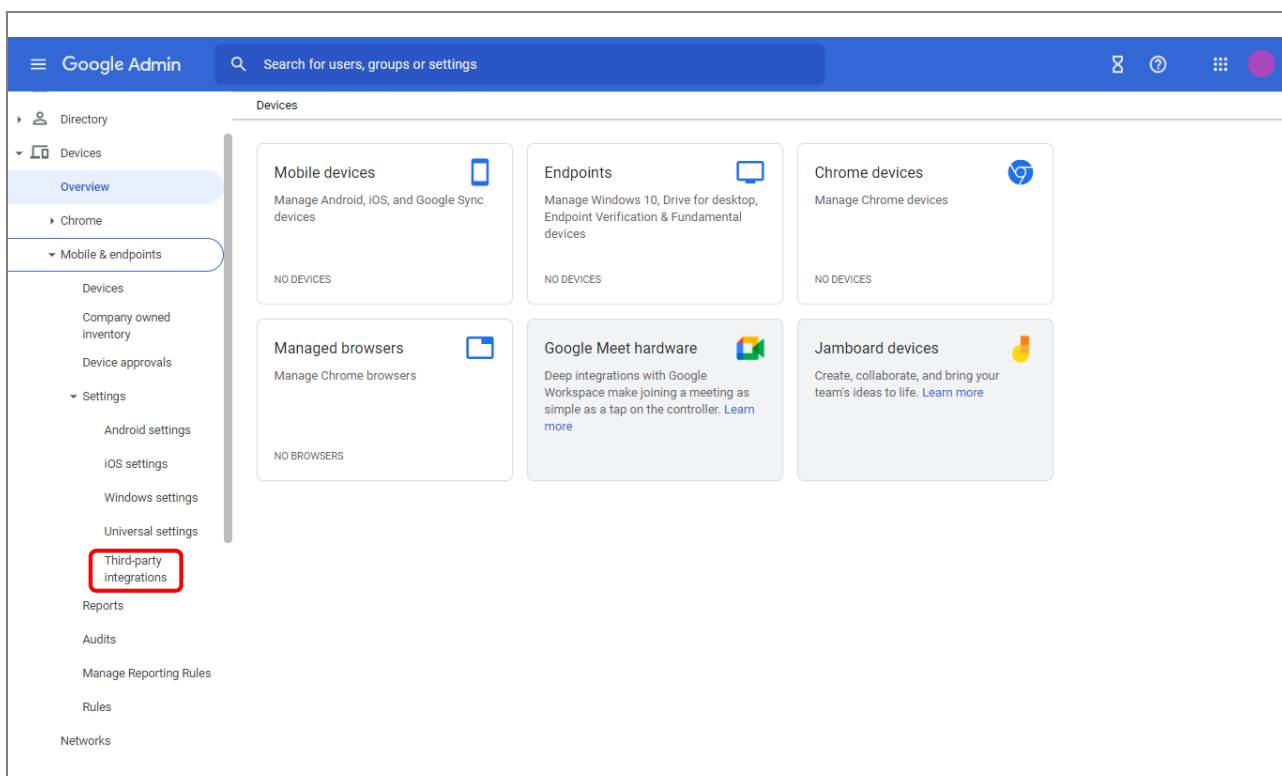
Follow the steps below to integrate this product with Google by using a Google Workspace (formerly G Suite) account.

[1] Go to the Google Admin console (<https://admin.google.com>) and click [Devices].

 (A) If [Security] shows "EMM provider management for Android", steps [6] to [12] are not required.



[2] Click [Settings]→[Third-party integrations].



[3] Uncheck "Enable third-party Android mobile management" in "Android EMM".

[4] Click [Save].

Android EMM
Applied at 'gdoctest001.optim-test.xyz'

Third-party Android mobile management

When you add a third-party EMM provider, you can't manage Android apps through Google endpoint management. You must manage them through the EMM provider. [Learn more](#)

3 ☐ Enable third-party Android mobile management

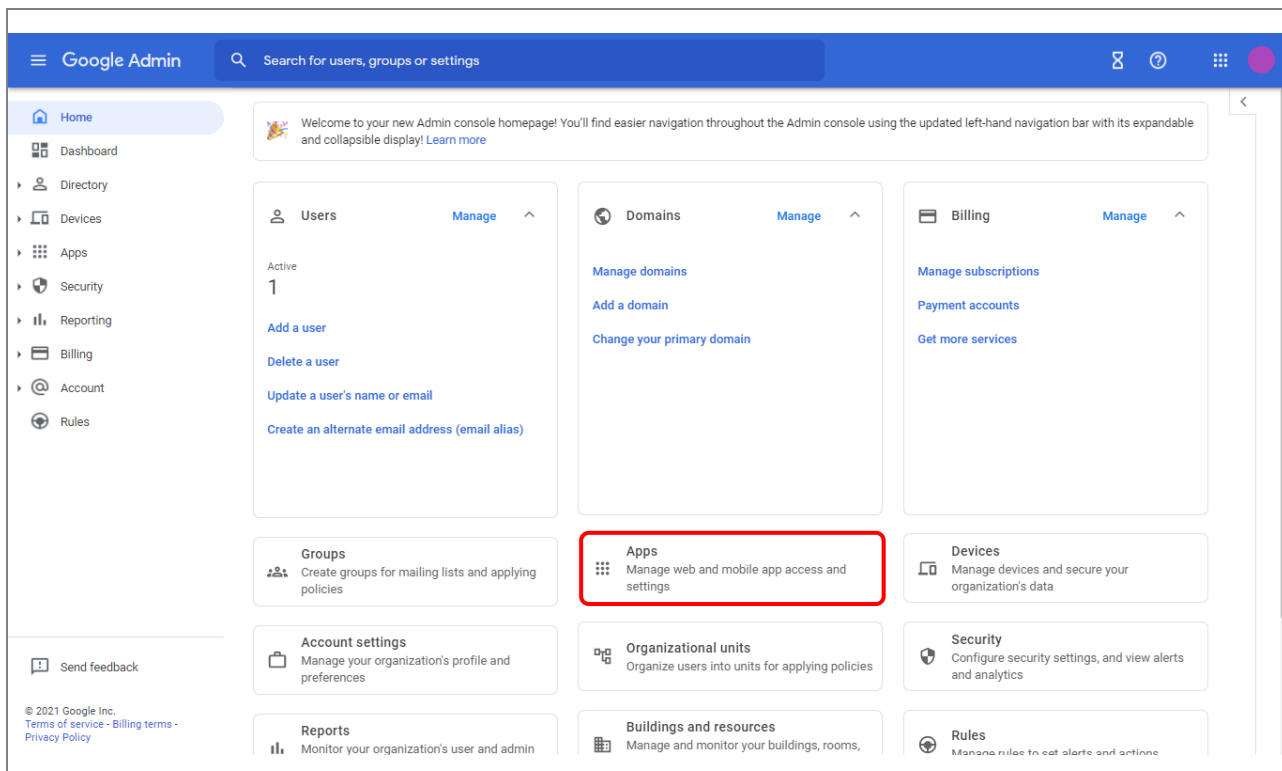
No EMM added [Add EMM provider](#)

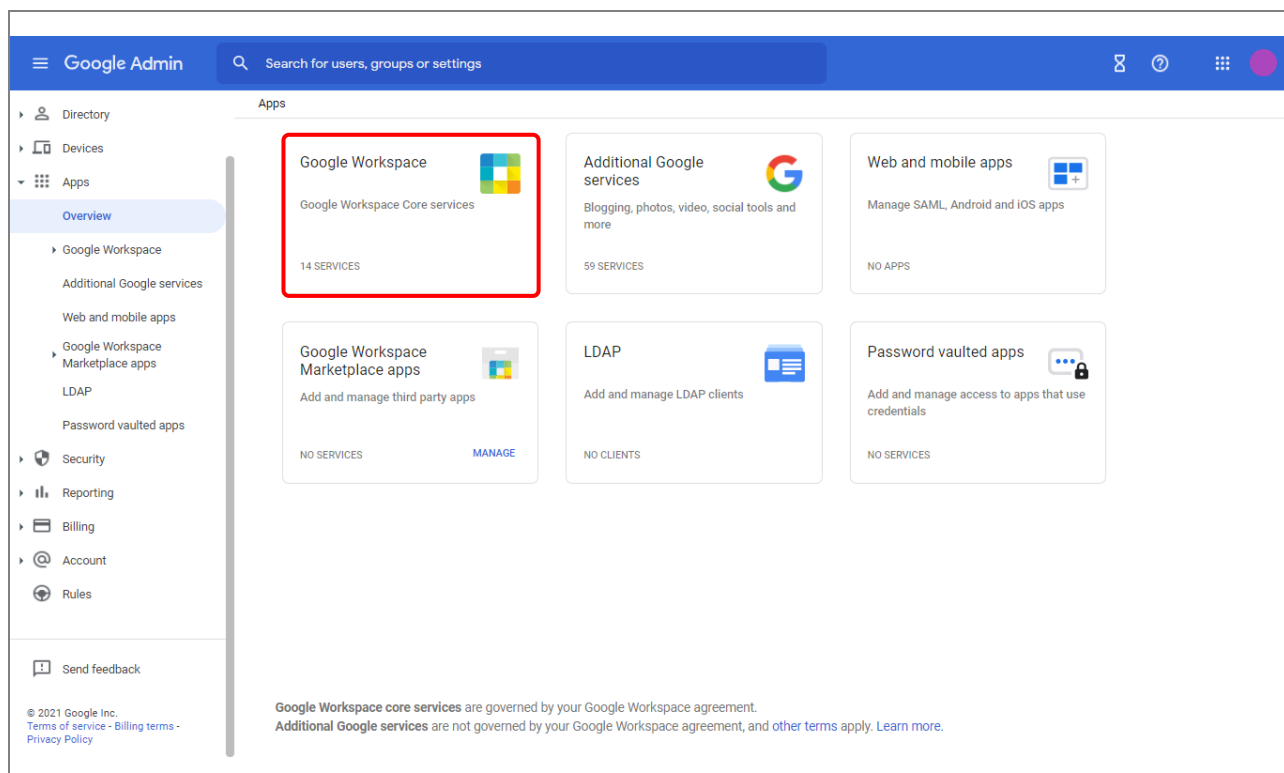
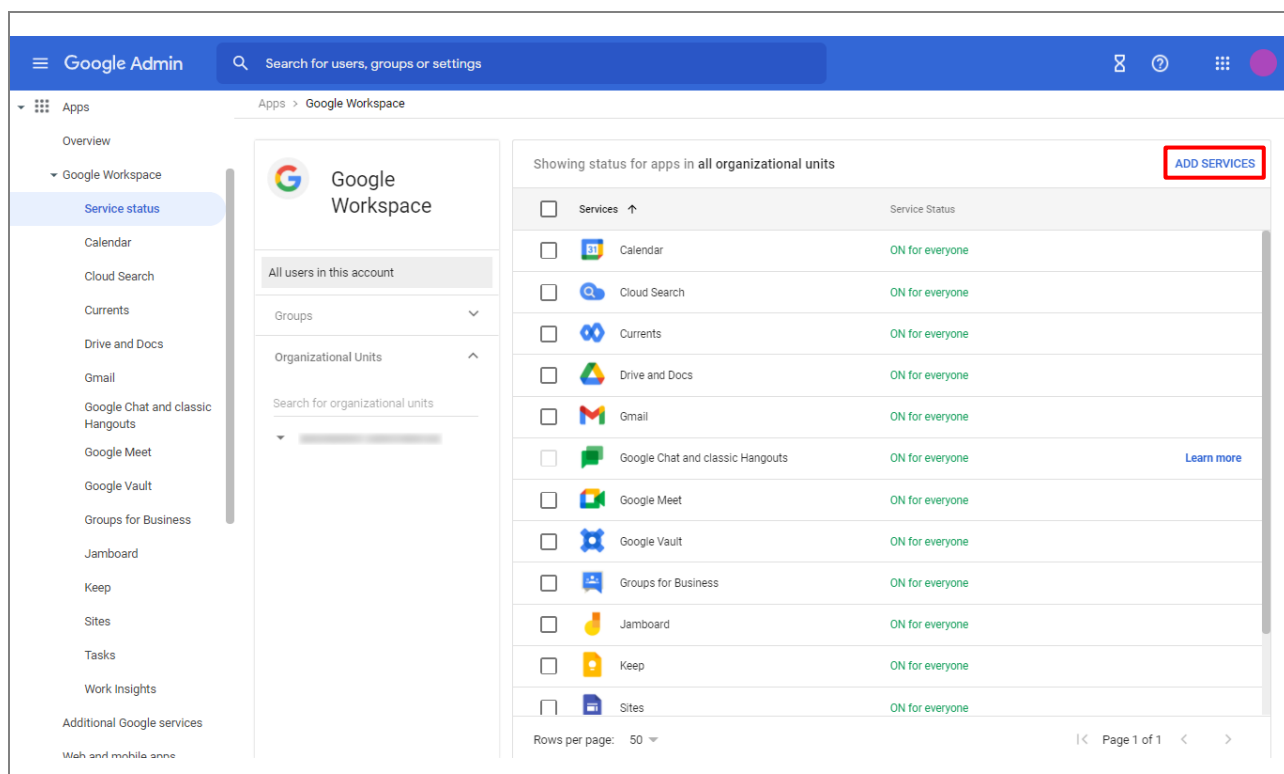
4 **SAVE**

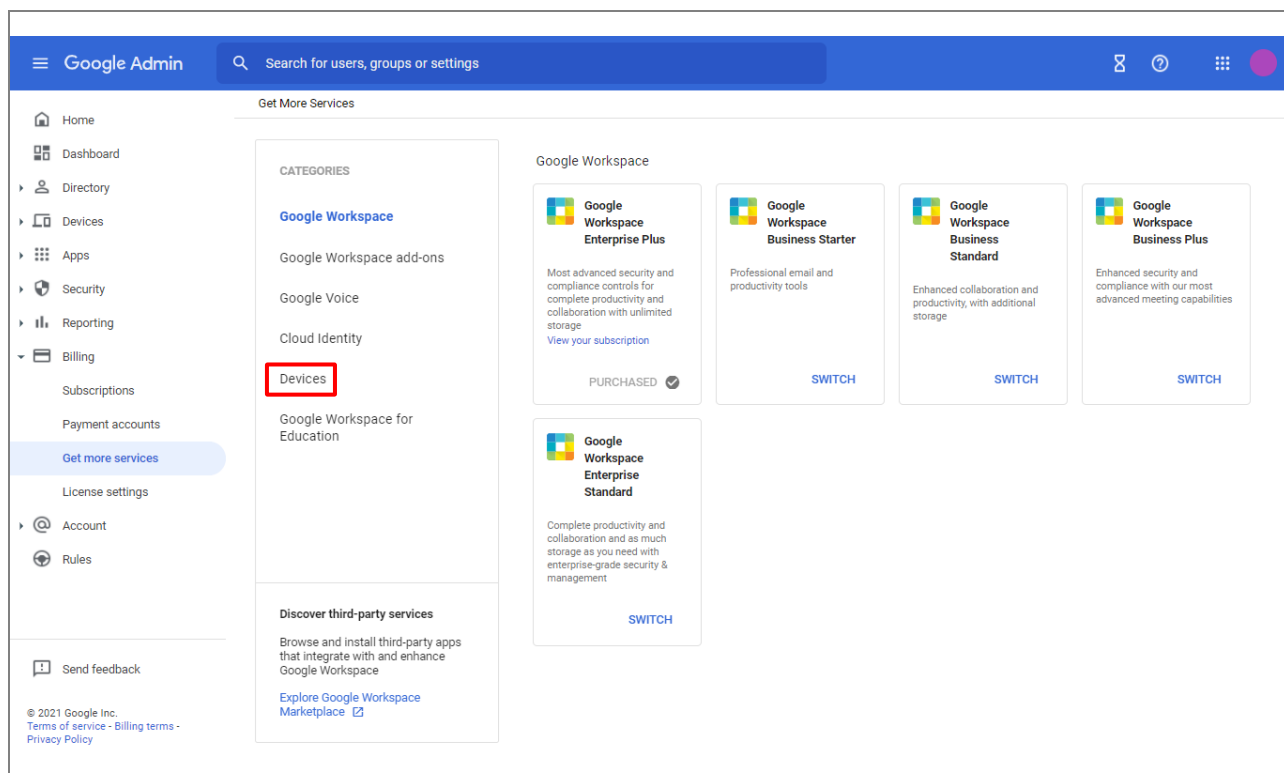
CANCEL

[5] Click [Apps].

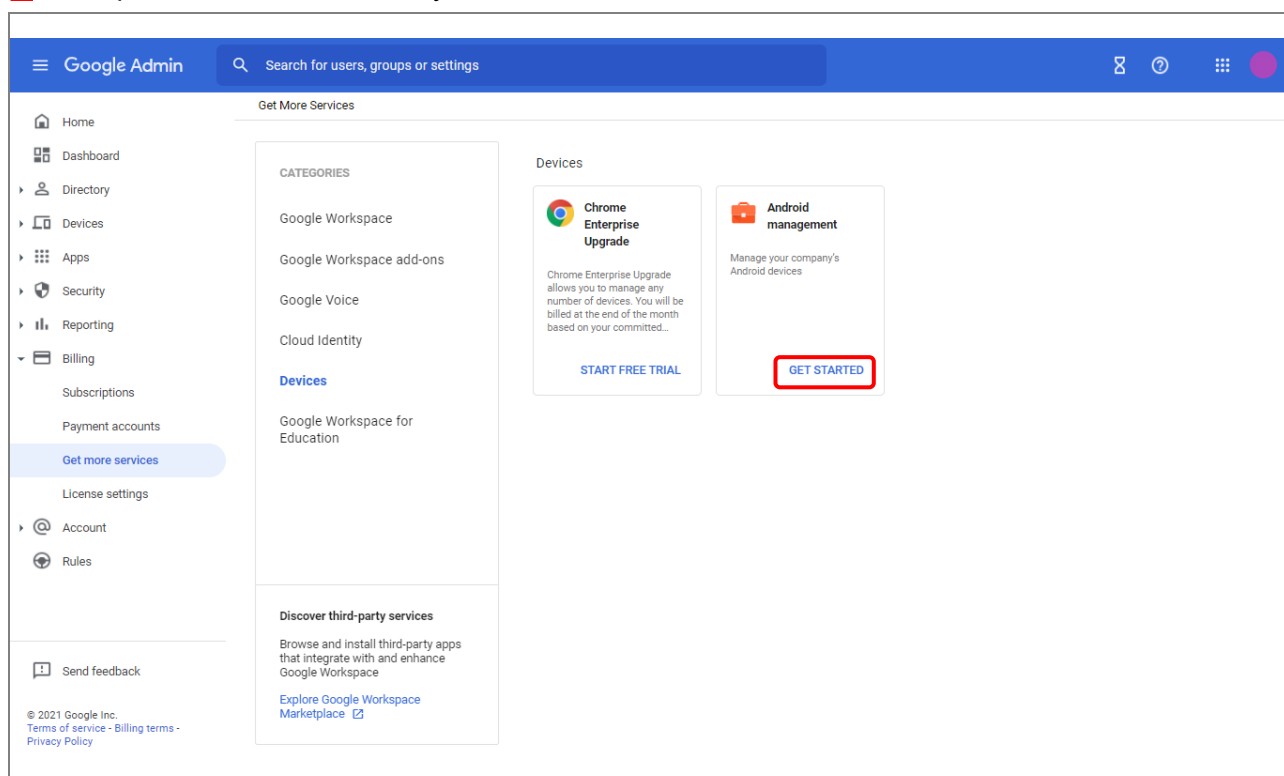
To display the Admin console, click [Google Admin] in the upper left corner of the screen.



[6] Click [Google Workspace].**[7] Click [ADD SERVICES].**

[8] Click [Devices].**[9] Click [GET STARTED] in "Android management".**

✂ This operation will not cause any costs to be incurred.



【10】 Click [CHECKOUT].

× Add a new subscription ?

1 Payment plan — 2 Checkout

Android management
Manage your company's Android devices

Country: Japan Currency: JPY

Review your payment plan

Free plan

- Free edition, no payment needed

Any applicable taxes and discounts will be applied on your monthly invoice. Prices exclude applicable taxes and VAT (varies based on your country). [Learn more](#)

By clicking **Checkout**, you agree to the [Managed Google Play](#) and [Cloud Identity](#) agreement. Notwithstanding anything to the contrary, any previous purchase of any Services will also be subject to the above terms and these terms will supersede any previous terms agreed to upon by the Customer and Google for any Services.

CHECKOUT

【11】 Click [PLACE ORDER].

⇒ The Admin console will appear.

× Add a new subscription ?

✓ Payment plan — 2 Checkout

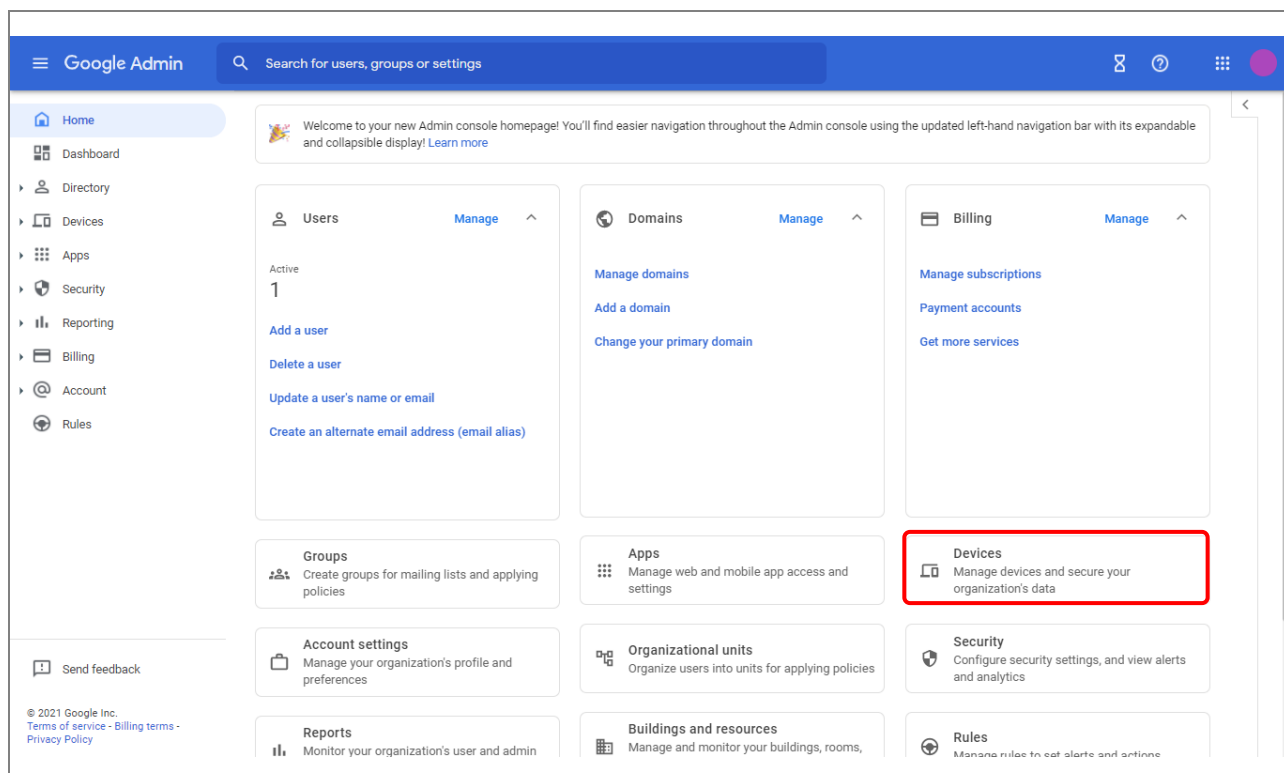
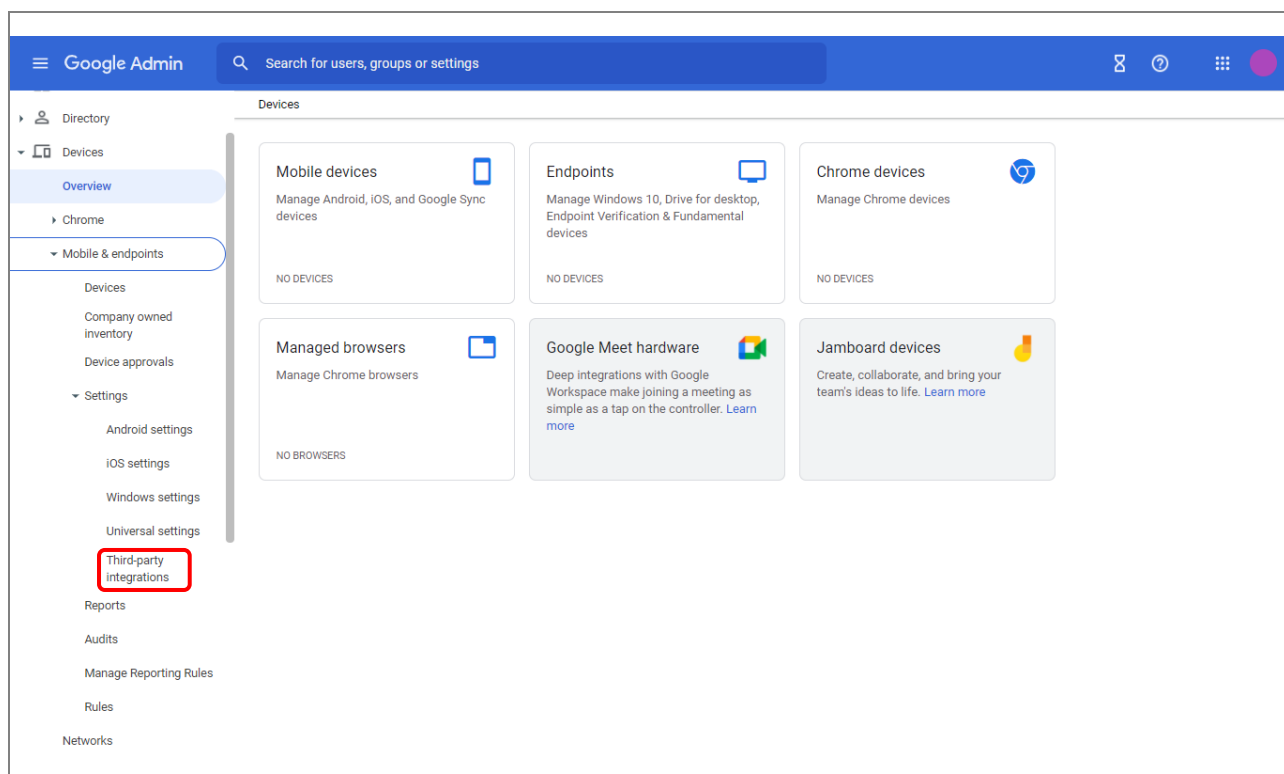
Checkout

Android management
Free plan

Free

BACK

PLACE ORDER

[12] Click [Devices].**[13] Click [Settings]→[Third-party integrations].**

[14] Click [Add EMM provider] on [Android EMM].

The screenshot shows the 'Android EMM' configuration page. On the left, it says 'Android EMM' and 'Applied at 'gdoctest001.optim-test.xyz''. The main heading is 'Third-party Android mobile management'. Below this is an information box with an 'i' icon: 'When you add a third-party EMM provider, you can't manage Android apps through Google endpoint management. You must manage them through the EMM provider. [Learn more](#)'. Below the info box is a checkbox labeled 'Enable third-party Android mobile management', which is currently unchecked. At the bottom left, it says 'No EMM added'. To its right is a red-bordered button labeled 'Add EMM provider'. At the bottom right of the page are 'CANCEL' and 'SAVE' buttons.

[15] Click [GENERATE TOKEN].

The screenshot shows the 'Token generator' page. It has the heading 'Token generator' and a sub-heading 'To bind an EMM provider, generate a token. In another window, open the EMM provider's site and use the token to bind the EMM provider with the Google Admin console.' Below this text is a red-bordered button labeled 'GENERATE TOKEN' next to a greyed-out button.

[16] A token will appear. Make a note of it because as you will need it to register your account.

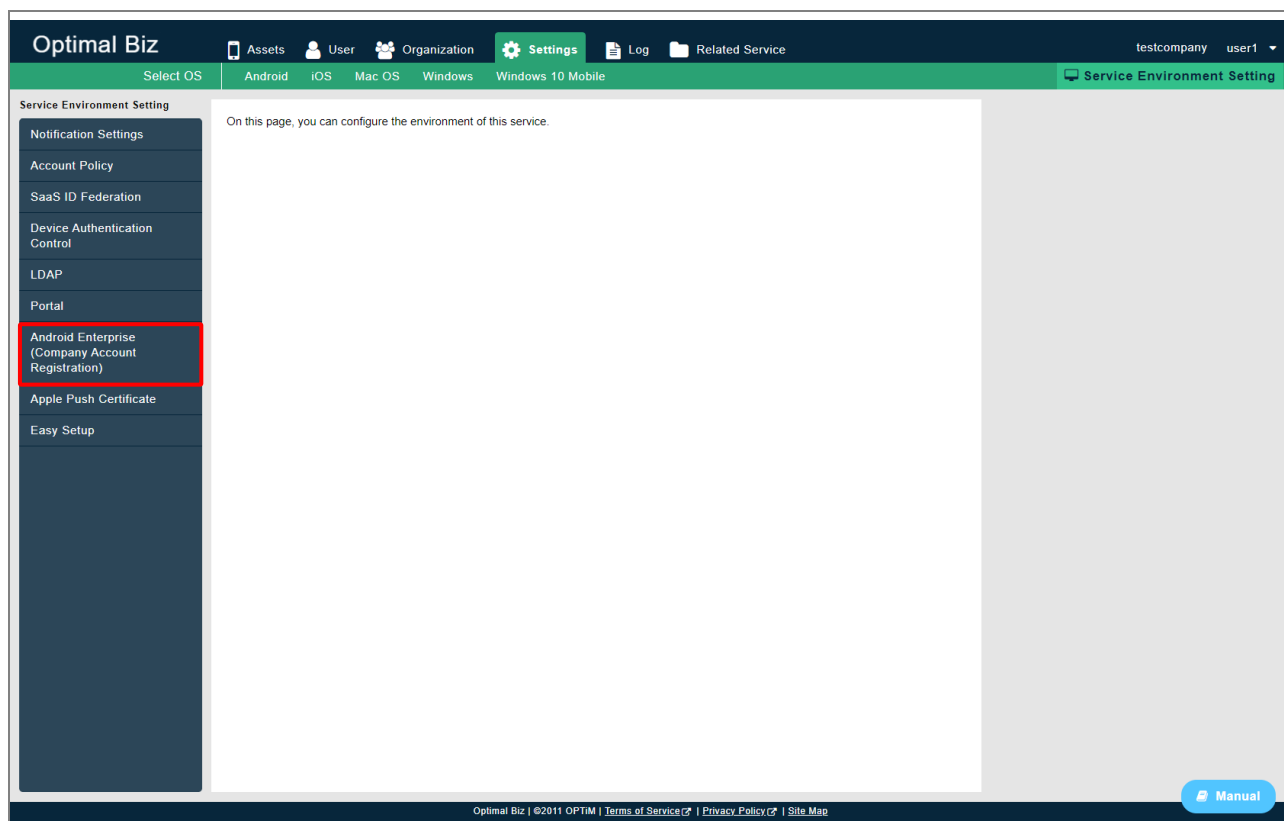
The screenshot shows the 'Token generator' page after the token has been generated. It has the heading 'Token generator' and the same sub-heading as before. Below the text, there is a 'GENERATE TOKEN' button, a red-bordered box containing a long alphanumeric token string, and a 'COPY' button. Below the token box, it says 'This token expires after 30 days or when it's used to bind a provider'.

4.2 Registering a Google Workspace (formerly G Suite) account

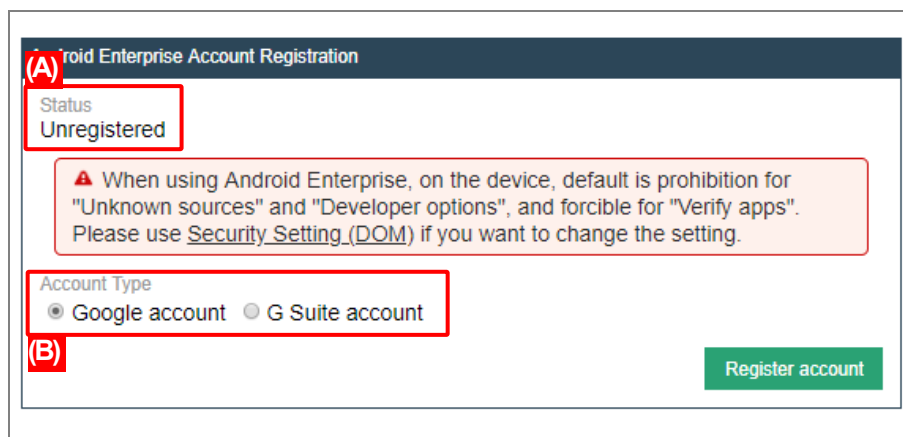
Follow the steps below to register a Google Workspace (formerly G Suite) account to the management site.

- ✍ Once you have registered your Google Workspace (formerly G Suite) account, do not change any settings on the Google side.
- ✍ If you used "Mobile management", a standard feature of Google Workspace (formerly G Suite), delete the "Devices" information of the mobile management feature.

[1] Click [Settings]→[Service Environment Setting]→[Android Enterprise(Company Account Registration)].



[2] The "Status" (A) shows "Unregistered". "Google account" is selected in "Account Type" (B) by default.



[3] Select "G Suite account".

[4] Go to <https://play.google.com/work/termsofservice> and accept the terms of use.

[5] Enter "Domain" and "EMM Token".

For "Domain", enter the domain of your Google Workspace (formerly G Suite) account. If your Google Workspace (formerly G Suite) account is "XXXXX@xxxxx.co.jp", your domain is "xxxxx.co.jp".

[6] Click [Register account].

The screenshot shows the 'Android Enterprise Account Registration' page. The status is 'Unregistered'. A warning message states: 'When using Android Enterprise, on the device, default is prohibition for "Unknown sources" and "Developer options", and forcible for "Verify apps". Please use Security Setting.(DOM) if you want to change the setting.' Under 'Account Type', 'G Suite account' is selected. Another warning message says: 'If you use G Suite account coordination, please login to G Suite with a super administrator account, access the following URL and agree to the terms.' Below this, the URL <https://play.google.com/work/termsofservice> is provided. There are input fields for 'Domain' and 'EMM Token'. A 'Register account' button is at the bottom right.

[7] The "Status" (A) shows "Registered".

(B) displays "Domain" and "EMM Token".

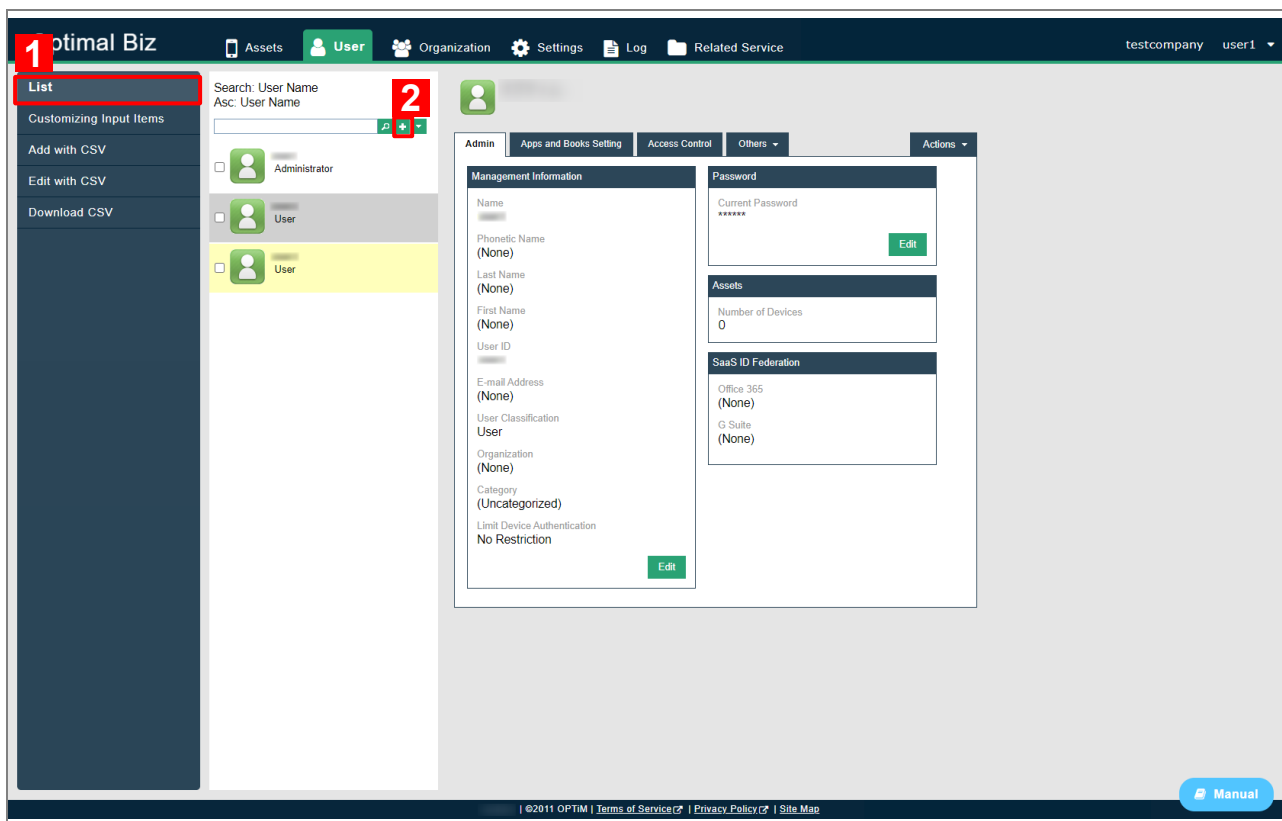
The screenshot shows the 'Android Enterprise Account Registration' page after successful registration. The status is now 'Registered'. The account type remains 'G Suite account'. The same warning messages are present. The 'Domain' and 'EMM Token' fields now contain masked text. A 'Delete account' button is visible at the bottom right.

4.3 Creating a user

Follow the steps below to create a user.

[1] Click [User]→[List].


[2] Click .





The screenshot displays the Optimal Biz user management interface. The top navigation bar includes 'Assets', 'User', 'Organization', 'Settings', 'Log', and 'Related Service'. The 'User' tab is active, and the 'List' view is selected in the left sidebar. A search bar at the top of the list view shows 'Search: User Name' and 'Asc: User Name'. A table lists three users: 'Administrator', 'User', and 'User'. The third 'User' entry is highlighted in yellow. To the right of the table, a user profile form is visible, showing fields for 'Management Information' (Name, Phonetic Name, Last Name, First Name, User ID, E-mail Address, User Classification, Organization, Category, Limit Device Authentication) and 'Password' (Current Password, Edit). The 'Assets' section shows 'Number of Devices' as 0. The 'SaaS ID Federation' section shows 'Office 365' and 'G Suite' as 'None'. The footer includes copyright information and a 'Manual' link.

[5] Enter an arbitrary name in "Name".

[6] Enter your Google Workspace (formerly G Suite) account in "E-mail Address".

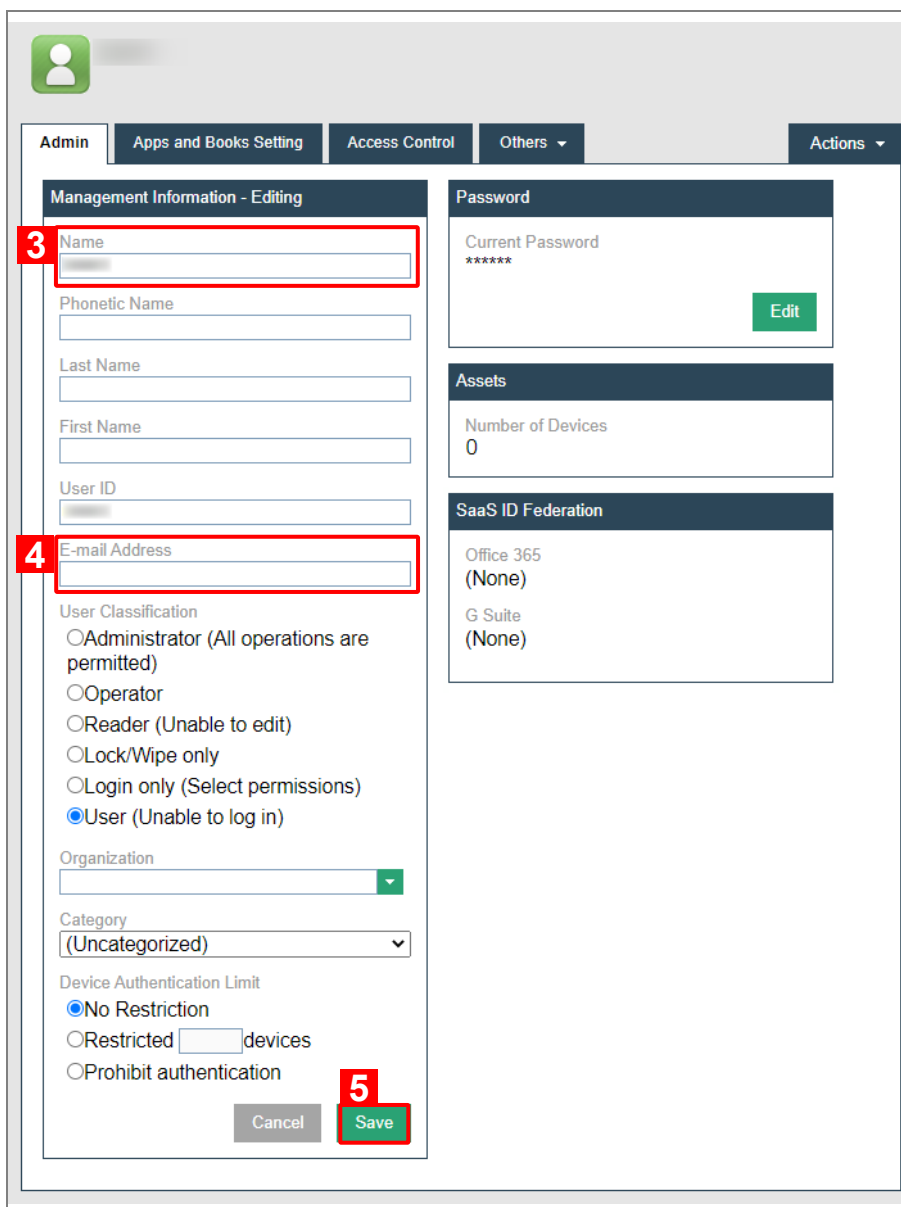
 If you have not registered a Google Workspace (formerly G Suite) account, license authentication during kitting will fail.

 For details of other input and setting items, refer to the following.

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

[7] Click [Save].

⇒ A user will be created.



The screenshot shows the 'Management Information - Editing' form in a web application. The form is divided into several sections:

- Name:** Includes fields for 'Name' (highlighted with a red box and a red '3'), 'Phonetic Name', 'Last Name', 'First Name', and 'User ID'.
- E-mail Address:** A text input field (highlighted with a red box and a red '4').
- User Classification:** A group of radio buttons with the following options:
 - ☐ Administrator (All operations are permitted)
 - ☐ Operator
 - ☐ Reader (Unable to edit)
 - ☐ Lock/Wipe only
 - ☐ Login only (Select permissions)
 - ☒ User (Unable to log in)
- Organization:** A dropdown menu.
- Category:** A dropdown menu showing '(Uncategorized)'.
- Device Authentication Limit:** A group of radio buttons:
 - ☒ No Restriction
 - ☐ Restricted devices
 - ☐ Prohibit authentication

At the bottom right of the form, there are two buttons: 'Cancel' and 'Save' (highlighted with a red box and a red '5').

4.3.1 Registering a Google Workspace (formerly G Suite) account to an existing user

To register a Google Workspace (formerly G Suite) account to an existing user, carry out the steps below.

✍ If you have not registered a Google Workspace (formerly G Suite) account, license authentication during kitting will fail.

[1] Go to [User]→[List], and select a target user from the list.

[2] Click [Edit].

The screenshot displays the Optimal Biz user management interface. The top navigation bar includes 'Assets', 'User', 'Organization', 'Settings', 'Log', and 'Related Service'. The 'User' tab is active, showing a 'List' of users on the left and a detailed 'Edit' form on the right. In the 'List' view, a user is highlighted with a red box and a red '1' next to it. The 'Edit' form on the right contains fields for 'Management Information' (Name, Phonetic Name, Last Name, First Name, User ID, E-mail Address, User Classification, Organization, Category, Limit Device Authentication) and 'Password' (Current Password, Edit). A red '2' and an 'Edit' button are visible at the bottom of the form. The footer includes copyright information and a 'Manual' link.

[3] Enter your Google Workspace (formerly G Suite) account in "E-mail Address".

[4] Click [Save].

⇒ The e-mail address will be registered to the user.

The screenshot displays a user management interface with a top navigation bar containing 'Admin', 'Apps and Books Setting', 'Access Control', 'Others', and 'Actions'. The main content area is divided into two columns. The left column, titled 'Management Information - Editing', contains fields for Name, Phonetic Name, Last Name, First Name, User ID, and E-mail Address. The 'E-mail Address' field is highlighted with a red box and a red '3'. Below these fields are radio buttons for User Classification: Administrator (All operations are permitted), Operator, Reader (Unable to edit), Lock/Wipe only, Login only (Select permissions), and User (Unable to log in). The 'User' option is selected. Below the radio buttons are dropdown menus for Organization and Category (Uncategorized). At the bottom of this column are radio buttons for Device Authentication Limit: No Restriction (selected), Restricted (with a text input field), and Prohibit authentication. The 'Save' button is highlighted with a red box and a red '4'. The right column contains a 'Password' section with a 'Current Password' field and an 'Edit' button. Below this is an 'Assets' section showing 'Number of Devices' as 0. At the bottom is a 'SaaS ID Federation' section with 'Office 365 (None)' and 'G Suite (None)' options.

4.4 Kitting by a Google Workspace (formerly G Suite) account

Follow the steps below to perform kitting for your device by using your Google Workspace (formerly G Suite) account.

Note that the operation is different between Android versions earlier than 12 and versions 12 or later. Depending on the Android version of your device, choose one of the following methods.

● **For less than Android 12**

● **For Android 12 or later**

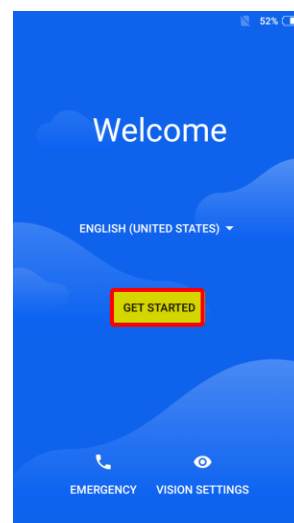
- ✎ When you are kitting Android 12 or later, kitting operation may not be able to complete if you have set Google Play Developer Services (com.google.android.gms) on the management site's "Application prohibition" blacklist and "Non-display application". Refer to the following to clear the setting in advance and then conduct kitting.

🔍 "Settings – Android" - "Application" - "Application prohibition" in <Management Site Reference Manual>

🔍 "Settings – Android" - "Device Owner Mode" - "Non-display application" in <Management Site Reference Manual>

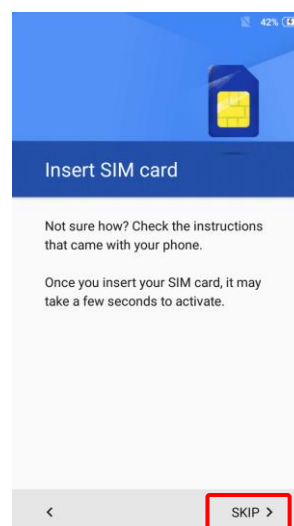
4.4.1 For less than Android 12

[1] Tap [GET STARTED].

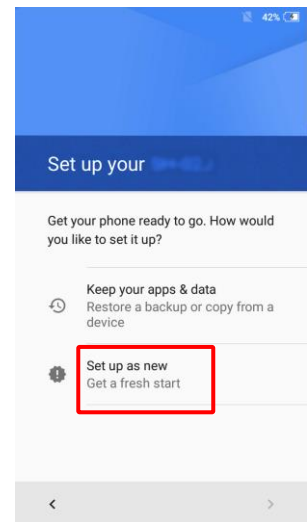


[2] Tap [SKIP].

- ✎ If a SIM card is already inserted, this screen does not appear.



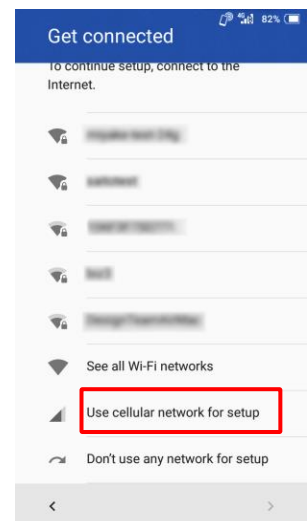
[3] Tap [Set up as new].



[4] Tap [Use cellular network for setup] or tap a Wi-Fi SSID to connect to Wi-Fi.

<<If you do not have a SIM>>

[Use cellular network for setup] will not be displayed, so connect to Wi-Fi.

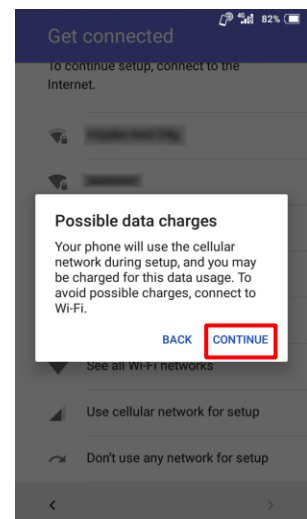


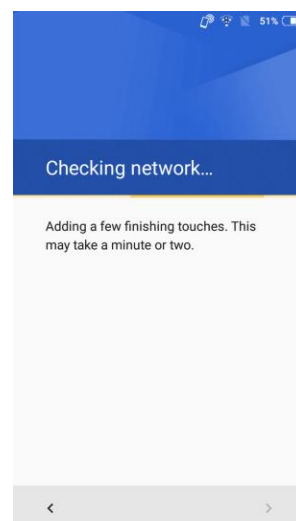
<<If you use a cellular network>>

When a pop-up appears as shown on the screen on the right, tap [Continue].

<<If you use a Wi-Fi connection>>

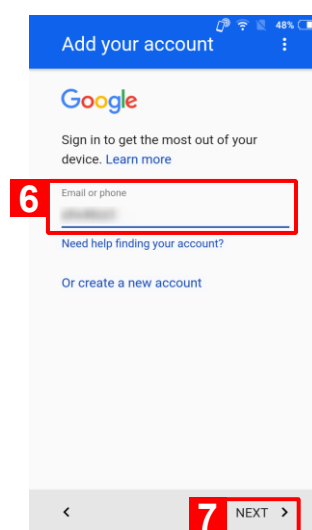
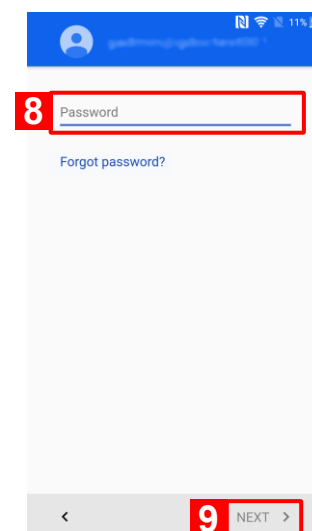
Continue with the next step.

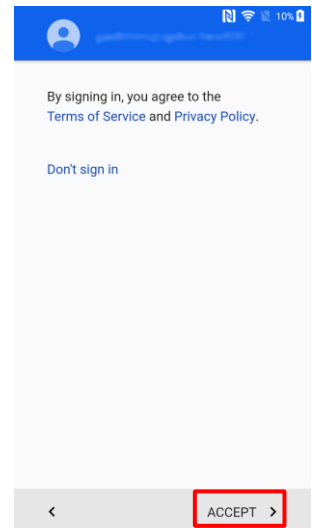


[5] Network connection starts.**[6] Enter your Google Workspace (formerly G Suite) account in "E-mail or phone".**

- ⚠ License authentication will fail if the Google Workspace (formerly G Suite) account has not been registered as a user of the management site.

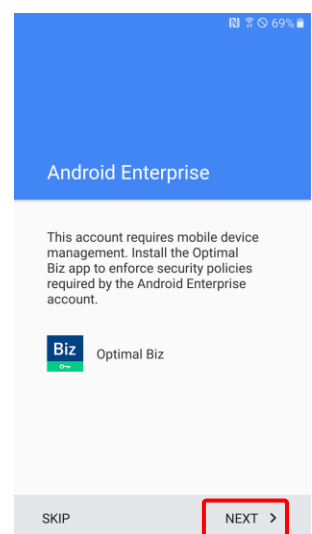
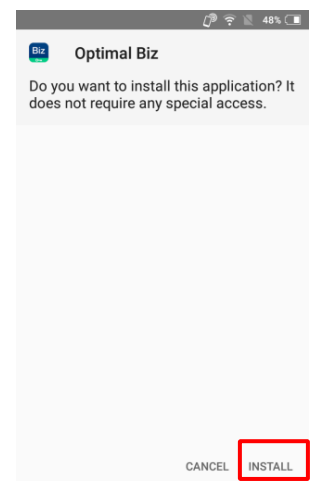
👉 "Registering a Google Workspace (formerly G Suite) account to an existing user" Page 52

[7] Tap [NEXT].**[8] Enter "Password".****[9] Tap [NEXT].**

[10] Tap [ACCEPT].**[11] Tap [Install].**

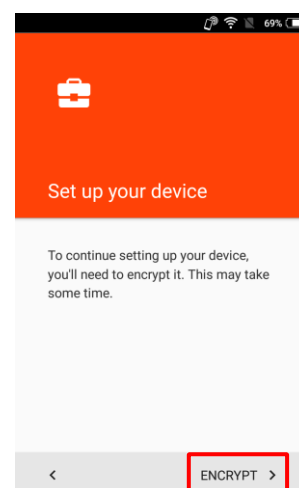
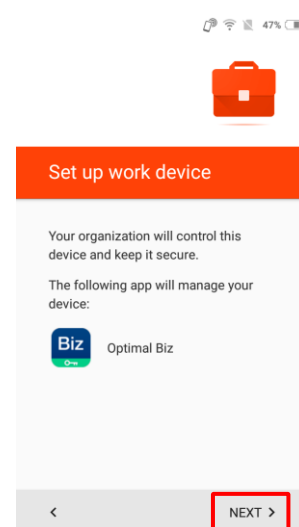
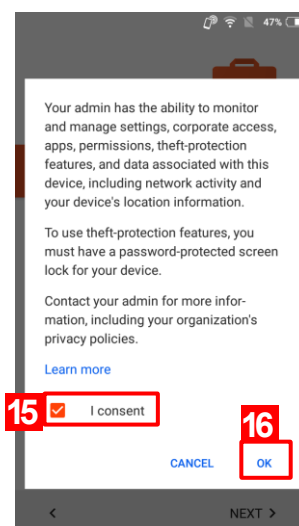
- ✎ If the installation screen does not appear, you may not have successfully registered your Google Workspace (formerly G Suite) account. Check the settings and initialize the device, then try kitting again from the step below.

👉 "Issuing a token" Page 41

**[12] Tap [INSTALL].**

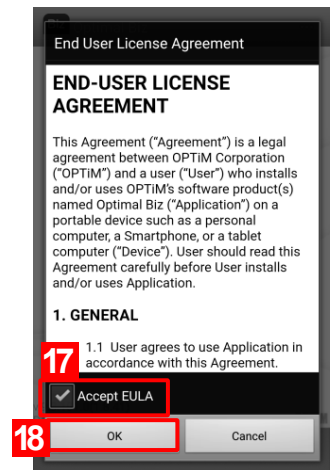
[13] Tap [ENCRYPT].

- ✔ Without encryption, kitting may not be performed properly for the agent in some devices. Some devices do not display this screen.
- ✎ Follow the on-screen instructions to perform encryption. Once encryption is complete, the device will reboot. On the network connection screen that appears after the reboot, select a network you want to use.

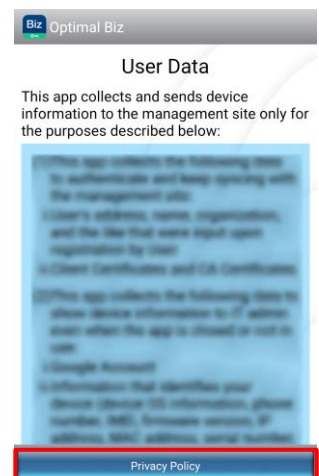
**[14] Tap [NEXT].****[15] Check "I consent".****[16] Tap [OK].**

[17] Check "Accept EULA".

[18] Tap [OK].



[19] Read the user data policy, and tap [Privacy Policy].



[20] Check "I agree to the privacy policy".

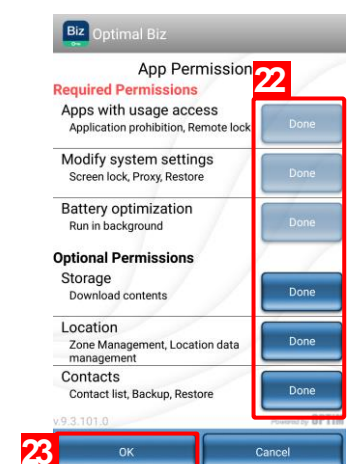
[21] Tap [OK].



[22] A screen that requests permission appears. Follow the on-screen instructions to set things up.

[23] Tap [OK].

⇒ The license authentication screen appears. Continue with the license authentication.




4.4.2 For Android 12 or later

[1] Tap [Get Started].

« If you are inserting SIM »

The following screen is displayed.


Activating network...



[2] Tap [Skip].


Connect to mobile
network
If you have a SIM card, insert it now



2  Skip

[3] Tap a Wi-Fi SSID to connect to Wi-Fi.

Android 12 or later cannot be kitted using mobile network. Be sure to connect to Wi-Fi.

⇒ Network connection starts.

**Connect to Wi-Fi**

Select a network



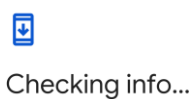
+ See all Wi-Fi networks

Use mobile network for setup

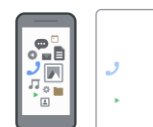
Set up offline

[4] Tap [Don't copy].

⇒ Checking information.

**Copy apps & data**

You can choose to transfer your apps, photos, contacts, Google Account, and more.



Don't copy

Next

[5] Enter your Google Workspace (formerly G Suite) account in "E-mail or phone".

- ☑ License authentication will fail if the Google Workspace (formerly G Suite) account has not been registered as a user of the management site.

☞ "Registering a Google Workspace (formerly G Suite) account to an existing user" Page 52

[6] Tap [Next].**[7] Enter "Password".****[8] Tap [Next].****[9] Tap [I agree].**


Sign in
with your Google Account. [Learn more](#)

5 Email or phone
Forgot email?

Create account

Skip

6 Next



Hi 1

7 Enter your password
Show password

Forgot password?

8 Next



Hi 1

We publish the [Google Terms of Service](#) so that you know what to expect as you use our services. By clicking 'I Agree,' you agree to these terms.

You are also agreeing to the [Google Play Terms of Service](#) to enable discovery and management of apps.

And remember, the Google [Privacy Policy](#) describes how Google handles information generated as you use Google services. You can always visit your Google Account ([account.google.com](#)) to take a Privacy Checkup or to adjust your privacy controls.

Don't add this account now

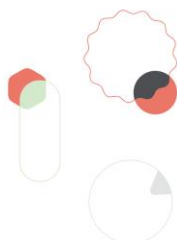
9 I agree

[10] Tap [Next].

⇒ Getting ready for work setup.

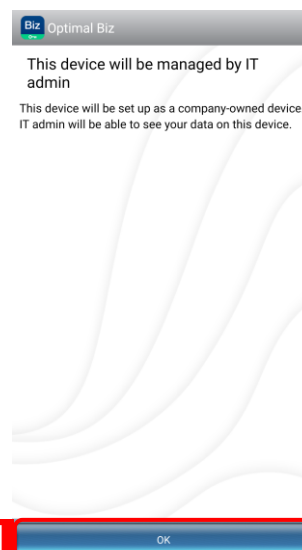


Getting ready for
work setup...



Your account is
managed

Your IT admin uses mobile device
management to enforce security policies

**[11] Tap [OK].**

11

OK

[12] Tap [Accept & Conetinue].

⇒ Setting up in the device.



Keep your work apps
at your fingertips

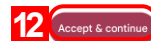


Setting up your device...



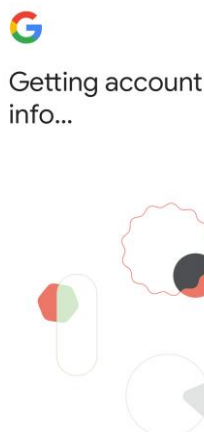
Let's set up your
work device

[View terms](#)



[13] Tap [Next].

⇒ Getting account information.

**This device isn't private**

🕒 Your activity & data

Your IT admin may be able to see your data and activity on this device.

📱 App permissions

Your IT admin can set permissions for apps on this device, such as microphone, camera, and location permissions.

Cancel setup

**[14] Tap [More].**

✎[More] is displayed several times on some devices. Tap [More] until [Accept] is displayed.

**Google Services**

Tap to learn more about each service, such as how to turn it on or off later. Data will be used according to Google's [Privacy Policy](#).

Location

📍 Use location ▾

Allow apps and services with location permission to use your device's location. Google may collect location data periodically and use this data in an anonymous way to improve location accuracy and location-based services.

📍 Allow scanning ▾

Allow apps and services to scan for Wi-Fi

**[15] Tap [Accept].**

Allow apps and services to scan for Wi-Fi networks and nearby devices at any time, even when Wi-Fi or Bluetooth is off.

Device maintenance

🔄 Send usage and diagnostic data ▾

Help improve your Android device experience by automatically sending diagnostic, device, and app usage data to Google. This will help battery life, system and app stability, and other improvements. Some aggregate data will also help Google apps and partners, such as Android developers. If your additional Web & App Activity setting is turned on, this data may be saved to your Google Account.

📶 Install updates & apps ▾

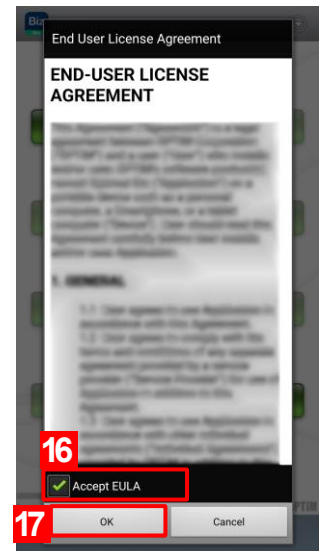
By continuing, you agree that this device may also automatically download and install updates and apps from Google, your carrier, and your device's manufacturer, possibly using cellular data. Data rates may apply. Some of these apps may offer in-app purchases.

Tap "Accept" to confirm your selection of these Google services settings.

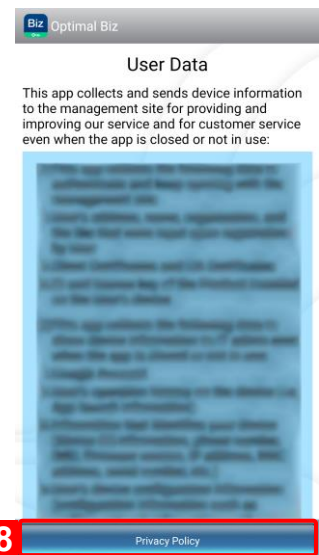


[16] Check "Accept EULA".

[17] Tap [OK].

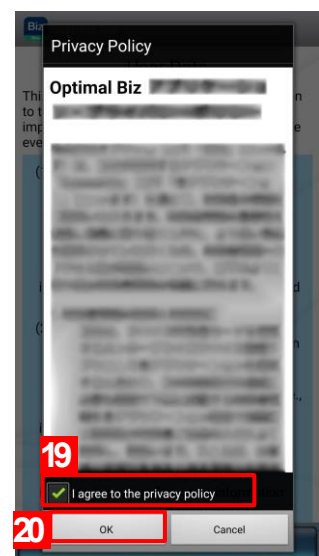


[18] Read the user data policy, and tap [Privacy Policy].

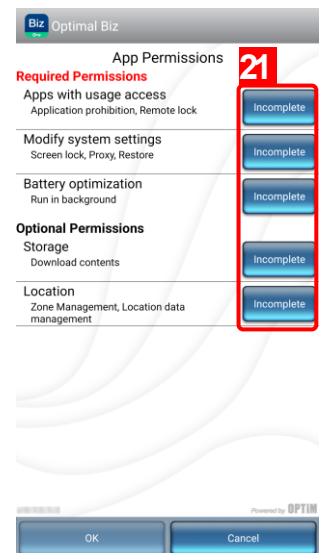


[19] Check "I agree to the privacy policy".

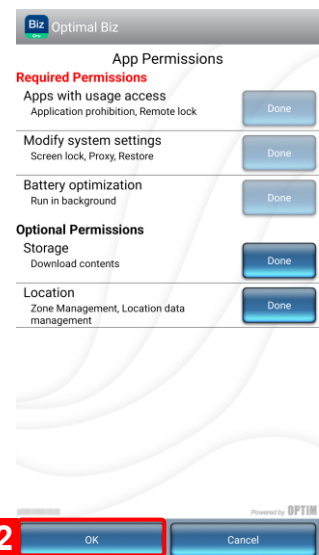
[20] Tap [OK].



[21] A screen that requests permission appears. Follow the on-screen instructions to set things up.

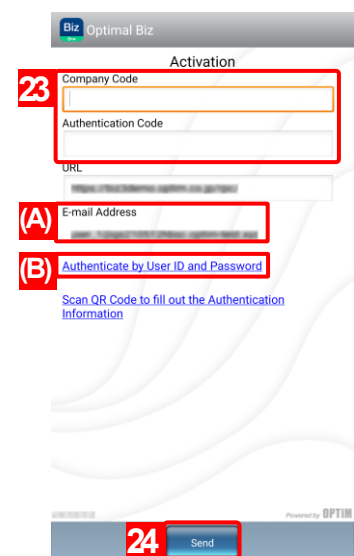


[22] Tap [OK].



[23] Enter a "company code" and "authentication code".

- ✍️ Contact your administrator for your company code and authentication code.
- ✍️ Your Google Workspace (formerly G Suite) account will appear as "Email Address" (A).
- ✍️ If you tap [Scan QR Code to fill out the Authentication information] (B) and scan a QR code for agent license activation, the "Company code", "Authentication code", and "URL" will be automatically entered. Contact your administrator for the QR code.



[24] Tap [Send].

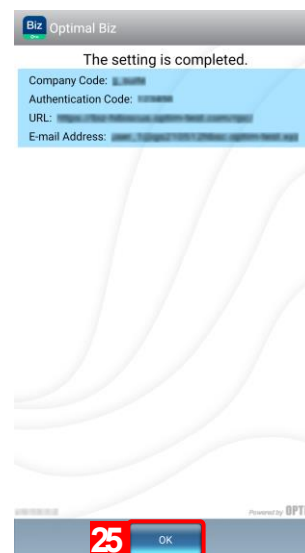
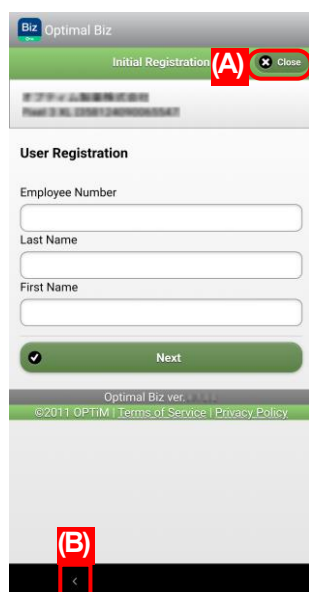


**[25] The license authentication completion screen appears.
Tap [OK].**

« When portal settings are set to be displayed on Management Site »

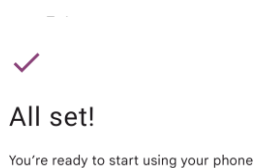
After you tap [OK], initial registration screen appears.
Enter items as necessary.

- ✎ The user will link to the device if the initial registration has been made.
- ✎ If you need not register, you can either tap [Close] (A) or (B) close the screen with the back button on the device.
- ✎ If the user is already linked to the device, a message will appear and say that the user has been linked. Close the screen.



[26] Tap [Skip].

⇒ Kitting is complete.
License authentication is also complete.



Swipe to navigate
your phone

Learn gestures to go Home, go back, and
switch apps



Try it

4.5 Performing license authentication

After kitting is complete, perform license authentication with your User ID or company code / authentication code.

✍ If you are using Android Enterprise, after you perform license authentication with the user ID registered from the management site, it will be integrated with Android Enterprise.

If you have not registered your user ID, the user ID can be integrated with Android Enterprise by performing a license authentication with a company code / authentication code, registering the user ID from the management site, and linking it with your device.

✍ Android 12 or later are license authenticated by kitting, so this operation is not necessary.

4.5.1 Authenticating by a user ID

[1] Tap [Authenticate with User ID and Password].

✍ Your Google Workspace (formerly G Suite) account will appear as "Email Address" (A).

[2] Enter the "Company Code", "User ID or E-mail Address", and "Password".

✍ Contact your administrator for your company code, user ID, and password.

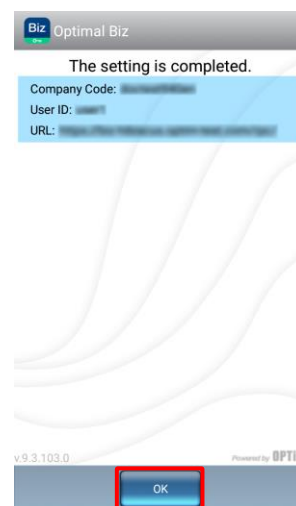
✍ You do not have to change the URL (A).

[3] Tap [Send].


The screenshot shows the 'Biz Optimal Biz' activation screen. The 'Activation' section has three input fields: 'Company Code', 'Authentication Code', and 'URL'. Below these is the 'E-mail Address' field, which is highlighted with a red box and labeled '(A)'. A red box with the number '1' highlights the 'Authenticate by User ID and Password' option. Below this is a link: 'Scan QR Code to fill out the Authentication Information'. At the bottom, there is a 'Send' button.

The screenshot shows the 'Biz Optimal Biz' activation screen. The 'Activation' section has three input fields: 'Company Code', 'User ID or E-mail Address', and 'Password'. Below these is the 'URL' field, which is highlighted with a red box and labeled '(A)'. A red box with the number '2' highlights the 'Authenticate by Authentication code' option. Below this is a link: 'Scan QR Code to fill out the Authentication Information'. At the bottom, there is a 'Send' button, which is highlighted with a red box and labeled '3'.

- [4] The license authentication completion screen appears. Tap [OK].**



- [5] The agent menu screen appears.**

-  After license authentication, users cannot interact with the agent screen until the initial synchronization is complete at the management site.



4.5.2 Authenticating by a company code / authentication code

✍ After license authentication is complete, allocate a user to the device on the management site.

🔍 "Asset" - "List" - "Asset management information" in <Management Site Reference Manual>

[1] Enter a "company code" and "authentication code".

- ✍ Contact your administrator for your company code and authentication code.
- ✍ Your Google Workspace (formerly G Suite) account will appear as "Email Address" (A).
- ✍ If you tap [Scan QR Code to fill out the Authentication information] (B) and scan a QR code for agent license activation, the "Company code", "Authentication code", and "URL" will be automatically entered. Contact your administrator for the QR code.

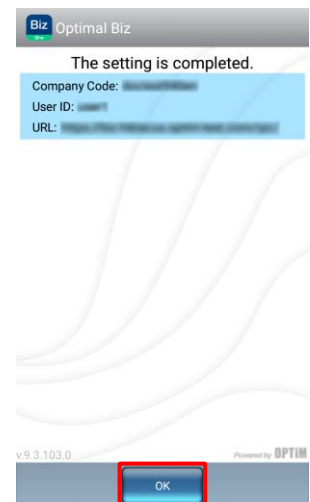
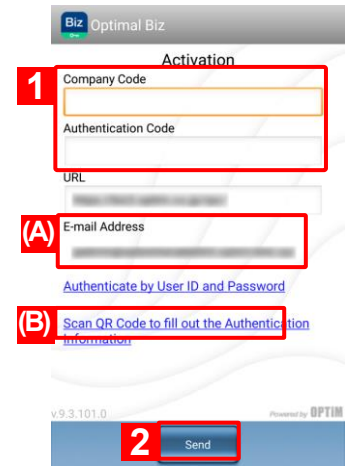
[2] Tap [Send].

[3] The license authentication completion screen appears. Tap [OK].

« When portal settings are set to be displayed on Management Site »

After you tap [OK], initial registration screen appears.
Enter items as necessary.

- ✍ The user will link to the device if the initial registration has been made.
- ✍ If you do not need to register, you can either tap [Close] (A) or (B) the back button on the device to close the screen.
- ✍ If the user is already linked to the device, a message will appear and say that the user has been linked. Close the screen.



[4] The agent menu screen appears.

- ✓ After license authentication, users cannot interact with the agent screen until the initial synchronization is complete at the management site.



5 Performing Android Enterprise integration by using zero-touch enrollment with a Google account

Zero-touch enrollment is one of the methods for kitting an agent. This method reduces the kitting procedure, making it easier and faster to introduce many devices. Zero-touch enrolled devices automatically install an agent as Device Owner Mode, enabling more secure device management.

By integrating a zero-touch server, the list of devices in this product will automatically display your device as a pre-kitting device. If you allocate a setting policy to a pre-kitting device and activate it, the settings will apply immediately.

This chapter describes the following items.

Item	Page
Registering a Google account *	74
Performing authentication settings of Google API *	80
Creating a user	105
Performing kitting with zero-touch registration (using a Google account)	107
Performing license authentication	121
Allocating a user to your device	125
Syncing with the zero-touch registration server	127



Attention

- For details of Zero Touch enrollment, refer to the following.
https://www.android.com/intl/ja_jp/enterprise/management/zero-touch/
- For accounts exclusively for zero-touch enrollment, contact your zero-touch device vendor.
- The items marked with * above are required only for the first kitting.



Reference

- By setting up the "Application Distribution" function of Android Enterprise on the management site in advance, apps can be distributed to your device at the same time as license authentication after kitting is complete. For details of app distribution, refer to the following.

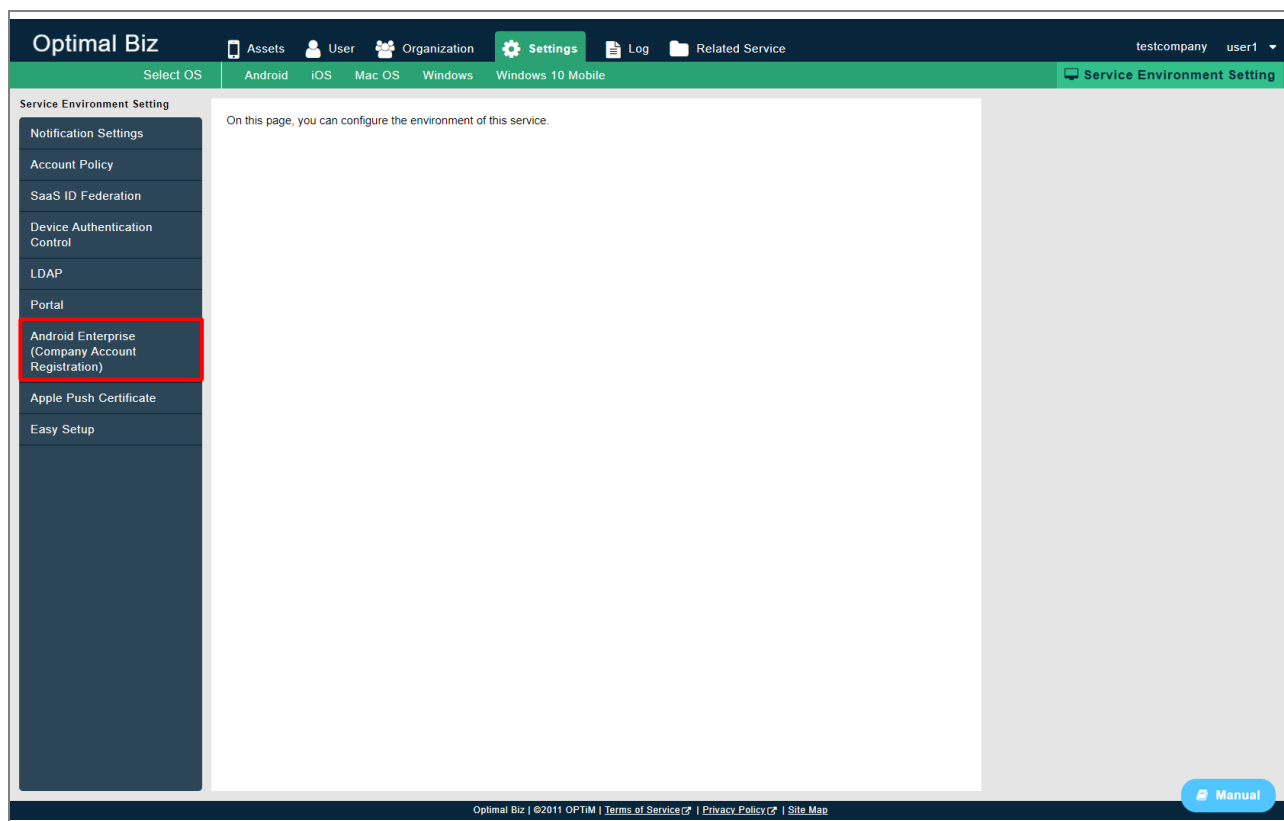


"Android Enterprise App distribution" in <Android Enterprise Manual>

5.1 Registering a Google account

Follow the steps below to register a Google account for integrating Android Enterprise with the management site.

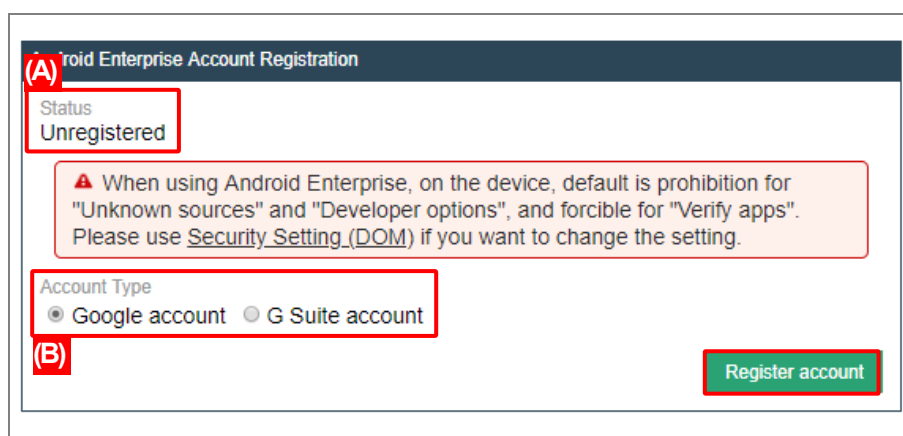
- [1] Click [Settings]→[Service Environment Setting]→[Android Enterprise (Company Account Registration)].**



- [2] The "Status" (A) shows "Unregistered".**
"Google account" is selected in "Account Type" (B) by default.
Click [Register account].

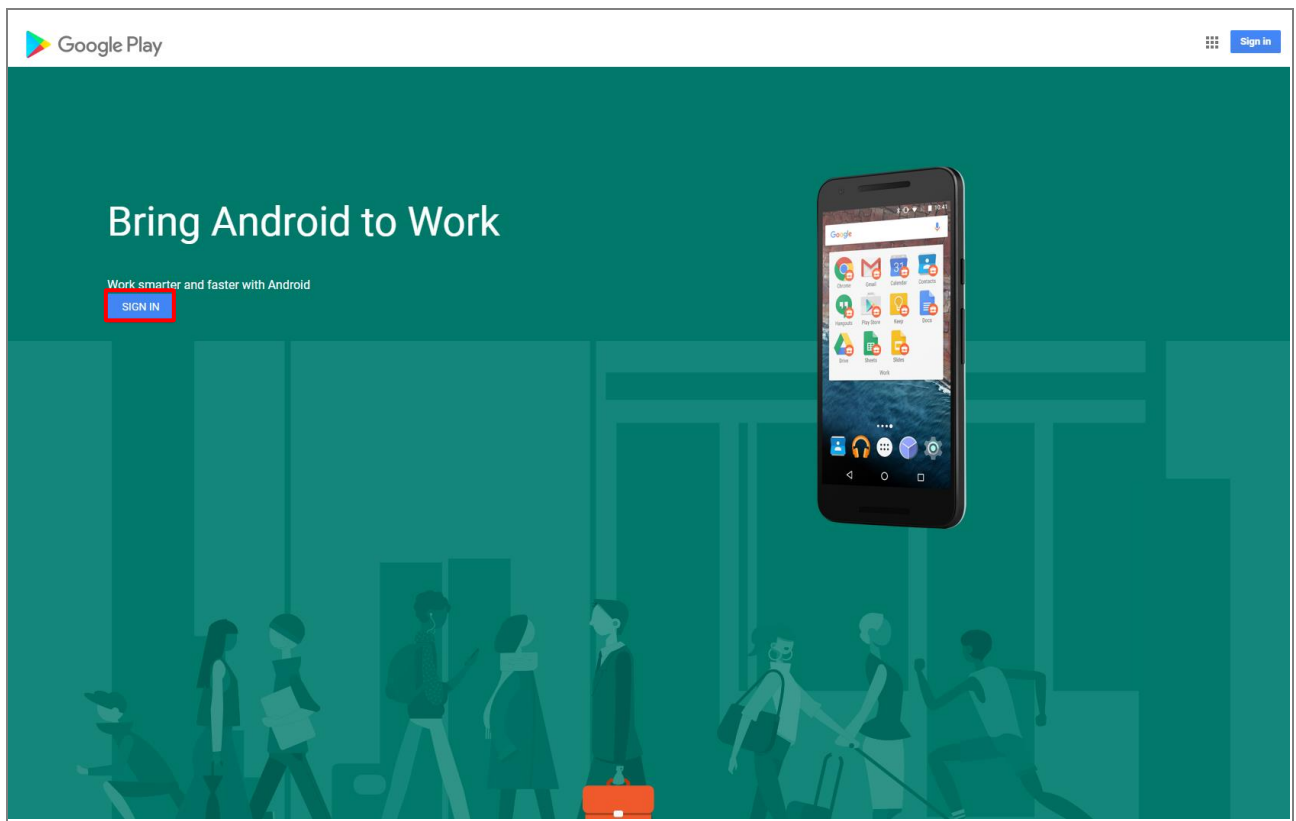
- ✓ After account registration is complete, the device's "Installation of unknown source apps" and "Developer options" will be set to "Prohibit" and "Force apps check" will be set to "Force". Create a configuration set that allows "Installation of unknown source apps" in "Security setting (DOM)", allocate it to your device, and perform a sync.

🔍 "Settings – Android" - "Device Owner Mode" - "Security setting (DOM)" in <Management Site Reference Manual>



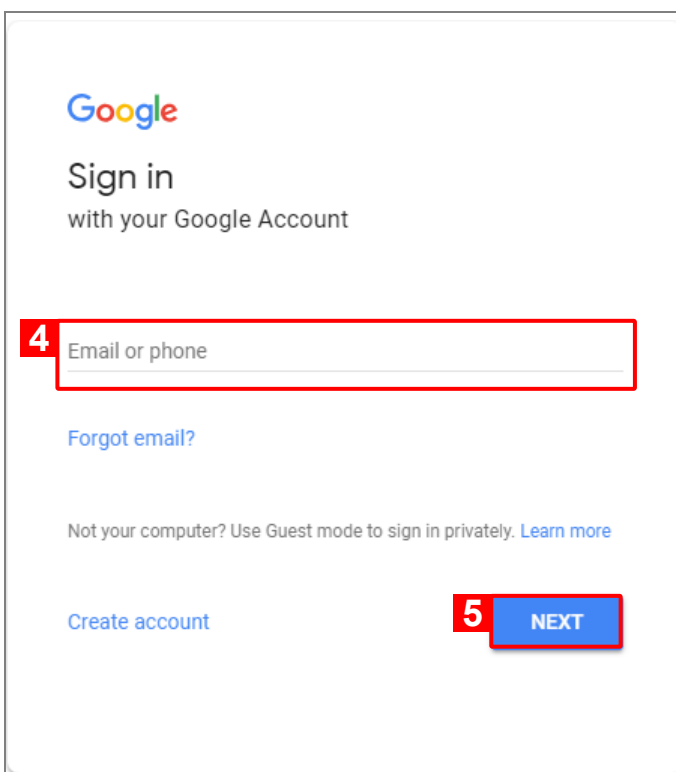
[3] Google Play will be displayed. Click [SIGN IN].

 Depending on the browser you are using, Google Play may not work properly.



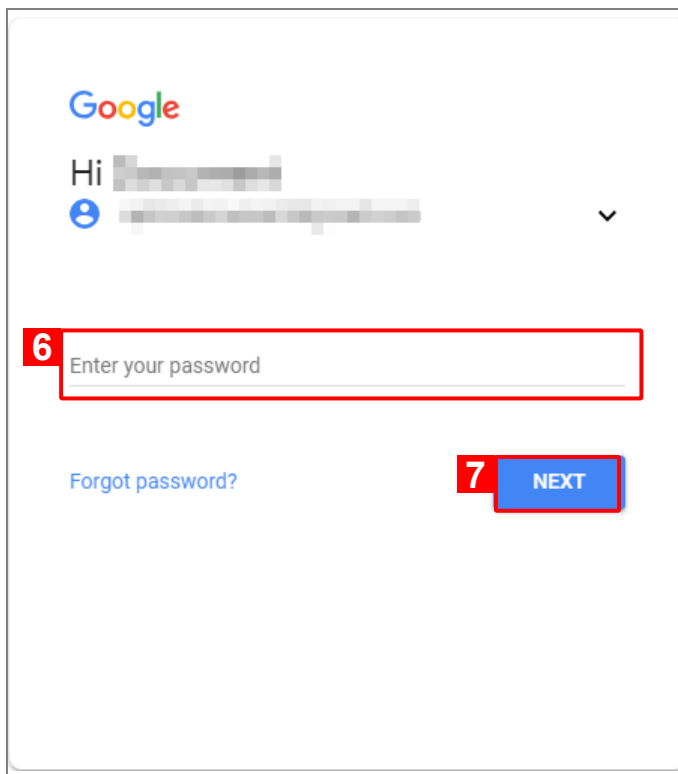
[4] Enter your company Google account.

[5] Click [NEXT].



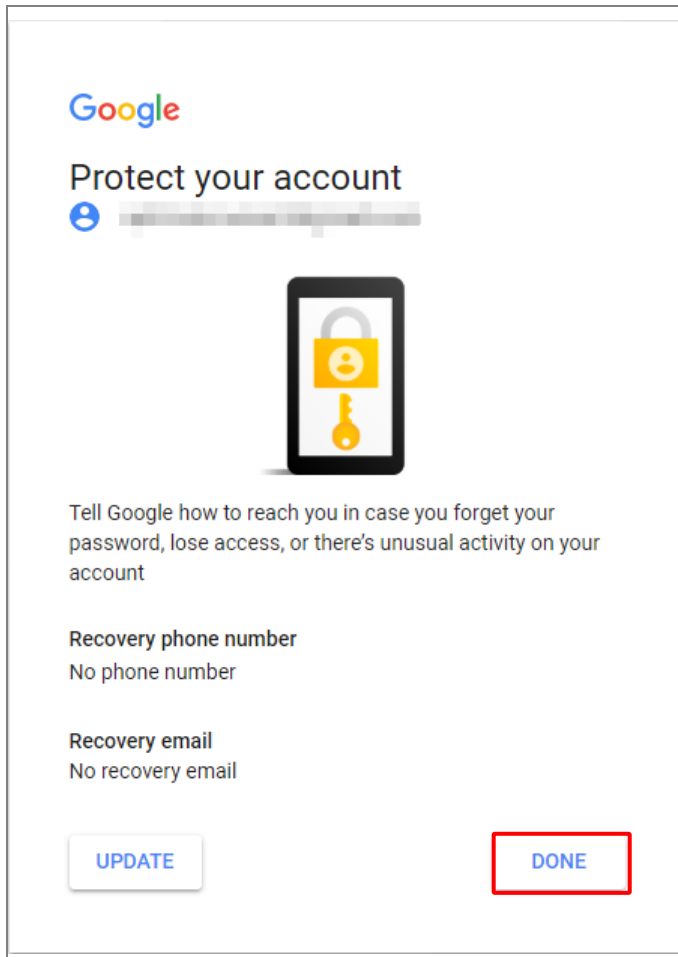
[6] Enter the password.

[7] Click [NEXT].



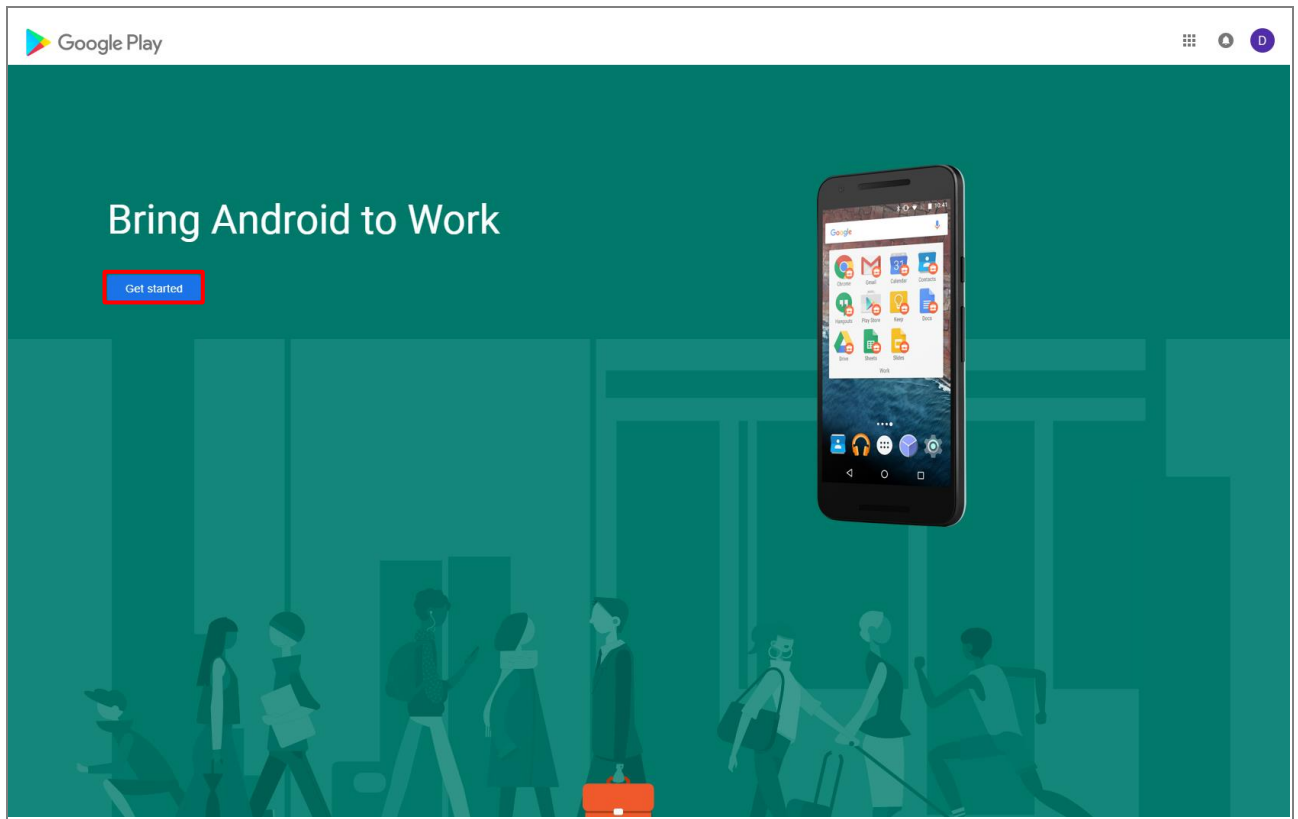
The image shows the Google login screen. At the top is the Google logo. Below it, the text "Hi" is followed by a blurred email address and a dropdown arrow. A red box labeled "6" highlights the password input field with the placeholder text "Enter your password". Below the input field is a link that says "Forgot password?". To the right of the input field is a blue button labeled "NEXT" with a red box labeled "7" highlighting it.

[8] Click [DONE].



The image shows the "Protect your account" screen. At the top is the Google logo. Below it, the text "Protect your account" is followed by a blurred email address. In the center is an icon of a smartphone with a yellow padlock and a key. Below the icon, the text reads: "Tell Google how to reach you in case you forget your password, lose access, or there's unusual activity on your account". There are two sections: "Recovery phone number" with the value "No phone number" and "Recovery email" with the value "No recovery email". At the bottom, there are two buttons: "UPDATE" and "DONE". The "DONE" button is highlighted with a red box.

[9] Click **[Get started]**.




[10] Enter **"Business name"**.

[11] Click **[Next]**.

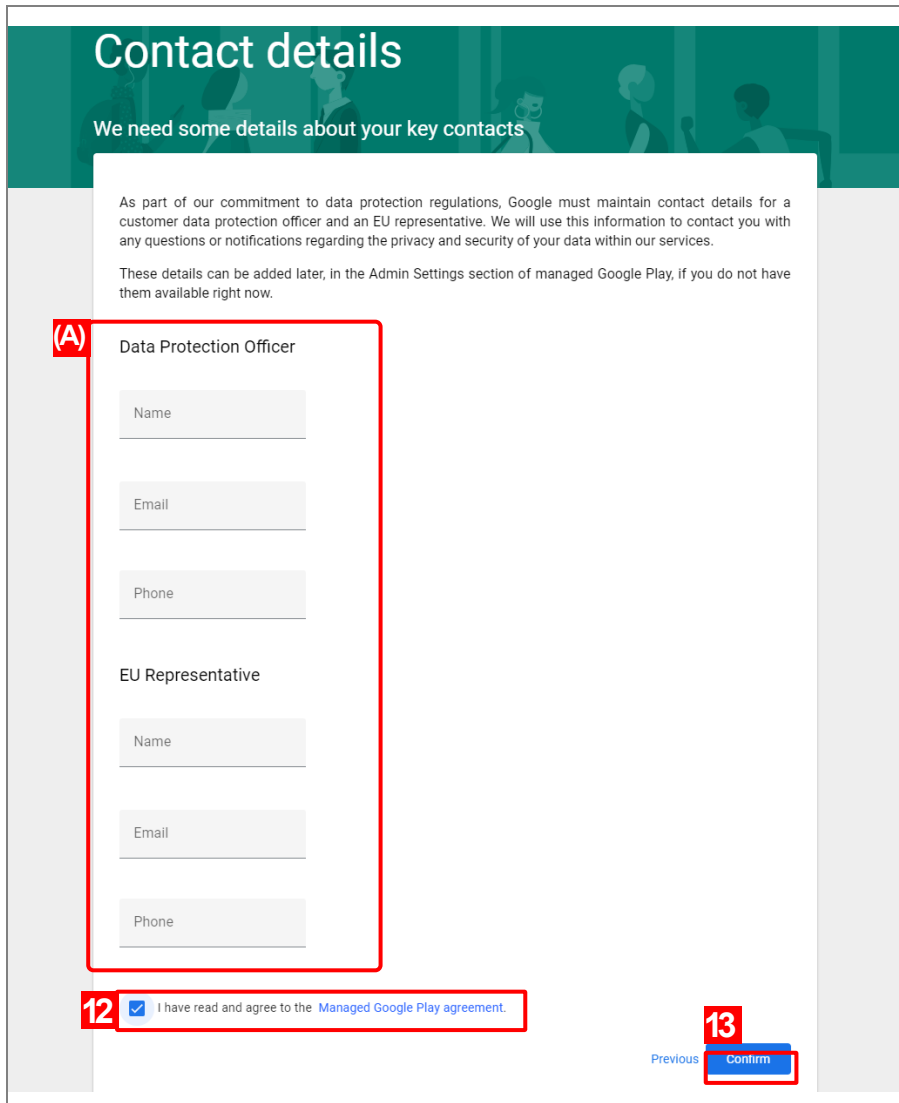
A screenshot of the 'Business name' setup screen. The title 'Business name' is at the top in large white font. Below it, the text 'We need some details about your business' is displayed. The screen contains two input fields. The first field is labeled 'Business name' and has a light green placeholder text 'Your answer'. This field is highlighted with a red rectangular box and a red number '10' in the top left corner. The second field is labeled 'Enterprise mobility management (EMM) provider' and contains the text 'Optimal Biz'. To the right of this field is a red number '11' in the top left corner, and a red rectangular box highlights the 'Next' button. At the bottom right, there are two buttons: 'Previous' and 'Next', both in blue. The 'Next' button is highlighted with a red rectangular box.

[12] Read the agreement and check the box.

[13] Click [Confirm].

-  The Data Protection Officer and EU Representative (A) are optional. Enter them if required. For details of Data Protection Officer and EU Representative, refer to the following.

 <https://support.google.com/googleplay/work/answer/7681629>



Contact details

We need some details about your key contacts

As part of our commitment to data protection regulations, Google must maintain contact details for a customer data protection officer and an EU representative. We will use this information to contact you with any questions or notifications regarding the privacy and security of your data within our services.

These details can be added later, in the Admin Settings section of managed Google Play, if you do not have them available right now.

(A) Data Protection Officer

Name

Email

Phone

EU Representative

Name

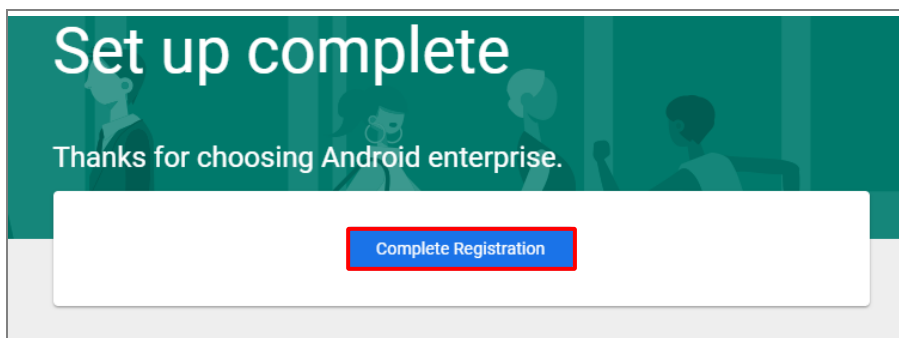
Email

Phone

12 ☒ I have read and agree to the [Managed Google Play agreement](#).

13 [Previous](#) [Confirm](#)

[14] Click [Complete Registration].



Set up complete

Thanks for choosing Android enterprise.

[Complete Registration](#)

- [15]** When you return to the management site, the "Status" (A) shows "Registered".
The email address registered for Google Play is displayed in "Account E-mail Address" (B).

The screenshot displays the 'Android Enterprise Account Registration' interface. At the top, a dark blue header contains the title. Below it, the 'Status' is shown as 'Registered', with a red box and label (A) highlighting this text. A red-bordered warning box follows, containing a triangle icon and text about device settings. Below the warning, the 'Account Type' is listed as 'Google account'. The 'Account E-mail Address' is shown in a greyed-out field, highlighted with a red box and label (B). A green 'Delete account' button is located at the bottom right of the main content area.

Android Enterprise Account Registration

(A) Status
Registered

⚠ When using Android Enterprise, on the device, default is prohibition for "Unknown sources" and "Developer options", and forcible for "Verify apps". Please use [Security Setting \(DOM\)](#) if you want to change the setting.

Account Type
Google account

(B) Account E-mail Address

Delete account

5.2 Performing authentication settings of Google API

Connect your Google account to your corporate e-mail address in the management site, and create and authenticate a JSON file.

5.2.1 Registering your e-mail address as a Google account

You can use your corporate or organizational e-mail address as your Google account.

- ✎ You do not have to perform these steps for all managed devices. Prepare one e-mail address for administration. It is recommended that you use the mailing list of an administrative department, not an administrator's e-mail address.
- ✎ If your Google account has been registered in your browser, you do not need to carry out this procedure.

[1] Click [Settings]→[Android]→[Zero-touch enrollment]→[Use Registration].

[2] Click [Register account].

The screenshot shows the Optimal Biz management console interface. The top navigation bar includes 'Assets', 'User', 'Organization', 'Settings', 'Log', and 'Related Service'. The 'Settings' tab is active, and the 'Android' sub-tab is selected. The left sidebar shows the 'Zero-touch enrollment' section expanded, with 'Use Registration' highlighted. The main content area displays a five-step process for registering a Google account. Step 1, 'Associate the Google account with the company/organization e-mail address', is the current step. It includes instructions to make an association and a link to 'Register account', which is highlighted with a red box and the number 2. Step 2 is 'Allow login to zero-touch portal'. Step 3 is 'Login to zero-touch portal and agree to terms of service'. Step 4 is 'API setting and downloading JSON file'. Step 5 is 'Upload JSON file'. A 'Manual' button is located in the bottom right corner.

[3] The "Create your Google Account" screen appears.

Enter "First name", "Last name", "Your email address", "Password", and "Confirm".

✍ In "Your email address", enter an email address with a corporate domain.

✍ If you click "Create a Gmail account instead" (A), you will create a Google Account with a Gmail account, so do not click the link. Be sure to create your account with your current email address.

[4] Click [Next].**[5] In "Enter code", enter the confirmation code that was sent to the email address you entered in step [3].****[6] Click [Verify].**

[7] Enter "Phone number", "Your birthday", and "Gender".

[8] Click [NEXT].

Google

welcome to Google

@gmail.com

7 Phone number (optional)

This won't make your number visible to others

Recovery email address (optional)

We'll use it to keep your account secure

Month Day Year

Your birthday

Gender

Your personal info is private & safe

Why we ask for this information

Back

8 NEXT

[9] Review the Terms, and click [I agree].

Google

Privacy and Terms

Combining data

We also combine this data among our services and across your devices for these purposes. For example, depending on your account settings, we show you ads based on information about your interests, which we can derive from your use of Search and YouTube, and we use data from trillions of search queries to build spell-correction models that we use across all of our services.

You're in control

Depending on your account settings, some of this data may be associated with your Google Account and we treat this data as personal information. You can control how we collect and use this data now by clicking "More Options" below. You can always adjust your controls later or withdraw your consent for the future by visiting My Account (myaccount.google.com).

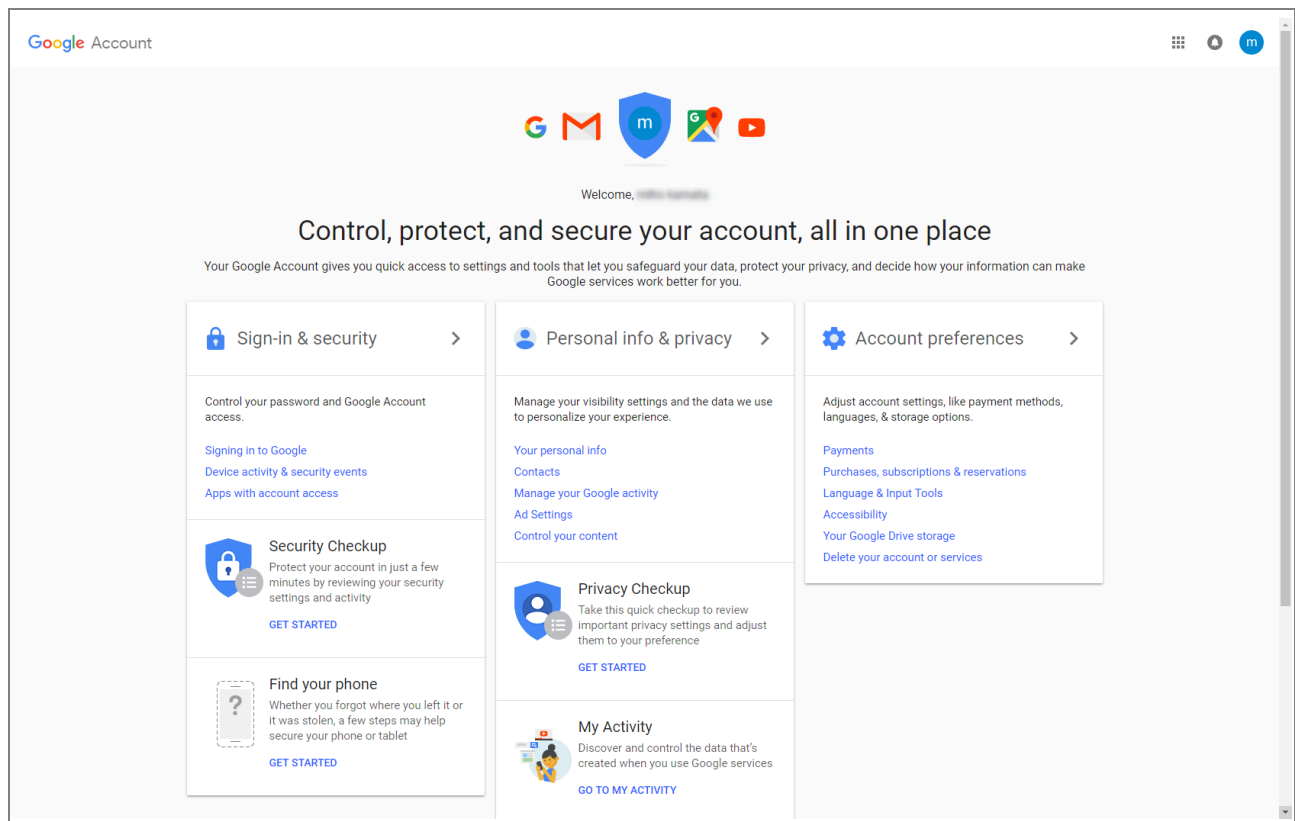
MORE OPTIONS

Cancel

9 I agree

You're in control of the data we collect & how it's used

[10] You have successfully registered your e-mail address if the screen below appears.



5.2.2 Logging in to the zero-touch portal

Inform your zero-touch device vendor of the registered Google account and ask them to allow logins to the zero-touch portal.

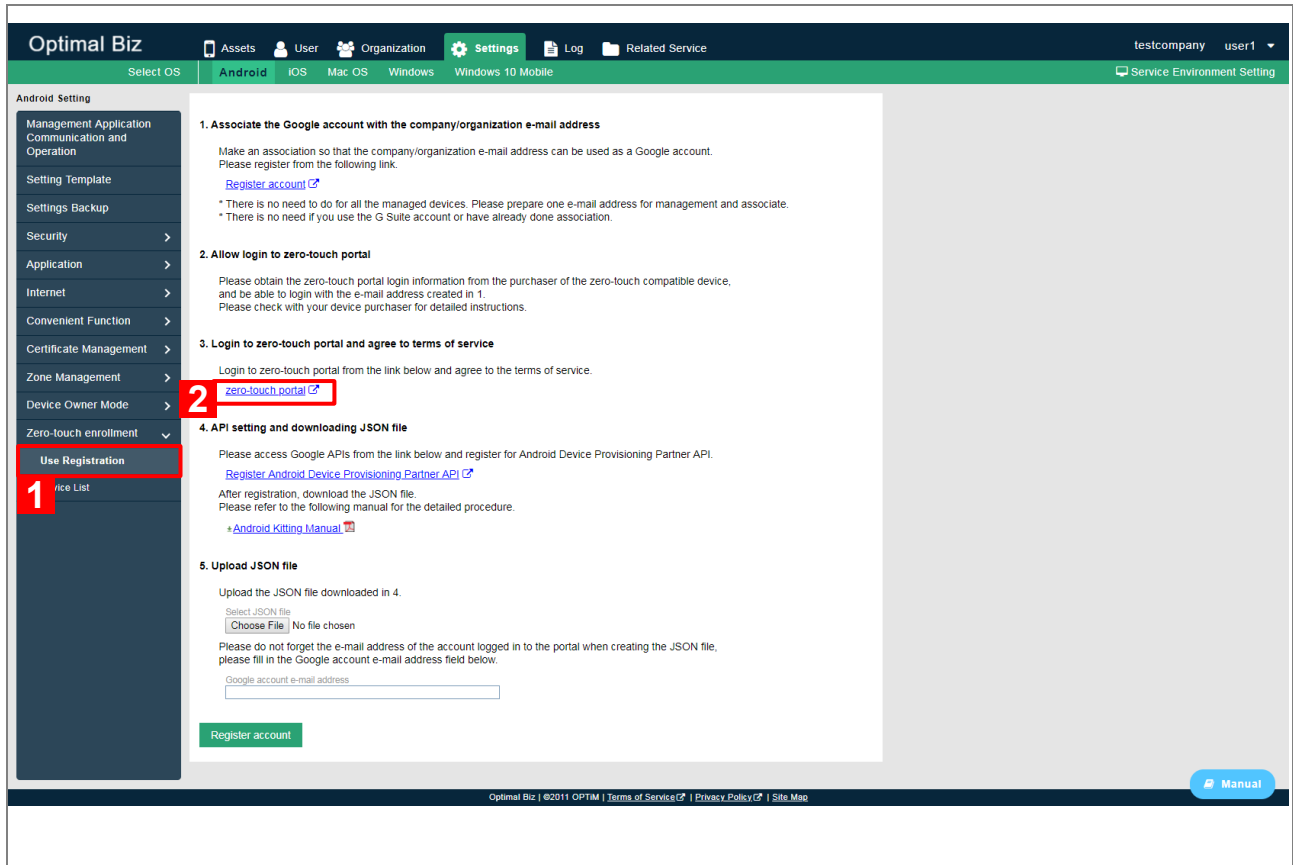
 For details, contact your zero-touch device vendor.

5.2.3 Accepting the terms of service

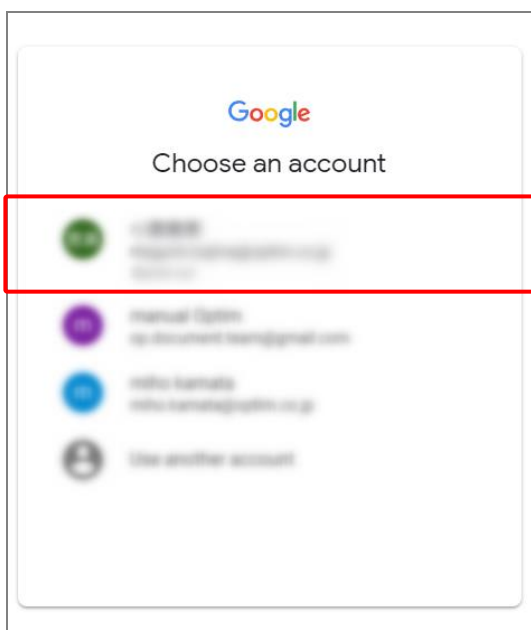
Log in to the zero touch portal and accept the terms of service.

[1] Click [Settings]→[Android]→[Zero-touch enrollment]→[Use Registration].

[2] Click [zero-touch portal].



[3] Select the Google account you registered.



[4] Select "I accept the Terms of Service."

[5] Click [Agree].

Terms of Service

Android Zero Touch End Customer Agreement

1.1 Services Use. Subject to this Agreement, during the Term, you, the Customer may: (a) use the Services, and (b) use any Software provided by Google as part of the Services. Customer may not sublicense or transfer these rights except as permitted under the Assignment section of the Agreement

1.2 Console. Google will provide the Services to Customer. As part of receiving the Services, Customer will have access to the Admin Console, through which Customer may administer the Services.

1.3 Facilities. All facilities used to store and process an Application and Customer Data will adhere to reasonable security standards no less protective than the security standards at facilities where Google processes and stores its own information of a similar type. Google has implemented at least industry standard systems and procedures to (i) ensure the security and confidentiality of an Application and Customer Data, (ii) protect against anticipated threats or hazards to the security or integrity of an Application and Customer Data, and (iii) protect against unauthorized access to or use of an Application and Customer Data.

immediately. If Customer does not agree to the revised Agreement, please stop using the Services. Google will

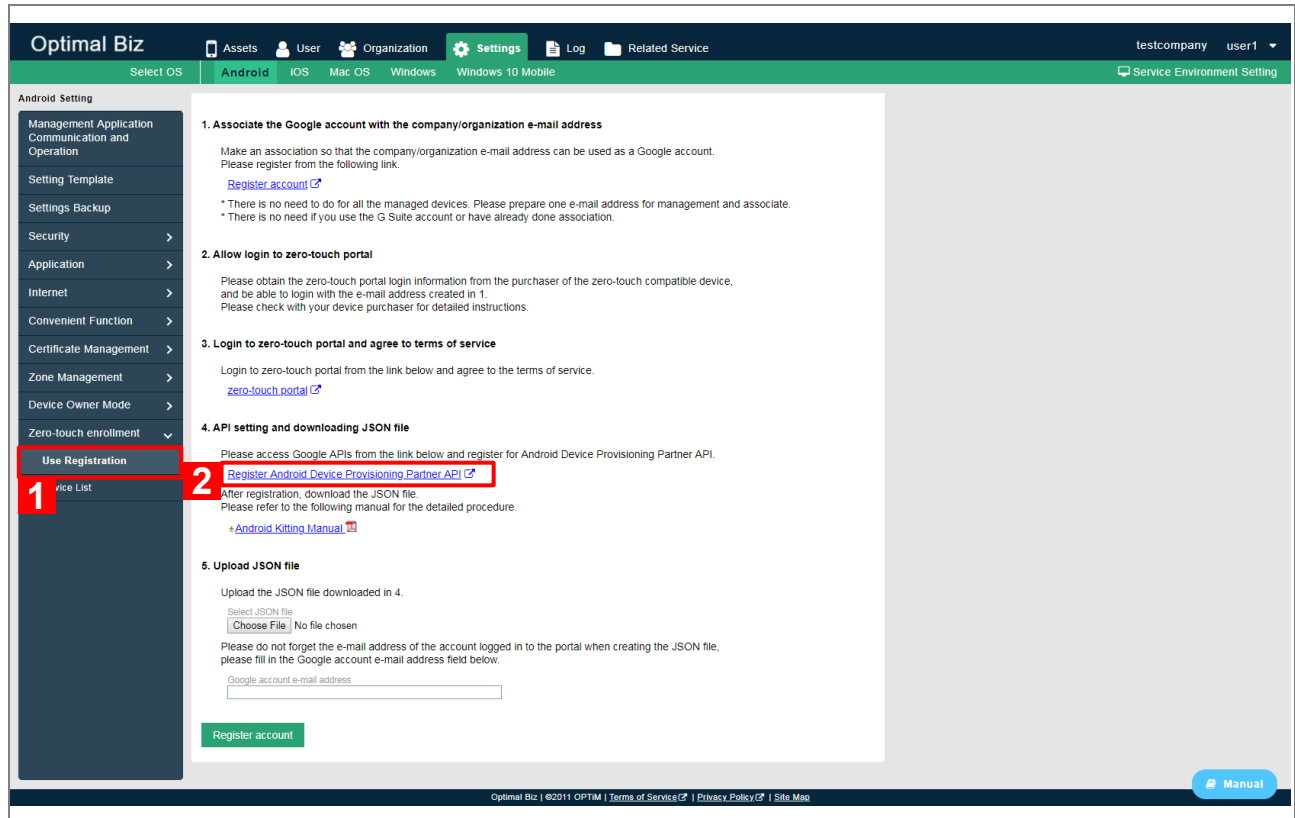
4 ☐ I accept the Terms of Service.

5

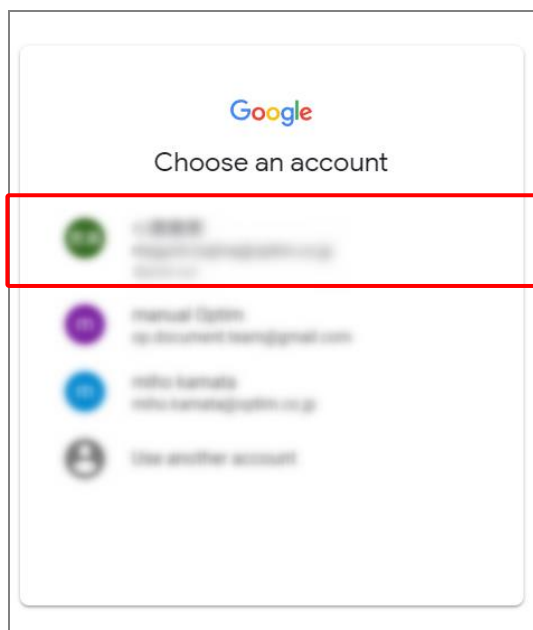
5.2.4 Downloading API settings and a JSON file

Register Android Device Provisioning Partner API on the Google Cloud Platform, and download a JSON file.

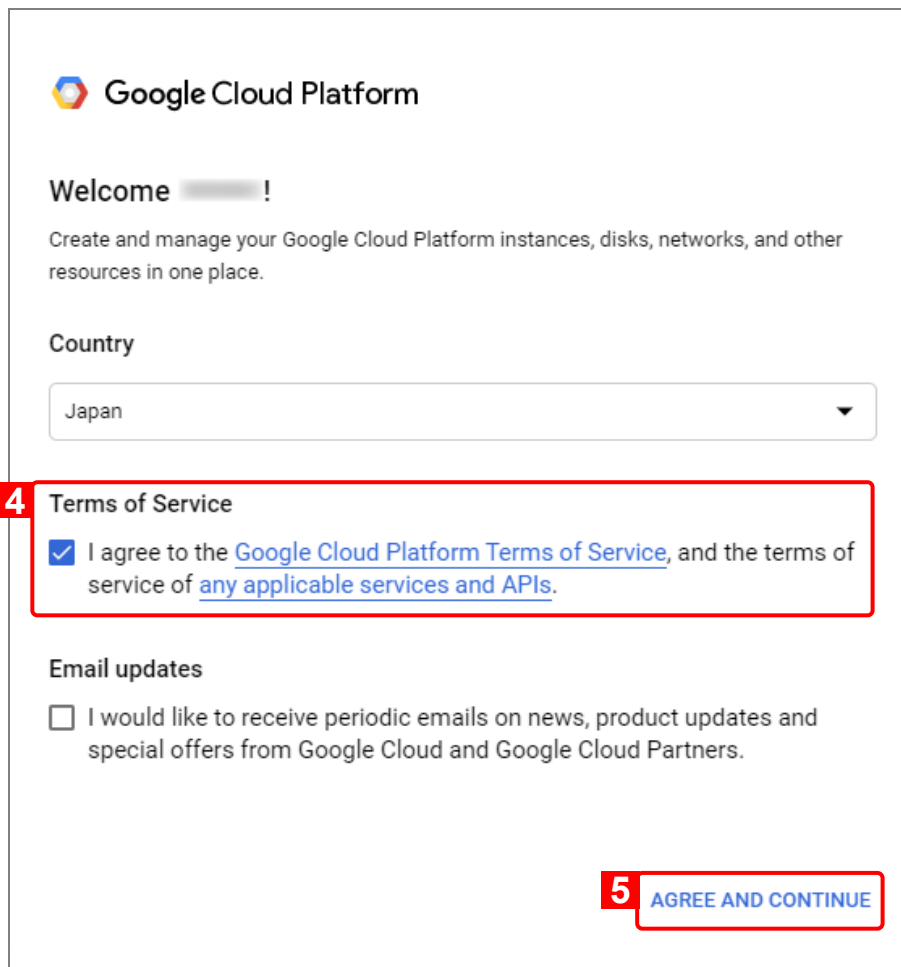
- [1]** Click [Settings]→[Android]→[Zero-touch enrollment]→[Use Registration].
- [2]** Click [Register Android Device Provisioning Partner API].



- [3]** Select the e-mail address that you have connected.

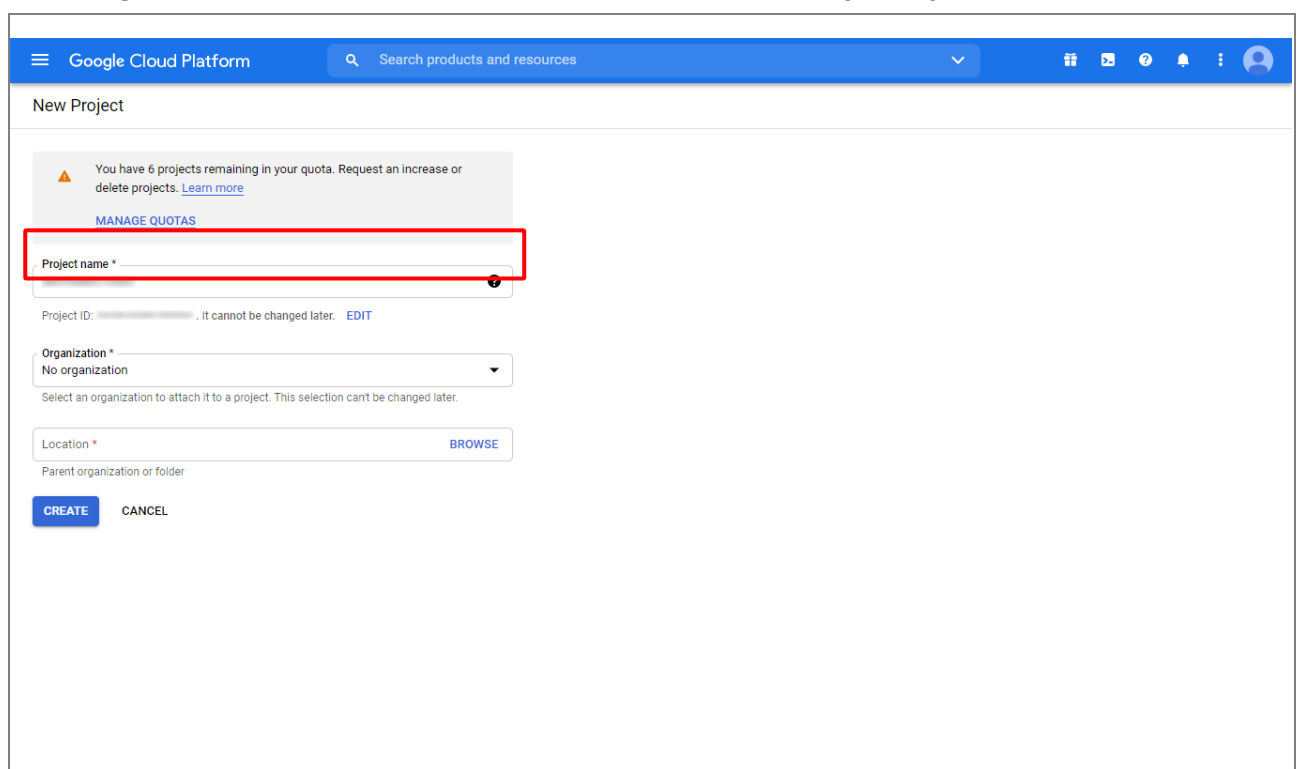


- [4]** In the first login, the consent screen for the terms of service will appear. Select the terms of service.
- [5]** Click [AGREE AND CONTINUE].

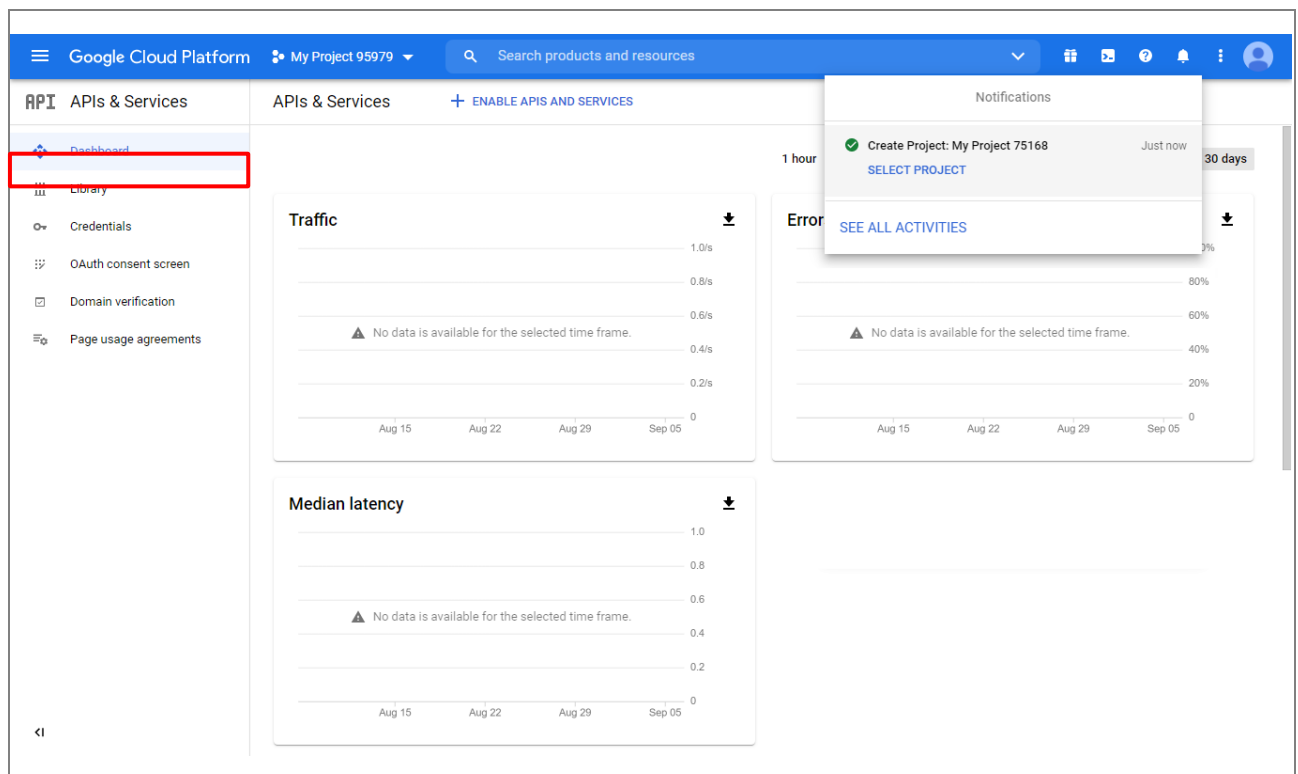
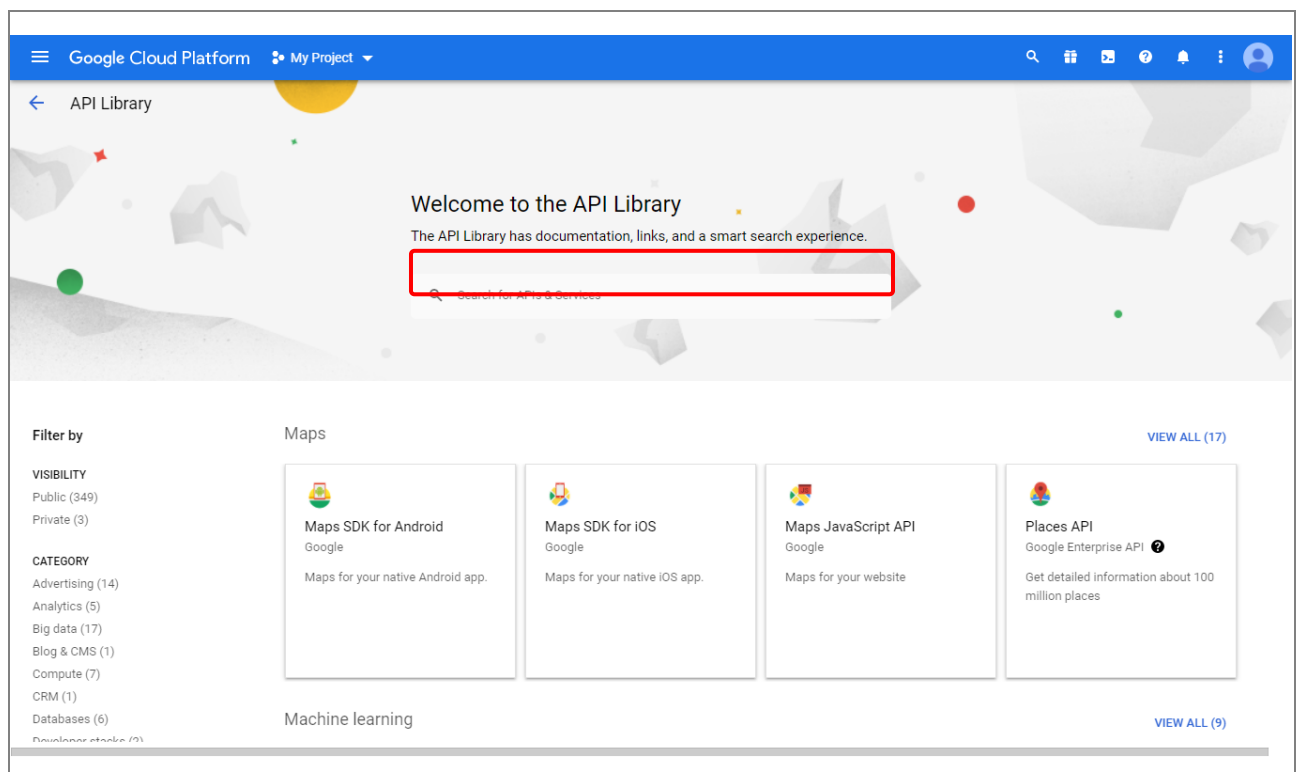


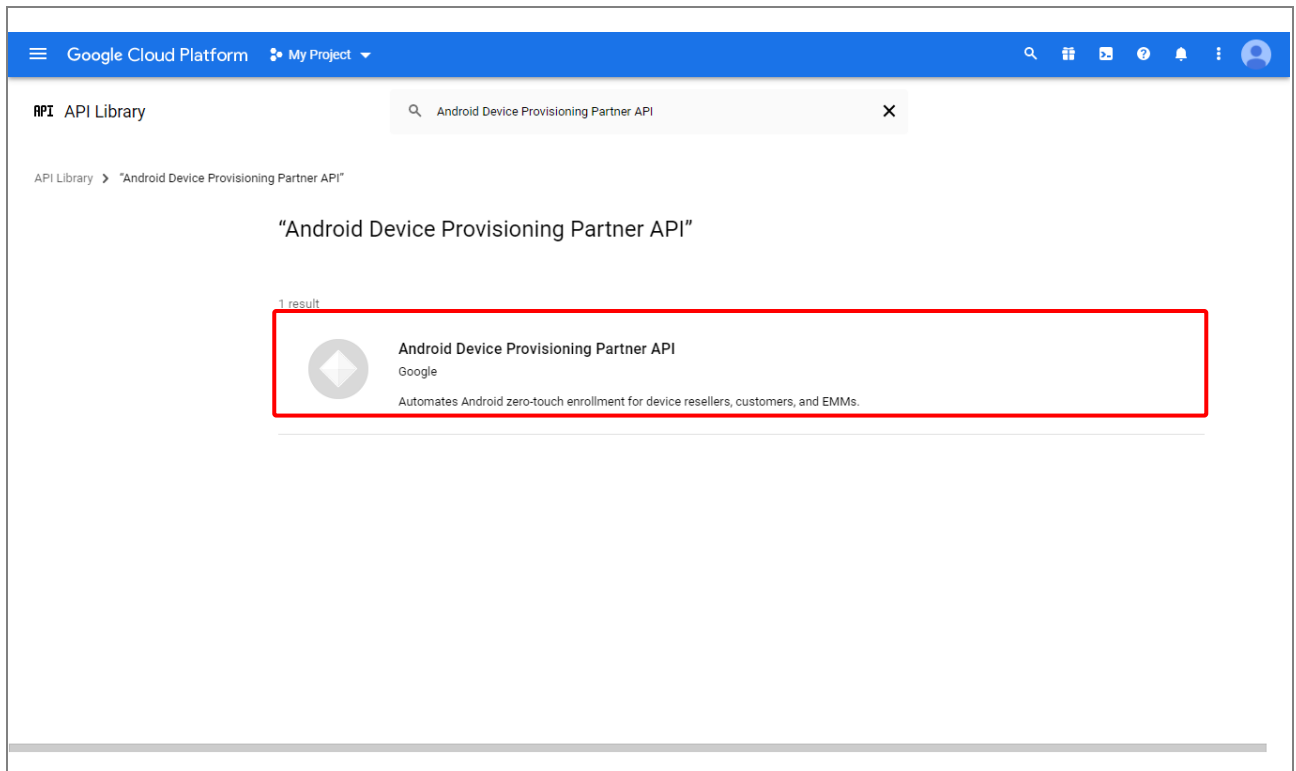
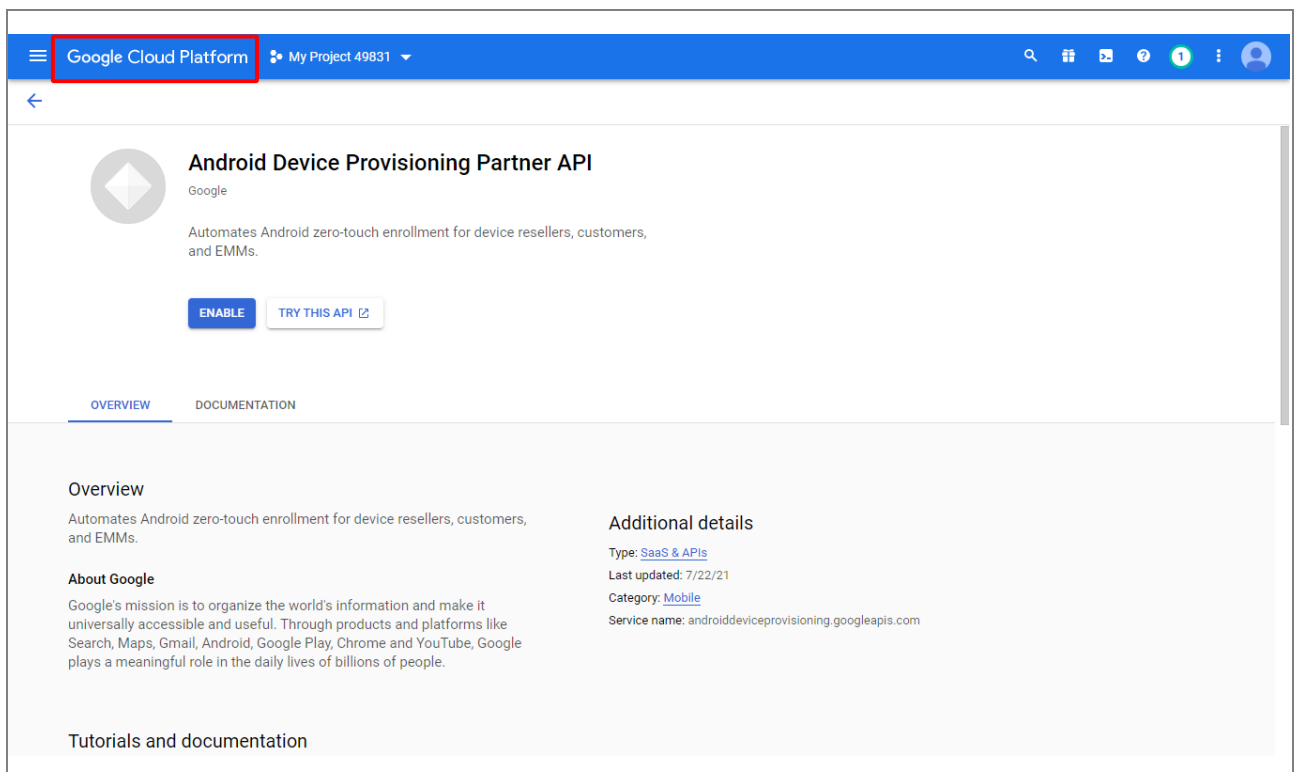
The screenshot shows the Google Cloud Platform 'Welcome' screen. At the top, it says 'Welcome [redacted]!' and 'Create and manage your Google Cloud Platform instances, disks, networks, and other resources in one place.' Below this is a 'Country' dropdown menu with 'Japan' selected. A red box labeled '4' highlights the 'Terms of Service' section, which contains a checked checkbox and the text: 'I agree to the [Google Cloud Platform Terms of Service](#), and the terms of service of [any applicable services and APIs](#).' Below this is the 'Email updates' section with an unchecked checkbox and the text: 'I would like to receive periodic emails on news, product updates and special offers from Google Cloud and Google Cloud Partners.' A red box labeled '5' highlights the 'AGREE AND CONTINUE' button at the bottom right.

- [6]** The Google Cloud Platform screen appears. Enter an arbitrary "Project name".



The screenshot shows the Google Cloud Platform 'New Project' screen. At the top, there is a blue header with the Google Cloud Platform logo, a search bar, and various icons. Below the header, there is a warning message: 'You have 6 projects remaining in your quota. Request an increase or delete projects. [Learn more](#)'. Below the warning is a 'MANAGE QUOTAS' link. A red box highlights the 'Project name *' input field. Below this is the 'Project ID' field, which is disabled and has a note: 'It cannot be changed later. [EDIT](#)'. Below the Project ID is the 'Organization *' dropdown menu, which is currently set to 'No organization'. Below the Organization dropdown is a note: 'Select an organization to attach it to a project. This selection can't be changed later.' Below this is the 'Location *' field, which has a 'BROWSE' link. Below the Location field is the 'Parent organization or folder' field. At the bottom, there are 'CREATE' and 'CANCEL' buttons.

[7] Click [Library].**[8] In "Search for APIs and Services", enter "Android Device Provisioning Partner API", and execute search.**

【9】 Click [Android Device Provisioning Partner API] in the results.**【10】 Click [Google Cloud Platform].**


[11] Click [Credentials].

The screenshot shows the Google Cloud Platform console for project 'My Project 49831'. The left sidebar has a red box around the 'Credentials' link. The main content area shows the 'Overview' page for the 'Android Device Provisioning Partner API'. A message at the top says 'To use this API, you may need credentials. Click 'Create credentials' to get started.' with a 'CREATE CREDENTIALS' button. The 'Details' section shows the API name, provider (Google), service name, and activation status (Enabled). The 'Traffic by response code' chart shows no data for the selected time frame. A 'Tutorials and documentation' section with a 'Learn more' link is also visible.

[12] Click [CONFIGURE CONSENT SCREEN].

The screenshot shows the 'Credentials' page in the Google Cloud Platform console. At the top, there are links for '+ CREATE CREDENTIALS' and 'DELETE'. Below this, a section titled 'Credentials compatible with this API' includes a link to 'Credentials in APIs & Services'. A warning message states: 'Remember to configure the OAuth consent screen with information about your application.' A red box highlights the 'CONFIGURE CONSENT SCREEN' button. Below the warning, there are two sections: 'OAuth 2.0 Client IDs' and 'Service Accounts'. Both sections show a table with columns for Name, Creation date, Type, Client ID, and Actions. The 'OAuth 2.0 Client IDs' section shows 'No OAuth clients to display'. The 'Service Accounts' section shows 'No service accounts to display' and a link to 'Manage service accounts'.


[13] Click [CREATE].

 You do not have to select "User Type" (A). For details of "User Type", contact Google.


OAuth consent screen

Choose how you want to configure and register your app, including your target users. You can only associate one app with your project.

(A) User Type

☐ Internal 


Only available to users within your organization. You will not need to submit your app for verification. [Learn more about user type](#)

☐ External 

Available to any test user with a Google Account. Your app will start in testing mode and will only be available to users you add to the list of test users. Once your app is ready to push to production, you may need to verify your app. [Learn more about user type](#)

CREATE

[Let us know what you think](#) about our OAuth experience

- [14] Enter "OptimalBiz" in "App Name".**
- [15] Click "User support email" and select an email address.**
- [16] Enter "optim.co.jp" in "Authorized domains", and press [Enter].**
 The domain name may change automatically after you press [Enter].
- [17] Enter your email address in [Developer contact information].**
- [18] Click [SAVE AND CONTINUE].**

Edit app registration

1 OAuth consent screen — 2 Scopes — 3 Test users — 4 Summary

App information

This shows in the consent screen, and helps end users know who you are and contact you

14

The name of the app asking for consent

15

User support email *

For users to contact you with questions about their consent

App logo

BROWSE

Upload an image, not larger than 1MB on the consent screen that will help users recognize your app. Allowed image formats are JPG, PNG, and BMP. Logos should be square and 120px by 120px for the best results.

App domain

To protect you and your users, Google only allows apps using OAuth to use Authorized Domains. The following information will be shown to your users on the consent screen.

Application home page

Provide users a link to your home page

Application privacy policy link

Provide users a link to your public privacy policy

Application terms of service link

Provide users a link to your public terms of service

16

Authorized domains

When a domain is used on the consent screen or in an OAuth client's configuration, it must be pre-registered here. If your app needs to go through verification, please go to the [Google Search Console](#) to check if your domains are authorized. [Learn more](#) about the authorized domain limit.

example.com

ADD DOMAIN

Developer contact information

17

Email addresses *

These email addresses are for Google to notify you about any changes to your project.

18


SAVE AND CONTINUE


CANCEL


[19] Click [SAVE AND CONTINUE].


 You do not have to add scopes.

Edit app registration

 OAuth consent screen


 **Scopes**

 Test users

 Summary

Scopes express the permissions you request users to authorize for your app and allow your project to access specific types of private user data from their Google Account. [Learn more](#)

ADD OR REMOVE SCOPES

 **Your restricted scopes**


Restricted scopes are scopes that request access to highly sensitive user data.

API ↑	Scope	User-facing description
No rows to display		


SAVE AND CONTINUE


CANCEL


[20] Click [SAVE AND CONTINUE].


 You do not have to add test users.

Edit app registration

 OAuth consent screen

 Scopes

 **Test users**

 Summary


Test users

While publishing status is set to "Testing", only test users are able to access the app. Allowed user cap prior to app verification is 100, and is counted over the entire lifetime of the app. [Learn more](#)

+ ADD USERS

Filter

Enter property name or value



User information
No rows to display

SAVE AND CONTINUE

CANCEL

[21] Review the settings details and click [BACK TO DASHBOARD].

Edit app registration

✓ OAuth consent screen — ✓ Scopes — ✓ Test users — 4 Summary

Authorized domains

Contact email addresses

Scopes [EDIT](#)

API ↑	Scope	User-facing description
No rows to display		

Test users [EDIT](#)

0 users (0 test, 0 other) / 100 user cap ?

Filter Enter property name or value ?

User information

No rows to display

BACK TO DASHBOARD

[22] The OAuth consent screen appears. Click [PUBLISH APP].

Google Cloud Platform My Project 49831 Search products and resources

APIs & Services OAuth consent screen Learn

OptimalBiz [EDIT APP](#)

Publishing status ?

Testing

PUBLISH APP

User type

External ?

[MAKE INTERNAL](#)

OAuth user cap ?

While publishing status is set to "Testing", only test users are able to access the app. Allowed user cap prior to app verification is 100, and is counted over the entire lifetime of the app. [Learn more](#)

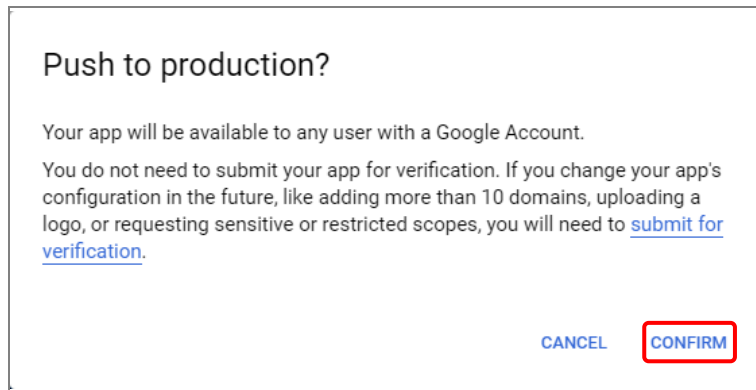
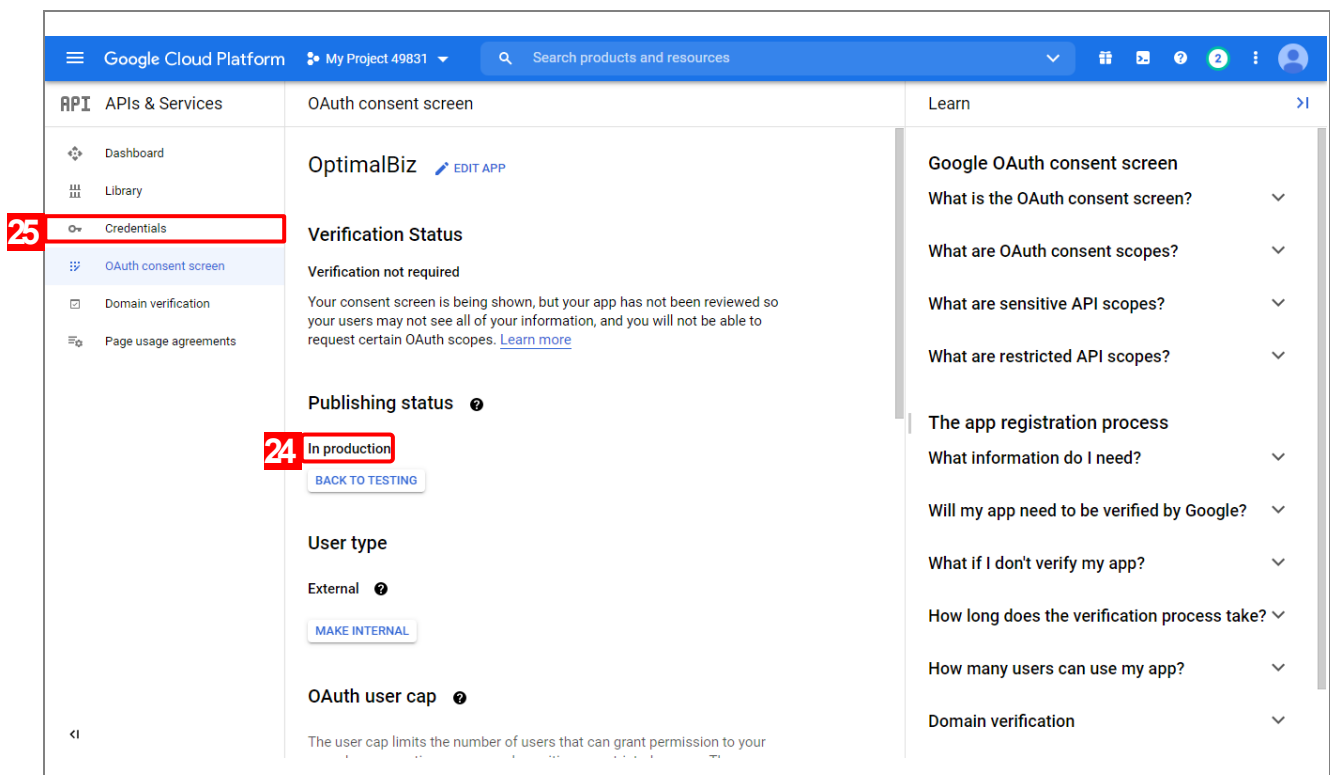
0 users (0 test, 0 other) / 100 user cap ?

Test users

[ADD USERS](#)

Google OAuth consent screen

- What is the OAuth consent screen? ▾
- What are OAuth consent scopes? ▾
- What are sensitive API scopes? ▾
- What are restricted API scopes? ▾
- The app registration process
- What information do I need? ▾
- Will my app need to be verified by Google? ▾
- What if I don't verify my app? ▾
- How long does the verification process take? ▾
- How many users can use my app? ▾
- Domain verification ▾

[23] Read the message and click [CONFIRM].**[24] Ensure that the publishing status is "In production".****[25] Click [Credentials].**

[26] Click [CREATE CREDENTIALS].

[27] Select "OAuth client ID".

The screenshot shows the Google Cloud IAM & Admin console. At the top, there's a 'Credentials' section with a '+ CREATE CREDENTIALS' button (highlighted with a red box and number 22) and a 'DELETE' button. Below this, there's a dropdown menu with four options: 'API key' (Identifies your project using a simple API key to check quota and access), 'OAuth client ID' (Requests user consent so your app can access the user's data, highlighted with a red box and number 23), 'Service account' (Enables server-to-server, app-level authentication using robot accounts), and 'Help me choose' (Asks a few questions to help you decide which type of credential to use). Below the dropdown, there are three sections: 'API Keys' (No API keys to display), 'OAuth 2.0 Client IDs' (No OAuth clients to display), and 'Service Accounts' (No service accounts to display). Each section has a table with columns for Name, Creation date, Type, Client ID, and Actions.

- [28]** Select "Web application" on the "Application type" pull-down menu.
- [29]** Enter an arbitrary name.
- [30]** Click [ADD URI] in "Authorized redirect URIs".

← Create OAuth client ID

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information. [Learn more](#) about OAuth client types.

28

Application type *
Web application

29

Name *
Web client 1

The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.

i

The domains of the URIs you add below will be automatically added to your [OAuth consent screen](#) as [authorized domains](#).

Authorized JavaScript origins ?

For use with requests from a browser

+ ADD URI

Authorized redirect URIs ?

For use with requests from a web server

URIs *

https://www.example.com

30

+ ADD URI

CREATE

CANCEL

97

[31] Enter `"https://biz3.optim.co.jp/company1/android_emm_zero_touch_auth/callback"` in "URI". (* Enter your company code in "company1".)

✎ If a warning message appears, make sure that you have entered an appropriate "Authorized domains" in step **[16]**.

[32] Click **[CREATE]**.

← Create OAuth client ID

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information. [Learn more](#) about OAuth client types.

Application type *
Web application

Name *
Web client 1

The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.

i The domains of the URIs you add below will be automatically added to your [OAuth consent screen](#) as [authorized domains](#).

Authorized JavaScript origins ?
For use with requests from a browser

+ ADD URI

Authorized redirect URIs ?
For use with requests from a web server

31 URIs *

+ ADD URI

32 **CREATE** CANCEL

【33】 Click [OK].

OAuth client created

The client ID and secret can always be accessed from Credentials in APIs & Services

i OAuth is limited to 100 [sensitive scope logins](#) until the [OAuth consent screen](#) is verified. This may require a verification process that can take several days.

Your Client ID

Your Client Secret

OK

[34] Click the download icon to download a JSON file.

Credentials

+ CREATE CREDENTIALS

DELETE

Create credentials to access your enabled APIs. [Learn more](#)

API Keys

☐

Name

Creation date ↓

Restrictions

Key

Actions

No API keys to display

OAuth 2.0 Client IDs

☐

Name

Creation date ↓

Type

Client ID

Actions

☐

Web client 1

Sep 6, 2021

Web application

Service Accounts

☐

Email

Name ↑

Actions

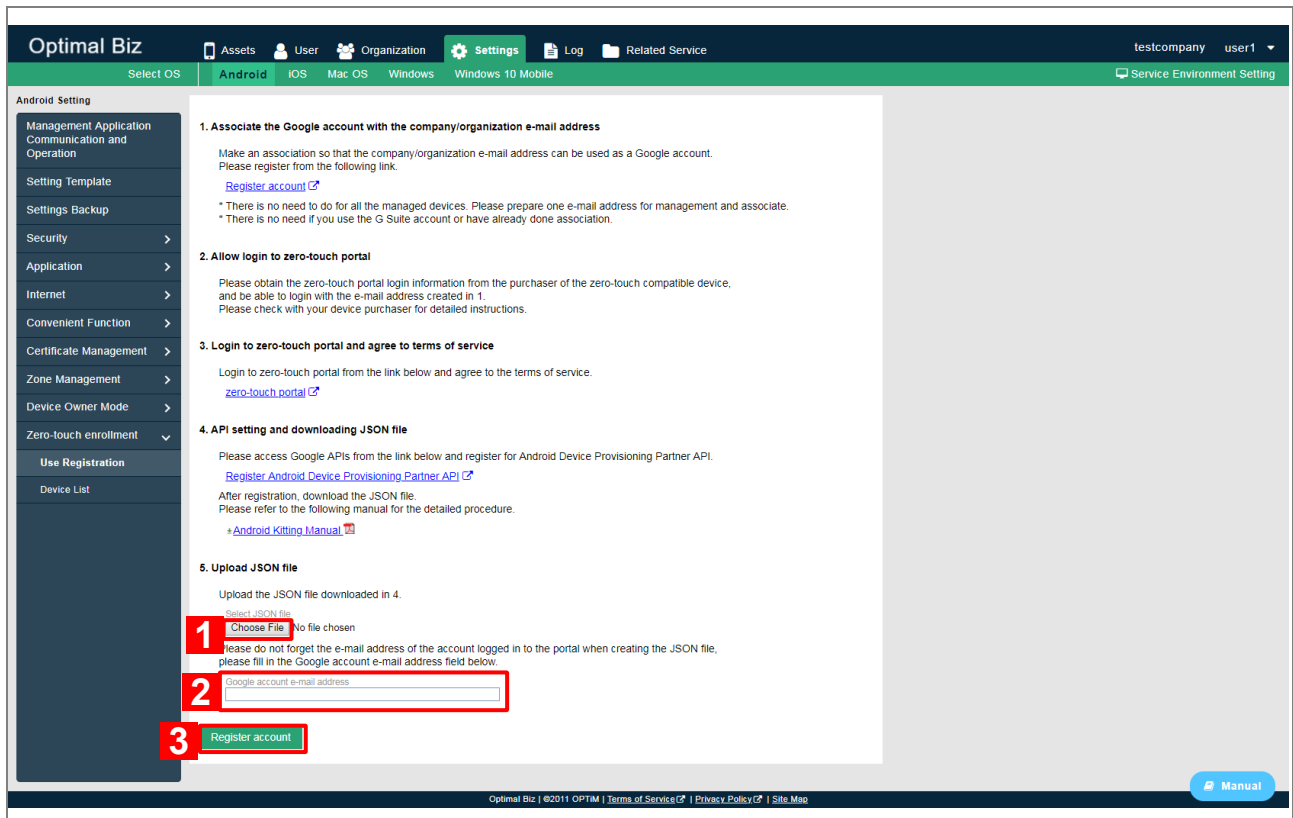
No service accounts to display

[Manage service accounts](#)

5.2.5 Uploading a JSON file

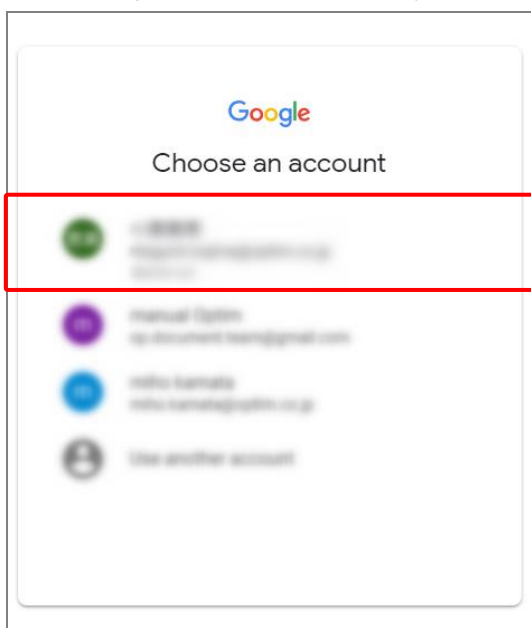
Upload the JSON file you downloaded with Google APIs to the management site and register device information.

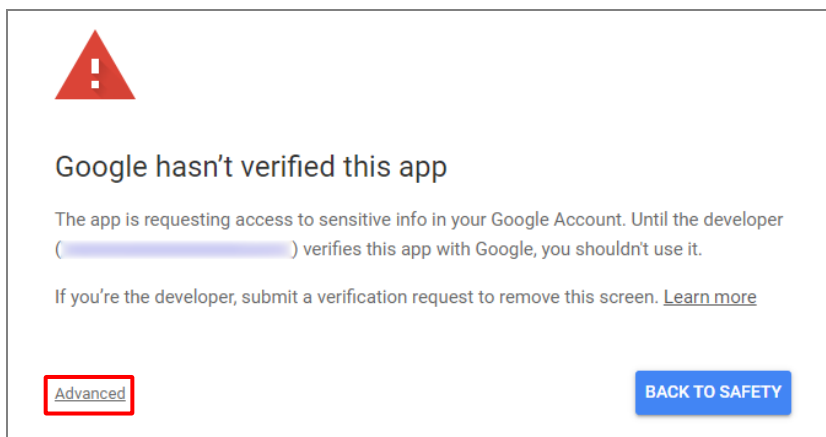
- [1]** Click [Choose File] and select the downloaded JSON file.
- [2]** Enter "Google account email address".
- [3]** Click [Register account].



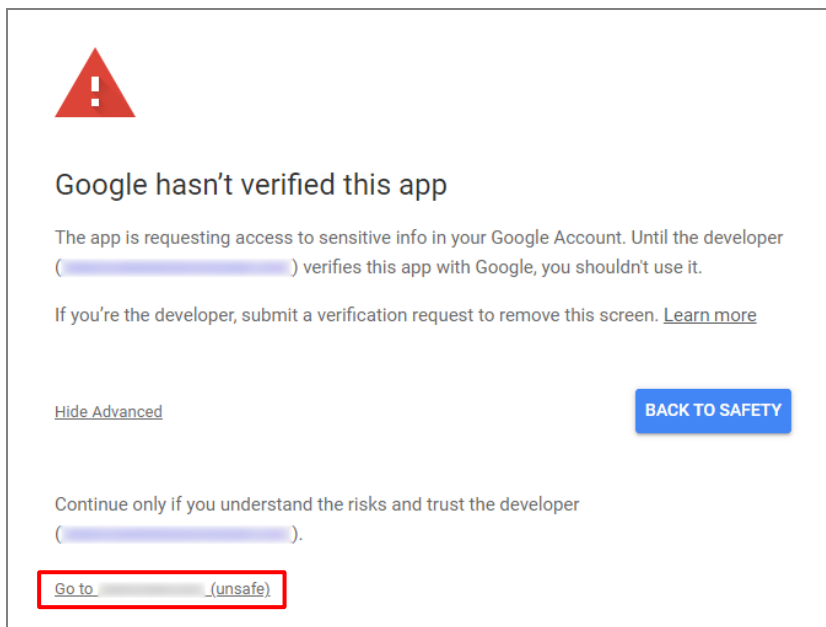
- [4]** The Google login screen appears. Select the Google account you registered.

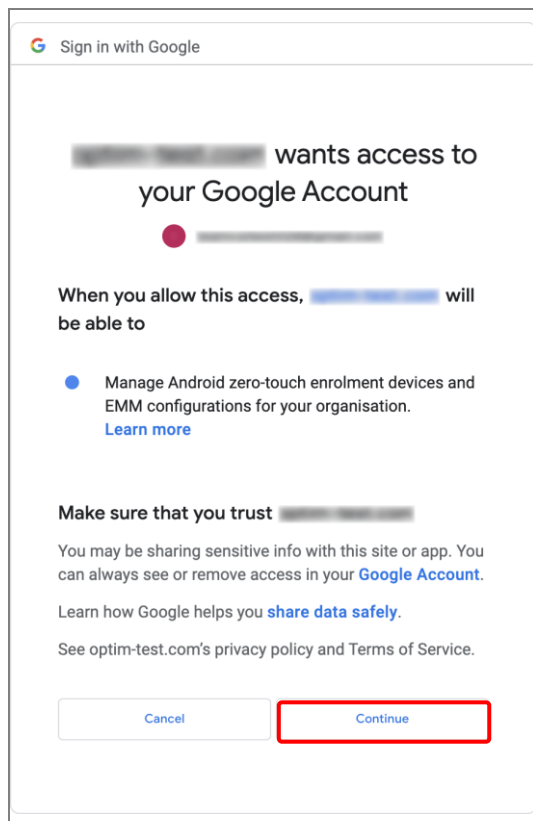
⇒ Warning window will be displayed.



[5] Click [Advanced].**[6] Click [Go to domain (unsafe)].**

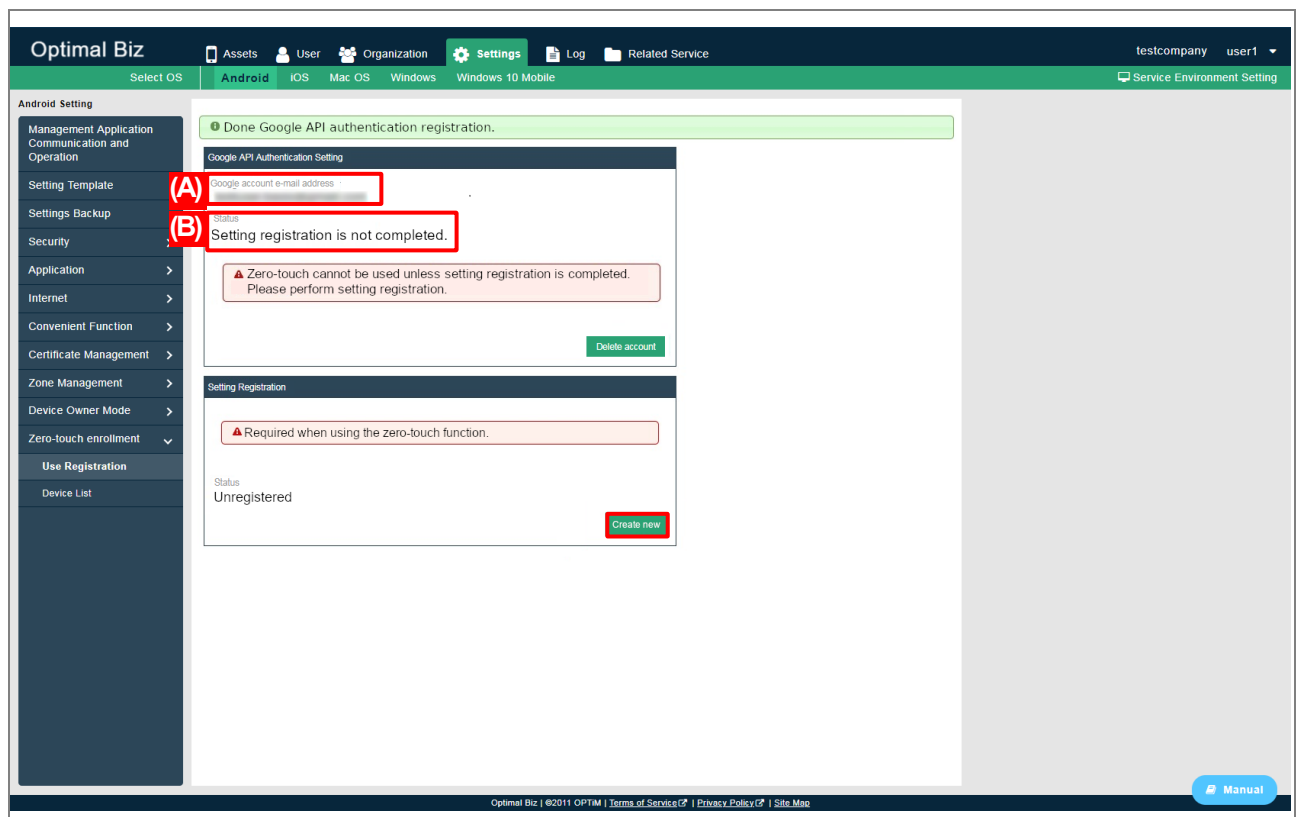
✎ If your Google account is "XXXXX@xxxxx.co.jp", "xxxxx.co.jp" is displayed for your domain.



[7] Click [Continue].**[8] Perform setting registration. Click [Create new].**

✎ If you do not register settings, you cannot sync zero-touch devices. "Status" (B) displays "Setting registration is not completed".

✎ "Google account email address" (A) displays the Google account you selected in step **[4]**.



[9] Click [Save].

- ✎ You cannot change "Customer Name" (A). "Support e-mail address", "Support phone number", and "Custom Message" (B) display the settings you entered during setting registration. Change them if necessary.

The screenshot displays the 'Optimal Biz' interface with the 'Settings' tab selected. The left sidebar lists various settings categories, including 'Zero-touch enrollment'. The main content area shows the 'Google API Authentication Setting' and 'Setting Registration' sections. The 'Setting Registration' section contains a form with the following fields:

- Customer Name** (A): A dropdown menu with a red box around it.
- Support e-mail address** (B): A text input field with a red box around it.
- Support phone number**: A text input field.
- Custom Message**: A text input field.

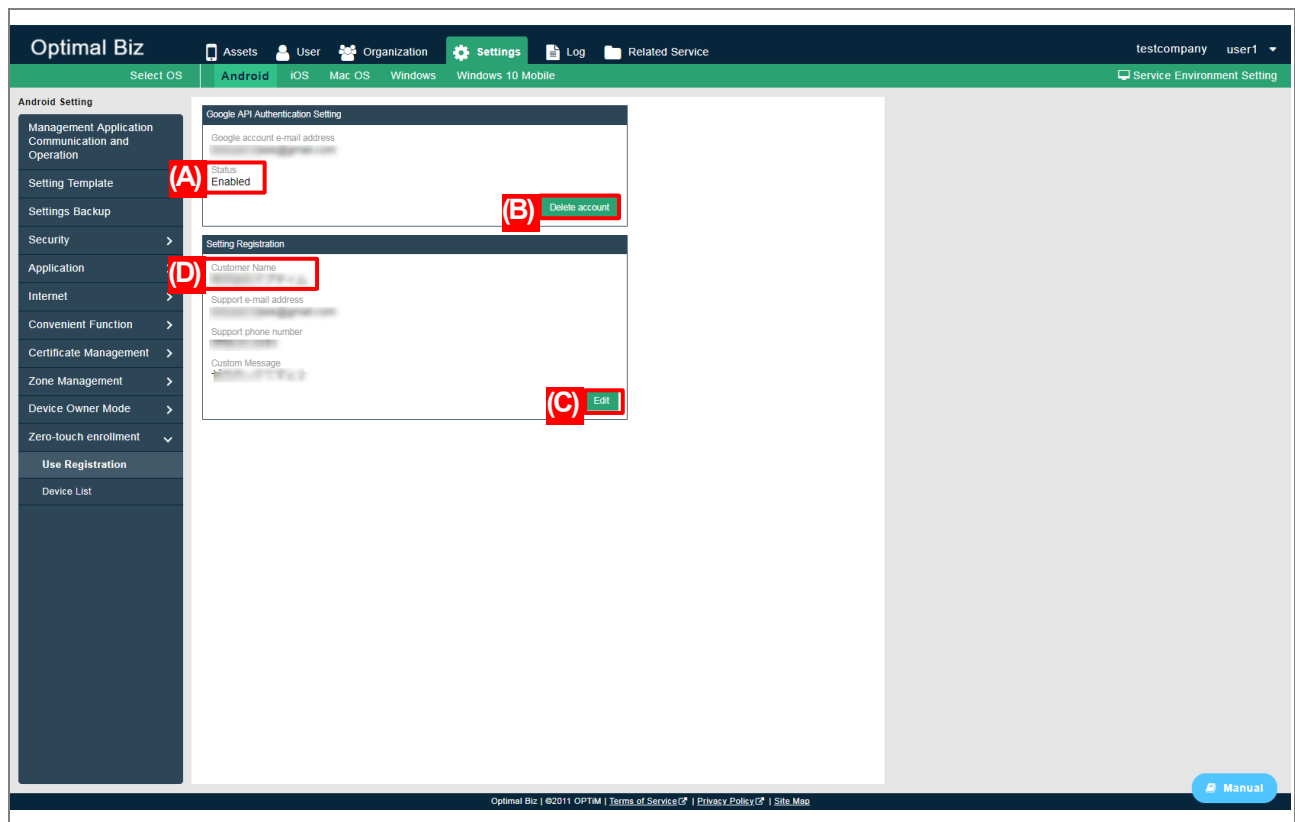
Below the form are 'Cancel' and 'Save' buttons. The 'Save' button is highlighted with a red box. A message at the top of the form states: 'Setting registration is not completed. Zero-touch cannot be used unless setting registration is completed. Please perform setting registration.' A 'Delete account' button is also visible.

[10] After the setting registration, the use registration screen appears as shown below.

⇒ The "Status" (A) shows "Enabled".

✎ If you want to delete your account, click [Delete account] (B).

✎ The settings you entered during setting registration are displayed. If you want to change the settings, click [Edit] (C). You cannot change "Customer Name" (D).

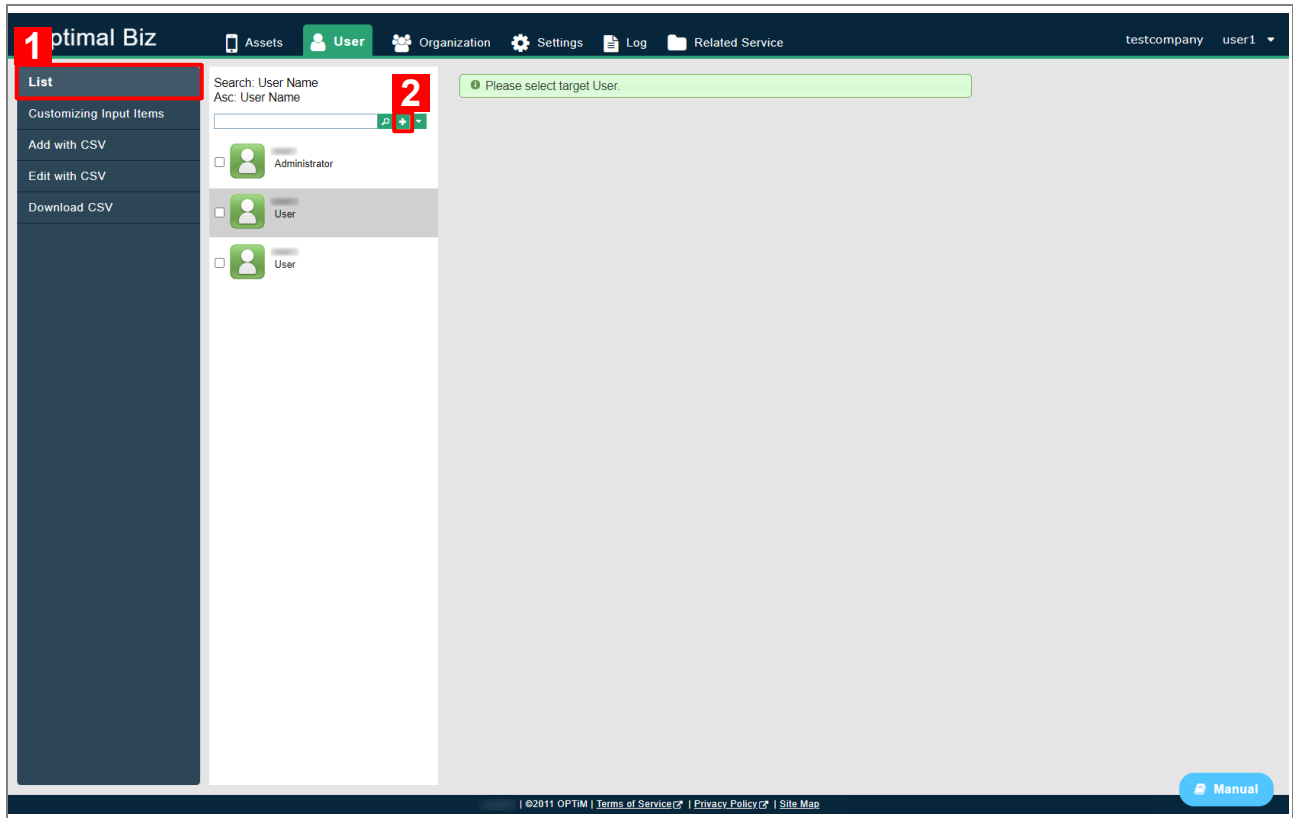


5.3 Creating a user

Follow the steps below to create a user.

[1] Click [User]→[List].

[2] Click .



[3] Enter an arbitrary name in "Name".

✎ For details of other input and setting items, refer to the following.

🔍 "User" - "List" - "Create a user" in <Management Site Reference Manual>

[4] Click [Save].

⇒ A user will be created.

The screenshot shows a web interface for managing users. At the top, there's a navigation bar with tabs: Admin, Apps and Books Setting, Access Control, Others, and Actions. The 'Admin' tab is selected. Below the navigation bar, there's a header for 'Management Information - Editing'. The main content area is divided into two columns. The left column contains various input fields: Name (highlighted with a red box and a red '3'), Phonetic Name, Last Name, First Name, User ID, E-mail Address, User Classification (with radio buttons for Administrator, Operator, Reader, Lock/Wipe only, Login only, and User), Organization (a dropdown menu), Category (a dropdown menu showing '(Uncategorized)'), and Device Authentication Limit (with radio buttons for No Restriction, Restricted, and Prohibit authentication). The right column contains a Password section with a Current Password field and an Edit button, an Assets section showing the Number of Devices as 0, and a SaaS ID Federation section showing Office 365 and G Suite as (None). At the bottom of the form, there are Cancel and Save buttons. The Save button is highlighted with a red box and a red '4'.

5.4 Performing kitting with zero-touch registration (using a Google account)

Follow the steps below to perform kitting for your device by means of zero-touch registration.

Note that the operation is different between Android versions earlier than 10 and versions 10 or later. Depending on the Android version of your device, choose one of the following methods.

● **For less than Android 10**

● **For Android 10 or later**

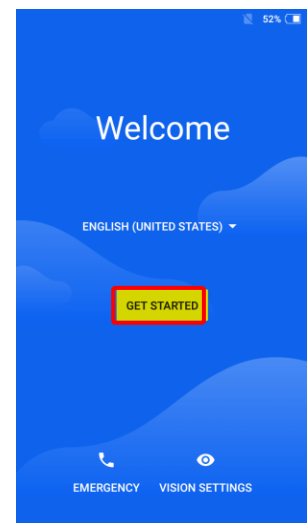
- ☑ When you are kitting Android 10 or later, kitting operation may not be able to complete if you have set Google Play Developer Services (com.google.android.gms) on the management site's "Application prohibition" blacklist and "Non-display application". Refer to the following to clear the setting in advance and then conduct kitting.

🔍 "Settings – Android" - "Application" - "Application prohibition" in <Management Site Reference Manual>

🔍 "Settings – Android" - "Device Owner Mode" - "Non-display application" in <Management Site Reference Manual>

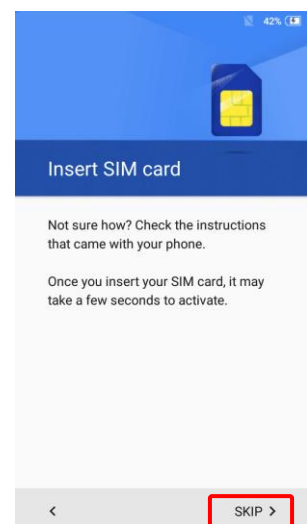
5.4.1 For less than Android 10

[1] Tap [GET STARTED].

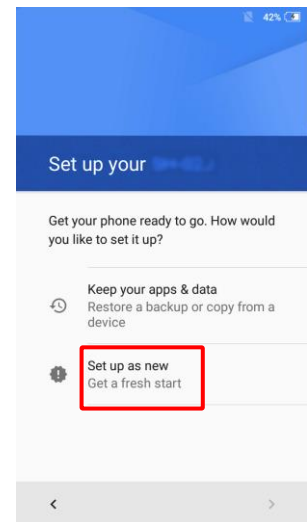


[2] Tap [SKIP].

- ☑ If a SIM card is already inserted, this screen does not appear.



[3] Tap [Set up as new].

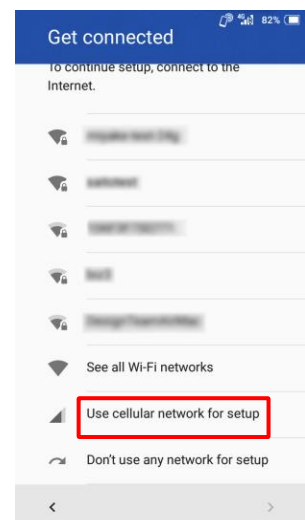


[4] Tap [Use cellular network for setup] or tap a Wi-Fi SSID to connect to Wi-Fi.

- ☑ Be sure to select a cellular network or available Wi-Fi. If you select "Don't use any network for setup" or "Skip", you will not be able to perform proper kitting. Doing so will require you to perform initialization.
- ☑ The wording displayed on the screen may vary depending on the device.

<<If you do not have a SIM>>

[Use cellular network for setup] will not be displayed, so connect to Wi-Fi.

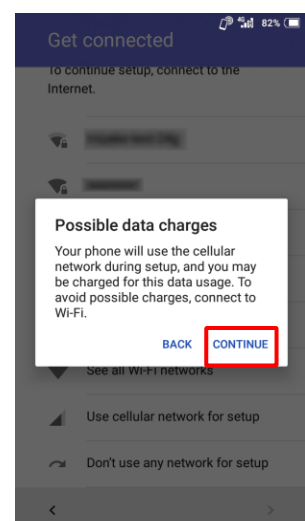


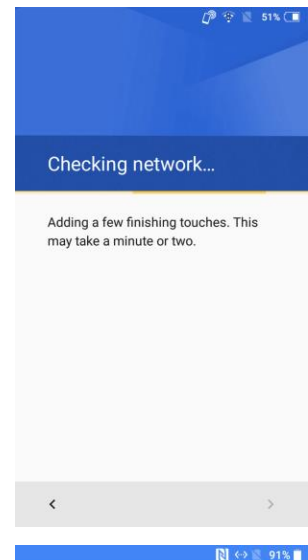
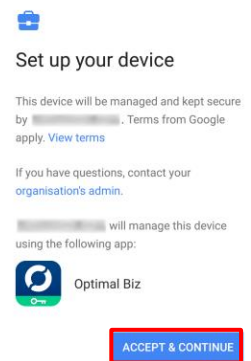
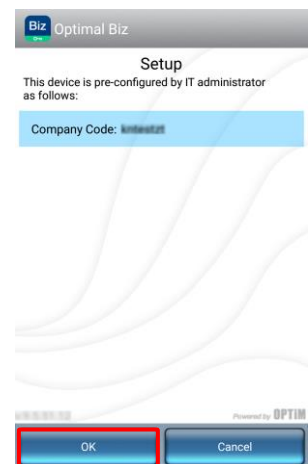
<<If you use a cellular network>>

When a pop-up appears as shown on the screen on the right, tap [CONTINUE].

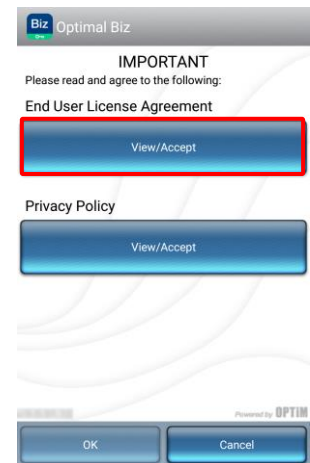
<<If you use a Wi-Fi connection>>

Continue with the next step.



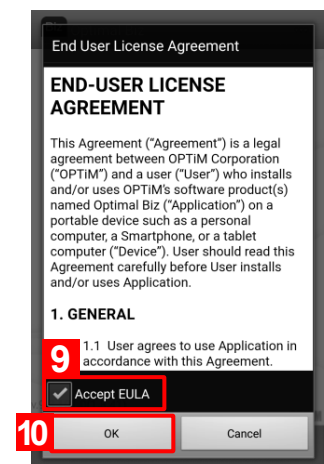
[5] Network connection starts.**[6] Tap [ACCEPT & CONTINUE].****[7] Tap [OK].**

[8] Tap [View/Accept] for the End User License Agreement.

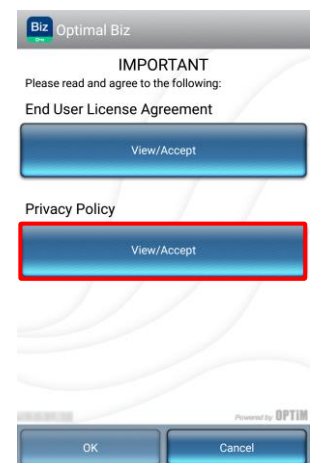


[9] Check "Accept EULA".

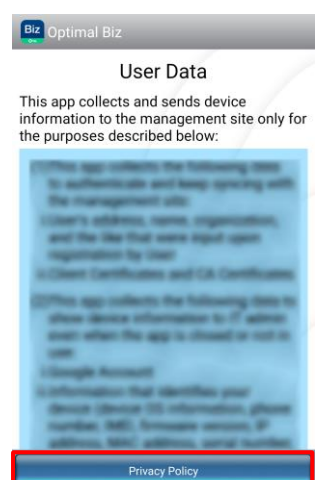
[10] Tap [OK].



[11] Tap [View/Accept] for the Privacy Policy.



[12] Read the user data policy, and tap [Privacy Policy].




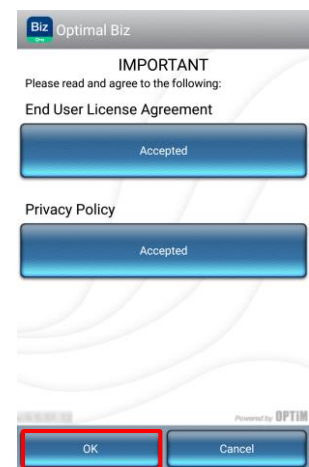
[13] Check "I agree to the privacy policy".

[14] Tap [OK].



[15] Tap [OK].

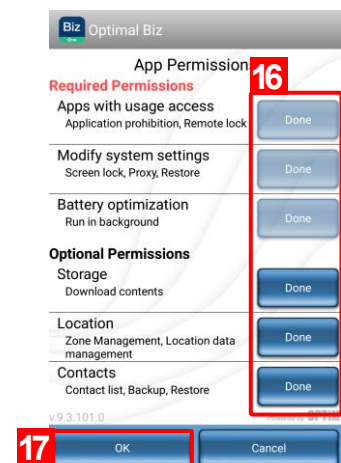
 You cannot tap [OK] unless you agree to both the EULA and privacy policy.



[16] A screen that requests permission appears. Follow the on-screen instructions to set things up.

[17] Tap [OK].

⇒ The license authentication screen appears. Continue with the license authentication.

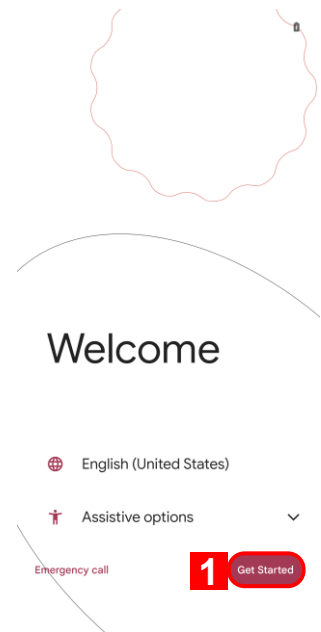
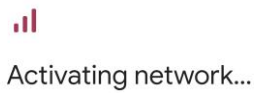


5.4.2 For Android 10 or later

[1] Tap [Get Started].

« If you are inserting SIM »

The following screen is displayed.



[2] Tap [Skip].

« If using a mobile network »

Insert a SIM if it is not already inserted.

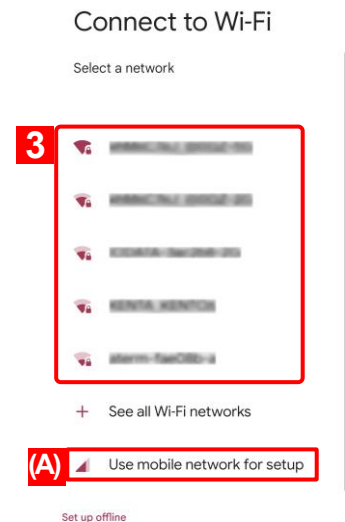
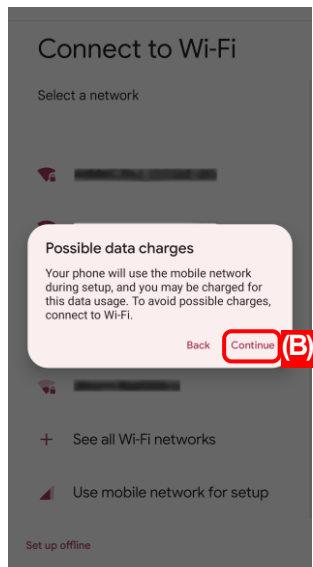


[3] Tap a Wi-Fi SSID to connect to Wi-Fi.

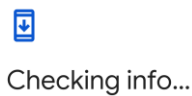
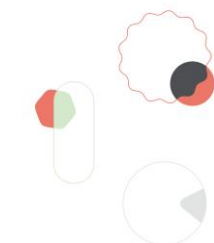
« If using a mobile network »

Tap [Use mobile network for setup] (A).

Tap [Continue] (B) when a following pop-up is displayed.



⇒ The network connection starts and checking information.



[4] Tap [Next].

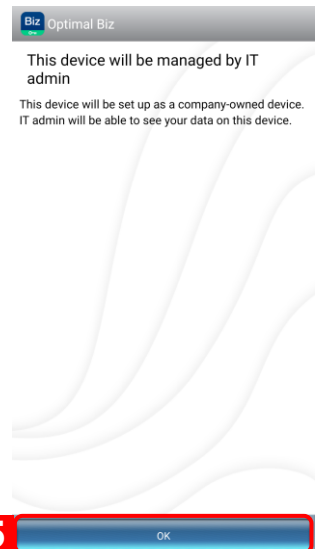
⇒ Getting ready for work setup.

Getting ready for
work setup...This device belongs
to your organization

To learn more, contact your IT admin.

4

Next

[5] Tap [OK].**5**

OK

[6] Tap [Accept & Conetinue].

⇒ Setting up in the device.

Keep your work apps
at your fingertipsLet's set up your
work device[View terms](#)**6**

Accept & continue

Setting up your device...

[7] Tap [Next].**This device isn't private****Your activity & data**


Your IT admin may be able to see your data and activity on this device.

**App permissions**

Your IT admin can set permissions for apps on this device, such as microphone, camera, and location permissions.

Cancel setup

**[8] Tap [More].**

 [More] is displayed several times on some devices. Tap [More] until [Accept] is displayed.

**Google Services**

Tap to learn more about each service, such as how to turn it on or off later. Data will be used according to Google's [Privacy Policy](#).

Location**Use location**

Allow apps and services with location permission to use your device's location. Google may collect location data periodically and use this data in an anonymous way to improve location accuracy and location-based services.

Allow scanning

Allow apps and services to scan for Wi-Fi

**[9] Tap [Accept].**

Allow apps and services to scan for Wi-Fi networks and nearby devices at any time, even when Wi-Fi or Bluetooth is off.

Device maintenance**Send usage and diagnostic data**

Help improve your Android device experience by automatically sending diagnostic, device, and app usage data to Google. This will help battery life, system and app stability, and other improvements. Some aggregate data will also help Google apps and partners, such as Android developers. If your additional Web & App Activity setting is turned on, this data may be saved to your Google Account.

Install updates & apps

By continuing, you agree that this device may also automatically download and install updates and apps from Google, your carrier, and your device's manufacturer, possibly using cellular data. Data rates may apply. Some of these apps may offer in-app purchases.

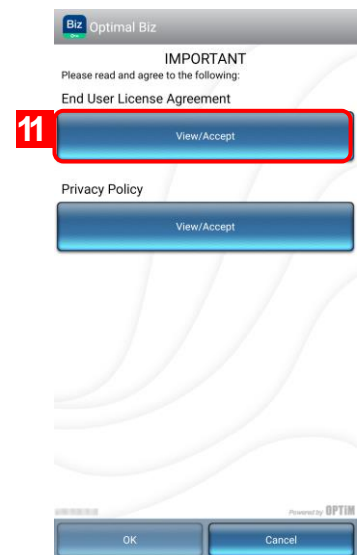
Tap "Accept" to confirm your selection of these Google services settings.



[10] Tap [OK].

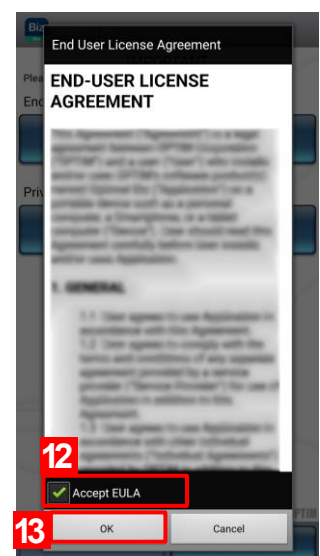


[11] Tap [View/Accept] for the End User License Agreement.

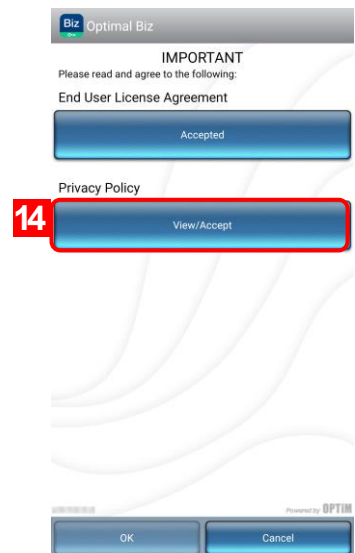


[12] Check "Accept EULA".

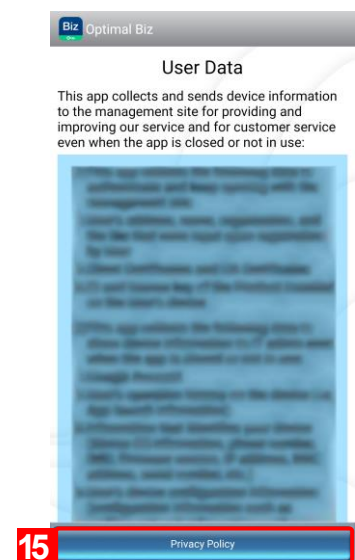
[13] Tap [OK].



【14】 Tap [View/Accept] for the Privacy Policy.

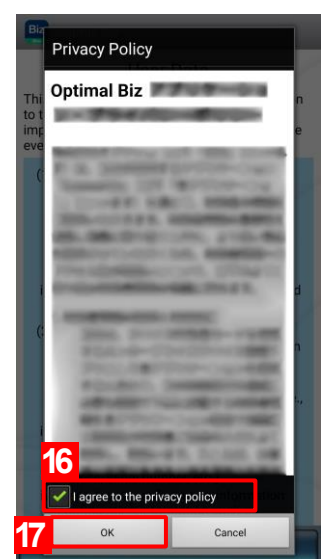


【15】 Read the user data policy, and tap [Privacy Policy].

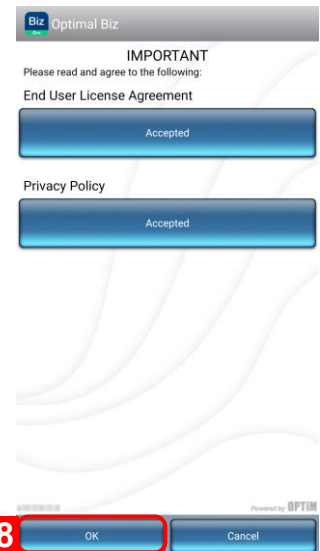


【16】 Check "I agree to the privacy policy".

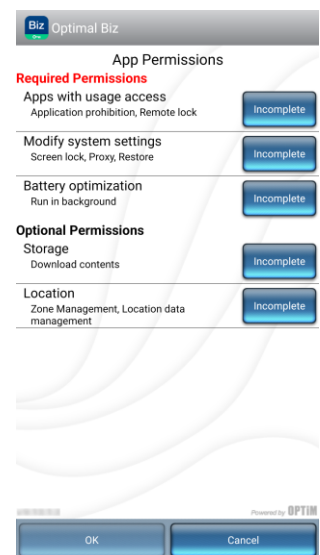
【17】 Tap [OK].



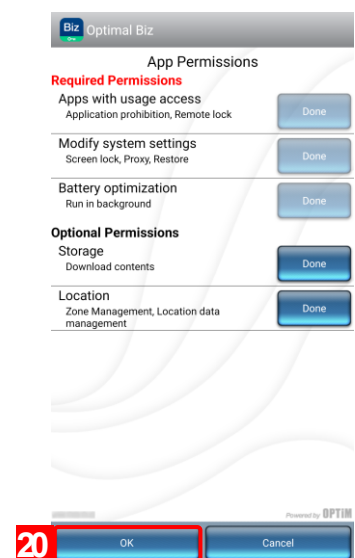
[18] Tap [OK].



[19] A screen that requests permission appears. Follow the on-screen instructions to set things up.



[20] Tap [OK].



[21] Enter an "Authentication Code".

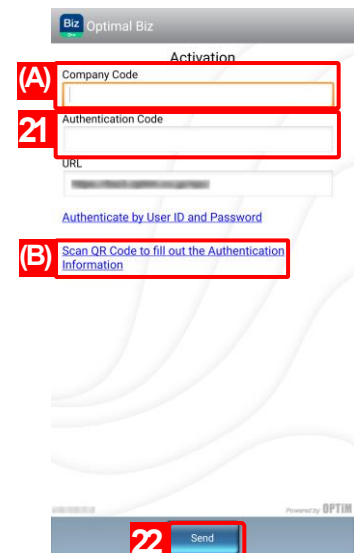
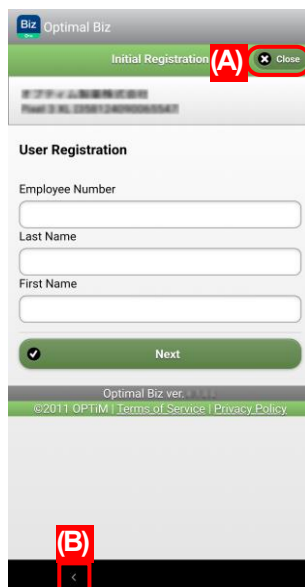
- ✔ Contact your administrator for your authentication code.
- ✎ "Company Code" (A) will be entered automatically.
- ✎ If you tap [Scan QR Code to fill out the Authentication information] (B) and scan a QR code for agent license activation, the "Company code", "Authentication code", and "URL" will be automatically entered. Contact your administrator for the QR code.

[22] Tap [Send].**[23] The license authentication completion screen appears. Tap [OK].**

« When portal settings are set to be displayed on Management Site »

After you tap [OK], initial registration screen appears.
Enter items as necessary.

- ✔ The user will link to the device if the initial registration has been made.
- ✔ If you do not need to register, you can either tap [Close] (A) or (B) the back button on the device to close the screen.
- ✔ If the user is already linked to the device, a message will appear and say that the user has been linked. Close the screen.



[24] Tap [Skip].

⇒ Kitting is complete.

License authentication is also complete. Proceed to "Allocating a user to your device".

☞ "Allocating a user to your device" Page 125



All set!

You're ready to start using your phone



Swipe to navigate
your phone

Learn gestures to go Home, go back, and
switch apps



Skip

Try it

System navigation settings

Swipe up to go Home



5.5 Performing license authentication

After kitting is complete, perform license authentication with your User ID or company code / authentication code.

✍ If you are using Android Enterprise after you perform license authentication with the user ID registered from the management site, it will be integrated with Android Enterprise.

If you have not registered your user ID, the user ID can be integrated with Android Enterprise by performing a license authentication with a company code / authentication code, registering the user ID from the management site, and linking it with your device.

✍ Android 10 or later are license authenticated by kitting, so this operation is not necessary. Proceed to the next operation.

👉 "Allocating a user to your device" Page 125

5.5.1 Authenticating by a user ID

[1] Tap [Authenticate with User ID and Password].

✍ "Company Code" (A) will be entered automatically.

[2] Enter "User ID or Email Address" and "Password".

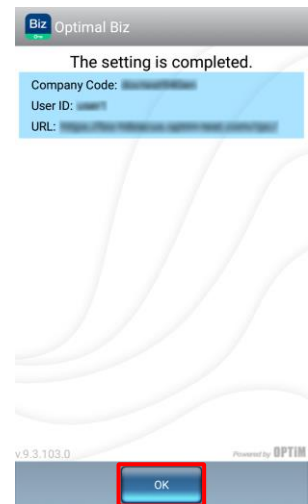
✍ If a user has been assigned to the device, "User ID or email address" will be entered automatically.

✍ Contact your administrator for your user ID and password.

✍ You do not have to change the URL (A).

[3] Tap [Send].

- [4] The license authentication completion screen appears. Tap [OK].**



- [5] The agent menu screen appears.**

- ✓ After license authentication, users cannot interact with the agent screen until the initial synchronization is complete at the management site.



5.5.2 Authenticating by a company code / authentication code

✍ After license authentication is complete, allocate a user to the device on the management site.

🔍 "Asset" - "List" - "Asset management information" in <Management Site Reference Manual>

[1] Enter an "Authentication Code".

- ✍ Contact your administrator for your authentication code.
- ✍ "Company Code" (A) will be entered automatically.
- ✍ If you tap [Scan QR Code to fill out the Authentication information] (B) and scan a QR code for agent license activation, the "Company code", "Authentication code", and "URL" will be automatically entered. Contact your administrator for the QR code.

[2] Tap [Send].

[3] The license authentication completion screen appears. Tap [OK].

« When portal settings are set to be displayed on Management Site »

After you tap [OK], initial registration screen appears.
Enter items as necessary.

- ✍ The user will link to the device if the initial registration has been made.
- ✍ If you do not need to register, you can either tap [Close] (A) or (B) the back button on the device to close the screen.
- ✍ If the user is already linked to the device, a message will appear and say that the user has been linked. Close the screen.

[4] The agent menu screen appears.

- ✓ After license authentication, users cannot interact with the agent screen until the initial synchronization is complete at the management site.



5.6 Allocating a user to your device

Follow the steps below to allocate the user created in "Creating a user" to a target device.

- [1]** Go to [Assets]→[List], and select a target device from the list.
- [2]** Click [Edit admin information].

The screenshot displays the 'Optimal Biz' web application interface. The top navigation bar includes 'Assets', 'User', 'Organization', 'Settings', 'Log', and 'Related Service'. The left sidebar contains a 'List' menu with options like 'Network Map', 'Authentication Procedure', and 'Download CSV'. The main content area is titled 'Assets' and features a search bar and a table of 14 devices. A red box labeled '1' highlights a row in the table. The right sidebar shows user details and a red box labeled '2' highlights the 'Edit admin information' button.

Asset Name	OS	Phone Number	User	Organization	Communication Date	Details
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	about 2 years ago	[Details]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	27 days ago	[Details]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	19 days ago	[Details]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	about 4 years ago	[Details]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	about 1 month ago	[Details]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	about 1 hour ago	[Details]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	for over 2 years ago	[Details]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	almost 2 years ago	[Details]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	almost 2 years ago	[Details]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	about 1 year ago	[Details]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	for over a year ago	[Details]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	about 2 years ago	[Details]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	about 1 year ago	[Details]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	almost 2 years ago	[Details]

Right sidebar details:

- Communication Date: 27 Aug 2021 09:11:59
- OS: [Redacted]
- Phone Number: [Redacted]
- User: [Redacted]
- Organization: [Redacted]
- Note: [Redacted]
- Edit admin information** (Highlighted)
- Settings:
 - Setting Allocation
 - Setting Template Allocation
 - Show other settings
- Actions:
 - Change screen lock password
 - Remote Lock
 - Show other operations
- Information:
 - Logs

- [3]** Select "User" in "Division" and specify the user selected in Creating a user from the pull-down menu.
- [4]** Click [Save].

The screenshot shows the Optimal Biz interface. On the left is a sidebar with navigation options like 'List', 'Network Map', 'Authentication Procedure', etc. The main area is titled 'Assets' and contains a table with 14 devices. The table columns are Asset Name, OS, Phone Number, User, Organization, and Communication Date. One row is highlighted in orange. On the right, the 'Management Information' panel is open, showing fields for Asset Name, Division (set to 'User'), Organization, and Note. A red box labeled '3' points to the 'Division' dropdown, and another red box labeled '4' points to the 'Save' button.

- [5]** Click [Sync].
- [6]** Click [OK].

⇒ The user will be allocated to the device.

This screenshot shows the same interface as the previous one, but with a sync process initiated. A dialog box is open in the center with the text 'Sync will start. Depending on device, it may take significant amount of time until the setting is applied. Click on [OK] button to proceed.' and buttons for 'OK' and 'Cancel'. A red box labeled '6' points to the 'OK' button. In the 'Management Information' panel on the right, a red box labeled '5' points to the 'Sync' button. The 'Sync' button is highlighted with a green border.

5.7 Syncing with the zero-touch registration server

Follow the steps below to sync with the zero-touch registration server and display device information on the management site.

- ✎ If each function setting has been registered, the function will be allocated to the device at the same time as kitting. To perform settings for functions, refer to the following.

🔍 "Settings - Android" in <Management Site Reference Manual>

[1] Click [Settings]→[Android]→[Zero-touch enrollment]→[Device List].

[2] Click [Sync with the zero-touch enrollment server].

- ✎ The zero-touch devices displayed in the zero-touch device list are displayed as devices waiting for license authentication in the device list of Device List.

🔍 "Asset" - "List" "Asset list" in <Management Site Reference Manual>

- ✎ Devices cannot be deleted from the zero-touch device list. Delete them from the device list of the device screen. If you delete a device from the device list of the device screen, it is also deleted from the zero-touch device list.

🔍 "Asset" - "List" - "Deleting asset individually" in <Management Site Reference Manual>

- ✎ Do not create a new zero-touch device from the device screen.

- ✎ Clicking [IMEI/Serial Number] (A) displays the device list of the device screen.

The screenshot shows the Optimal Biz management interface. The top navigation bar includes 'Assets', 'User', 'Organization', 'Settings', 'Log', and 'Related Service'. The 'Settings' tab is active, and the 'Android' sub-tab is selected. The left sidebar shows the 'Device List' option under the 'Zero-touch enrollment' category, marked with a red box and the number '1'. The main content area displays a table of zero-touch enrollment settings, with the 'Sync with the zero-touch enrollment server' button marked with a red box and the number '2'. A red box labeled '(A)' highlights the 'IMEI/Serial Number' column header. The table contains five rows of data, all with update and sync dates of 14 Nov 2018 17:15.

IMEI/Serial Number	User Name	Manufacturer	Update Date/Time of zero-touch enrollment setting	Sync Date/Time of zero-touch enrollment setting
			14 Nov 2018 17:15	14 Nov 2018 17:15
			14 Nov 2018 13:33	14 Nov 2018 17:15
			14 Nov 2018 13:33	14 Nov 2018 17:15
			14 Nov 2018 13:33	14 Nov 2018 17:15

6 Integrating with Android Enterprise by a Google Workspace (formerly G Suite) account using zero-touch enrollment

Zero-touch enrollment is one of the methods for kitting an agent. This method reduces the kitting procedure, making it easier and faster to introduce many devices. Zero-touch enrolled devices automatically install an agent as Device Owner Mode, enabling more secure device management.

By integrating a zero-touch server, the list of devices in this product will automatically display your device as a pre-kitting device. If you allocate a setting policy to a pre-kitting device and activate it, the settings will apply immediately.

This chapter describes the following items.

Item	Page
Issuing a token *	129
Registering a Google Workspace (formerly G Suite) account *	136
Performing authentication settings of Google API	138
Creating a user	163
Performing kitting with zero-touch enrollment (using a Google Workspace (formerly G Suite) account)	167
Performing license authentication	185
Syncing with the zero-touch registration server	189



Attention

- For details of zero-touch enrollment, refer to the following.
https://www.android.com/intl/ja_jp/enterprise/management/zero-touch/
- For accounts exclusively for zero-touch enrollment, contact your zero-touch device vendor.
- The items marked with * above are required only for the first kitting.



Reference

- By setting up the "Application Distribution" function of Android Enterprise on the management site in advance, apps can be distributed to your device at the same time as license authentication after kitting is complete. For details of on app distribution, refer to the following.



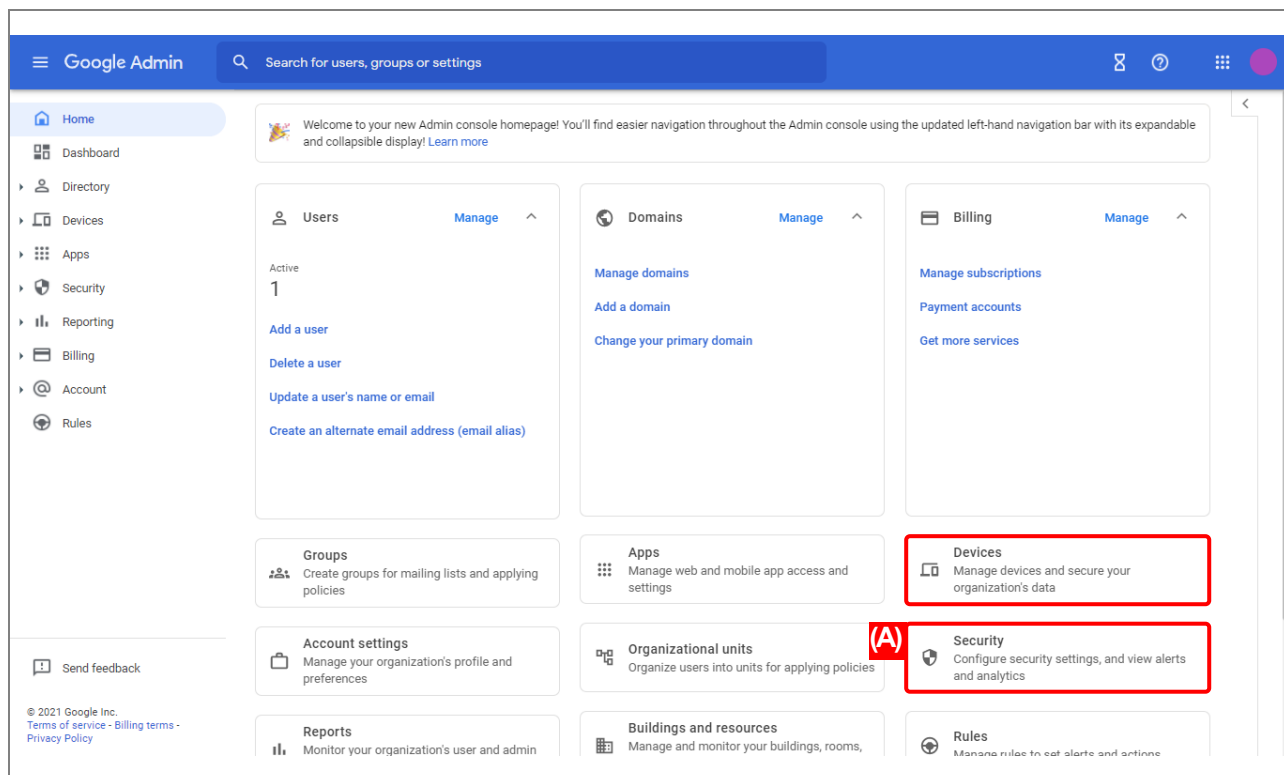
"Android Enterprise App distribution" in <Android Enterprise Manual>

6.1 Issuing a token

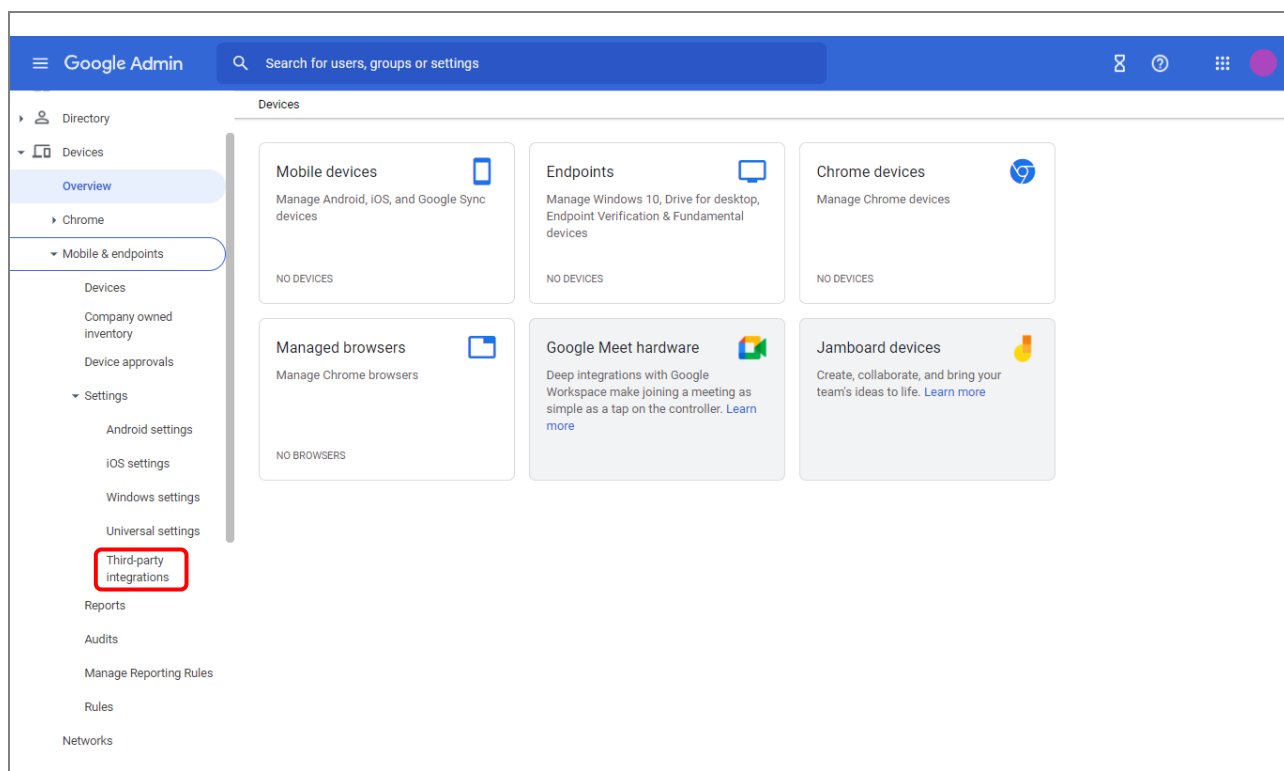
Follow the steps below to integrate this product with Google by using a Google Workspace (formerly G Suite) account.

[1] Go to the Google Admin console <https://admin.google.com> and click [Devices].

(A) If [Security] shows "EMM provider management for Android", steps [5] to [11] are not required.



[2] Click [Settings]→[Third-party integrations].



[3] Uncheck "Enable third-party Android mobile management" in "Android EMM".

[4] Click [SAVE].

Android EMM
Applied at 'gdoctest001.optim-test.xyz'

Third-party Android mobile management

When you add a third-party EMM provider, you can't manage Android apps through Google endpoint management. You must manage them through the EMM provider. [Learn more](#)

3 ☐ Enable third-party Android mobile management

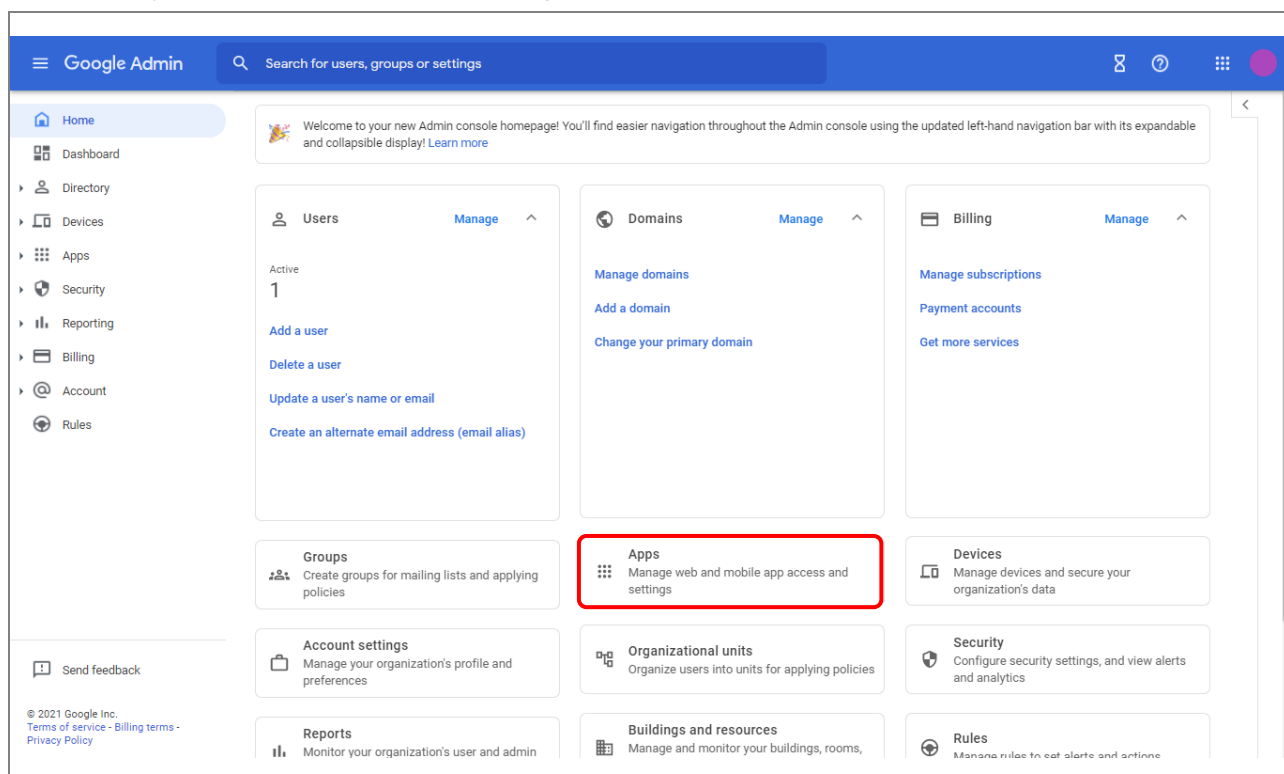
No EMM added [Add EMM provider](#)

4 **SAVE**

CANCEL

[5] Click [Apps].

To display the Admin console, click [Google Admin] in the upper left corner of the screen.



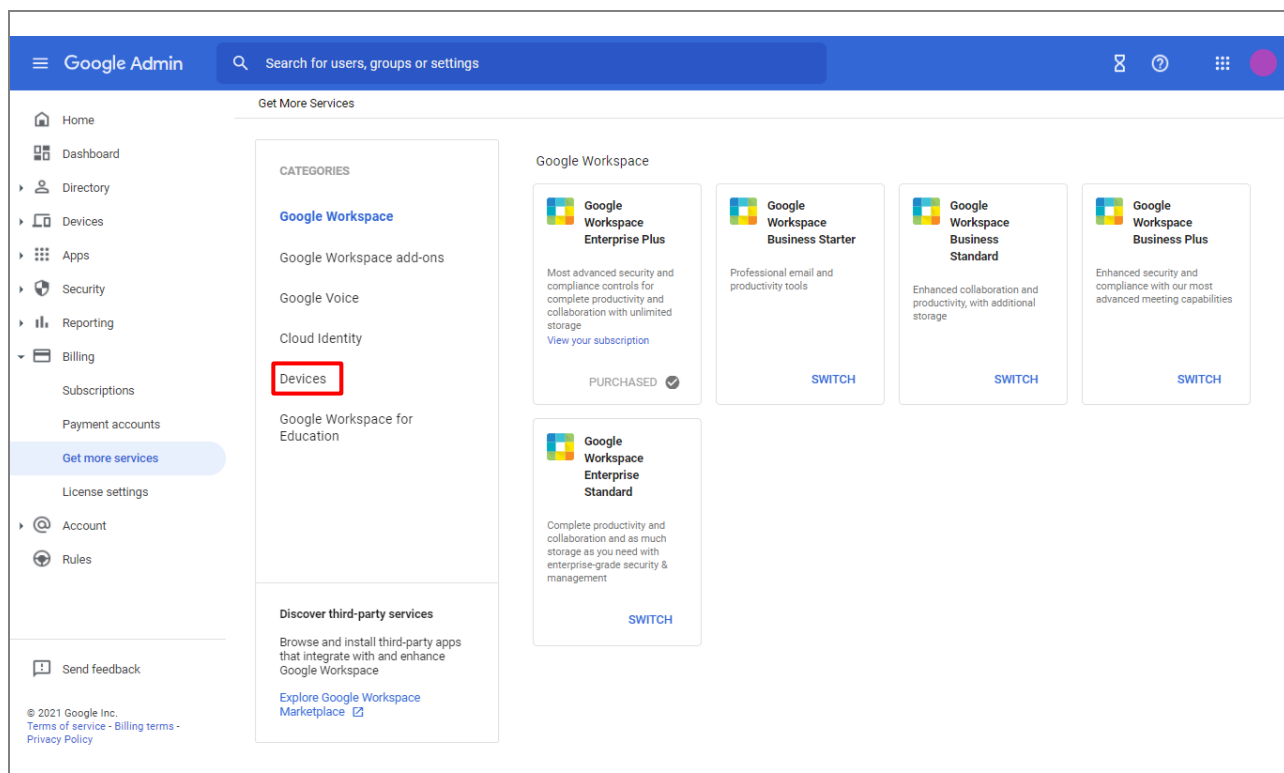
[6] Click [Google Workspace].


The screenshot shows the Google Admin console interface. On the left is a navigation menu with categories like Directory, Devices, Apps, Security, Reporting, Billing, Account, and Rules. The 'Apps' section is selected, and the 'Overview' sub-section is active. The main content area displays several service cards. The 'Google Workspace' card is highlighted with a red rectangular box. It features the Google Workspace logo, the text 'Google Workspace Core services', and '14 SERVICES'. Other visible cards include 'Additional Google services' (59 SERVICES), 'Web and mobile apps' (NO APPS), 'Google Workspace Marketplace apps' (NO SERVICES, with a 'MANAGE' button), 'LDAP' (NO CLIENTS), and 'Password vaulted apps' (NO SERVICES). At the bottom, there is a disclaimer: 'Google Workspace core services are governed by your Google Workspace agreement. Additional Google services are not governed by your Google Workspace agreement, and other terms apply. Learn more.'

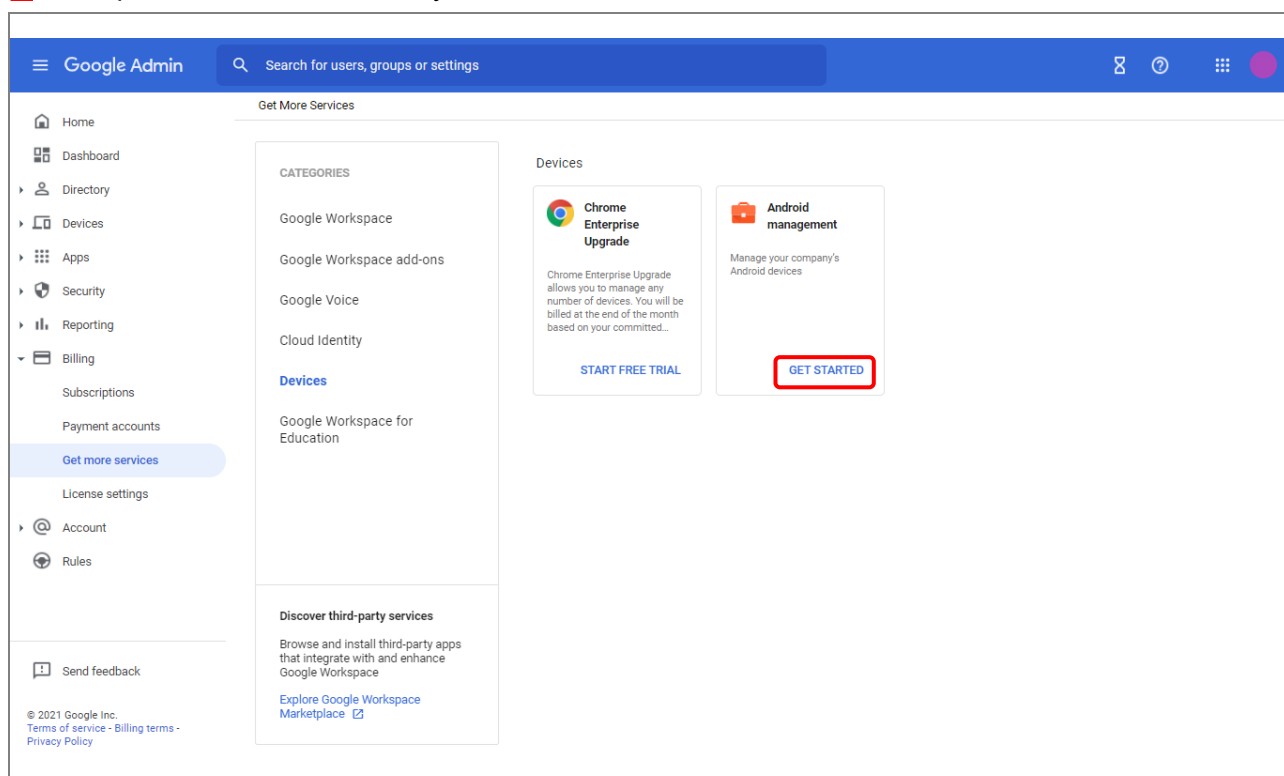
[7] Click [ADD SERVICES].

The screenshot shows the Google Admin console interface, specifically the 'Google Workspace' service status page. The left navigation menu is expanded, showing 'Apps' > 'Google Workspace' > 'Service status'. The main content area is titled 'Showing status for apps in all organizational units'. A red box highlights the 'ADD SERVICES' button in the top right corner. Below this, there is a table listing various Google Workspace services and their status. The table has two columns: 'Services' and 'Service Status'. All services listed are 'ON for everyone'. The services include Calendar, Cloud Search, Currents, Drive and Docs, Gmail, Google Chat and classic Hangouts, Google Meet, Google Vault, Groups for Business, Jamboard, Keep, Sites, and Work Insights. At the bottom right, there is a 'Page 1 of 1' indicator and a 'Rows per page: 50' dropdown menu.

Services	Service Status
<input type="checkbox"/> Calendar	ON for everyone
<input type="checkbox"/> Cloud Search	ON for everyone
<input type="checkbox"/> Currents	ON for everyone
<input type="checkbox"/> Drive and Docs	ON for everyone
<input type="checkbox"/> Gmail	ON for everyone
<input type="checkbox"/> Google Chat and classic Hangouts	ON for everyone
<input type="checkbox"/> Google Meet	ON for everyone
<input type="checkbox"/> Google Vault	ON for everyone
<input type="checkbox"/> Groups for Business	ON for everyone
<input type="checkbox"/> Jamboard	ON for everyone
<input type="checkbox"/> Keep	ON for everyone
<input type="checkbox"/> Sites	ON for everyone

[8] Click [Devices].**[9] Click [GET STARTED] in "Android management".**

 This operation will not cause any costs to be incurred.



【10】 Click [CHECKOUT].

× Add a new subscription ?

1 Payment plan — 2 Checkout

Android management
Manage your company's Android devices

Country
Japan

Currency
JPY

Review your payment plan

Free plan

- Free edition, no payment needed

Any applicable taxes and discounts will be applied on your monthly invoice. Prices exclude applicable taxes and VAT (varies based on your country). [Learn more](#)

By clicking **Checkout**, you agree to the [Managed Google Play](#) and [Cloud Identity](#) agreement. Notwithstanding anything to the contrary, any previous purchase of any Services will also be subject to the above terms and these terms will supersede any previous terms agreed to upon by the Customer and Google for any Services.

CHECKOUT

【11】 Click [PLACE ORDER].

⇒ The Admin console will appear.

× Add a new subscription ?

✓ Payment plan — 2 Checkout

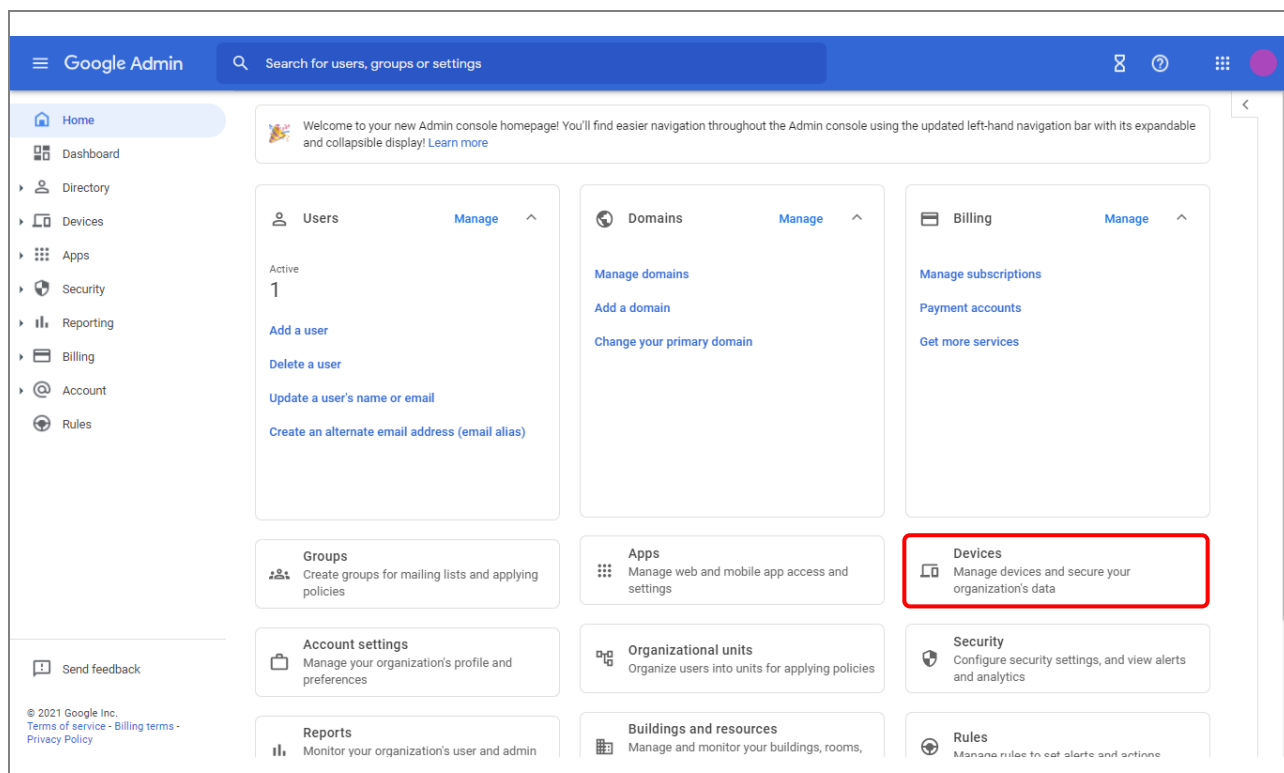
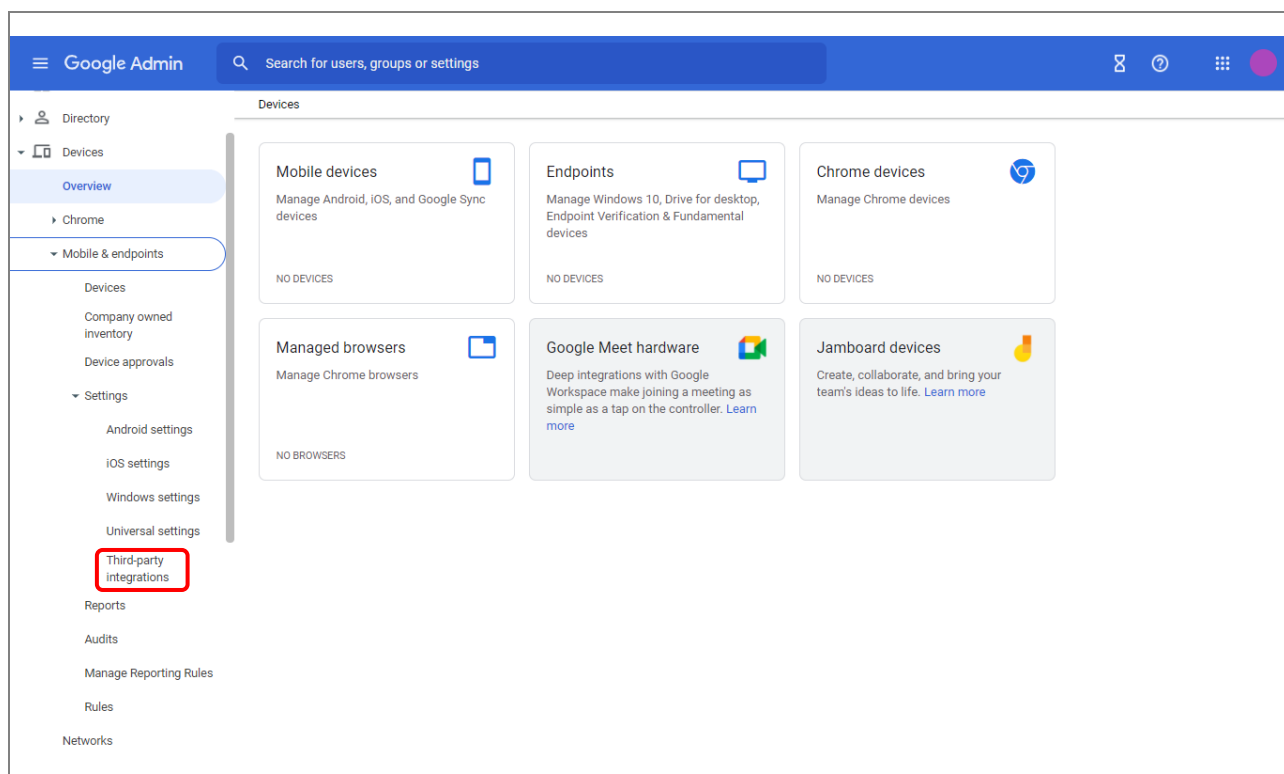
Checkout

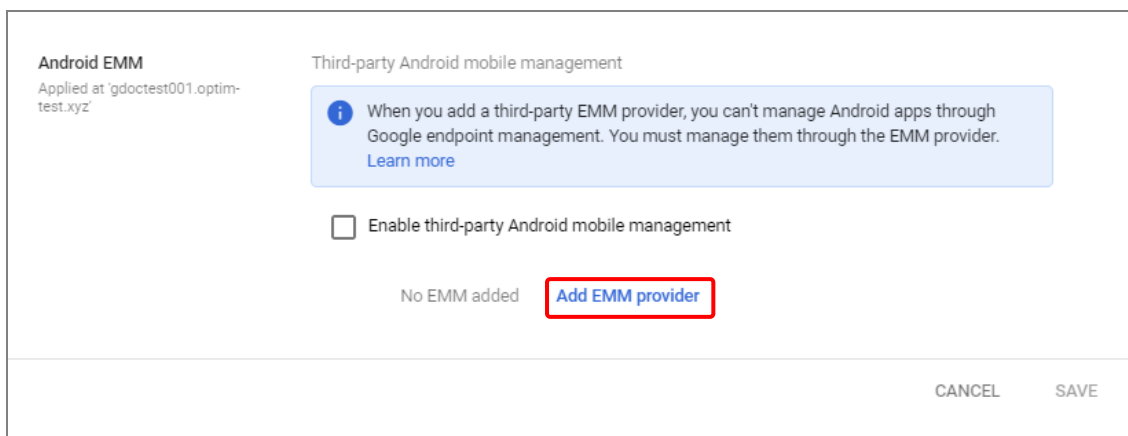
Android management
Free plan

Free

BACK

PLACE ORDER

[12] Click [Devices].**[13] Click [Settings]→[Third-party integrations].**

[14] Click [Add EMM provider] on [Android EMM].

Android EMM
Applied at 'gdoctest001.optim-test.xyz'

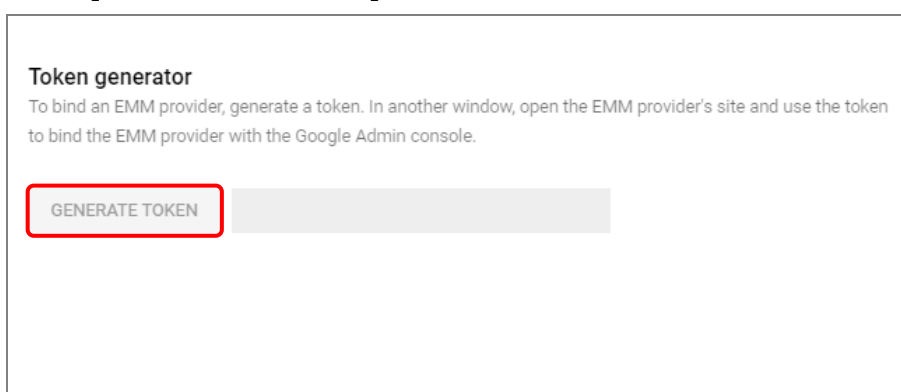
Third-party Android mobile management

When you add a third-party EMM provider, you can't manage Android apps through Google endpoint management. You must manage them through the EMM provider. [Learn more](#)

☐ Enable third-party Android mobile management

No EMM added **Add EMM provider**

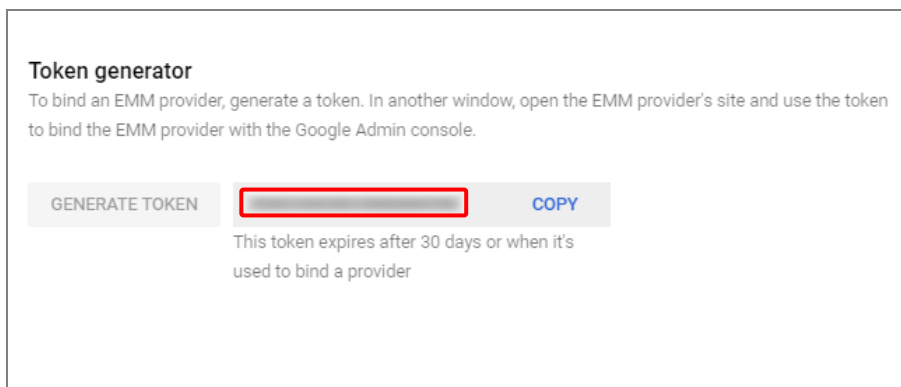
CANCEL SAVE

[15] Click [GENERATE TOKEN].

Token generator

To bind an EMM provider, generate a token. In another window, open the EMM provider's site and use the token to bind the EMM provider with the Google Admin console.

GENERATE TOKEN

[16] A token will appear. Make a note of it because as you will need it to register your account.

Token generator

To bind an EMM provider, generate a token. In another window, open the EMM provider's site and use the token to bind the EMM provider with the Google Admin console.

GENERATE TOKEN **COPY**

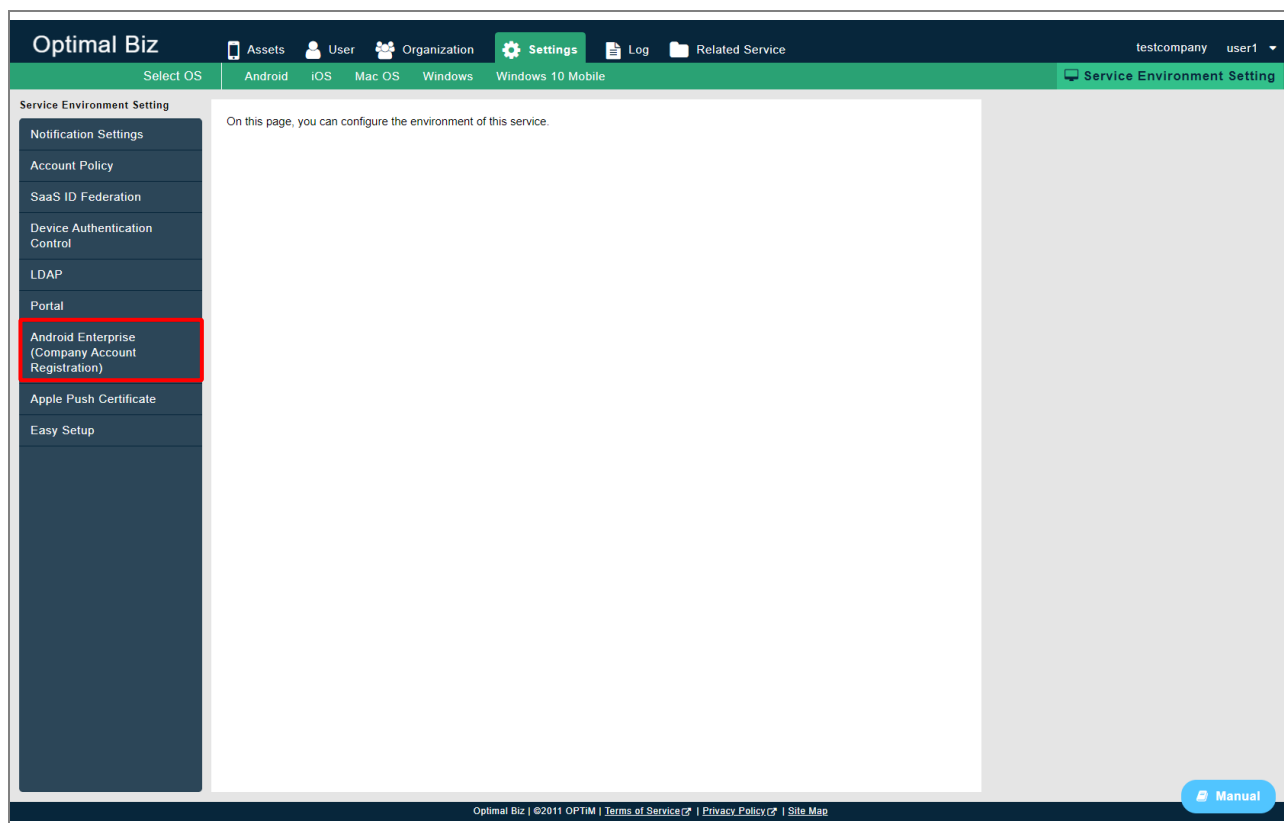
This token expires after 30 days or when it's used to bind a provider

6.2 Registering a Google Workspace (formerly G Suite) account

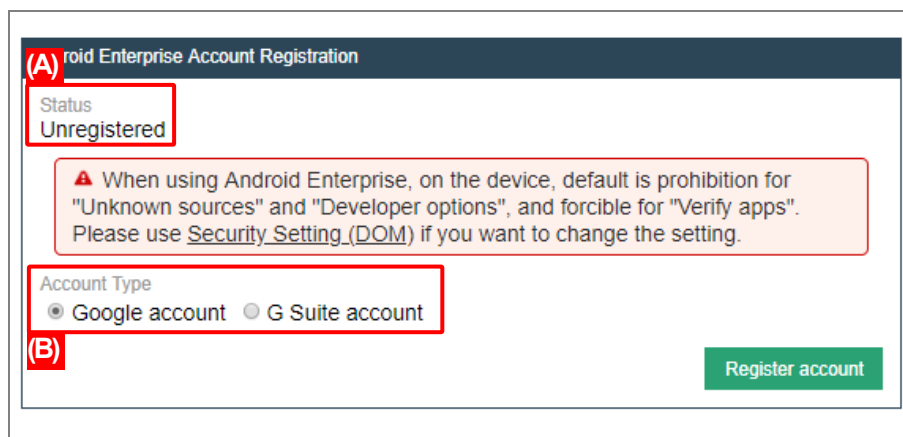
Follow the steps below to register a Google Workspace (formerly G Suite) account to the management site.

- ✍ Once you have registered your Google Workspace (formerly G Suite) account, do not change any settings on the Google side.
- ✍ If you use "Mobile management", a standard feature of Google Workspace (formerly G Suite), delete the "Devices" information of the mobile management feature.

- [1] Click [Settings]→[Service Environment Setting]→[Android Enterprise (Company Account Registration)].**



- [2] The "Status" (A) shows "Unregistered". "Google account" is selected in "Account Type" (B) by default.**



[3] Select "G Suite account".

[4] Go to <https://play.google.com/work/termsofservice> and accept the terms of use.

[5] Enter "Domain" and "EMM Token".

☑ In "Domain", enter the domain of your G Suite account. If your G Suite account is "XXXXXX@xxxxx.co.jp", your domain is "xxxxx.co.jp".

[6] Click [Register account].

The screenshot shows the 'Android Enterprise Account Registration' screen. At the top, the status is 'Unregistered'. A warning message states: 'When using Android Enterprise, on the device, default is prohibition for "Unknown sources" and "Developer options", and forcible for "Verify apps". Please use Security Setting_(DOM) if you want to change the setting.' Below this, under 'Account Type', the 'G Suite account' option is selected, indicated by a red box and the number 3. Another warning message follows: 'If you use G Suite account coordination, please login to G Suite with a super administrator account, access the following URL and agree to the terms.' Below this, the URL <https://play.google.com/work/termsofservice> is displayed, highlighted with a red box and the number 4. There are input fields for 'Domain' and 'EMM Token', both highlighted with a red box and the number 5. At the bottom right, the 'Register account' button is highlighted with a red box and the number 6.

[7] The "Status" (A) shows "Registered".

(B) displays "Domain" and "EMM Token".

The screenshot shows the 'Android Enterprise Account Registration' screen after successful registration. The status is now 'Registered', indicated by a red box and the label (A). The 'Account Type' remains 'G Suite account'. The same warning messages are present. The 'Domain' and 'EMM Token' fields are now filled with greyed-out text, highlighted with a red box and the label (B). A 'Delete account' button is now visible at the bottom right.

6.3 Performing authentication settings of Google API

Connect your Google Workspace (formerly G Suite) account to your corporate e-mail address in the management site, and create and authenticate a JSON file.

- ✎ If you use a zero-touch device with a Google Workspace (formerly G Suite) account, you must integrate this product with the Google Workspace (formerly G Suite) account. You cannot integrate a Google Workspace (formerly G Suite) account after Google API authentication setting. Always perform the procedures in advance.

✎ "Issuing a token" Page 129

✎ "Registering a Google Workspace (formerly G Suite) account" Page 136

6.3.1 Registering your e-mail address as a Google account

You can use your corporate or organizational e-mail address as your Google account.

- ✎ You do not have to perform these steps for all managed devices. Prepare one e-mail address for administration. It is recommended that you use the mailing list of an administrative department, not an administrator's e-mail address.
- ✎ If your Google account has been registered in your browser, you do not need to carry out this procedure.

[1] Click [Settings]→[Android]→[Zero-touch enrollment]→[Use Registration].

[2] Click [Register account].

The screenshot shows the Optimal Biz management console interface. The top navigation bar includes 'Assets', 'User', 'Organization', 'Settings' (highlighted), 'Log', and 'Related Service'. The left sidebar lists various settings categories, with 'Zero-touch enrollment' expanded to show 'Use Registration' (highlighted with a red box and a red '1'). The main content area displays the 'Register account' process, which includes steps for associating a Google account, allowing login to the zero-touch portal, logging in, and uploading a JSON file. A red box with a red '2' highlights the 'Register account' button at the bottom of the page.

- [3] The "Create your Google Account" screen appears.**
Enter "First name", "Last name", "Your email address", "Password", and "Confirm".

✍ In "Your email address", enter an email address with a corporate domain.

✍ If you click "Create a Gmail account instead" (A), you will create a Google Account with a Gmail account, so do not click the link. Be sure to create your account with your current email address.

- [4] Click [Next].**

- [5] In "Enter code", enter the confirmation code that was sent to the email address you entered in step [3] .**

- [6] Click [Verify].**

[7] Enter "Phone number", "Your birthday", and "Gender".

[8] Click [NEXT].

Google

welcome to Google

@gmail.com

7 Phone number (optional)

This won't make your number visible to others

Recovery email address (optional)

We'll use it to keep your account secure

Month Day Year

Your birthday

Gender

Your personal info is private & safe

[Why we ask for this information](#)

[Back](#) **8** [NEXT](#)

[9] Review the Terms, and click [I agree].

Google

Privacy and Terms

Combining data
We also combine this data among our services and across your devices for these purposes. For example, depending on your account settings, we show you ads based on information about your interests, which we can derive from your use of Search and YouTube, and we use data from trillions of search queries to build spell-correction models that we use across all of our services.

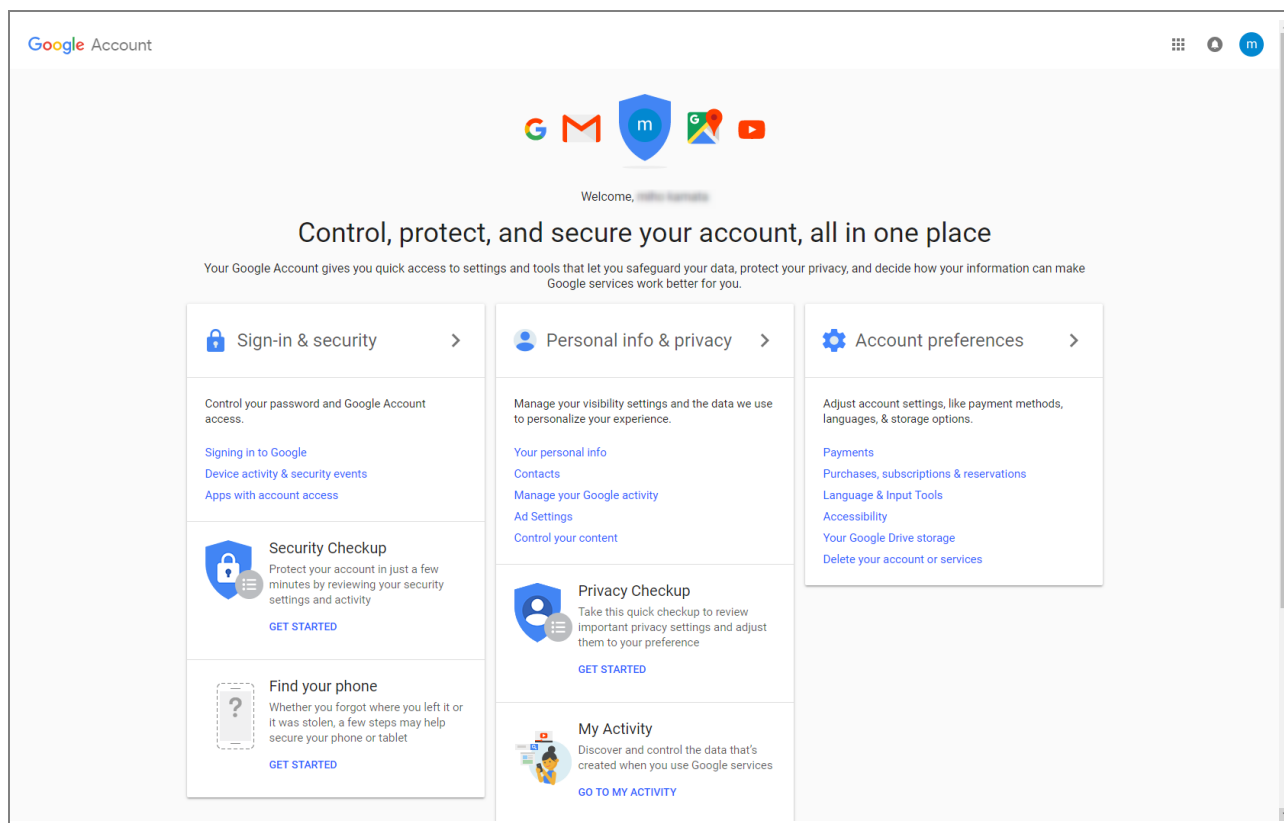
You're in control
Depending on your account settings, some of this data may be associated with your Google Account and we treat this data as personal information. You can control how we collect and use this data now by clicking "More Options" below. You can always adjust your controls later or withdraw your consent for the future by visiting My Account (myaccount.google.com).

[MORE OPTIONS](#)

[Cancel](#) **9** [I agree](#)

You're in control of the data we collect & how it's used

[10] You have successfully registered your e-mail address if the screen below appears.



6.3.2 Logging in to the zero-touch portal

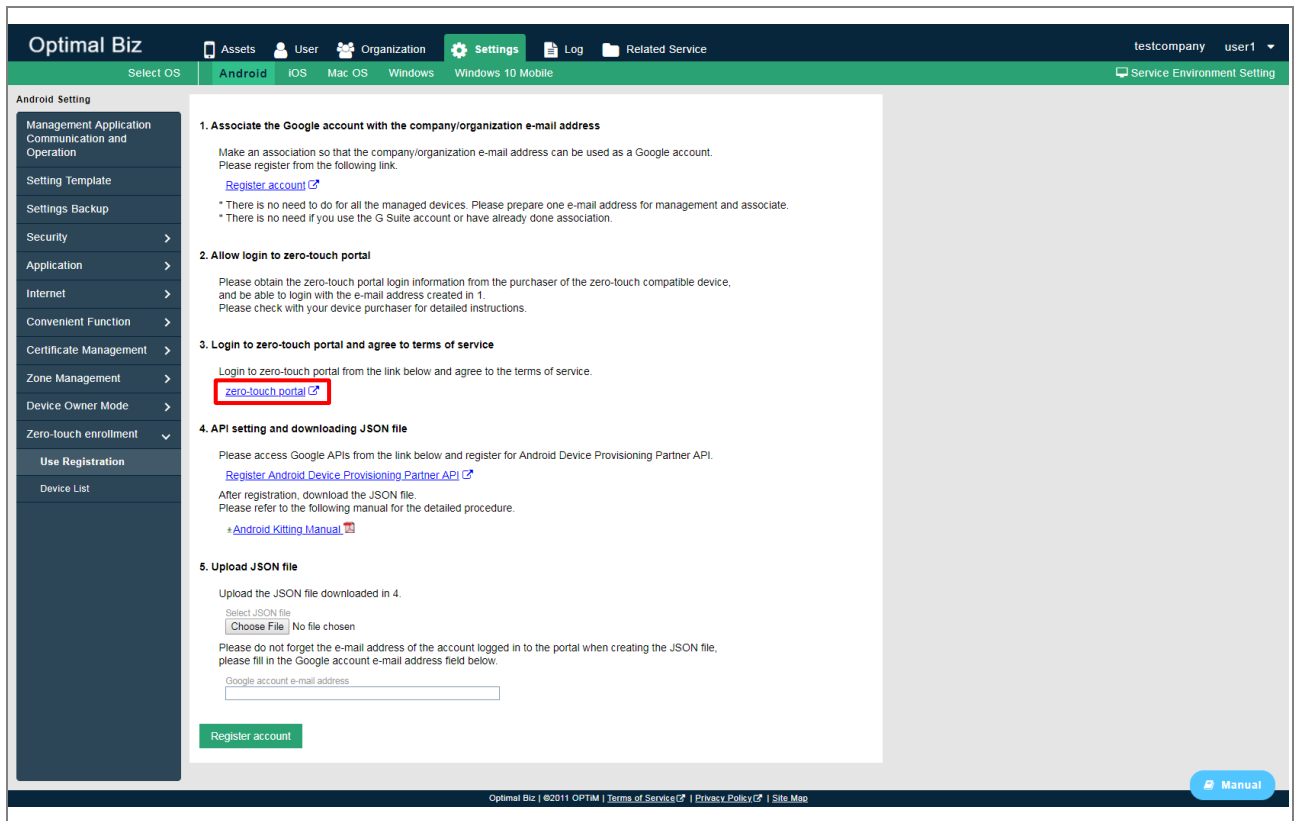
Inform your zero-touch device vendor of the registered Google account and ask them to allow logins to the zero-touch portal.

 For details, contact your zero-touch device vendor.

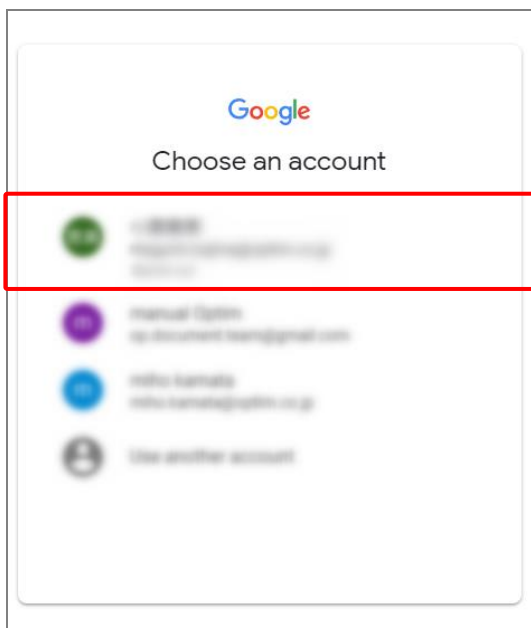
6.3.3 Accepting the terms of service

Log in to the zero touch portal and accept the terms of service.

[1] Click [zero-touch portal].



[2] Select the Google account you registered.



[3] Select "I accept the Terms of Service."

[4] Click [Agree].

Terms of Service

Android Zero Touch End Customer Agreement

1.1 Services Use. Subject to this Agreement, during the Term, you, the Customer may: (a) use the Services, and (b) use any Software provided by Google as part of the Services. Customer may not sublicense or transfer these rights except as permitted under the Assignment section of the Agreement

1.2 Console. Google will provide the Services to Customer. As part of receiving the Services, Customer will have access to the Admin Console, through which Customer may administer the Services.

1.3 Facilities. All facilities used to store and process an Application and Customer Data will adhere to reasonable security standards no less protective than the security standards at facilities where Google processes and stores its own information of a similar type. Google has implemented at least industry standard systems and procedures to (i) ensure the security and confidentiality of an Application and Customer Data, (ii) protect against anticipated threats or hazards to the security or integrity of an Application and Customer Data, and (iii) protect against unauthorized access to or use of an Application and Customer Data.

immediately. If Customer does not agree to the revised Agreement, please stop using the Services. Google will

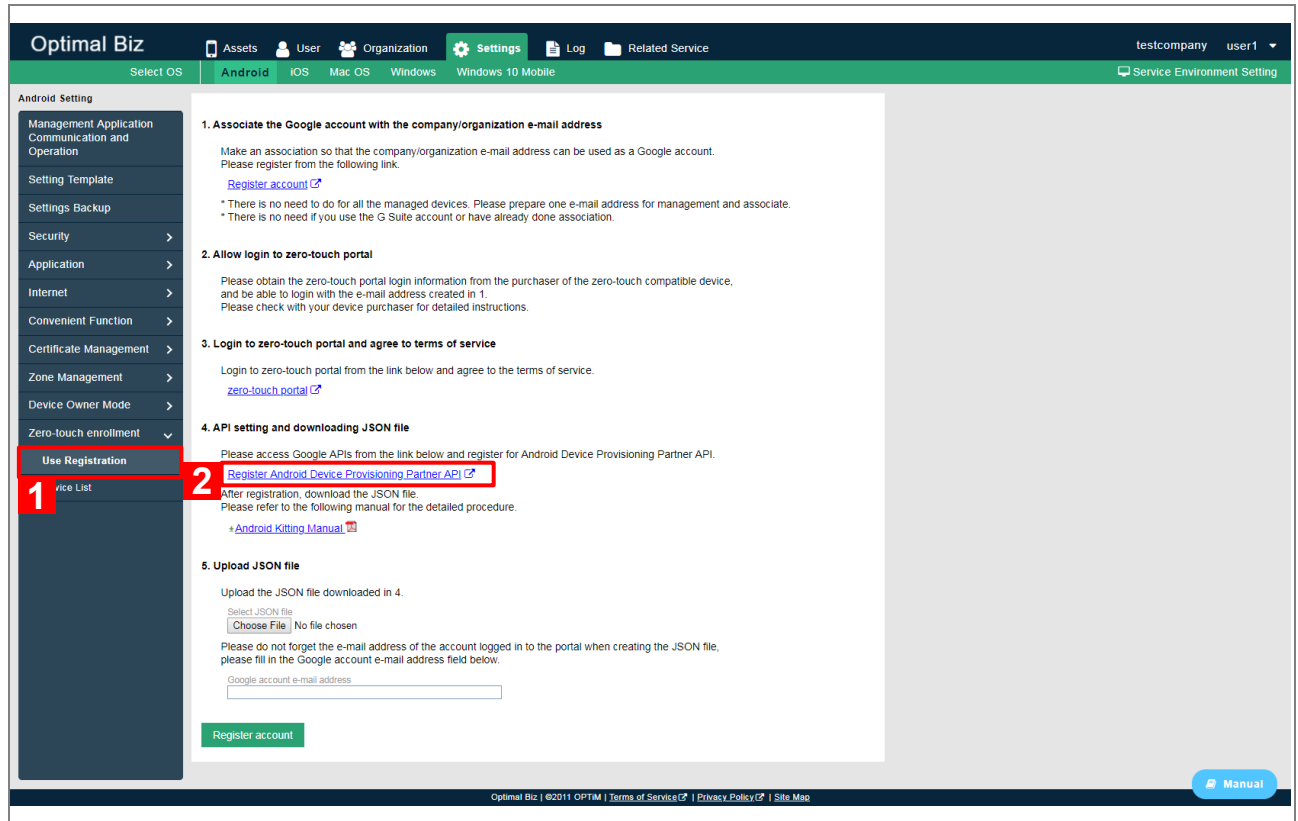
3 ☐ I accept the Terms of Service.

4

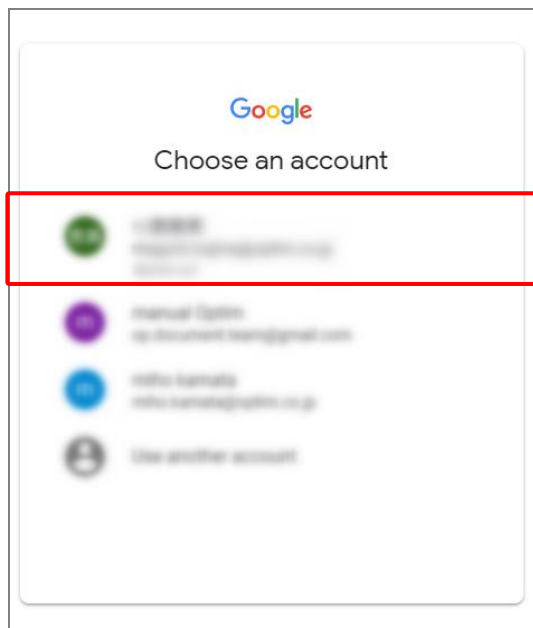
6.3.4 Downloading API settings and a JSON file

Register Android Device Provisioning Partner API on the Google Cloud Platform, and download a JSON file.

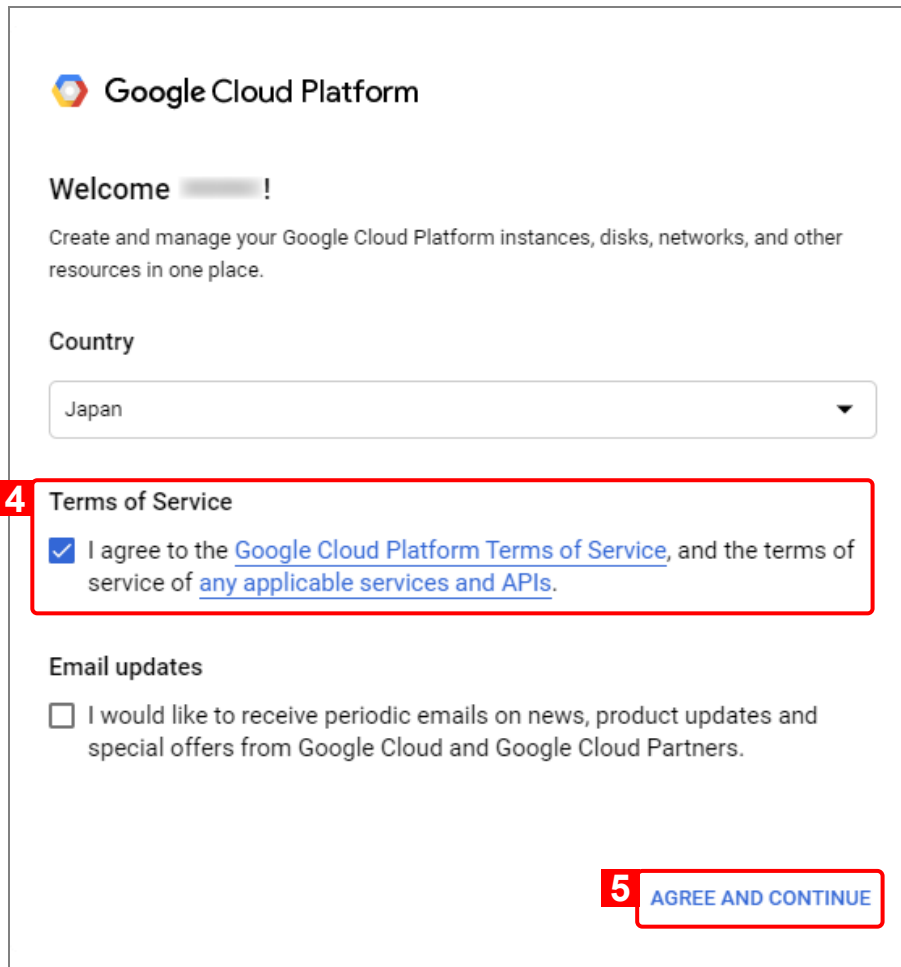
- [1]** Click [Settings]→[Android]→[Zero-touch enrollment]→[Use Registration].
- [2]** Click [Register Android Device Provisioning Partner API].



- [3]** Select the e-mail address that you have connected.

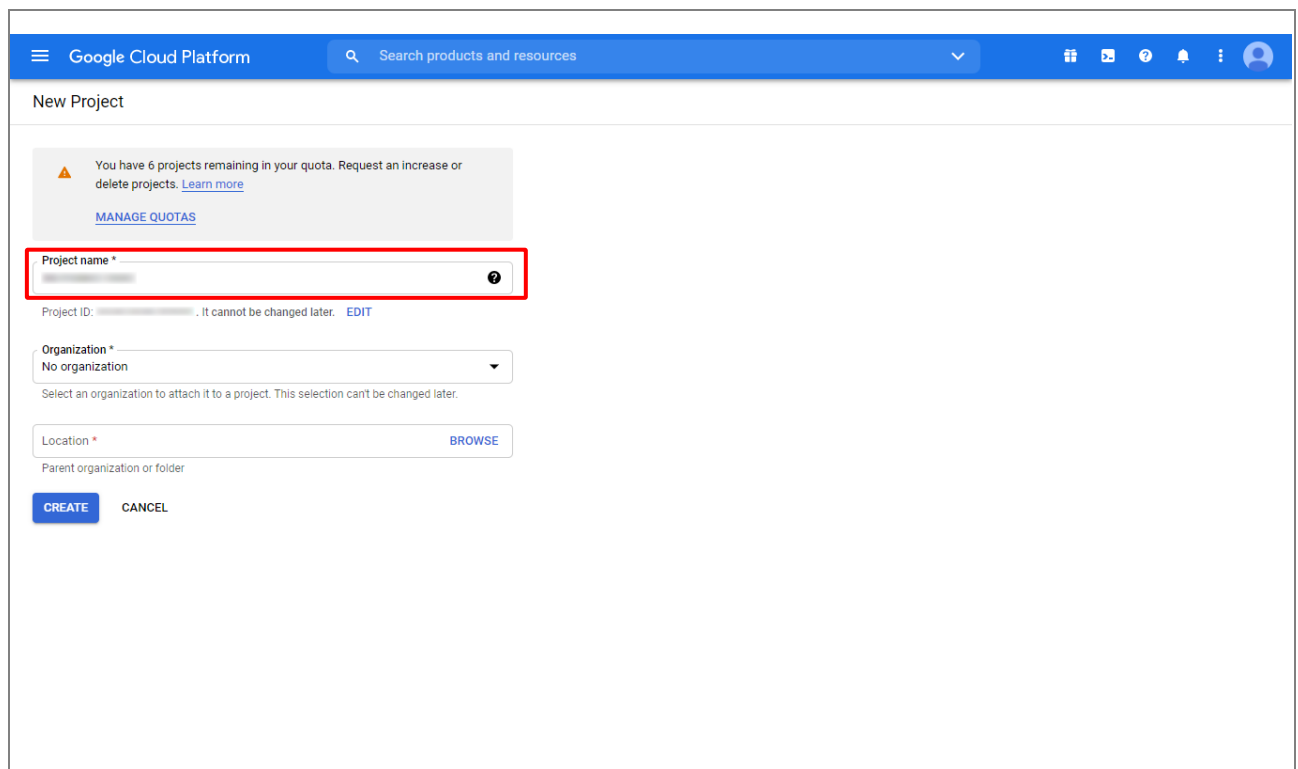


- [4] In the first login, the consent screen for the terms of service will appear. Select the terms of service.**
- [5] Click [AGREE AND CONTINUE].**

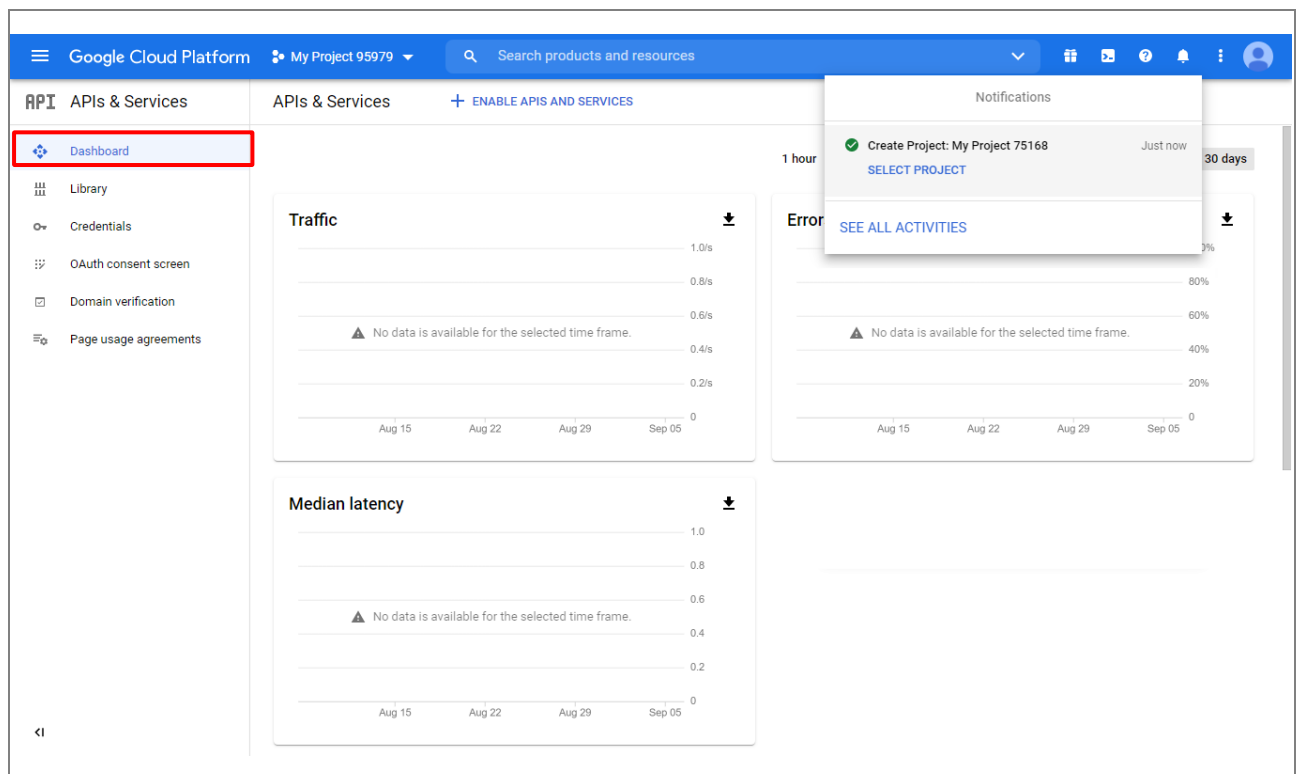
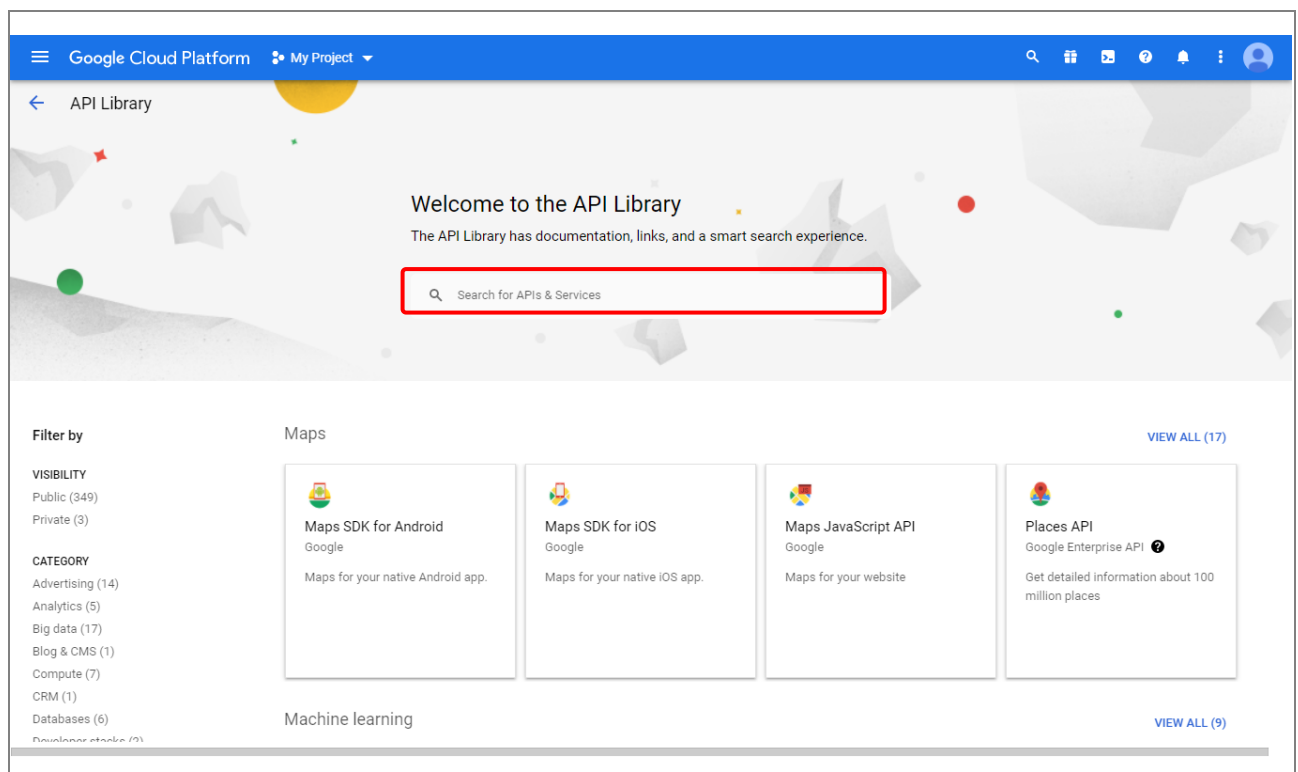


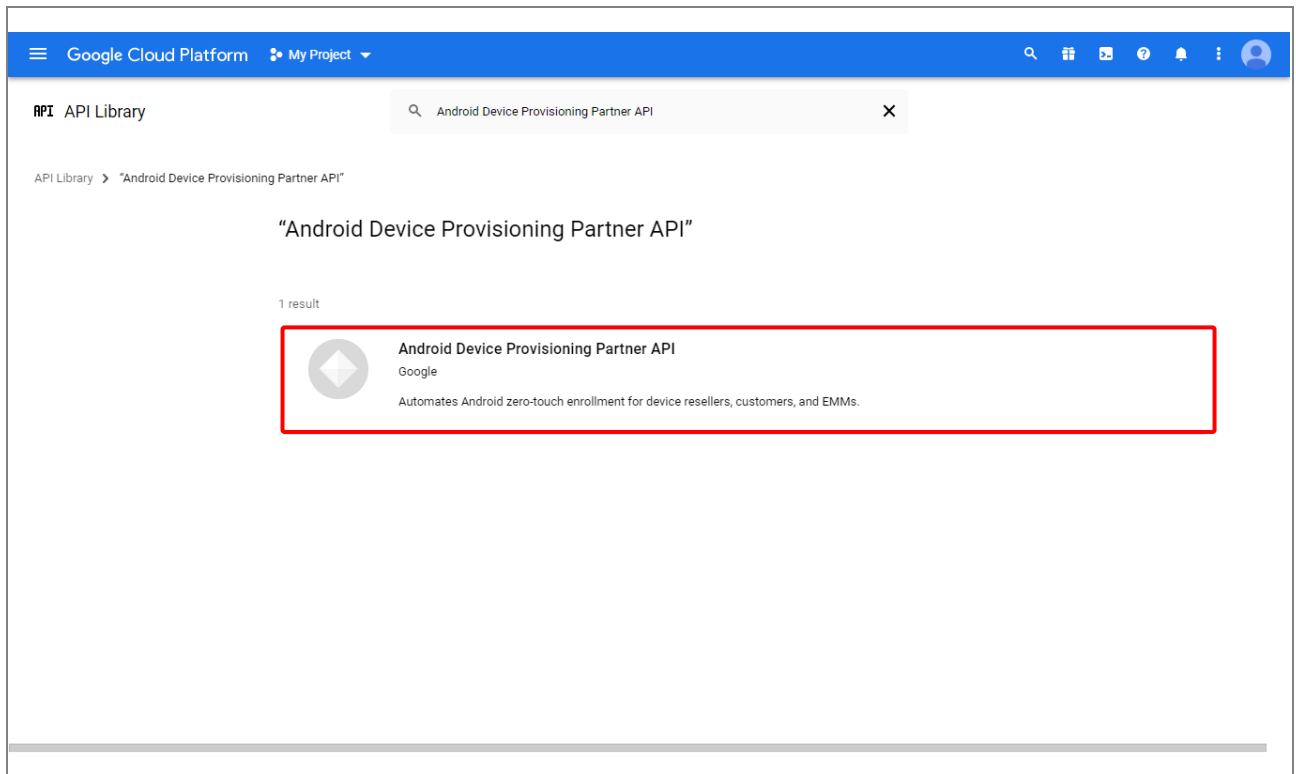
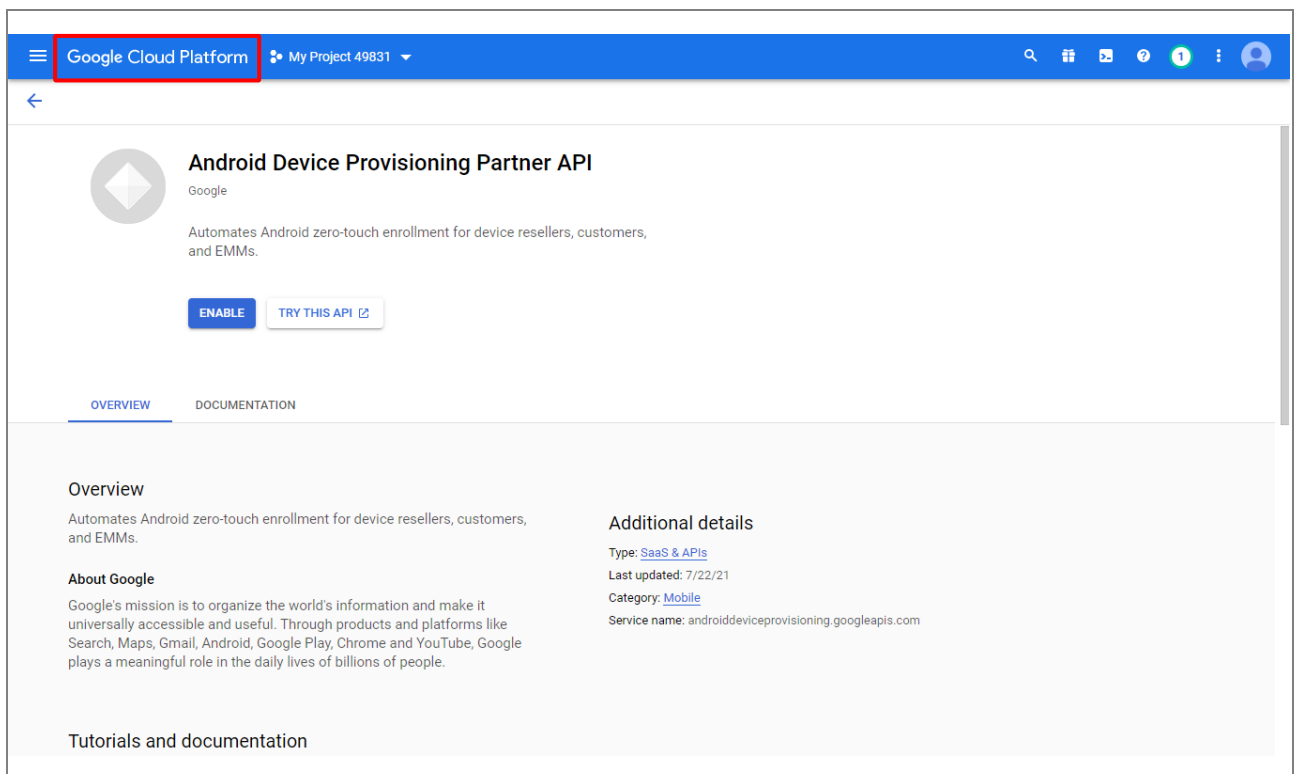
The screenshot shows the Google Cloud Platform Terms of Service screen. At the top, it says "Google Cloud Platform" with the logo. Below that, it says "Welcome [redacted]!" and "Create and manage your Google Cloud Platform instances, disks, networks, and other resources in one place." There is a "Country" dropdown menu with "Japan" selected. A red box labeled "4" highlights the "Terms of Service" section, which contains a checked checkbox and the text "I agree to the [Google Cloud Platform Terms of Service](#), and the terms of service of [any applicable services and APIs](#)." Below this is the "Email updates" section with an unchecked checkbox and the text "I would like to receive periodic emails on news, product updates and special offers from Google Cloud and Google Cloud Partners." A red box labeled "5" highlights the "AGREE AND CONTINUE" button at the bottom right.

- [6] The Google Cloud Platform screen appears. Enter an arbitrary "Project name".**



The screenshot shows the Google Cloud Platform "New Project" screen. At the top, there is a blue header with the Google Cloud Platform logo, a search bar, and various icons. Below the header, there is a "New Project" section. A warning message states: "You have 6 projects remaining in your quota. Request an increase or delete projects. [Learn more](#)" with a "MANAGE QUOTAS" link. A red box highlights the "Project name *" input field. Below it, the "Project ID" is shown as a placeholder, with a note: ". It cannot be changed later. [EDIT](#)". There is an "Organization *" dropdown menu with "No organization" selected. Below that, a note says: "Select an organization to attach it to a project. This selection can't be changed later." There is a "Location *" input field with a "BROWSE" link. At the bottom, there are "CREATE" and "CANCEL" buttons.

[7] Click [Library].**[8] In "Search for APIs and Services", enter "Android Device Provisioning Partner API", and execute search.**

【9】 Click [Android Device Provisioning Partner API] in the results.**【10】 Click [Google Cloud Platform].**


[11] Click [Credentials].

The screenshot shows the Google Cloud Platform console interface. The top navigation bar includes the Google Cloud Platform logo, the project name 'My Project 49831', a search bar, and user profile information. The left sidebar contains a menu with 'Overview', 'Metrics', 'Quotas', and 'Credentials'. The 'Credentials' option is highlighted with a red rectangle. The main content area shows the 'Overview' tab for the 'Android Device Provisioning Partner API'. A message at the top states: 'To use this API, you may need credentials. Click 'Create credentials' to get started.' with a 'CREATE CREDENTIALS' button. Below this, the 'Details' section shows the API name, provider (Google), service name, overview, and activation status (Enabled). The 'Traffic by response code' section shows a line graph with the text 'No data is available for the selected time frame.' and a 'View metrics' link.

[12] Click [CONFIGURE CONSENT SCREEN].

The screenshot shows the 'Credentials' page in the Google Cloud Platform console. At the top, there are buttons for '+ CREATE CREDENTIALS' and 'DELETE'. The main heading is 'Credentials compatible with this API', followed by a link to 'Credentials in APIs & Services'. A warning message states: 'Remember to configure the OAuth consent screen with information about your application.' with a 'CONFIGURE CONSENT SCREEN' button highlighted by a red rectangle. Below this, there are two sections: 'OAuth 2.0 Client IDs' and 'Service Accounts'. The 'OAuth 2.0 Client IDs' section shows a table with columns: Name, Creation date (sorted down), Type, Client ID, and Actions. It currently displays 'No OAuth clients to display'. The 'Service Accounts' section shows a table with columns: Email, Name (sorted up), and Actions. It currently displays 'No service accounts to display'.

[13] Click [CREATE].


 You do not have to select "User Type" (A). For details of "User Type", contact Google.

OAuth consent screen


Choose how you want to configure and register your app, including your target users. You can only associate one app with your project.

(A)

User Type

☐ Internal 


Only available to users within your organization. You will not need to submit your app for verification. [Learn more about user type](#)

☐ External 

Available to any test user with a Google Account. Your app will start in testing mode and will only be available to users you add to the list of test users. Once your app is ready to push to production, you may need to verify your app. [Learn more about user type](#)

CREATE

[Let us know what you think](#) about our OAuth experience

- [14] Enter "OptimalBiz" in "App Name".**
- [15] Click "User support email" and select an email address.**
- [16] Enter "optim.co.jp" in "Authorized domains", and press [Enter].**
 The domain name may change automatically after you press [Enter].
- [17] Enter your email address in [Developer contact information].**
- [18] Click [SAVE AND CONTINUE].**

Edit app registration

1 OAuth consent screen — 2 Scopes — 3 Test users — 4 Summary

App information

This shows in the consent screen, and helps end users know who you are and contact you

14

App name *

The name of the app asking for consent

15

User support email *

For users to contact you with questions about their consent

App logo

BROWSE

Upload an image, not larger than 1MB on the consent screen that will help users recognize your app. Allowed image formats are JPG, PNG, and BMP. Logos should be square and 120px by 120px for the best results.

App domain

To protect you and your users, Google only allows apps using OAuth to use Authorized Domains. The following information will be shown to your users on the consent screen.

Application home page

Provide users a link to your home page

Application privacy policy link

Provide users a link to your public privacy policy

Application terms of service link

Provide users a link to your public terms of service

16

Authorized domains

When a domain is used on the consent screen or in an OAuth client's configuration, it must be pre-registered here. If your app needs to go through verification, please go to the [Google Search Console](#) to check if your domains are authorized. [Learn more](#) about the authorized domain limit.

example.com

ADD DOMAIN

Developer contact information

17

Email addresses *

These email addresses are for Google to notify you about any changes to your project.

18

SAVE AND CONTINUE

CANCEL

[19] Click [SAVE AND CONTINUE].

 You do not have to add scopes.

Edit app registration

✓

OAuth consent screen

2

Scopes

3

Test users

4

Summary

Scopes express the permissions you request users to authorize for your app and allow your project to access specific types of private user data from their Google Account. [Learn more](#)

ADD OR REMOVE SCOPES

Your restricted scopes


Restricted scopes are scopes that request access to highly sensitive user data.

API ↑	Scope	User-facing description
No rows to display		

SAVE AND CONTINUE

CANCEL

[20] Click [SAVE AND CONTINUE].

 You do not have to add test users.

Edit app registration

✓

OAuth consent screen

✓

Scopes

3

Test users

4

Summary

Test users

While publishing status is set to "Testing", only test users are able to access the app. Allowed user cap prior to app verification is 100, and is counted over the entire lifetime of the app. [Learn more](#)

+ ADD USERS

Filter

Enter property name or value

?

User information

No rows to display

SAVE AND CONTINUE

CANCEL

[21] Review the settings details and click [BACK TO DASHBOARD].

Edit app registration

☒ OAuth consent screen —
 ☒ Scopes —
 ☒ Test users —
 4 Summary

Authorized domains

Contact email addresses

Scopes [EDIT](#)

API ↑	Scope	User-facing description
No rows to display		

Test users [EDIT](#)

0 users (0 test, 0 other) / 100 user cap ?

Filter Enter property name or value ?

User information

No rows to display

BACK TO DASHBOARD

[22] The OAuth consent screen appears. Click [PUBLISH APP].

Google Cloud Platform My Project 49831 Search products and resources

APIs & Services OAuth consent screen Learn

OptimalBiz [EDIT APP](#)

Publishing status ?

Testing

PUBLISH APP

User type

External ?

[MAKE INTERNAL](#)

OAuth user cap ?

While publishing status is set to "Testing", only test users are able to access the app. Allowed user cap prior to app verification is 100, and is counted over the entire lifetime of the app. [Learn more](#)

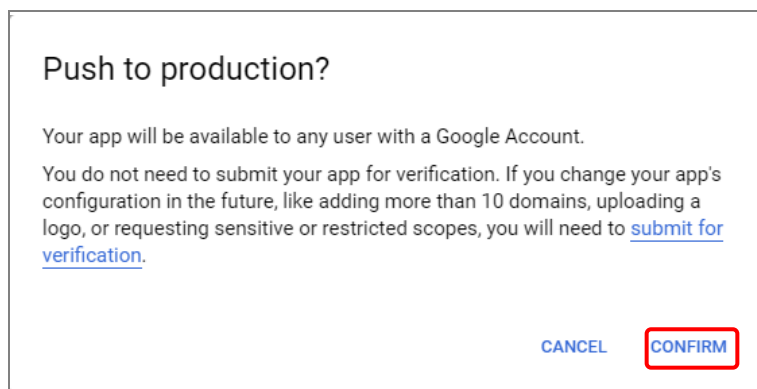
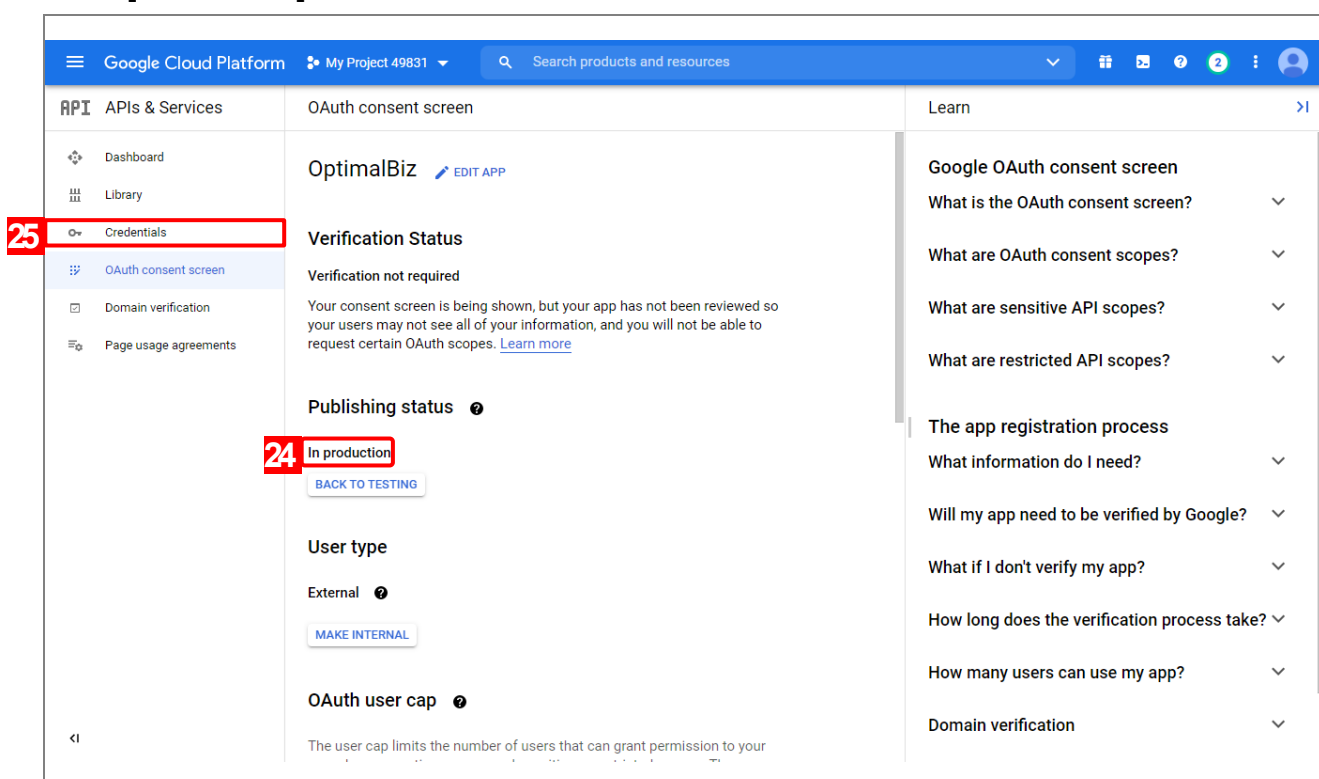
0 users (0 test, 0 other) / 100 user cap ?

Test users

[ADD USERS](#)

Google OAuth consent screen

- What is the OAuth consent screen? ▾
- What are OAuth consent scopes? ▾
- What are sensitive API scopes? ▾
- What are restricted API scopes? ▾
- The app registration process
- What information do I need? ▾
- Will my app need to be verified by Google? ▾
- What if I don't verify my app? ▾
- How long does the verification process take? ▾
- How many users can use my app? ▾
- Domain verification ▾

[23] Read the message and click [CONFIRM].**[24] Ensure that the publishing status is "In production".****[25] Click [Credentials].**

[26] Click [CREATE CREDENTIALS].

[27] Select "OAuth client ID".

The screenshot shows the Google Cloud 'Credentials' page. At the top, there is a '+ CREATE CREDENTIALS' button highlighted with a red box and the number 22. Below this, a dropdown menu is open, showing three options: 'API key', 'OAuth client ID', and 'Service account'. The 'OAuth client ID' option is highlighted with a red box and the number 23. Below the dropdown, there are three sections: 'API Keys', 'OAuth 2.0 Client IDs', and 'Service Accounts'. Each section has a table with columns for Name, Creation date, Type, Client ID, and Actions. The 'API Keys' section shows 'No API keys to display'. The 'OAuth 2.0 Client IDs' section shows 'No OAuth clients to display'. The 'Service Accounts' section shows 'No service accounts to display'.

Credentials **22** + CREATE CREDENTIALS DELETE

Create credentials to access your project's APIs

API Keys **23** **OAuth client ID**

- API key**
Identifies your project using a simple API key to check quota and access
- OAuth client ID**
Requests user consent so your app can access the user's data
- Service account**
Enables server-to-server, app-level authentication using robot accounts

OAuth 2.0 Client IDs **Help me choose**
Asks a few questions to help you decide which type of credential to use

<input type="checkbox"/>	Name	Creation date	Type	Client ID	Actions
No OAuth clients to display					

Service Accounts [Manage service accounts](#)

<input type="checkbox"/>	Email	Name	Actions
No service accounts to display			

- [28]** Select "Web application" on the "Application type" pull-down menu.
- [29]** Enter an arbitrary name.
- [30]** Click [ADD URI] in "Authorized redirect URIs".

← Create OAuth client ID

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information. [Learn more](#) about OAuth client types.

28

Application type *
Web application

29

Name *
Web client 1

The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.

i

The domains of the URIs you add below will be automatically added to your [OAuth consent screen](#) as [authorized domains](#).

Authorized JavaScript origins ?

For use with requests from a browser

+ ADD URI

Authorized redirect URIs ?

For use with requests from a web server

URIs *

https://www.example.com

30

+ ADD URI

CREATE

CANCEL

155

[31] Enter `"https://biz3.optim.co.jp/company1/android_emm_zero_touch_auth/callback"` in "URI". (* Enter your company code in "company1".)

✍ If a warning message appears, make sure that you have entered an appropriate "Authorized domains" in step **[16]**.

[32] Click **[CREATE]**.

← Create OAuth client ID

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information. [Learn more](#) about OAuth client types.

Application type *
Web application

Name *
Web client 1

The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.

i The domains of the URIs you add below will be automatically added to your [OAuth consent screen](#) as [authorized domains](#).

Authorized JavaScript origins ?
For use with requests from a browser

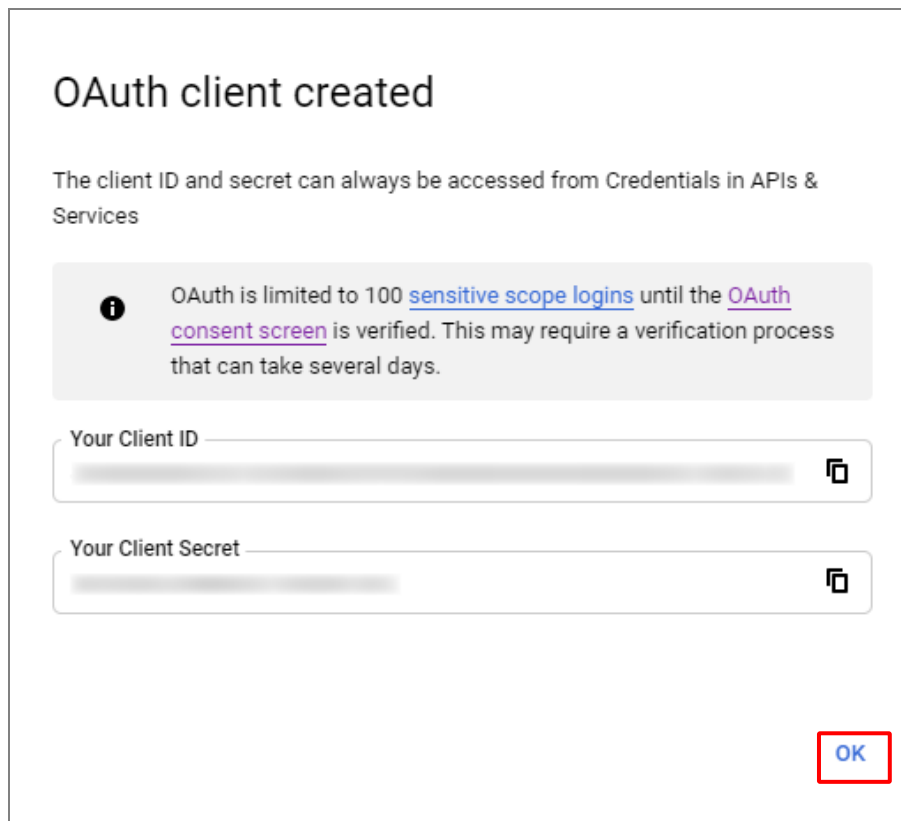
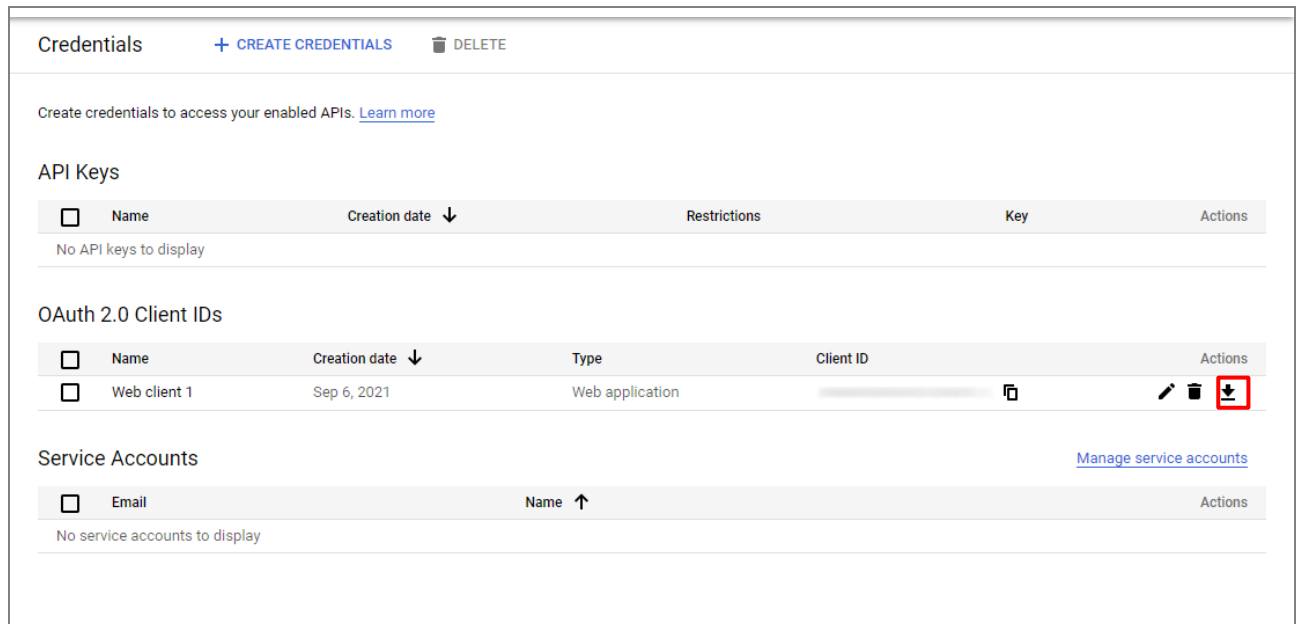
+ ADD URI

Authorized redirect URIs ?
For use with requests from a web server

31 URIs *

+ ADD URI

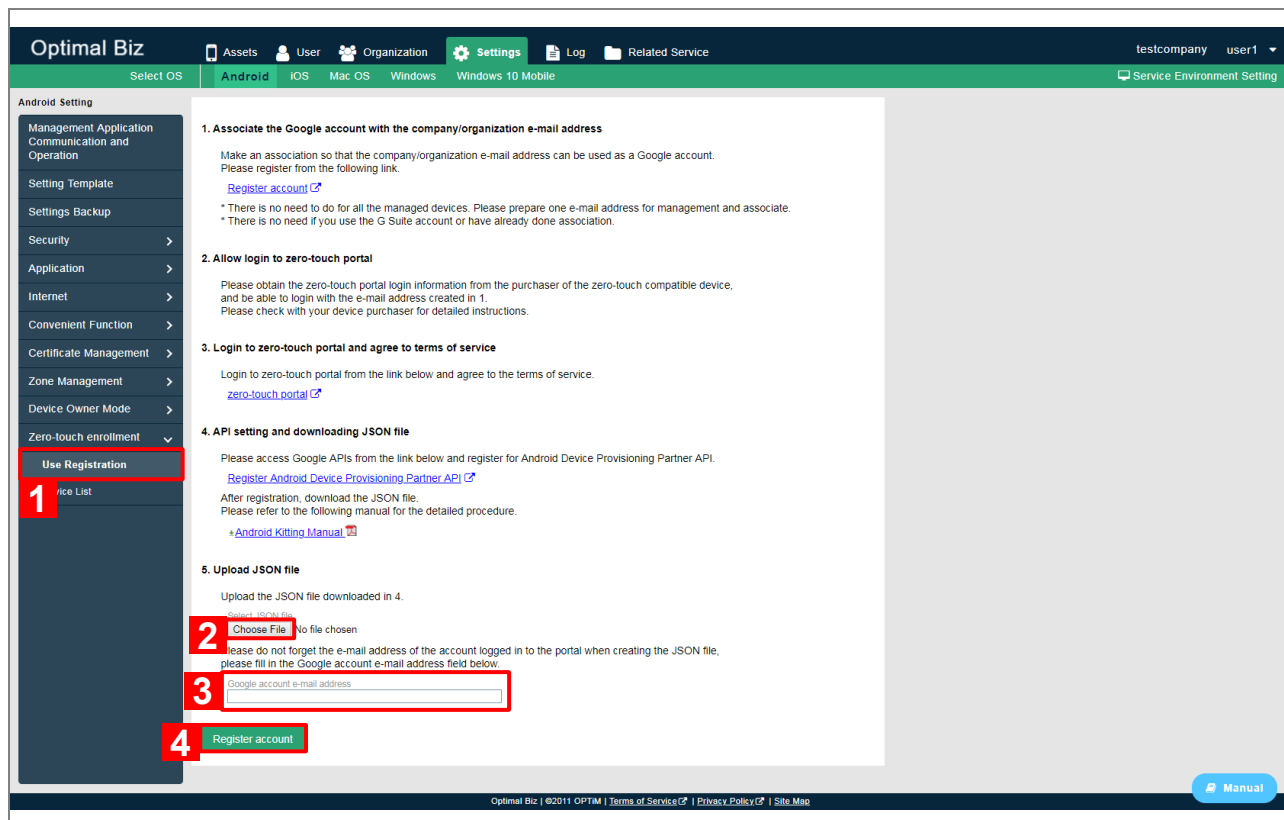
32 **CREATE** CANCEL

[33] Click [OK].**[34] Click the download icon to download a JSON file.**

6.3.5 Uploading a JSON file

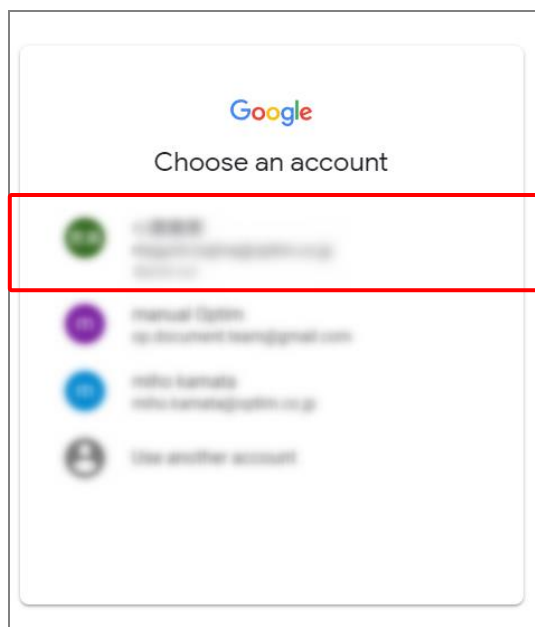
Upload the JSON file you downloaded with Google APIs to the management site and register device information.

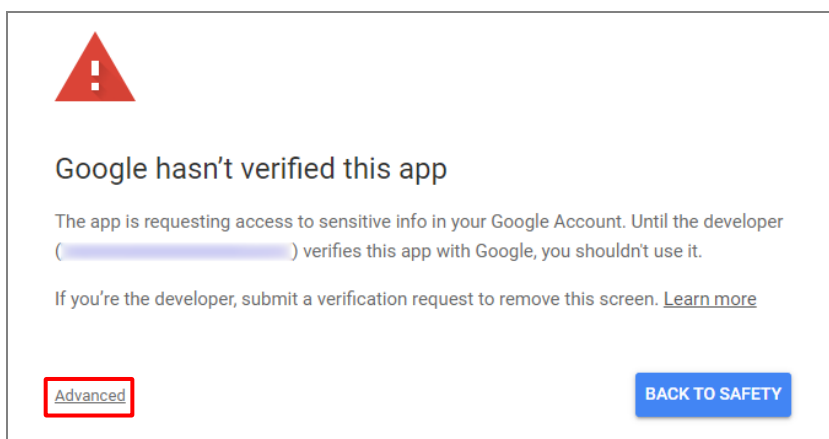
- [1]** Click [Settings]→[Android]→[Zero-touch enrollment]→[Use Registration].
- [2]** Click [Choose File] and select the downloaded JSON file.
- [3]** Enter "Google account email address".
- [4]** Click [Register account].



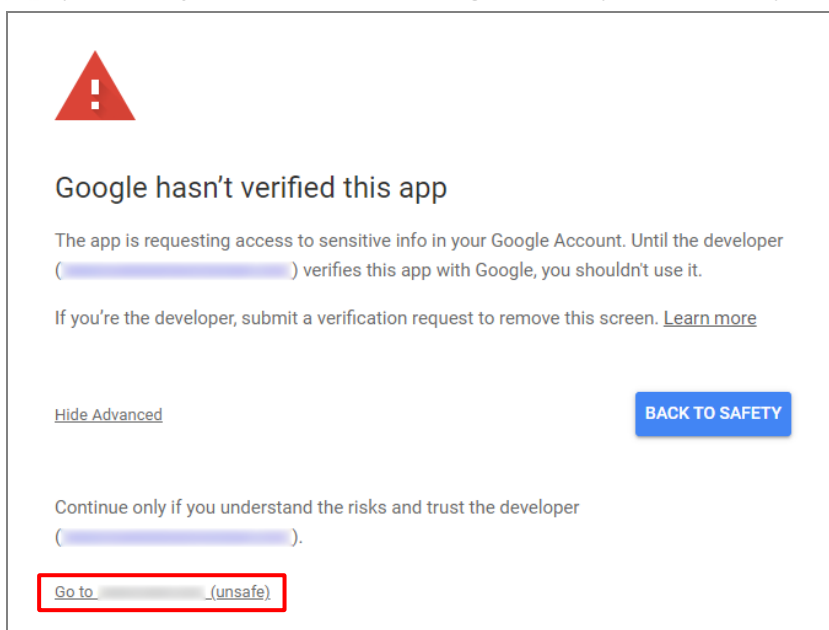
- [5]** Redirect to Google login screen.
Select the Google account you registered.

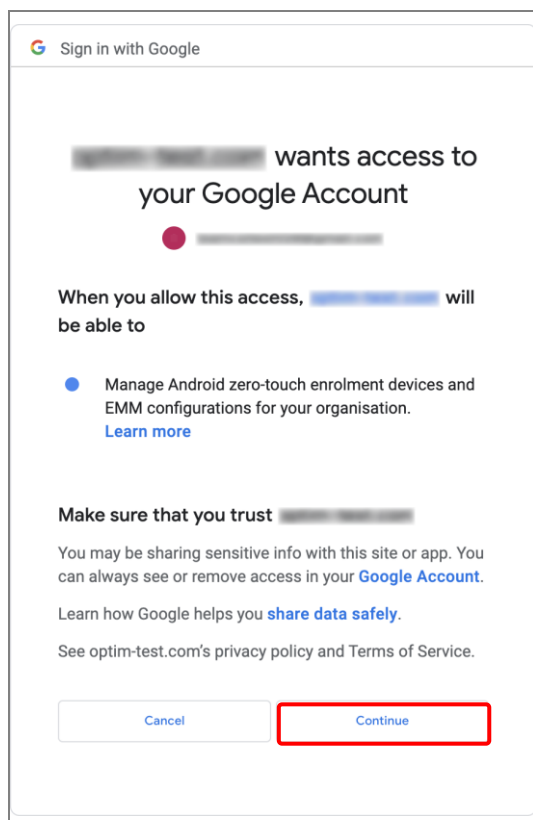
⇒ Warning window will be displayed.



[6] Click [Advanced].**[7] Click [Go to domain (unsafe)].**

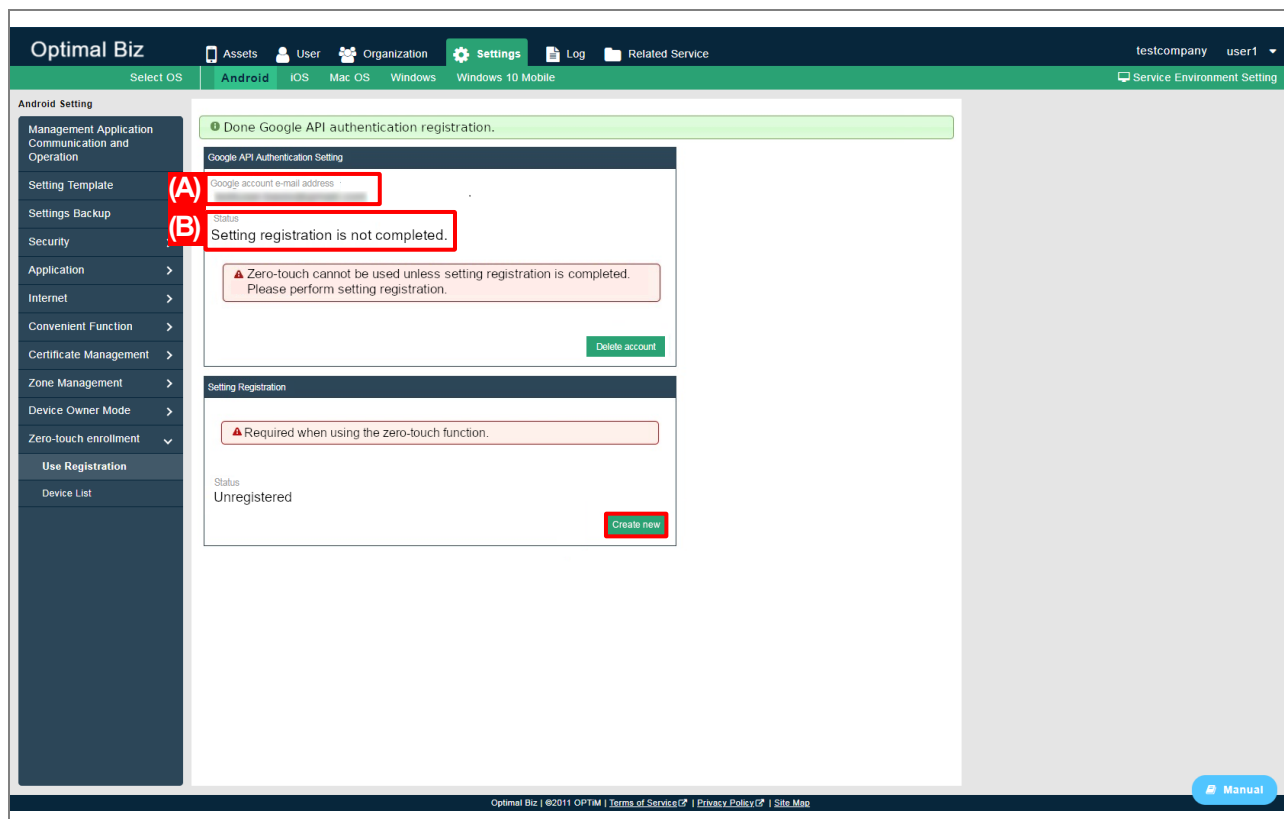
✎ If your Google account is "XXXXX@xxxxx.co.jp", "xxxxx.co.jp" is displayed for your domain.




[8] Click [Continue].**[9] Perform setting registration. Click [Create new].**

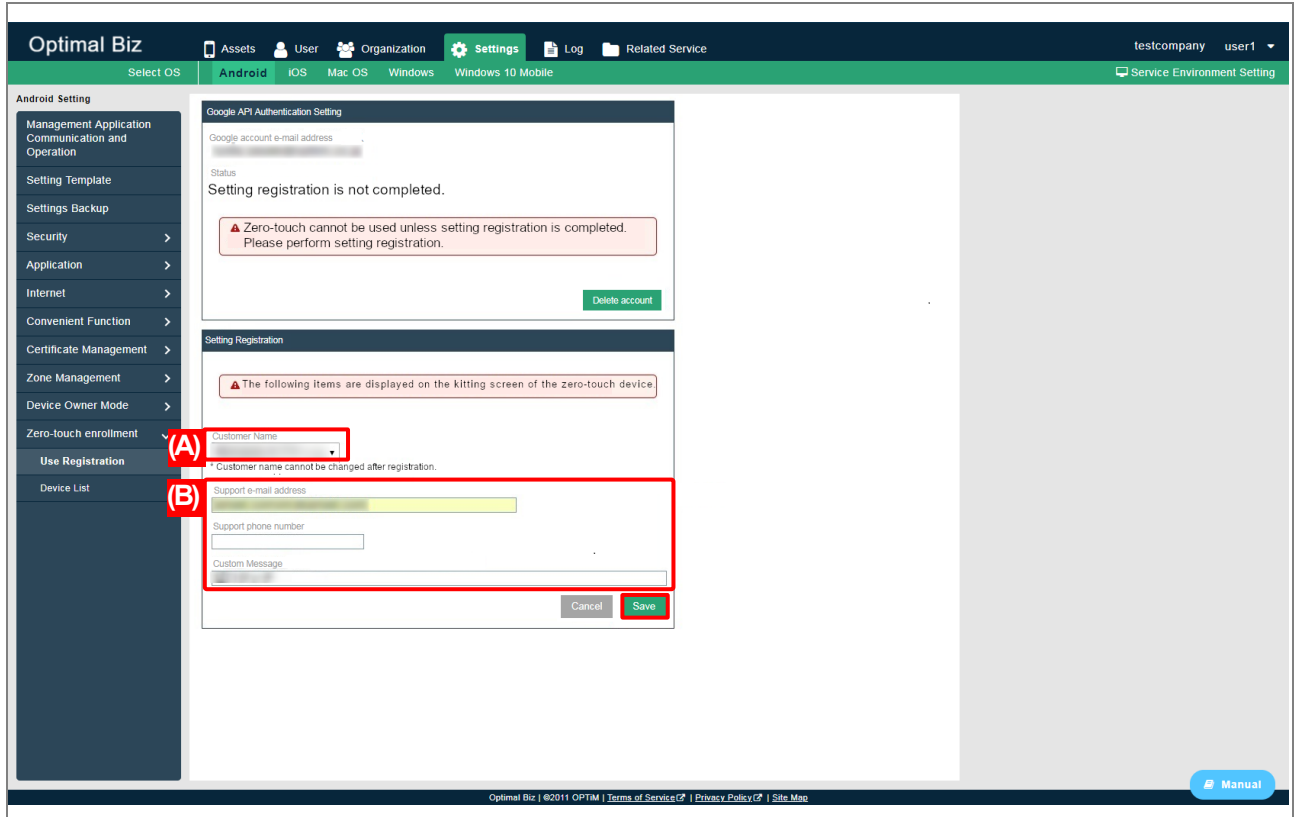
✎ If you do not register settings, you cannot sync zero-touch devices. "Status" (B) displays "Setting registration is not completed".

✎ "Google account email address" (A) displays the Google account you selected in step **[4]**.



[10] Click [Save].

 You cannot change "Customer Name" (A). "Support e-mail address", "Support phone number", and "Custom Message" (B) display the settings you entered during setting registration. Change them if necessary.



The screenshot shows the 'Optimal Biz' interface with the 'Settings' tab selected. The left sidebar lists various settings categories, with 'Zero-touch enrollment' expanded. The main content area displays the 'Setting Registration' form. A red box highlights the 'Customer Name' field (A) and the 'Support e-mail address', 'Support phone number', and 'Custom Message' fields (B). A 'Save' button is visible at the bottom right of the form.

Google API Authentication Setting

Google account e-mail address: [redacted]

Status: Setting registration is not completed.

⚠ Zero-touch cannot be used unless setting registration is completed. Please perform setting registration.

[Delete account](#)

Setting Registration

⚠ The following items are displayed on the kitting screen of the zero-touch device.

(A) Customer Name: [redacted]

* Customer name cannot be changed after registration.

(B) Support e-mail address: [redacted]

Support phone number: [redacted]

Custom Message: [redacted]

[Cancel](#) [Save](#)

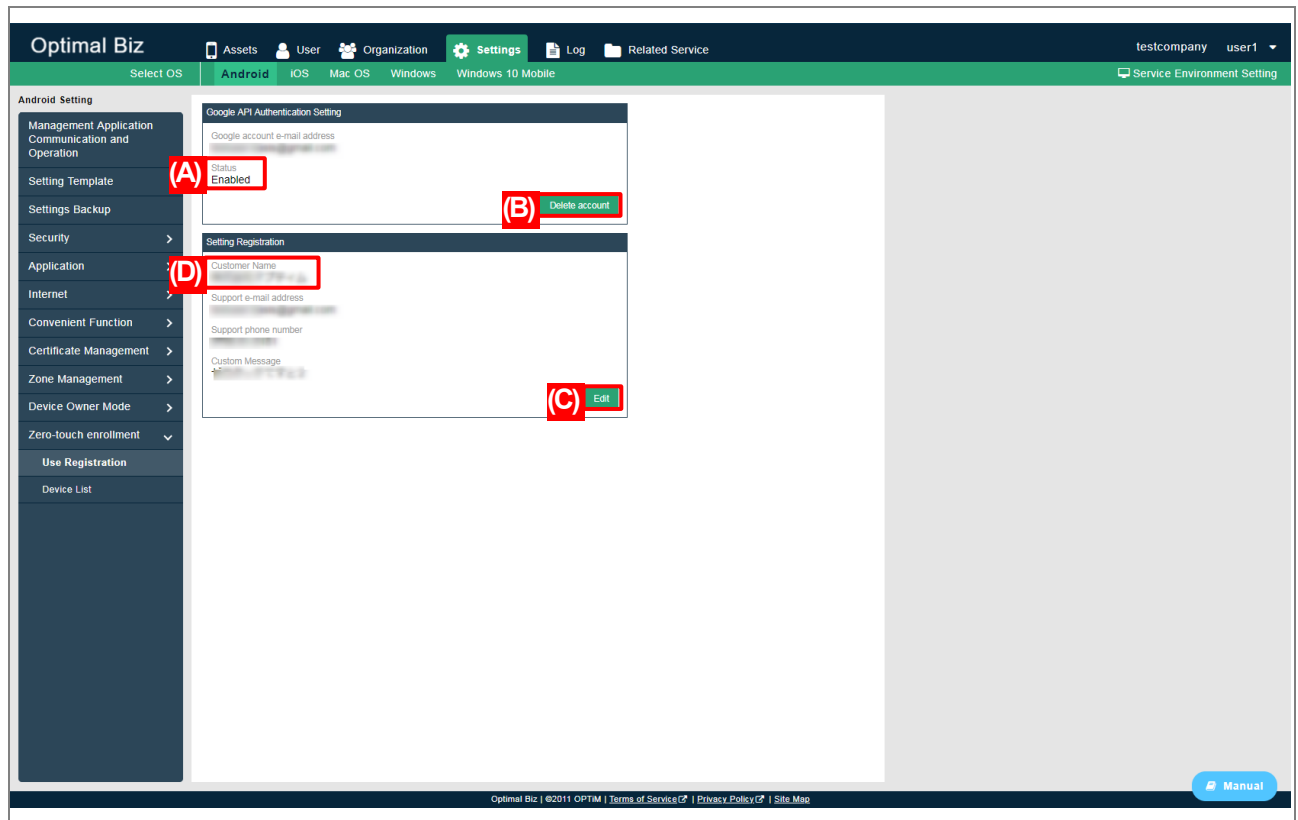
Optimal Biz | ©2011 OPTIM | [Terms of Service](#) | [Privacy Policy](#) | [Site Map](#) [Manual](#)

[11] After the setting registration, the use registration screen appears as shown below.

⇒ The "Status" (A) shows "Enabled".

✎ If you want to delete your account, click [Delete account] (B).

✎ The settings you entered during setting registration are displayed. If you want to change the settings, click [Edit] (C). You cannot change "Customer Name" (D).

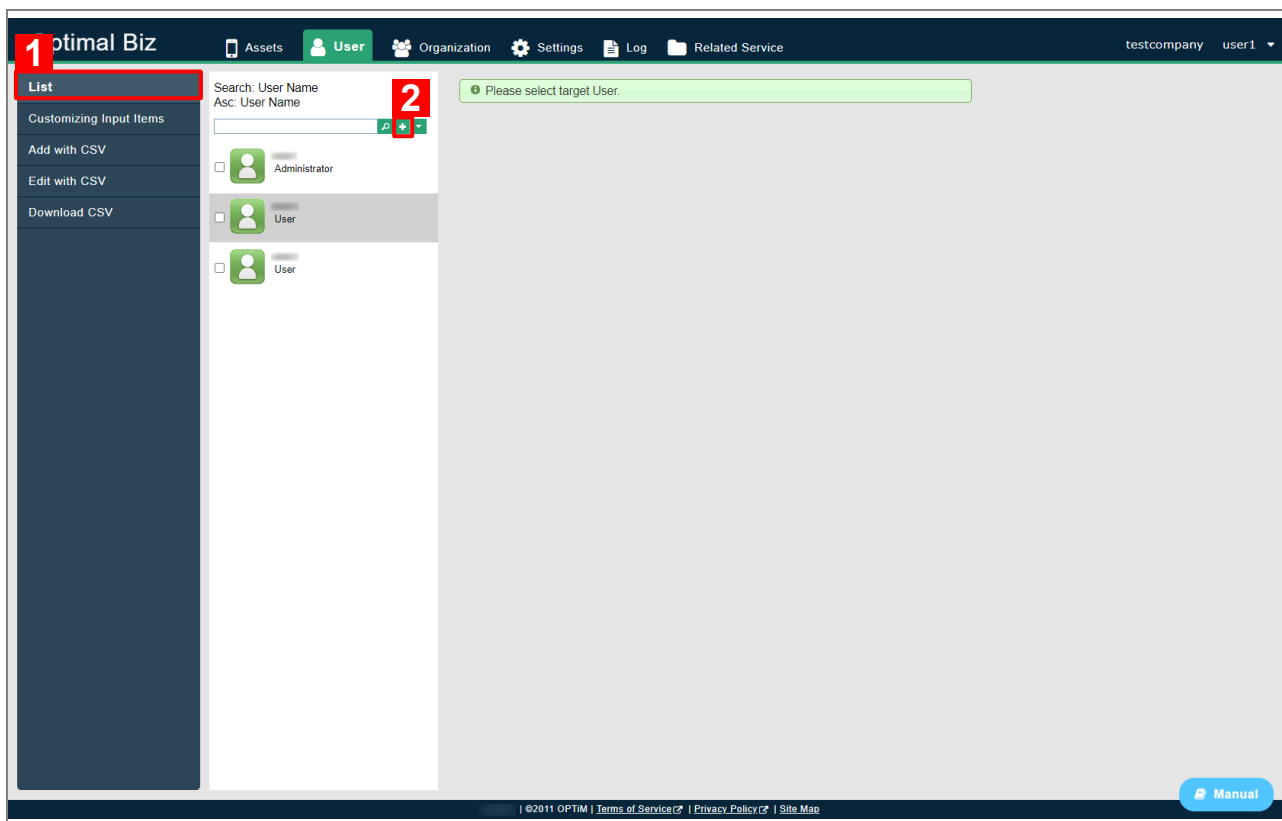


6.4 Creating a user

Follow the steps below to create a user.

[1] Click [User]→[List].

[2] Click .



[3] Enter an arbitrary name in "Name".

✎ For details of other input and setting items, refer to the following.

🔍 "User" - "List" - "Create a user" in <Management Site Reference Manual>

[4] Click [Save].

⇒ A user will be created.

The screenshot shows the 'Management Information - Editing' form in a web application. The form is divided into several sections:

- Management Information - Editing:** Contains fields for Name, Phonetic Name, Last Name, First Name, User ID, E-mail Address, User Classification (with radio buttons for Administrator, Operator, Reader, Lock/Wipe, Login only, and User), Organization, Category, and Device Authentication Limit.
- Password:** Contains a field for Current Password and an Edit button.
- Assets:** Contains a field for Number of Devices.
- SaaS ID Federation:** Contains fields for Office 365 and G Suite.

A red box highlights the 'Name' field, and a red '3' is placed next to it. The 'Save' button is highlighted with a red '4' next to it.

6.4.1 Registering a Google Workspace (formerly G Suite) account to an existing user

To register a Google Workspace (formerly G Suite) account to an existing user, carry out the steps below.

✍ If you have not registered a Google Workspace (formerly G Suite) account, license authentication during kitting will fail.

- [1] Go to [User]→[List], and select a target user from the list.**
- [2] Click [Edit].**

The screenshot displays the Optimal Biz user management interface. The top navigation bar includes 'Assets', 'User', 'Organization', 'Settings', 'Log', and 'Related Service'. The 'User' tab is active, showing a 'List' of users on the left and a detailed 'Edit' form on the right.

Step 1: In the 'List' view, the 'User' entry is highlighted with a red box and a red '1'.

Step 2: In the 'Edit' form, the 'Edit' button is highlighted with a red box and a red '2'.

The 'Edit' form contains the following sections:

- Management Information:** Fields for Name, Phonetic Name, Last Name, First Name, User ID, E-mail Address, User Classification, Organization, Category, and Limit Device Authentication.
- Password:** Fields for Current Password and a green 'Edit' button.
- Assets:** Field for Number of Devices.
- SaaS ID Federation:** Fields for Office 365 and G Suite.

The footer of the interface includes copyright information for ©2011 OPTIM and links to Terms of Service, Privacy Policy, and Site Map. A 'Manual' button is also present in the bottom right corner.

[3] Enter your Google Workspace (formerly G Suite) account in "E-mail Address".

[4] Click [Save].

⇒ The e-mail address will be registered to the user.

The screenshot displays a user management interface with a top navigation bar containing 'Admin', 'Apps and Books Setting', 'Access Control', 'Others', and 'Actions'. The 'Management Information - Editing' tab is active, showing various user details and settings. The 'E-mail Address' field is highlighted with a red box and a red '3'. The 'Save' button is highlighted with a red box and a red '4'.

Management Information - Editing

Name
Phonetic Name
Last Name
First Name
User ID
3 E-mail Address
User Classification
☐ Administrator (All operations are permitted)
☐ Operator
☐ Reader (Unable to edit)
☐ Lock/Wipe only
☐ Login only (Select permissions)
☒ User (Unable to log in)
Organization
Category
(Uncategorized)
Device Authentication Limit
☒ No Restriction
☐ Restricted devices
☐ Prohibit authentication
Cancel **4** Save

Password
Current Password

Edit

Assets
Number of Devices
0

SaaS ID Federation
Office 365
(None)
G Suite
(None)

6.5 Performing kitting with zero-touch enrollment (using a Google Workspace (formerly G Suite) account)

Follow the steps below to perform kitting for your device by means of zero-touch registration.

Note that the operation is different between Android versions earlier than 10 and versions 10 or later. Depending on the Android version of your device, choose one of the following methods.

● **For less than Android 10**

● **For Android 10 or later**

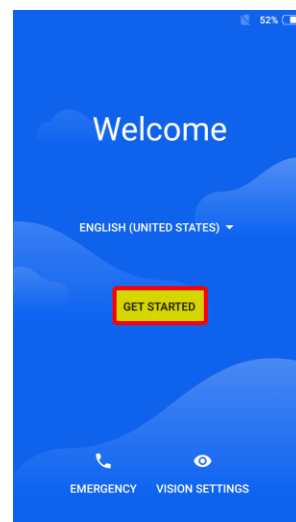
- ✚ When you are kitting Android 10 or later, kitting operation may not be able to complete if you have set Google Play Developer Services (com.google.android.gms) on the management site's "Application prohibition" blacklist and "Non-display application". Refer to the following to clear the setting in advance and then conduct kitting.

🔍 "Settings – Android" - "Application" - "Application prohibition" in <Management Site Reference Manual>

🔍 "Settings – Android" - "Device Owner Mode" - "Non-display application" in <Management Site Reference Manual>

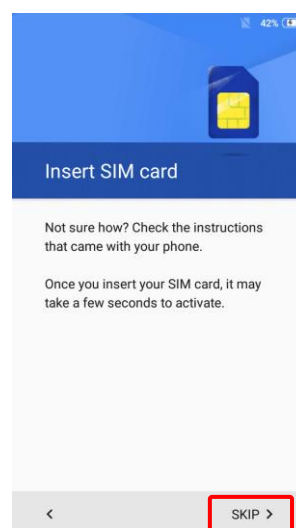
6.5.1 For less than Android 10

[1] Tap [GET STARTED].

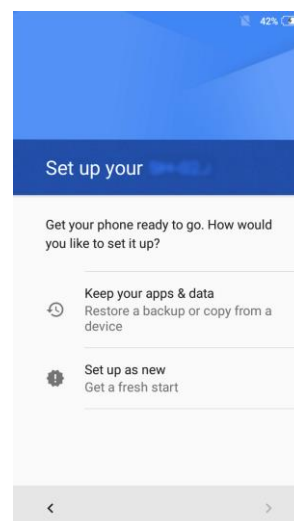


[2] Tap [SKIP].

- ✚ If a SIM card is already inserted, this screen does not appear.



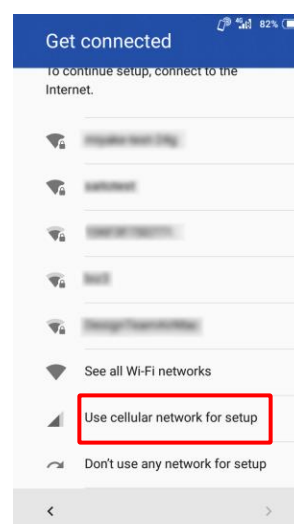
[3] Tap [Set up as new].



[4] Tap [Use cellular network for setup] or tap a Wi-Fi SSID to connect to Wi-Fi.

<<If you do not have a SIM>>

[Use cellular network for setup] will not be displayed, so connect to Wi-Fi.

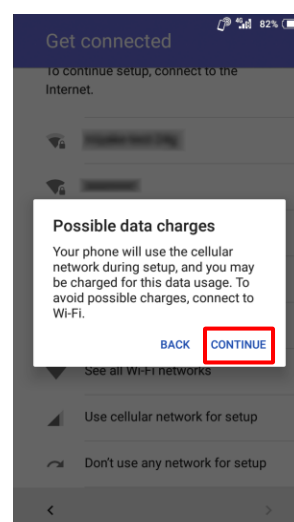


<<If you use a cellular network>>

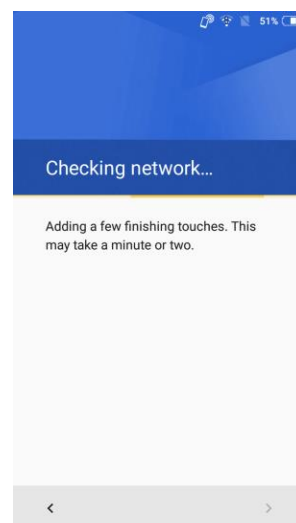
When a pop-up appears as shown on the screen on the right, tap [CONTINUE].

<<If you use a Wi-Fi connection>>

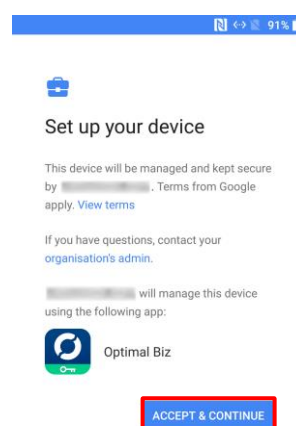
Continue with the next step.



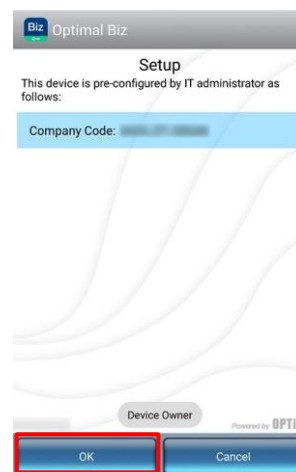
[5] Network connection starts.



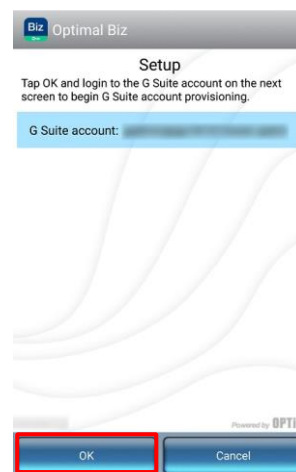
[6] Tap [ACCEPT & CONTINUE].



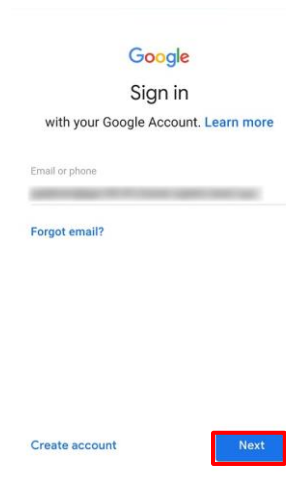
[7] Tap [OK].



[8] Tap [OK].

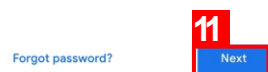
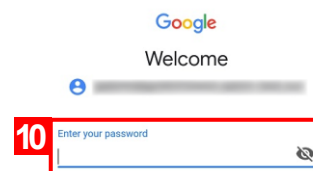


[9] Tap [Next].

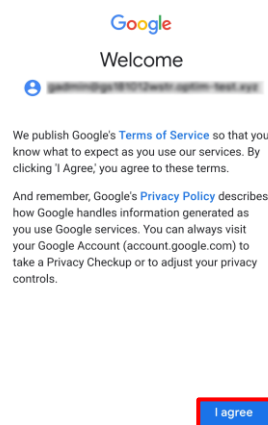


[10] Enter the password.

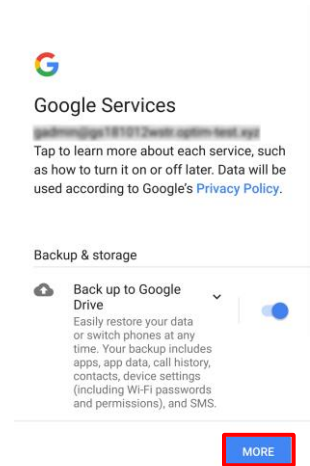
[11] Tap [Next].



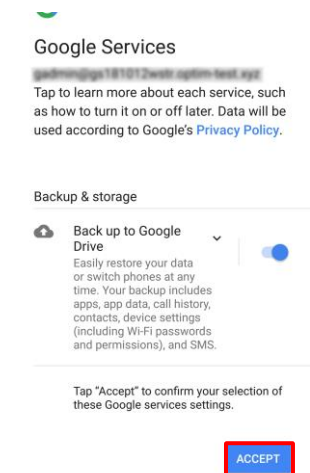
[12] Tap [I agree].



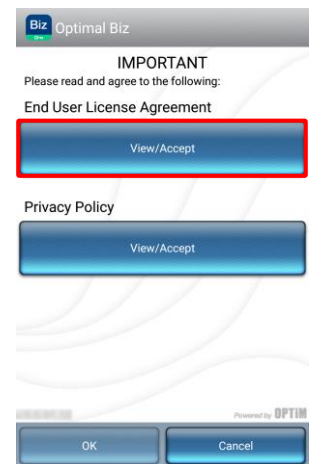
[13] Tap [MORE].



[14] Tap [ACCEPT].

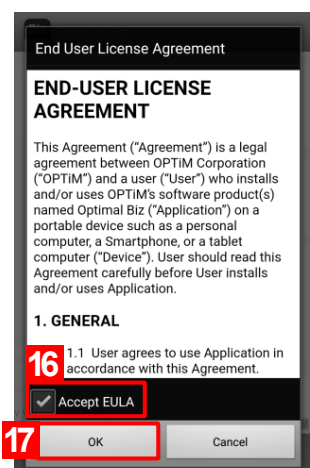


[15] Tap [View/Accept] for the End User License Agreement.



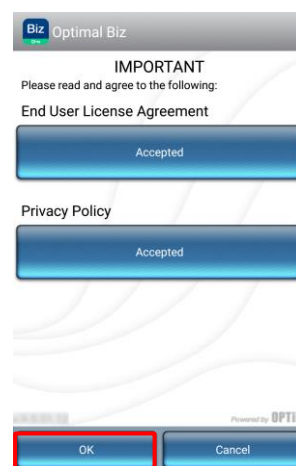
[16] Check "Accept EULA".

[17] Tap [OK].

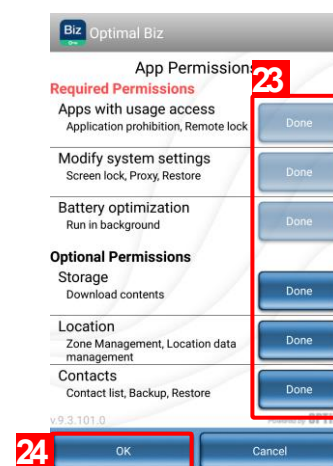


[22] Tap [OK].

- ☑ You cannot tap [OK] unless you agree to both the EULA and privacy policy.

**[23] A screen that requests permission appears. Follow the on-screen instructions to set things up.****[24] Tap [OK].**

- ⇒ The license authentication screen appears. Continue with the license authentication.

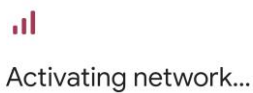


6.5.2 For Android 10 or later

[1] Tap [Get Started].

« If you are inserting SIM »

The following screen is displayed.



[2] Tap [Skip].

« If using a mobile network »

Insert a SIM if it is not already inserted.

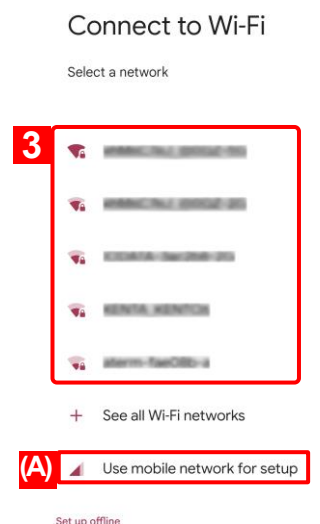
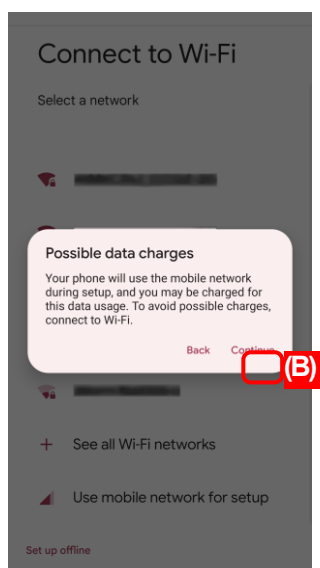


[3] Tap a Wi-Fi SSID to connect to Wi-Fi.

« If using a mobile network »

Tap [Use mobile network for setup] (A).

Tap [Continue] (B) when a following pop-up is displayed.



⇒ The network connection starts and checking information.



Getting your phone ready...

This may take a few minutes



Checking info...

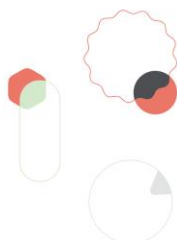


[4] Tap [Next].

⇒ Getting ready for work setup.



Getting ready for
work setup...

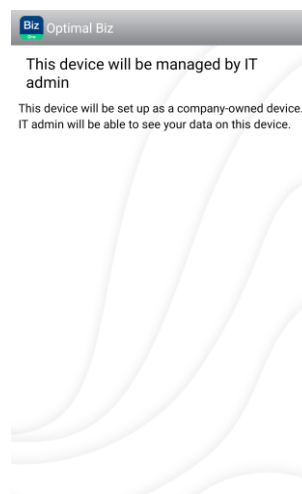


This device belongs
to your organization

To learn more, contact your IT admin.

4 Next

[5] Tap [OK].



5 OK

[6] Tap [Accept & Conetinue].

⇒ Setting up in the device.



Keep your work apps
at your fingertips



Let's set up your
work device

[View terms](#)



6 Accept & continue

Setting up your device...

[7] Tap [Next].**This device isn't private****Your activity & data**


Your IT admin may be able to see your data and activity on this device.

App permissions

Your IT admin can set permissions for apps on this device, such as microphone, camera, and location permissions.

Cancel setup

**[8] Tap [More].**

 [More] is displayed several times on some devices. Tap [More] until [Accept] is displayed.

**Google Services**

Tap to learn more about each service, such as how to turn it on or off later. Data will be used according to Google's [Privacy Policy](#).

Location**Use location**

Allow apps and services with location permission to use your device's location. Google may collect location data periodically and use this data in an anonymous way to improve location accuracy and location-based services.

Allow scanning

Allow apps and services to scan for Wi-Fi

**[9] Tap [Accept].**

Allow apps and services to scan for Wi-Fi networks and nearby devices at any time, even when Wi-Fi or Bluetooth is off.

Device maintenance**Send usage and diagnostic data**

Help improve your Android device experience by automatically sending diagnostic, device, and app usage data to Google. This will help battery life, system and app stability, and other improvements. Some aggregate data will also help Google apps and partners, such as Android developers. If your additional Web & App Activity setting is turned on, this data may be saved to your Google Account.

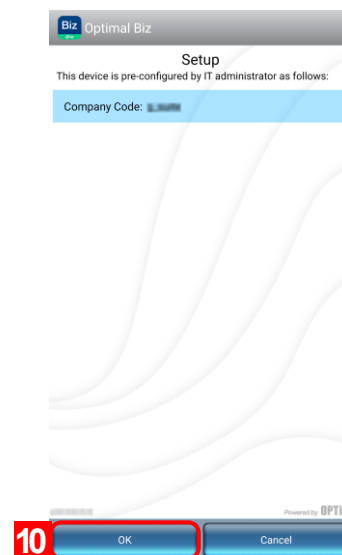
Install updates & apps

By continuing, you agree that this device may also automatically download and install updates and apps from Google, your carrier, and your device's manufacturer, possibly using cellular data. Data rates may apply. Some of these apps may offer in-app purchases.

Tap "Accept" to confirm your selection of these Google services settings.



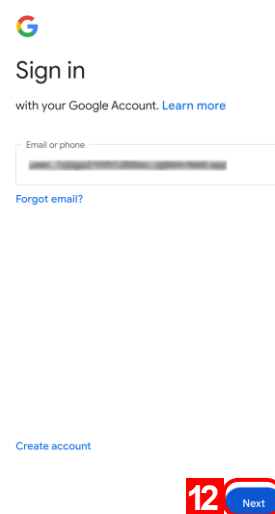
[10] Tap [OK].



[11] Tap [OK].



[12] Tap [Next].



[13] Enter "Password".

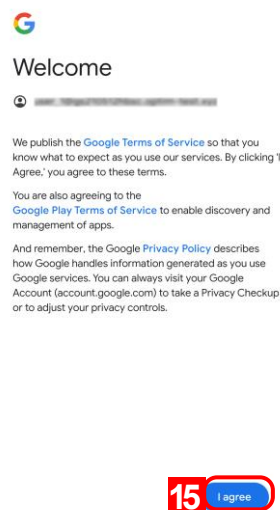
[14] Tap [Next].



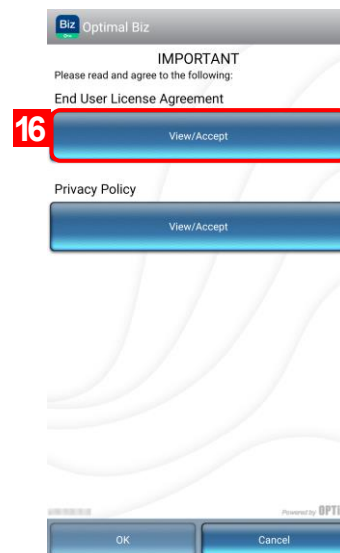
[15] Tap [I agree].

<<For Android 12>>

When you tap [I agree], the following dialog is displayed. Tap [OK] (A).

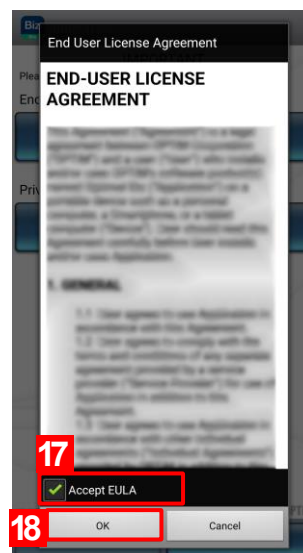


[16] Tap [View/Accept] for the End User License Agreement.

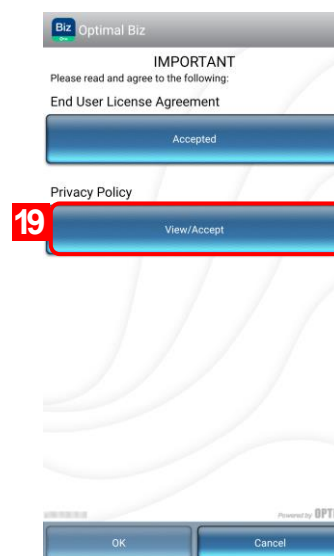


[17] Check "Accept EULA".

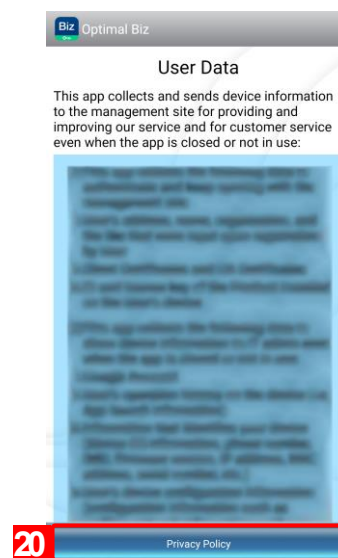
[18] Tap [OK].



[19] Tap [View/Accept] for the Privacy Policy.

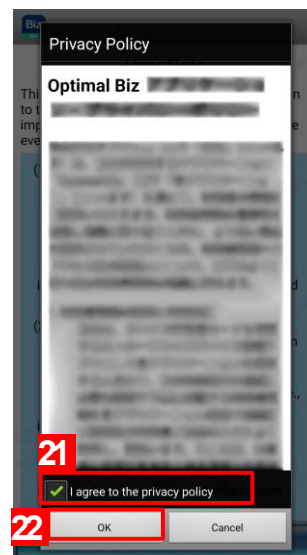


[20] Read the user data policy, and tap [Privacy Policy].

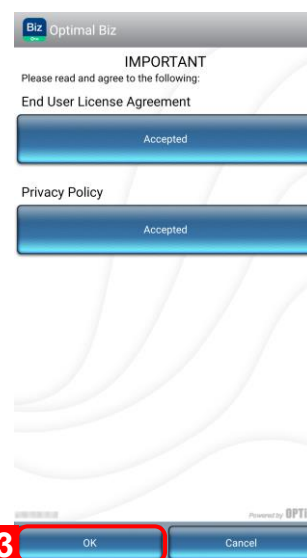


[21] Check "I agree to the privacy policy".

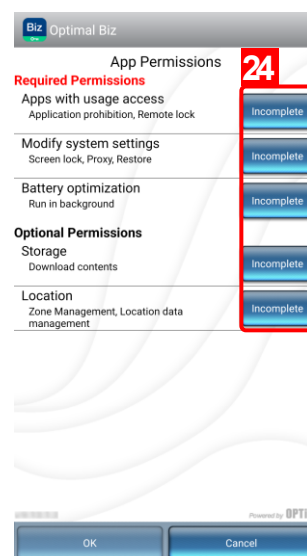
[22] Tap [OK].

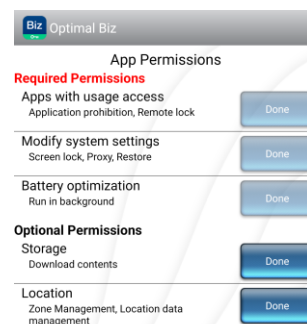


[23] Tap [OK].

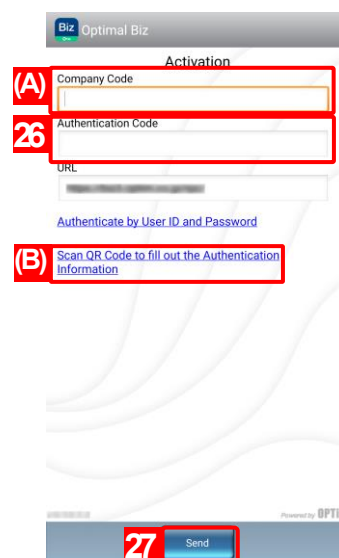


[24] A screen that requests permission appears. Follow the on-screen instructions to set things up.



[25] Tap [OK].**[26] Enter an "Authentication Code".**

- ✓ Contact your administrator for your authentication code.
- ✎ "Company Code" (A) will be entered automatically.
- ✎ If you tap [Scan QR Code to fill out the Authentication information] (B) and scan a QR code for agent license activation, the "Company code", "Authentication code", and "URL" will be automatically entered. Contact your administrator for the QR code.

**[27] Tap [Send].**

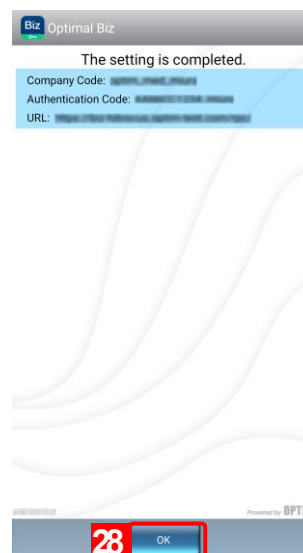
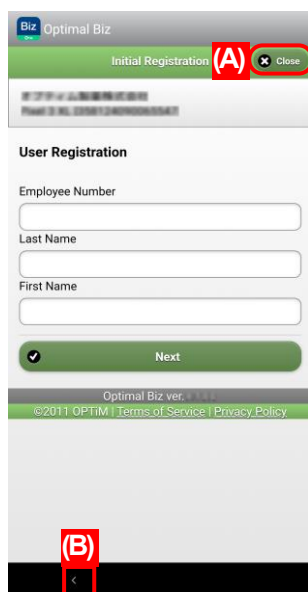
**[28] The license authentication completion screen appears.
Tap [OK].**

« When portal settings are set to be displayed on Management Site »

After you tap [OK], initial registration screen appears.

Enter items as necessary.

- ☑ The user will link to the device if the initial registration has been made.
- ☑ If you do not need to register, you can either tap [Close] (A) or (B) the back button on the device to close the screen.
- ☑ If the user is already linked to the device, a message will appear and say that the user has been linked. Close the screen.



[29] Tap [Skip].

⇒ Kitting is complete.

License authentication is also complete. Proceed to "Syncing with the zero-touch registration server".

☞ "Syncing with the zero-touch registration server" Page 189



All set!

You're ready to start using your phone



Swipe to navigate
your phone

Learn gestures to go Home, go back, and
switch apps



29

Skip

Try it

System navigation settings

Swipe up to go Home



6.6 Performing license authentication

After kitting is complete, perform license authentication with your User ID or company code / authentication code.

- ✍ If you are using Android Enterprise, after you perform license authentication with the user ID registered from the management site, it will be integrated with Android Enterprise.
If you have not registered your user ID, the user ID can be integrated with Android Enterprise by performing a license authentication with a company code / authentication code, registering the user ID from the management site, and linking it with your device.
- ✍ Android 10 or later are license authenticated by kitting, so this operation is not necessary. Proceed to the next operation.

☞ "Syncing with the zero-touch registration server" Page 189

6.6.1 Authenticating by a user ID

[1] Tap [Authenticate with User ID and Password].

- ✍ "Company Code" (A) will be entered automatically.
- ✍ Your Google Workspace (formerly G Suite) account will appear as "Email Address" (B).

The screenshot shows the 'Optimal Biz' activation screen. At the top, it says 'Biz Optimal Biz'. Below that is the title 'Activation'. There are three input fields: 'Company Code' (labeled with a red box and 'A'), 'Authentication Code', and 'URL'. Below these is a red box labeled 'B' containing 'E-mail Address'. A red box labeled '1' highlights the button 'Authenticate by User ID and Password'. Below this button is a link: 'Scan QR Code to fill out the Authentication Information'. At the bottom, it says 'v9.3.101.0' and 'Powered by OPTIM'. A 'Send' button is at the very bottom.

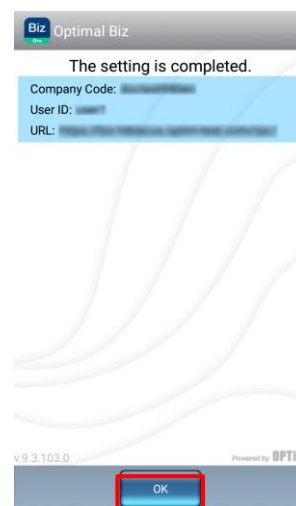
[2] Enter "User ID or Email Address" and "Password".

- ✍ If a user has been assigned to the device, "User ID or email address" will be entered automatically.
- ✍ Contact your administrator for your user ID and password.
- ✍ You do not have to change the URL (A).


[3] Tap [Send].

The screenshot shows the 'Optimal Biz' activation screen. At the top, it says 'Biz Optimal Biz'. Below that is the title 'Activation'. There are three input fields: 'Company Code', 'User ID or E-mail Address' (labeled with a red box and '2'), and 'Password'. Below these is a red box labeled 'A' containing 'URL'. A red box labeled '3' highlights the 'Send' button at the bottom. Below the 'URL' field is a link: 'Authenticate by Authentication code.' Below that is another link: 'Scan QR Code to fill out the Authentication Information'. At the bottom, it says 'v9.3.103.0' and 'Powered by OPTIM'.

- [4] The license authentication completion screen appears. Tap [OK].**



- [5] The agent menu screen appears.**

-  After license authentication, users cannot interact with the agent screen until the initial synchronization is complete at the management site.



6.6.2 Authenticating by a company code / authentication code

✍ After license authentication is complete, allocate a user to the device on the management site.

🔍 "Asset" - "List" - "Asset management information" in <Management Site Reference Manual>

[1] Enter an "Authentication Code".

- ✍ Contact your administrator for your authentication code.
- ✍ "Company Code" (A) will be entered automatically.
- ✍ Your Google Workspace (formerly G Suite) account will appear as "Email Address" (B).
- ✍ If you tap [Scan QR Code to fill out the Authentication information] (C) and scan a QR code for agent license activation, the "Company code", "Authentication code", and "URL" will be automatically entered. Contact your administrator for the QR code.

[2] Tap [Send].

[3] The license authentication completion screen appears. Tap [OK].

« When portal settings are set to be displayed on Management Site »

After you tap [OK], initial registration screen appears.
Enter items as necessary.

- ✍ The user will link to the device if the initial registration has been made.
- ✍ If you do not need to register, you can either tap [Close] (A) or (B) the back button on the device to close the screen.
- ✍ If the user is already linked to the device, a message will appear and say that the user has been linked. Close the screen.

[4] The agent menu screen appears.

- ✓ After license authentication, users cannot interact with the agent screen until the initial synchronization is complete at the management site.



6.7 Syncing with the zero-touch registration server

Follow the steps below to sync with the zero-touch registration server and display device information on the management site.

- ✎ If each function setting has been registered, the function will be allocated to the device at the same time as kitting. To perform settings for functions, refer to the following.

🔍 "Settings - Android" in <Management Site Reference Manual>

[1] Click [Settings]→[Android]→[Zero-touch enrollment]→[Device List].

[2] Click [Sync with the zero-touch enrollment server].

- ✎ The zero-touch devices displayed in the zero-touch device list are displayed as devices waiting for license authentication in the device list of Device List.

🔍 "Asset" "List"-"Asset list" in -<Management Site Reference Manual>

- ✎ Devices cannot be deleted from the zero-touch device list. Delete them from the device list of the device screen. If you delete a device from the device list of the device screen, it is also deleted from the zero-touch device list.

🔍 "Asset" - "List" - "Deleting asset individually" in <Management Site Reference Manual>

- ✎ Do not create a new zero-touch device from the device screen.

- ✎ Clicking [IMEI/Serial Number] (A) displays the device list of the device screen.

The screenshot shows the Optimal Biz management site interface. The top navigation bar includes 'Assets', 'User', 'Organization', 'Settings', 'Log', and 'Related Service'. The 'Settings' tab is active, and the 'Android' sub-tab is selected. The left sidebar shows the 'Device List' option under 'Zero-touch enrollment'. The main content area displays a table of zero-touch enrollment settings. A red box labeled '1' highlights the 'Device List' option in the sidebar. A red box labeled '2' highlights the 'Sync with the zero-touch enrollment server' button. A red box labeled '(A)' highlights the 'IMEI/Serial Number' column header in the table.

IMEI/Serial Number	User Name	Manufacturer	Update Date/Time of zero-touch enrollment setting	Sync Date/Time of zero-touch enrollment setting
			14 Nov 2018 17:15	14 Nov 2018 17:15
			14 Nov 2018 13:33	14 Nov 2018 17:15
			14 Nov 2018 13:33	14 Nov 2018 17:15
			14 Nov 2018 13:33	14 Nov 2018 17:15

7 Other kitting methods

Perform kitting for your device using a QR code or NFC.




The kitting method will vary depending on the device and account you use. Choose an appropriate kitting method.

This chapter describes the following items.

Item	Page
Performing kitting using a QR code	191
Performing kitting using NFC	206
Performing license authentication	212




Attention

- To execute kitting, you must factory reset the device (initial setup screen).
- If you are using Android Enterprise, you must first register your Google account on the management site. For details, refer to the following.
 "Integrating Android Enterprise with a Google account Google" Page 11
- Kitting can be performed on Android 6.0 or later. However, some devices do not support it. For details, refer to the following.
 <Android Support Device List>
-  Performance is guaranteed only for Android 9 or later.
- If you are switching from a legacy agent, factory reset the device and then perform kitting.



Reference

- By setting up the "Application Distribution" function of Android Enterprise on the management site in advance, apps can be distributed to your device at the same time as license authentication after kitting is complete. For details of app distribution, refer to the following.
 "Android Enterprise App distribution" in <Android Enterprise Manual>

7.1 Performing kitting using a QR code

You can perform kitting by scanning a QR code.


7.1.1 Displaying a QR code

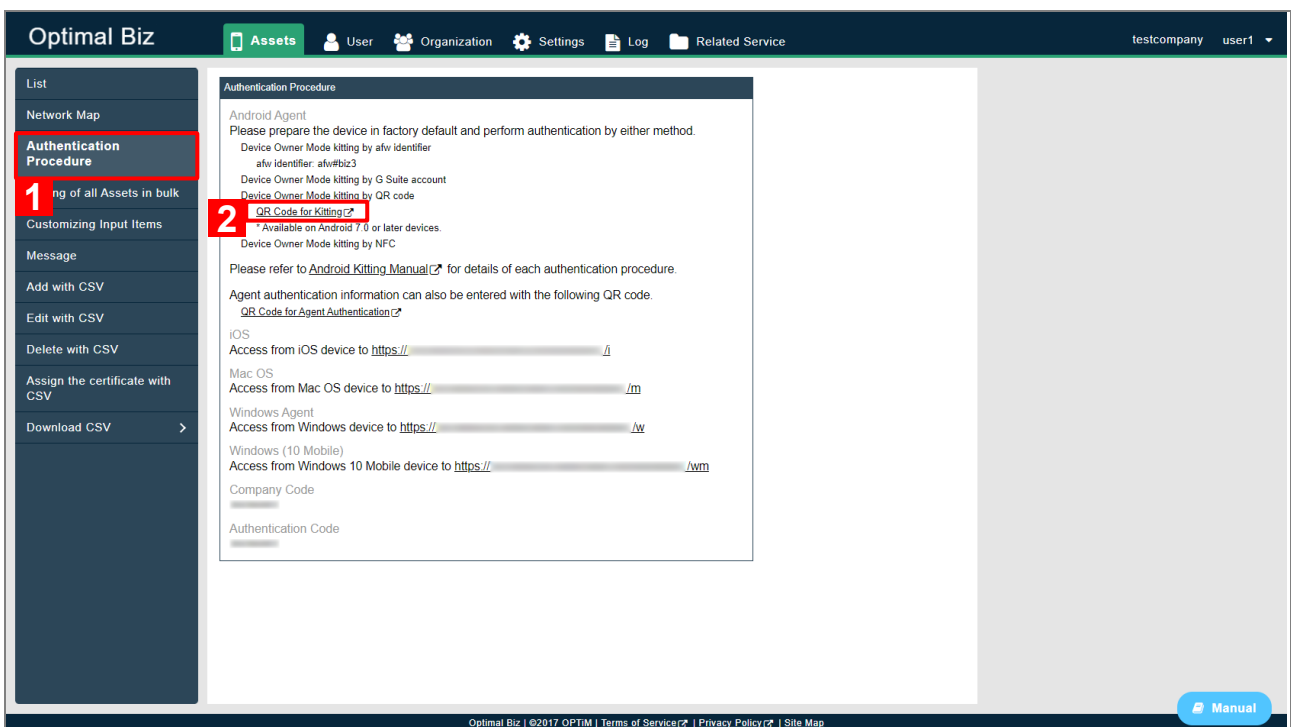
[1] Click [Assets]→[Authentication Procedure].

[2] Click [QR Code for Kitting].

⇒ Clicking it will display a QR code for Device Owner Mode kitting.

Scan the displayed QR code into your device as described in step **[6]** of Scanning a QR code into your device.

 If the agent version is updated, the QR code changes. Check the management site for the latest QR code.



Optimal Biz

Assets User Organization Settings Log Related Service testcompany user1

List

Network Map

Authentication Procedure

1 ing of all Assets in bulk

Customizing Input Items

Message

Add with CSV

Edit with CSV

Delete with CSV

Assign the certificate with CSV

Download CSV >

2 QR Code for Kitting

Authentication Procedure

Android Agent

Please prepare the device in factory default and perform authentication by either method.

Device Owner Mode kitting by afw identifier
afw identifier: afw#biz3

Device Owner Mode kitting by G Suite account

Device Owner Mode kitting by QR code

Device Owner Mode kitting by NFC
* Available on Android 7.0 or later devices.

Please refer to [Android Kitting Manual](#) for details of each authentication procedure.

Agent authentication information can also be entered with the following QR code.
[QR Code for Agent Authentication](#)

iOS
Access from iOS device to <https://.../i>

Mac OS
Access from Mac OS device to <https://.../m>

Windows Agent
Access from Windows device to <https://.../w>

Windows (10 Mobile)
Access from Windows 10 Mobile device to <https://.../wm>

Company Code

Authentication Code

Manual

Optimal Biz | ©2017 OPTIM | [Terms of Service](#) | [Privacy Policy](#) | [Site Map](#)

7.1.2 Scanning a QR code into your device

Configure settings from the factory reset status (initial setup screen).

Note that the operation is different between Android versions earlier than 10 and versions 10 or later. Depending on the Android version of your device, choose one of the following methods.

● **For less than Android 10**

● **For Android 10 or later**

- ✎ When you are kitting Android 10 or later, kitting operation may not be able to complete if you have set Google Play Developer Services (com.google.android.gms) on the management site's "Application prohibition" blacklist and "Non-display application". Refer to the following to clear the setting in advance and then conduct kitting.

🔍 "Settings – Android" - "Application" - "Application prohibition" in <Management Site Reference Manual>

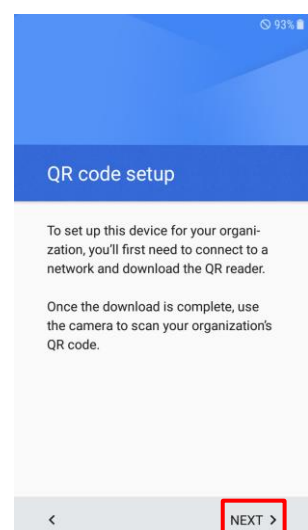
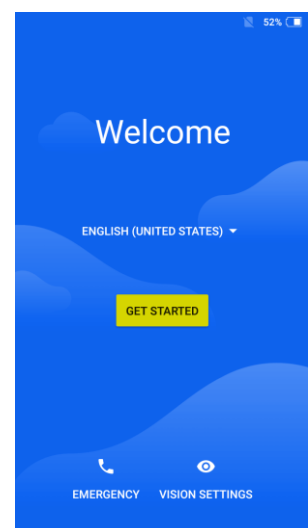
🔍 "Settings – Android" - "Device Owner Mode" - "Non-display application" in <Management Site Reference Manual>

7.1.2.1 For less than Android 10


[1] Tap the initial setup screen six times.

- ✎ Avoid links such as [GET STARTED] or "Emergency" and tap anywhere on the background six times.

[2] Tap [NEXT].



[3] Tap [Use cellular network for setup] or tap a Wi-Fi SSID to connect to Wi-Fi.

 A cellular network may not be available.

<<If you do not have a SIM>>

[Use cellular network for setup] will not be displayed, so connect to Wi-Fi.

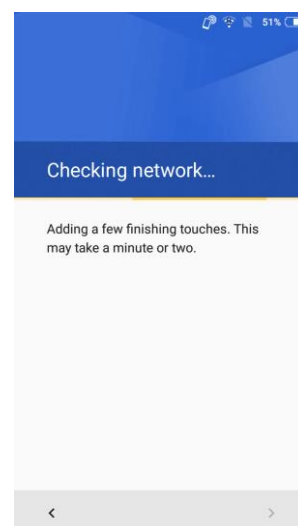
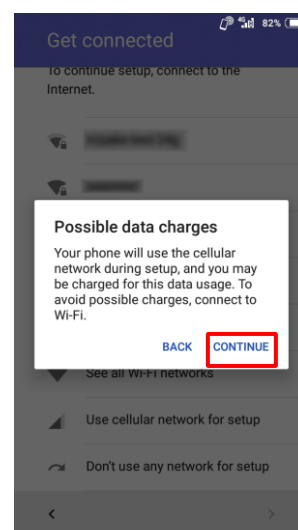
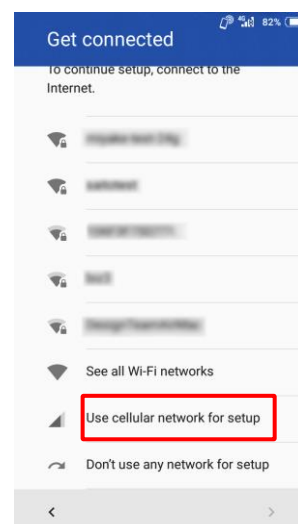
<<If you use a cellular network>>

When a pop-up appears as shown on the screen on the right, tap [CONTINUE].

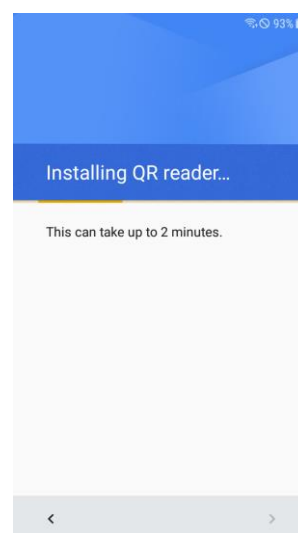
<<If you use a Wi-Fi connection>>

Continue with the next step.

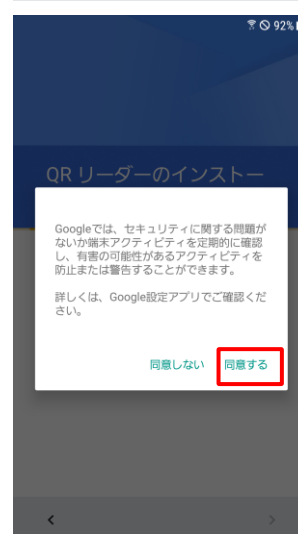
[4] Network connection starts.



【5】 The QR reader will be installed.



【6】 Tap [ACCEPT].



【7】 The camera starts up. Scan the QR code for Device Owner Mode kitting displayed on the management site.

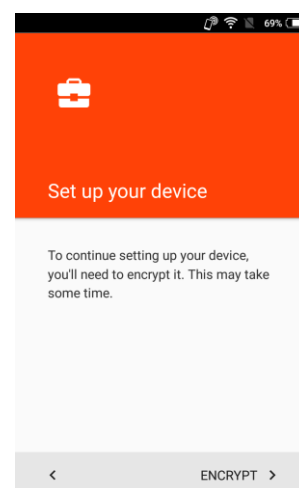
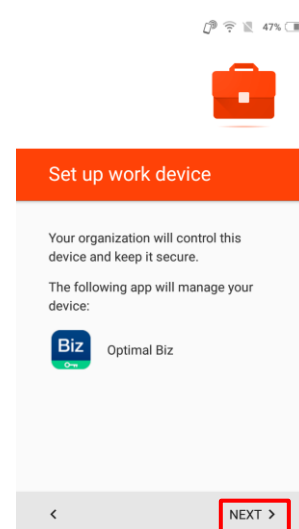
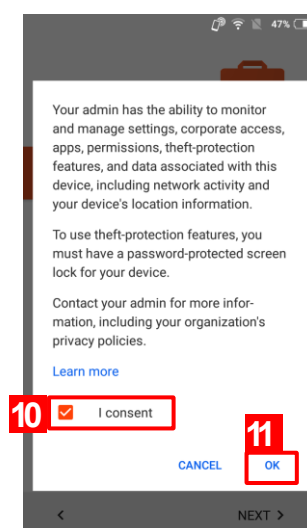
 For details, refer to the following.

 "Displaying a QR code" Page 152



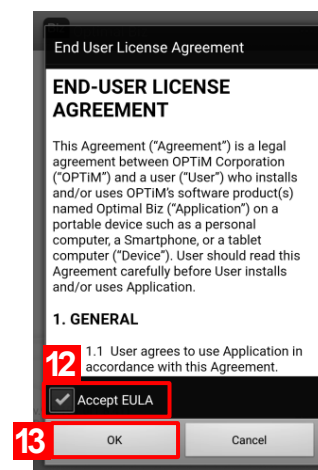
[8] Tap [Encrypt].

- ✓ Without encryption, kitting may not be performed properly for the agent in some devices. Some devices do not display this screen.
- ✎ Follow the on-screen instructions to perform encryption. Once encryption is complete, the device will reboot. On the network connection screen that appears after the reboot, select a network you want to use.

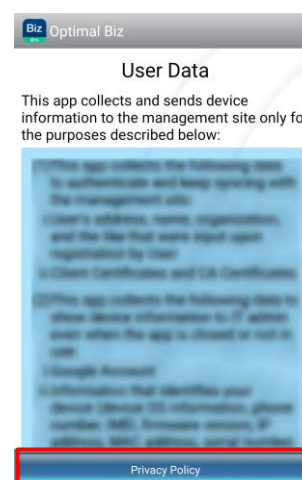
**[9] Kitting is performed for the agent while it is enabled.****[10] Check "I consent".****[11] Tap [OK].**

[12] Check "Accept EULA".

[13] Tap [OK].



[14] Read the user data policy, and tap [Privacy Policy].



[15] Check "I agree to the privacy policy".

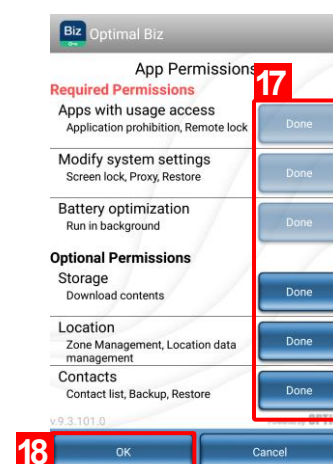
[16] Tap [OK].



[17] A screen that requests permission appears. Follow the on-screen instructions to set things up.

[18] Tap [OK].

⇒ The license authentication screen appears. Continue with the license authentication.



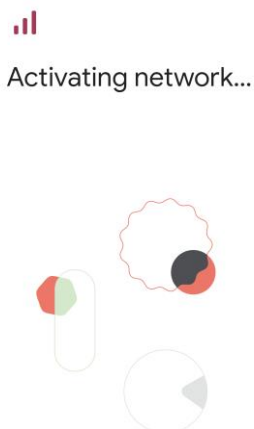
7.1.2.2 For Android 10 or later

[1] Tap the initial setup screen six times.

✎ Avoid links such as [Get Started] or "Emergency" and tap anywhere on the background six times.

« If you are inserting SIM »

The following screen is displayed.



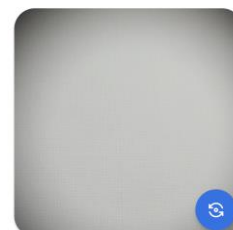
[2] The camera starts up. Scan the QR code for Device Owner Mode kitting displayed on the management site.

✎ For details, refer to the following.

👉 "Displaying a QR code" Page 191



Scanning for a QR code...



[3] Tap [Skip].

« If using a mobile network »

Insert a SIM if it is not already inserted.



Connect to mobile network

If you have a SIM card, insert it now



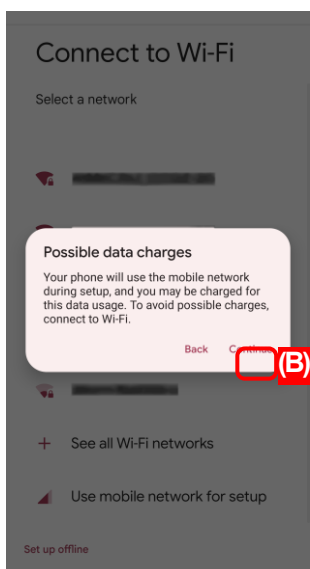
3 Skip

[4] Tap a Wi-Fi SSID to connect to Wi-Fi.

« If using a mobile network »

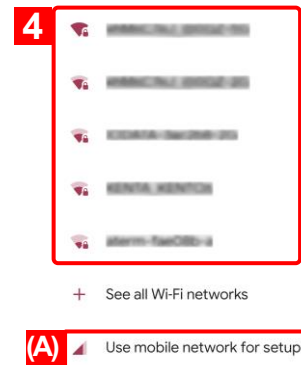
Tap [Use mobile network for setup] (A).

Tap [Continue] (B) when a following pop-up is displayed.



Connect to Wi-Fi

Select a network



Set up offline

⇒ Network connection starts.



Getting your phone
ready...

This may take a few minutes



[5] Tap [Next].

⇒ Getting ready for work setup.



Getting ready for
work setup...



This device belongs
to your organization

To learn more, contact your IT admin.



[6] Tap [OK].



This device will be managed by IT
admin

This device will be set up as a company-owned device.
IT admin will be able to see your data on this device.



[7] Tap [Accept & Conetinue].

⇒ Setting up in the device.



Keep your work apps
at your fingertips

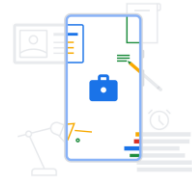


Setting up your device...



Let's set up your
work device

[View terms](#)



7 Accept & continue

[8] Tap [Next].

This device isn't
private

🔒 Your activity & data

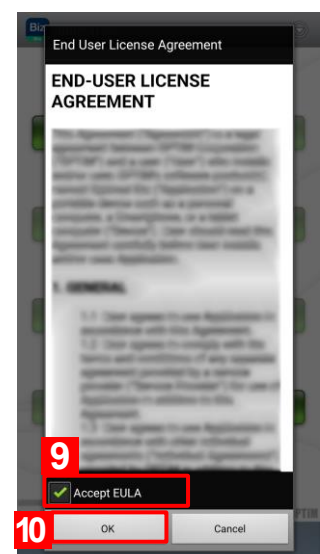
Your IT admin may be able to see your data and activity on this device.

📱 App permissions

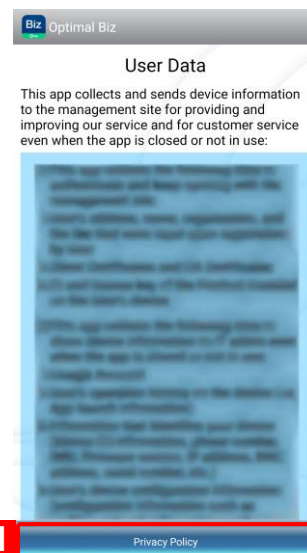
Your IT admin can set permissions for apps on this device, such as microphone, camera, and location permissions.

Cancel setup

8 Next

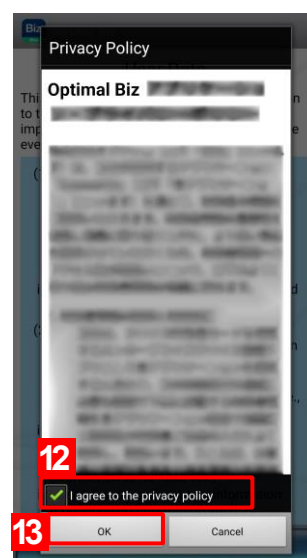
[9] Check "Accept EULA".**[10] Tap [OK].**

[11] Read the user data policy, and tap [Privacy Policy].

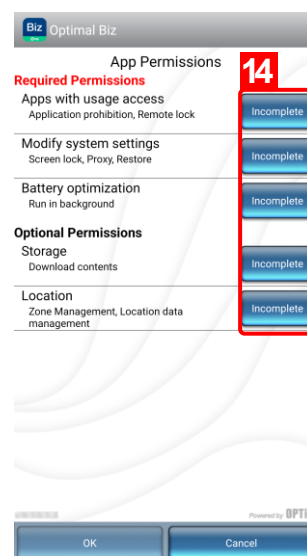


[12] Check "I agree to the privacy policy".

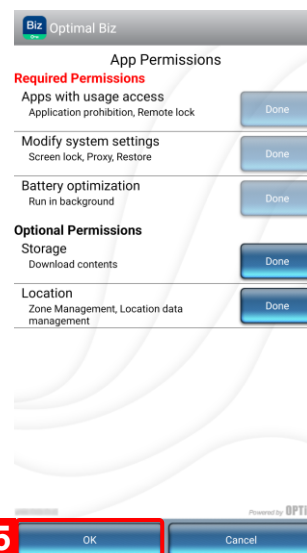
[13] Tap [OK].



[14] A screen that requests permission appears. Follow the on-screen instructions to set things up.



[15] Tap [OK].



[16] Enter an "Authentication Code".

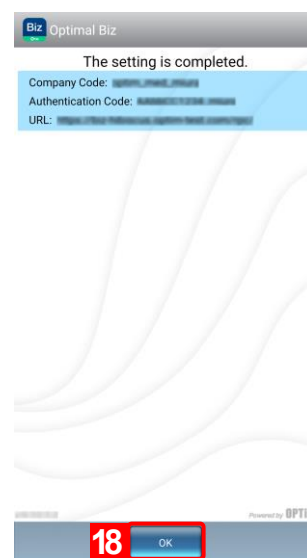
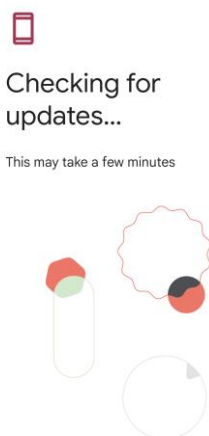
- ✍️ Contact your administrator for your authentication code.
- ✍️ "Company Code" (A) will be entered automatically.
- ✍️ If you tap [Scan QR Code to fill out the Authentication information] (B) and scan a QR code for agent license activation, the "Company code", "Authentication code", and "URL" will be automatically entered. Contact your administrator for the QR code.



[17] Tap [Send].

[18] The license authentication completion screen appears. Tap [OK].

⇒ Checking for updates.



« When portal settings are set to be displayed on Management Site »

After you tap [OK], initial registration screen appears.

Enter items as necessary.

- ✎ The user will link to the device if the initial registration has been made.
- ✎ If you do not need to register, you can either tap [Close] (A) or (B) the back button on the device to close the screen.
- ✎ If the user is already linked to the device, a message will appear and say that the user has been linked. Close the screen.

[19] Tap [More].

- ✎ [More] is displayed several times on some devices. Tap [More] until [Accept] is displayed.



Google Services

Tap to learn more about each service, such as how to turn it on or off later. Data will be used according to Google's [Privacy Policy](#).

Location

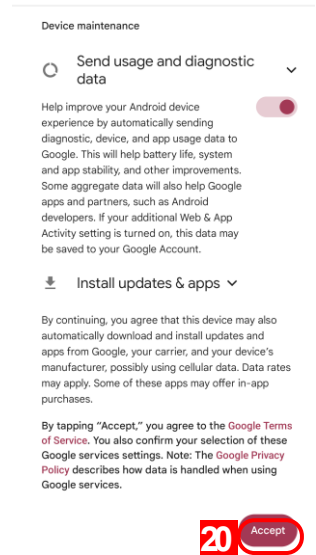
Use location ▾

Allow apps and services with location permission to use your device's location. Google may collect location data periodically and use this data in an anonymous way to improve location accuracy and location-based services.

Allow scanning ▾

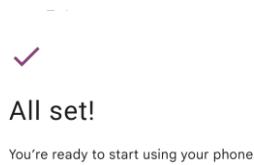
Allow apps and services to scan for Wi-Fi networks and nearby devices at any time.



[20] Tap [Accept].**[21] Tap [Skip].**

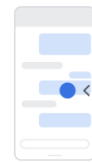
⇒ Kitting is complete.

License authentication is also complete.



Swipe to navigate
your phone

Learn gestures to go Home, go back, and
switch apps



System navigation settings

Swipe up to go Home




7.2 Performing kitting using NFC

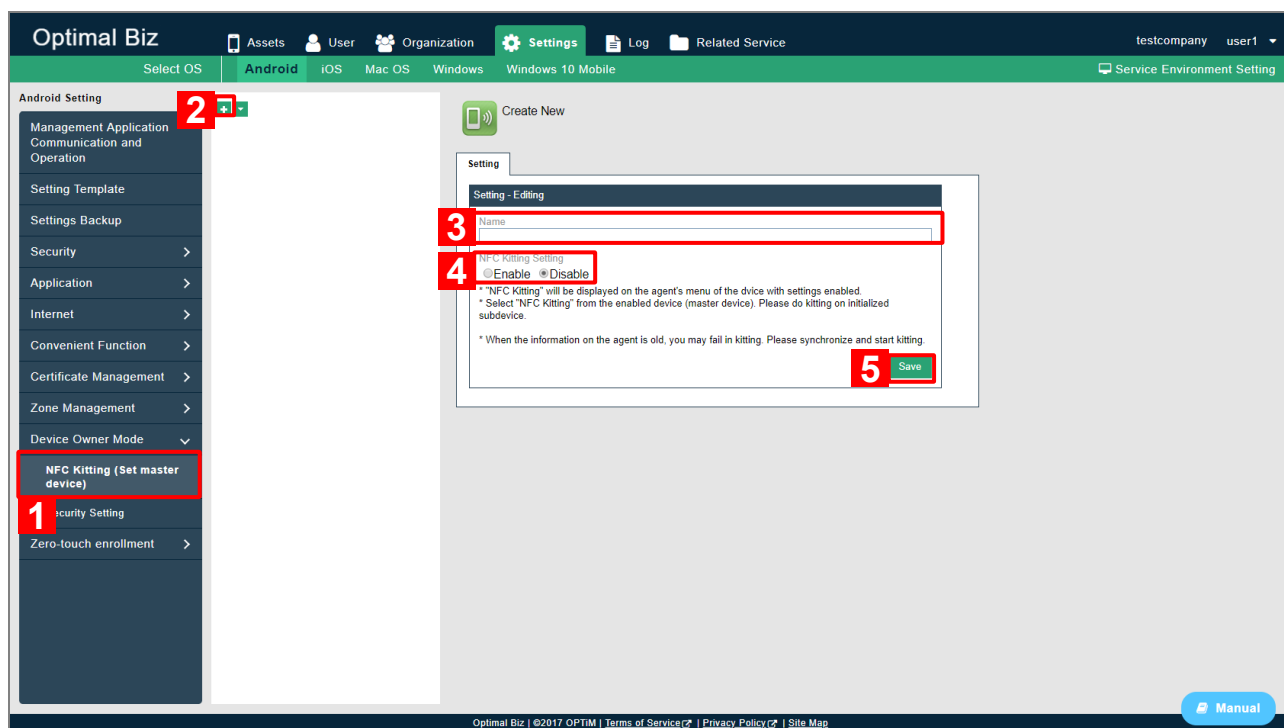
NFC allows you to easily perform kitting for multiple subdevices (kitting target devices) by setting up a master device.

- Available on NFC-supported devices with Android 6.0 to 9, but guaranteed to operate in Android 9 or later. For NFC-supported devices, refer to the following.


 <Android Support Device List>

7.2.1 Creating a configuration set

- Click [Settings]→[Android]→[Device Owner Mode]→[NFC Kitting (Set master device)].
- Click  to display the Create New screen.
You can create a maximum of 50 configuration sets.
- Enter a configuration name.
- Select [Enable] in NFC Kitting Setting.
- Click [Save].



- Go to [Assets]→[List], and select a target device. Click  →[Setting]→[Setting Allocation]→[NFC kitting settings], and apply the created configuration set to a master device.
For details, refer to the following.

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

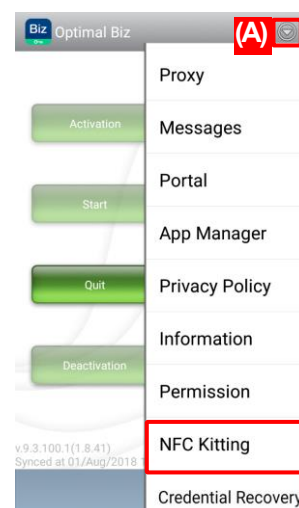
7.2.2 Setting a master device

Perform NFC kitting settings for a device that you want to treat as a master device.

- ☑ If NFC kitting is not enabled on the management site, this function is not available.
- ☑ If the agent information of a master device is out of date, kitting may fail. Perform a sync in advance and make sure the agent app is up to date before kitting.

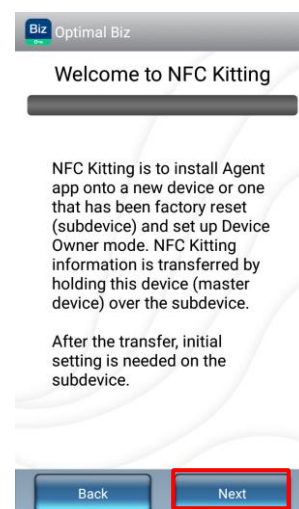
- [1]** On the agent menu screen, click the menu button (A) to display the option menu, and then tap [NFC Kitting].

⇒ A message will appear that informs you of the kitting procedure.




- [2]** Tap [Next].

⇒ The Wi-Fi Settings screen appears.




- [3]** The Wi-Fi Settings screen appears. Select "Send Wi-Fi settings from this device", enter the "SSID" and "Password" of the Wi-Fi you want to connect to, and select "Proxy".

 If you select [Skip] (A), you will enter the Wi-Fi network information when you set up subdevices.

- [4]** Tap [Next].

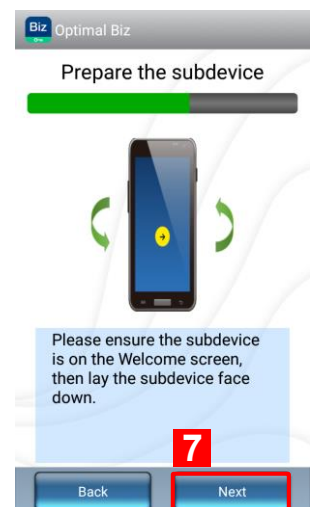
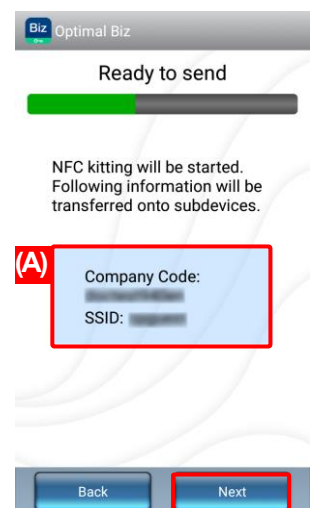
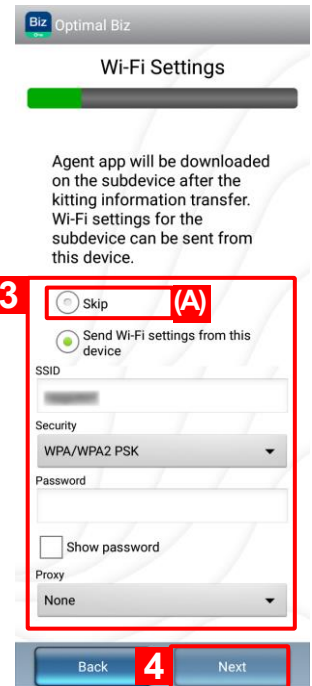
- [5]** Verify that the displayed "Company Code" (A) and "SSID" are correct, and tap [Next].

- [6]** Turn your subdevice upside down.

 The subdevice must be in its factory default state (initial setup screen).

 Refer to the animation displayed on the master device screen.

- [1]** Tap [Next].

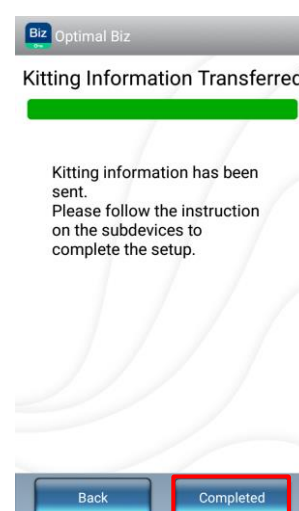
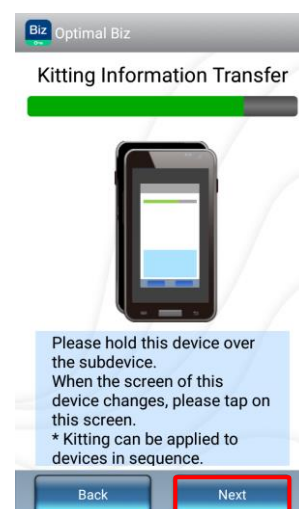


[7] Hold the master device over the subdevice. When the master device screen changes, tap the master device screen. Tap [Next].

- ☑ If performing kitting for multiple devices, do not tap [Next], but rather hold the master device over another subdevice while this screen is displayed.
- ☑ Some devices may not have NFC on their back. Check your device's manual for the NFC location.
- ☑ On some subdevices, encryption may begin. Kitting may fail when the battery is low.

[8] Kitting information has been transferred. Follow the instructions on the subdevice screen to perform initial setup. Tapping [Completed] will display the agent's menu screen.

- ☑ If a subdevice does not support NFC, the device will not respond even when the master device displays that it has transferred information.



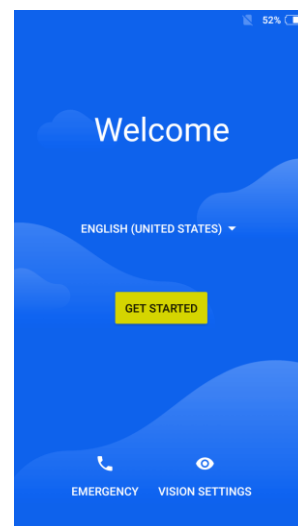
7.2.3 Setting a subdevice

Perform kitting for a subdevice using NFC kitting.

- ✔ To perform kitting, you must have a master device with NFC kitting setting enabled.
- ✔ The subdevice must be in its factory default state (initial setup screen).

[1] Turn the subdevice that displays the initial setup screen upside down, and hold the master device over it.

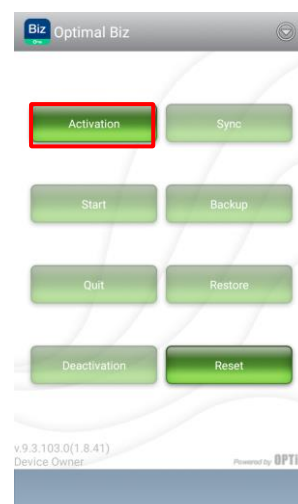
- ✔ Refer to steps [6] to [7] of "Setting a master device" for details.



[2] Tap [Optimal Biz].

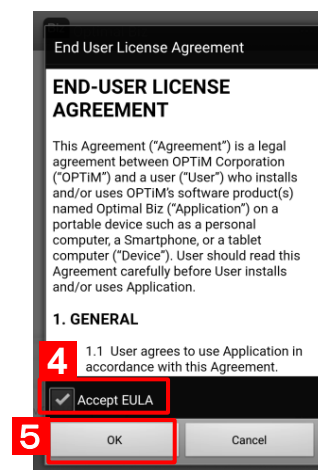


[3] Tap [Activation] and accept the EULA.

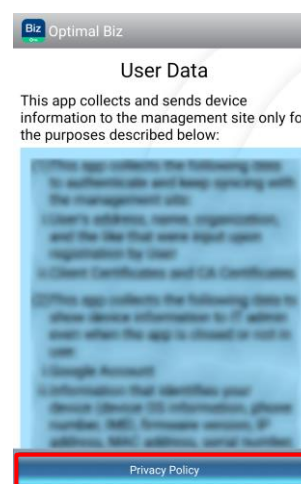


[4] Check "Accept EULA".

[5] Tap [OK].



[6] Read the user data policy, and tap [Privacy Policy].



[7] Check "I agree to the privacy policy".

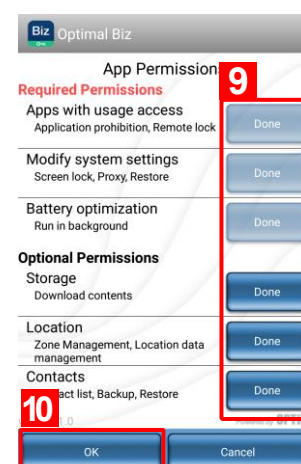
[8] Tap [OK].



[9] A screen that requests permission appears. Follow the on-screen instructions to set things up.

[10] Tap [OK].

⇒ The license authentication screen appears. Continue with the license authentication.



7.3 Performing license authentication

After kitting is complete, perform license authentication with your User ID or company code / authentication code.

- ✍ If you are using Android Enterprise, after you perform license authentication with the user ID registered from the management site, it will be integrated with Android Enterprise.
If you have not registered your user ID, the user ID can be integrated with Android Enterprise by performing a license authentication with a company code / authentication code, registering the user ID from the management site, and linking it with your device
- ✍ When kitting is performed with QR code for Android 10 or later, license authentication is conducted by kitting, so this operation is not necessary.

7.3.1 Authenticating by a user ID

[1] Tap [Authenticate with User ID and Password].

- ✍ "Company Code" (A) will be entered automatically.

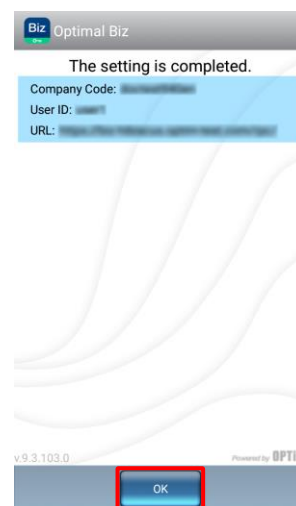
[2] Enter the "Company Code", "User ID or E-mail Address", and "Password".

- ✍ Contact your administrator for your company code, user ID, and password.
- ✍ You do not have to change the URL (A).

[3] Tap [Send].

The image shows two screenshots of the 'Biz Optimal Biz' activation interface. The top screenshot is for 'Authenticate by User ID and Password' (labeled with a red '1'). It features a red box labeled '(A)' around the 'Company Code' field. Below it are fields for 'Authentication Code', 'URL', and 'E-mail Address'. A 'Send' button is at the bottom. The bottom screenshot is for 'Authenticate by Authentication code' (labeled with a red '2'). It features red boxes labeled '(A)' around the 'Company Code' and 'URL' fields. Below the 'URL' field is a link 'Authenticate by Authentication code.' and another link 'Scan QR Code to fill out the Authentication Information'. A 'Send' button is at the bottom, labeled with a red '3'. Both screenshots show the version 'v9.3.101.0' and 'Powered by OPTIM'.

- [4]** The license authentication completion screen appears. Tap [OK].



- [5]** The agent menu screen appears.

- ✓ After license authentication, users cannot interact with the agent screen until the initial synchronization is complete at the management site.



7.3.2 Authenticating by a company code / authentication code

- ✍ If you are using Android Enterprise, allocate a user to the device on the management site after license authentication is complete

🔍 "Asset" - "List" - "Asset management information" in <Management Site Reference Manual>

[1] Enter an "Authentication Code".

- ✍ Contact your administrator for your authentication code.
- ✍ "Company Code" (A) will be entered automatically.
- ✍ If you tap [Scan QR Code to fill out the Authentication information] (B) and scan a QR code for agent license activation, the "Company code", "Authentication code", and "URL" will be automatically entered. Contact your administrator for the QR code.

[2] Tap [Send].

[3] The license authentication completion screen appears. Tap [OK].

« When portal settings are set to be displayed on Management Site »

After you tap [OK], initial registration screen appears.

Enter items as necessary.

- ✍ The user will link to the device if the initial registration has been made.
- ✍ If you do not need to register, you can either tap [Close] (A) or (B) the back button on the device to close the screen.
- ✍ If the user is already linked to the device, a message will appear and say that the user has been linked. Close the screen.

[4] The agent menu screen appears.

- ✓ After license authentication, users cannot interact with the agent screen until the initial synchronization is complete at the management site.



8 Changing the owner of your device

To change the owner of your device, you must carry out the following procedures and perform kitting again.

Item	Page
Factory resetting the device	217
Deleting device information	218



Attention

- Do not delete the Google account you registered in "Integrating Android Enterprise with a Google account Google".
 - To prevent information leakage from the terminal, you cannot terminate the license using the agent or uninstall the agent from your device.
-

8.1 Factory resetting the device


Factory reset your device to the initial setup screen.

There are three ways below to initialize the device.

8.1.1 Factory reset using remote wipe

Perform remote wipe for a target device from the management site.

 A remote wipe immediately factory resets a device. Exercise extreme caution when you perform it.

 "Asset" - "List" - "Settings of assets" - "(Operation – Android) Remote Wipe" in <Management Site Reference Manual>

8.1.2 Factory reset using the device reset function

If you are unable to connect to the management site or the agent does not start, perform an initialization using the device reset function.

 Each device provides a different reset function. For details, see the manual and help information of your device.


8.1.3 Factory reset using the agent

[1] Tap [Quit].

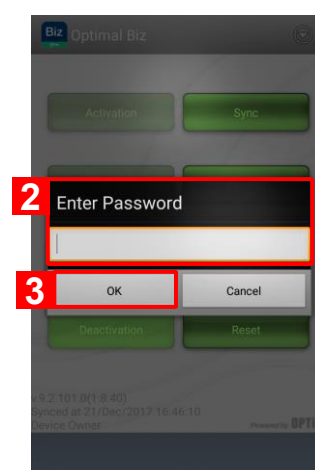
 You cannot factory reset the terminal while the agent is running.



[2] Enter "Password".

 Contact your administrator for your password.
Some settings on the management site do not require you to enter a password.

[3] Tap [OK].

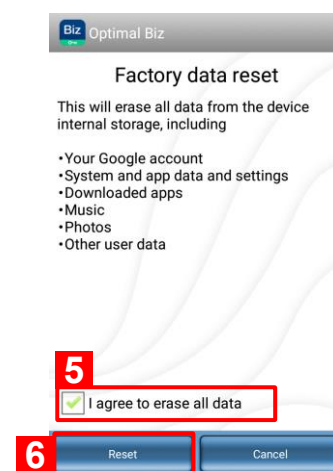


[4] Tap [Reset].




[5] Check "I agree to erase all data".


[6] Tap [Reset].



8.2 Deleting device information

Factory resetting your device does not delete device information on the management site. Delete the information of a target device on the management site.

 "Asset" - "List" - "Deleting asset individually" in <Management Site Reference Manual>

 If you delete device information, the associated users will also be removed.

9 Changing integration settings between Optimal Biz - Google

You can delete or re-register a Google Workspace (formerly G Suite) account that you registered in "Integrating Android Enterprise with a Google account Google" or a G Suite account.

This chapter describes the following items.

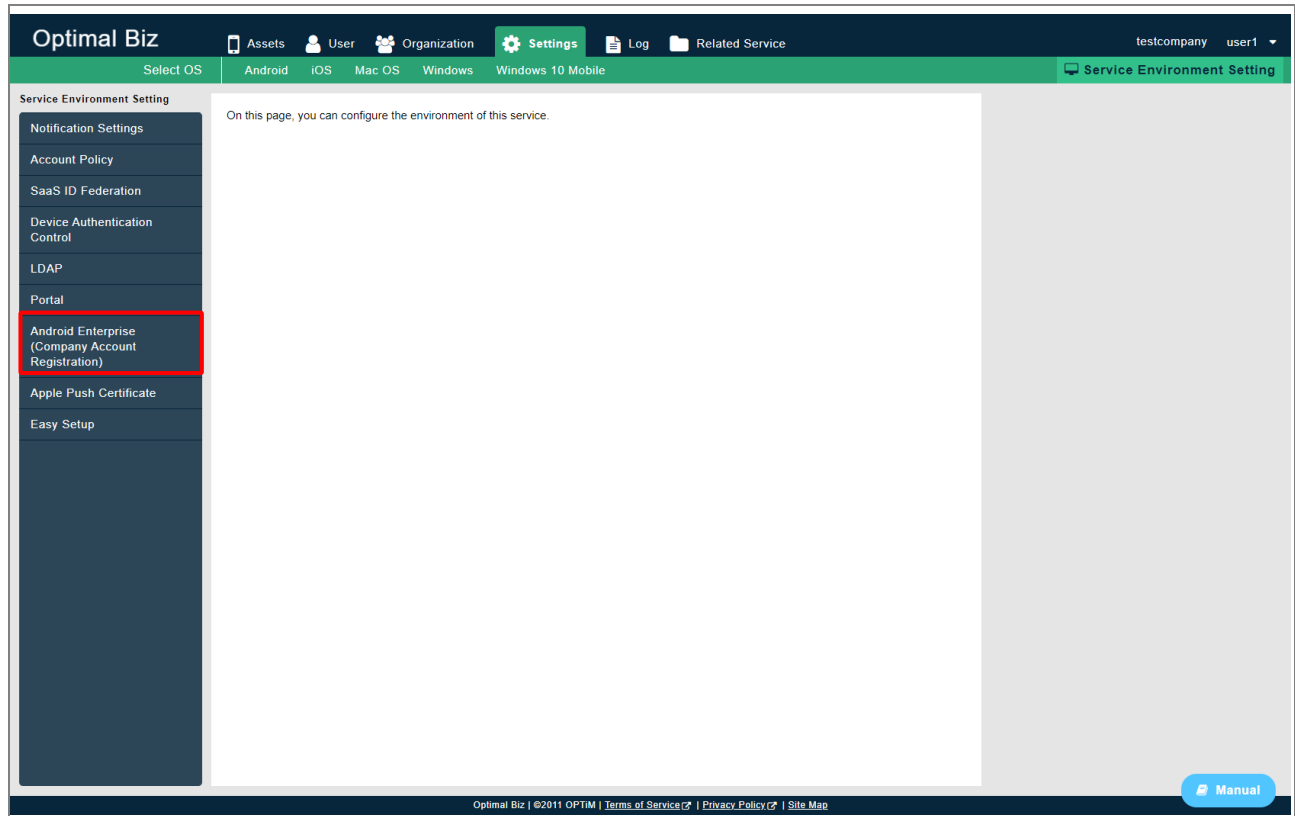
Item	Page
Deleting your Google account	220
Re-registering your Google account	223
Deleting your Google Workspace (formerly G Suite) account	225

9.1 Deleting your Google account

If the registered Google account is no longer available, follow the steps below to delete it.

- ✍ If you delete your Google account and then re-register another Google account, you will need to perform kitting for your device again.
- ✍ Deleting your Google account will also delete the app distribution settings, individual app settings, and app permission policy settings of Android Enterprise.

[1] Click [Settings]→[Service Environment Setting]→[Android Enterprise (Company Account Registration)].



[2] Check "Agree".

[3] Click [Delete account].

Android Enterprise Account Registration

Status
Registered

⚠ When using Android Enterprise, on the device, default is prohibition for "Unknown sources" and "Developer options", and forcible for "Verify apps". Please use [Security Setting_\(DOM\)](#) if you want to change the setting.

Account Type
[Redacted]

Account E-mail Address
[Redacted]

⚠ Delete the Enterprise account. When the deletion is executed, the Android Enterprise setting is deleted and you cannot use the app distribution function using the Android Enterprise function.
If you re-register within 30 days after deleting data, the data will be restored.
If you do not mind, please check "Agree" and click the "Delete account" button.

☒ Agree

2

3 Delete account

【4】 The "State" (A) shows "Unregistered (With restoration data)" and the data retention period.

<<Re-registering the same account>>

✎ Click [Re-register account] (C).

✎ For details, refer to the following.

👉 "Re-registering your Google account" Page 223

<<Registering another account>>

✎ Click [New Account Registration] (B).

✎ For details, refer to the following.

👉 "Registering a Google account" Page 12

Android Enterprise Account Registration

(A) Status
Unregistered(With restoration data)
Data Retention Period: 2018/06/20

⚠ When using Android Enterprise, on the device, default is prohibition for "Unknown sources" and "Developer options", and forcible for "Verify apps". Please use [Security Setting \(DOM\)](#) if you want to change the setting.

Account Type
Google account

Account E-mail Address
[Redacted]

⚠ If you re-register your account within the data retention period, the previous account data will be handed over. After the data retention period expires, the handover data will be deleted.

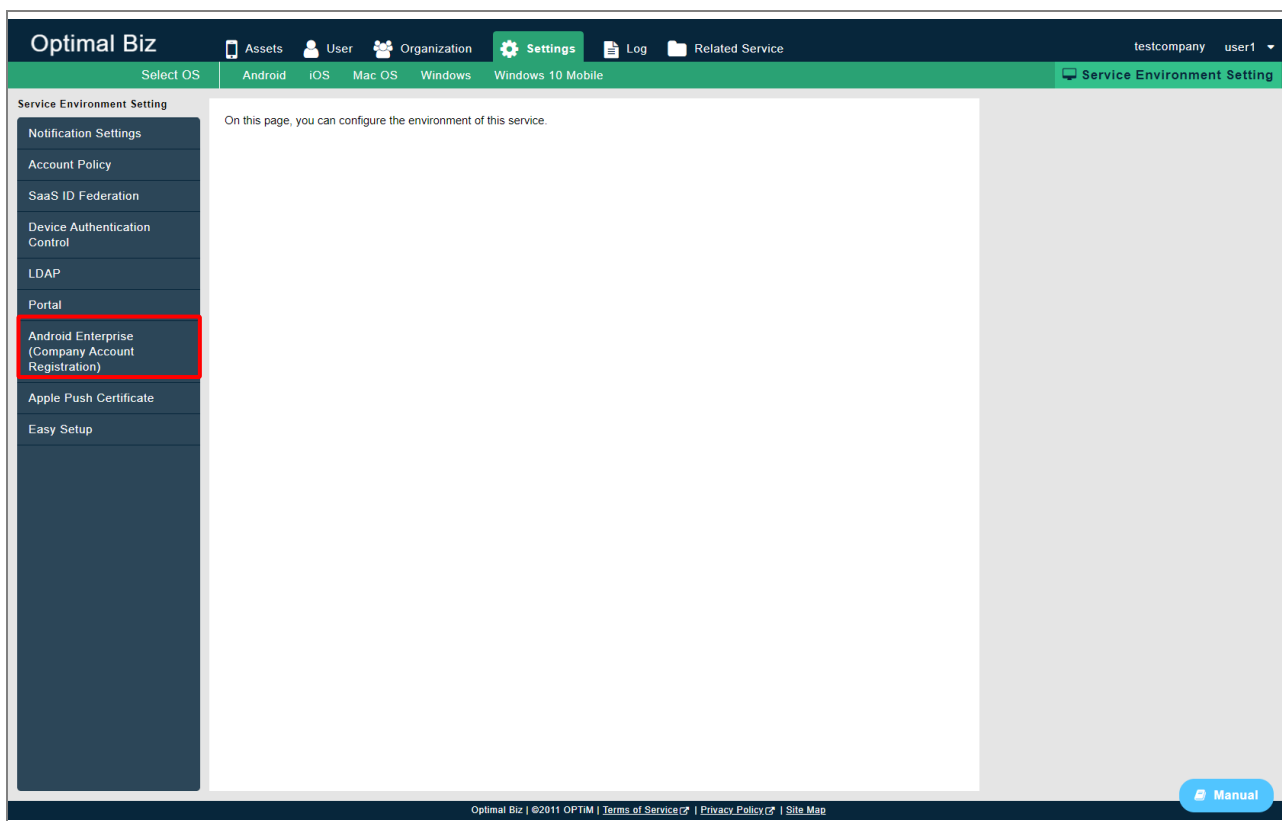
(B) New Account Registration (C) Re-register account

9.2 Re-registering your Google account

You can re-register a deleted Google account by following the steps below.

- ✔ You can only re-register the last Google account you deleted.
- ✔ Re-registering your Google account does not re-register app distribution settings of Android Enterprise, individual app settings, and app permission policy settings.

[1] Click [Settings]→[Service Environment Setting]→[Android Enterprise (Company Account Registration)].



[2] Click [Re-register account].

Android Enterprise Account Registration

Status
Unregistered(With restoration data)
Data Retention Period: 2018/06/20

⚠ When using Android Enterprise, on the device, default is prohibition for "Unknown sources" and "Developer options", and forcible for "Verify apps". Please use [Security Setting \(DOM\)](#) if you want to change the setting.

Account Type
Google account

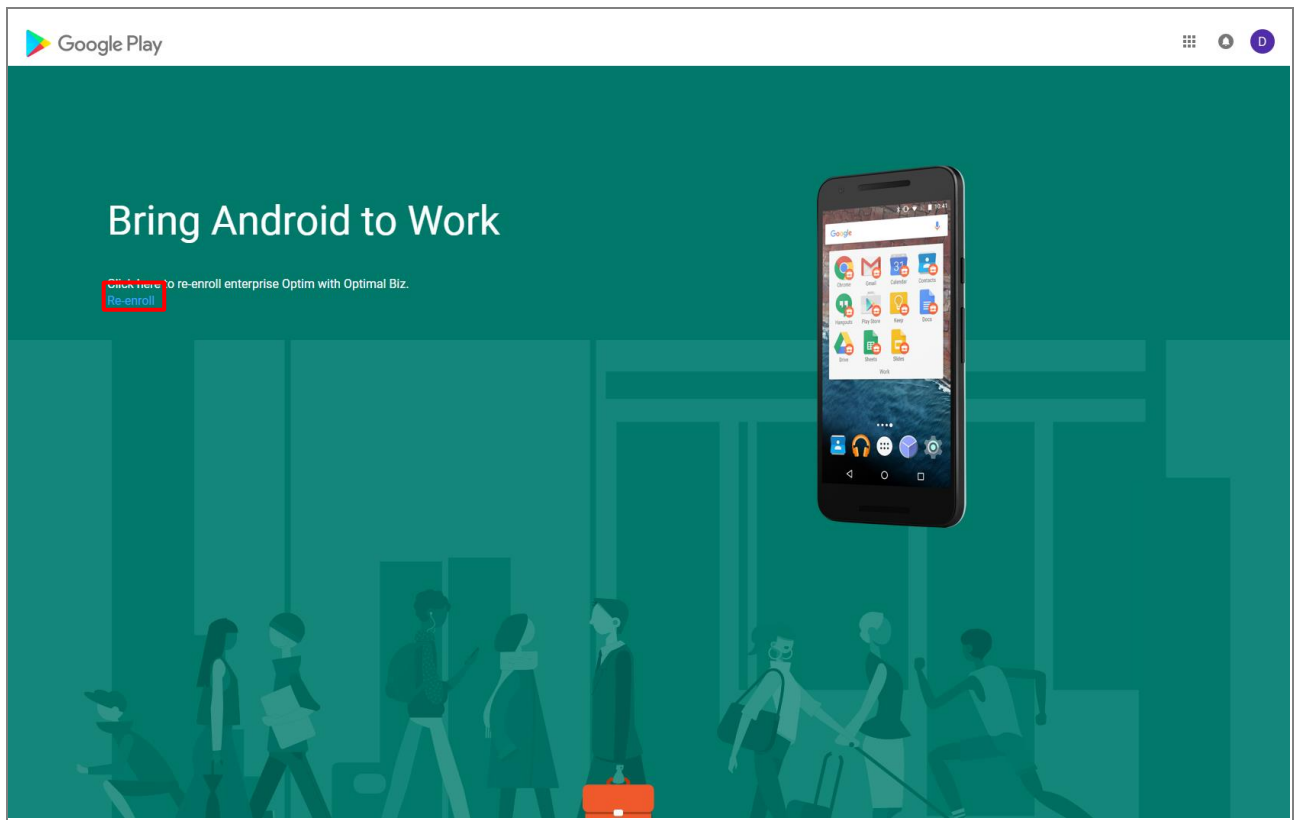
Account E-mail Address
[Redacted]

⚠ If you re-register your account within the data retention period, the previous account data will be handed over. After the data retention period expires, the handover data will be deleted.

New Account Registration
Re-register account

[3] Google Play will be displayed. Click [Re-enroll].

✎ Depending on the browser you are using, Google Play may not work properly.



[4] When you return to the management site, the "Status" shows "Registered".

Android Enterprise Account Registration

Status

Registered

⚠ When using Android Enterprise, on the device, default is prohibition for "Unknown sources" and "Developer options", and forcible for "Verify apps". Please use Security Setting (DOM) if you want to change the setting.

Account Type

Google account

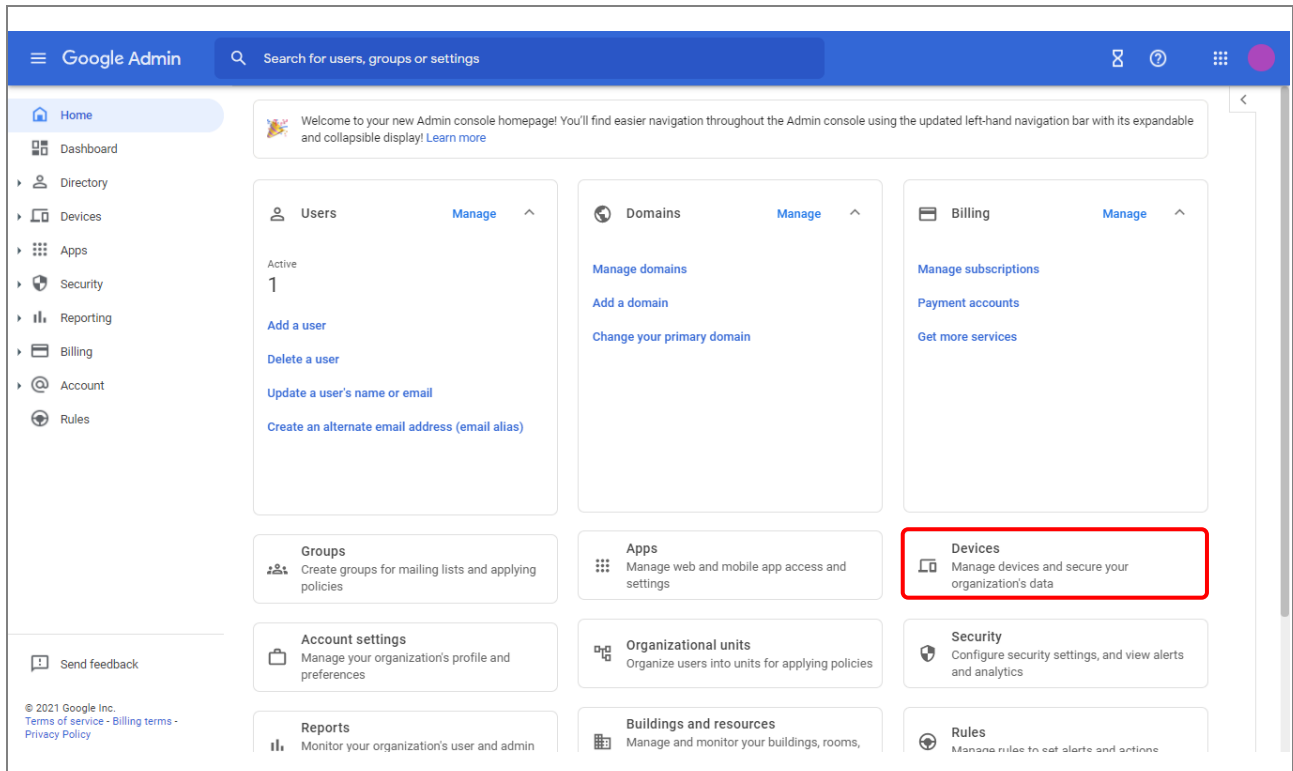
Account E-mail Address

Delete account

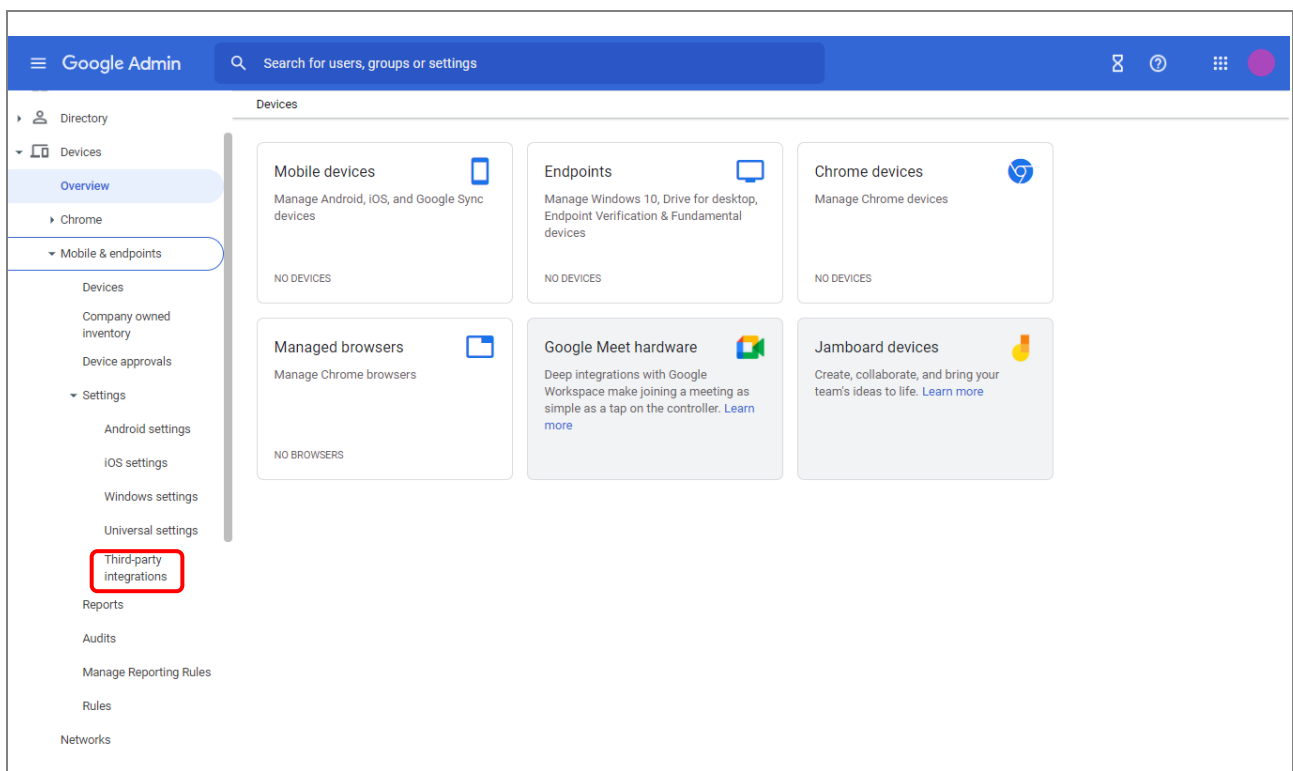
9.3 Deleting your Google Workspace (formerly G Suite) account

If the registered Google Workspace (formerly G Suite) account is no longer available, follow the steps below to delete it.

[1] Go to the Google Admin console (<https://admin.google.com>) and click [Devices].



[2] Click [Settings]→[Third-party integrations].



[3] Uncheck "Enable third-party Android mobile management" in "Android EMM".

[4] Click [SAVE].

Android EMM
Applied at 'gdoctest001.optim-test.xyz'

Third-party Android mobile management

3 ☐ Enable third-party Android mobile management

No EMM added [Add EMM provider](#)

4 **SAVE**

CANCEL

The following steps are performed on the management site.

[5] Click [Settings]→[Service Environment Setting]→[Android Enterprise (Company Account Registration)].

Optimal Biz

Assets User Organization **Settings** Log Related Service

Select OS Android iOS Mac OS Windows Windows 10 Mobile

testcompany user1

Service Environment Setting

Notification Settings

Account Policy

SaaS ID Federation

Device Authentication Control

LDAP

Portal

Android Enterprise (Company Account Registration)

Apple Push Certificate

Easy Setup

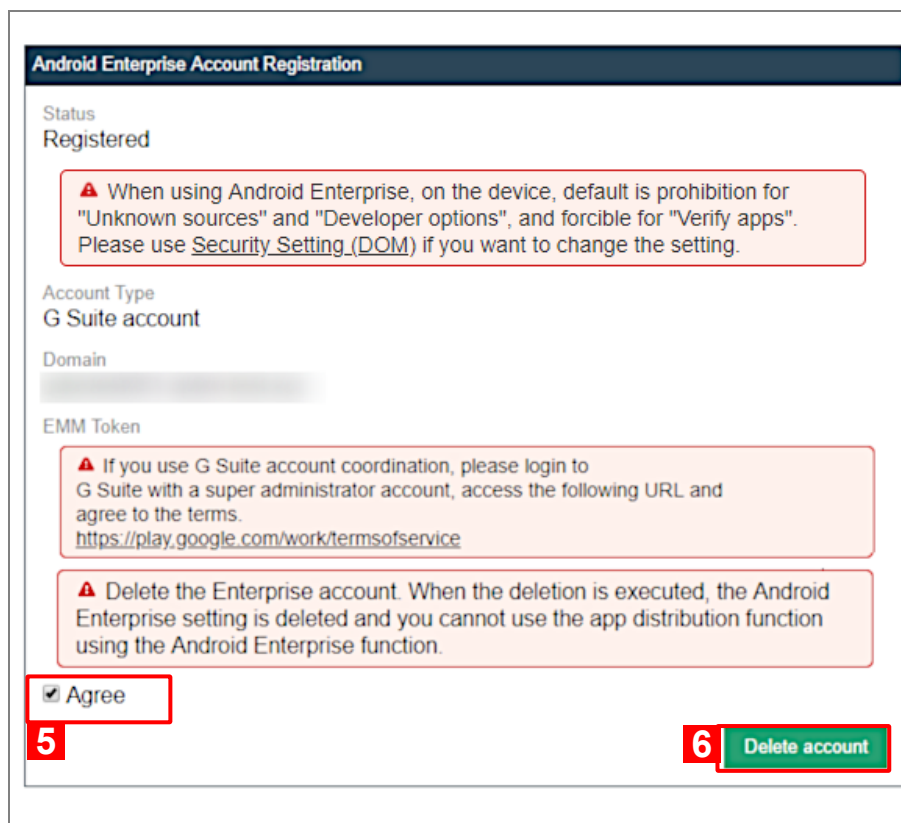
On this page, you can configure the environment of this service.

Manual

Optimal Biz | ©2011 OPTIM | Terms of Service | Privacy Policy | Site Map

[6] Check "Agree".

[7] Click [Delete account].



Android Enterprise Account Registration

Status
Registered

⚠ When using Android Enterprise, on the device, default is prohibition for "Unknown sources" and "Developer options", and forcible for "Verify apps". Please use [Security Setting \(DOM\)](#) if you want to change the setting.

Account Type
G Suite account

Domain
[Redacted]

EMM Token

⚠ If you use G Suite account coordination, please login to G Suite with a super administrator account, access the following URL and agree to the terms.
<https://play.google.com/work/termsofservice>

⚠ Delete the Enterprise account. When the deletion is executed, the Android Enterprise setting is deleted and you cannot use the app distribution function using the Android Enterprise function.

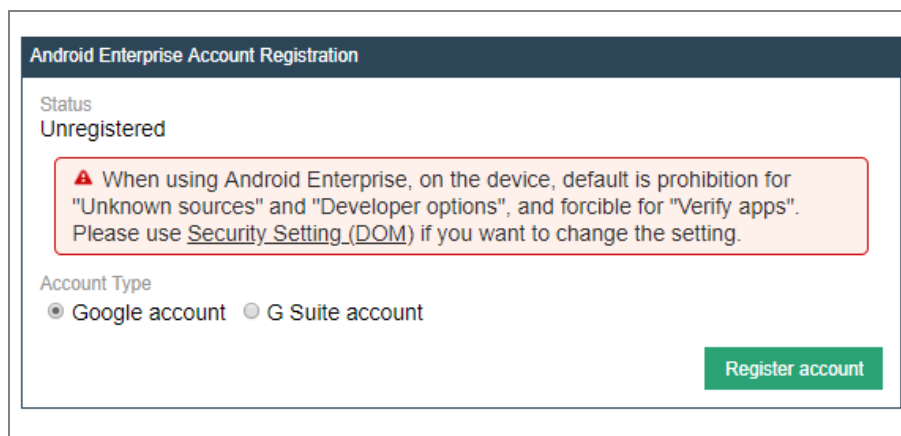
☒ Agree

5 **6** Delete account

[8] The initial account registration screen appears.

✍ To register an account again, refer to the following.

👉 "Registering a Google Workspace (formerly G Suite) account" Page 48



Android Enterprise Account Registration

Status
Unregistered

⚠ When using Android Enterprise, on the device, default is prohibition for "Unknown sources" and "Developer options", and forcible for "Verify apps". Please use [Security Setting \(DOM\)](#) if you want to change the setting.

Account Type
☒ Google account ☐ G Suite account

Register account

10 Legacy Android agent

The legacy Android agent can be installed to Android 5.x or lower, but the agent is guaranteed to operate in Android 9 or later.

This chapter describes the following items.

Item	Page
Installing the legacy agent	229
Activating the legacy agent	231

10.1 Installing the legacy agent

This product uses the agent to manage and configure Android devices. Follow the steps below to install the agent.

- ✎ You must select "unknown source apps" when you install the agent. If you have not selected "unknown sources", select it and install the agent.
- ✎ In some devices, you cannot download and install the Android agent if an SD card is not inserted. Download and install the agent after inserting an SD card. If the agent has been installed and the SD card is set to "Prohibited", change the setting to "Allow" and then download and install the agent. Contact your administrator for details of the SD Card prohibition setting. Refer to the following for the devices.

 <Android Support Device List>

[1] There are two ways to install the legacy Android agent.

<<Entering a download URL directly>>

- ✎ Launch the browser, enter the URL of the agent download site in the red box (A), tap [Run], and the screen shown on the right will appear.

- ✎ Contact your administrator or operator for the URL of the download site.

<<Scanning a QR code>>

- ✎ Launch the built-in QR code scanner on your device and scan the QR code for downloading the agent. After scanning the QR code successfully, open the URL in your browser to display the screen shown on the right.

- ✎ Contact your administrator or operator for a QR code for downloading the agent.

[2] Tap [Terms of Service] and read the content.

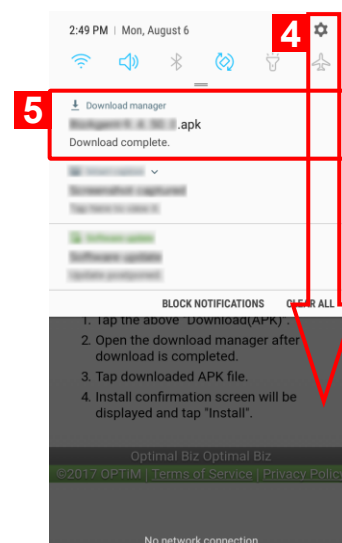
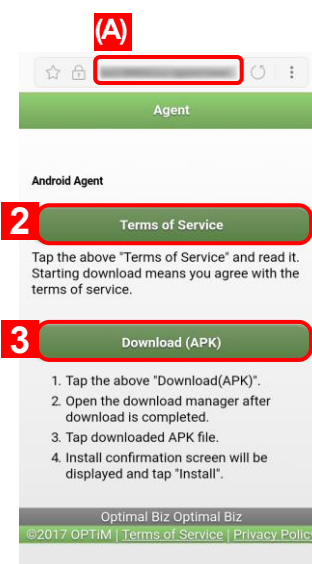
[3] Tap [Download (APK)].

⇒ Tapping it will start downloading the agent. Please wait for a while.

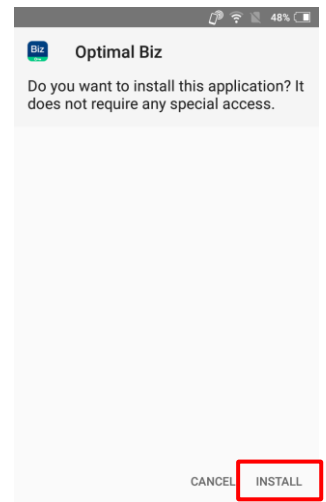
[4] Swipe the screen downward to display the download notification screen.

- ✎ For Android 3.x devices, tap the notification at the bottom right.

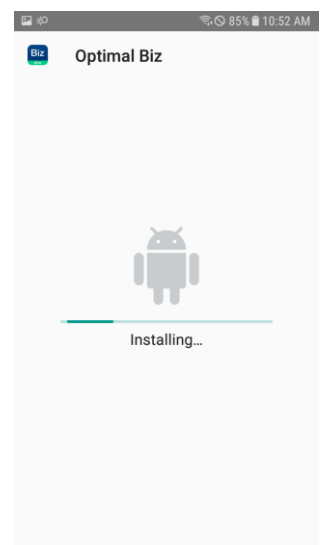
[5] Tap the downloaded agent.



[6] The install confirmation screen will be displayed. Read the text and tap [INSTALL].

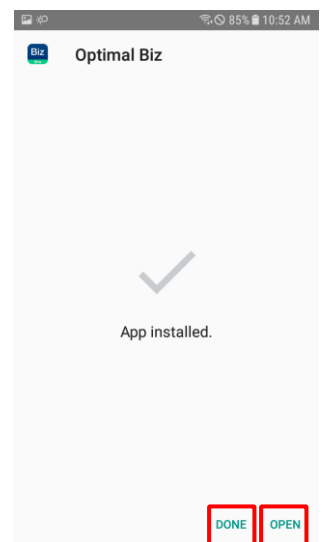


[7] The agent will be installed. Please wait for a while.



[8] Installation complete.

[9] Tap [OPEN] or [DONE].




10.2 Activating the legacy agent

When the installation is complete, launch the agent to perform license authentication.


In the proxy environment, you must first configure the proxy settings. For proxy settings, refer to the following.

 "Set Proxy" in <Android Client Reference Manual>

 If the authentication control setting on the management site only allows license authentication for devices registered by an administrator, you must have your administrator register your device before the procedure below. Contact your administrator for details.


[1] Tap [Activation] on the menu screen.

 Refer to the following on how to display the menu screen.

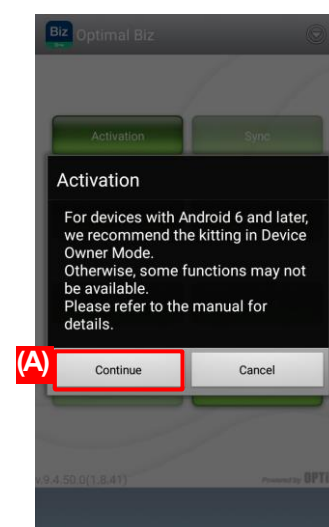
 "Menu Screen" – "Agent Basic Operations" in
<Android Client Reference Manual>



<<Authenticating the legacy agent on Android 6.0 or later>>

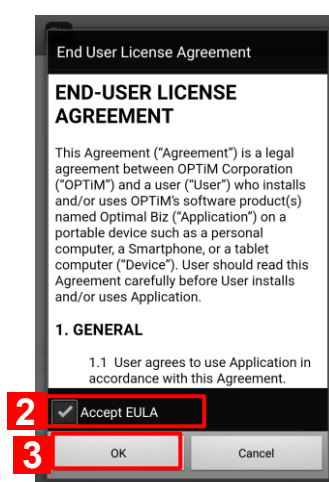
 When you install and perform license authentication for the legacy agent on Android 6.0 or later, the dialog shown on the right will be displayed.

If you tap [Continue] (A), you can continue the license authentication of the legacy agent, but some functions may not be available. We recommend kitting for the store version agent.



[2] Read the End User License Agreement, and select "Accept EULA".

[3] Tap [OK].



[4] The screen may be different depending on the license authentication method.

<<Authenticate by a company code / authentication code>>

- ✎ Enter "Company Code" / "Authentication Code" (A).
- ✎ Tap [Send] (B).

- ✎ You do not have to change "URL"(C).
- ✎ "Company Code" may not appear depending on your usage.
- ✎ If you want to perform activation with a user ID or email address, tap "Authenticate by user ID and Password" (D).
- ✎ Contact your administrator for your company code and authentication code.

<<Authenticating by a user ID or e-mail address>>

- ✎ Enter the (A) "Company Code", "User ID or E-mail Address", and "Password".
- ✎ Tap [Send] (B).

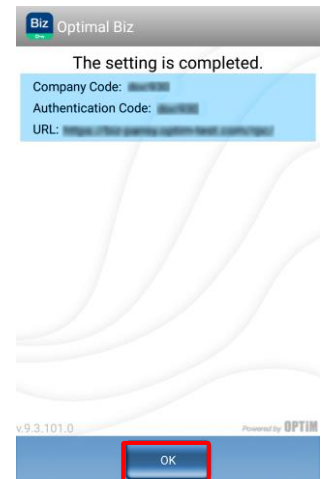
- ✎ You do not have to change the URL (C).
- ✎ If you want to authenticate by a company code / authentication code, tap "Authenticate by Authentication code" (D).
- ✎ Contact your administrator for your company code, user ID, and password.

<<Authenticating by scanning a QR code>>

- ✎ Tap "Scan QR Code to fill out the Authentication Information" (A) to scan the QR code for agent license activation. After scanning, the confirmation screen is displayed again, and a company code, authorization code, and URL are entered in (C).
- ✎ Tap [Send] (B).

- ✎ You can perform a license authentication without entering your company code, authorization code, or URL.
- ✎ Contact your administrator or operator for a QR code for downloading the agent.

- [5] The license authentication completion screen appears. Tap [OK].**



- [6] Register your device information.**

✎ Enter the required fields (A).

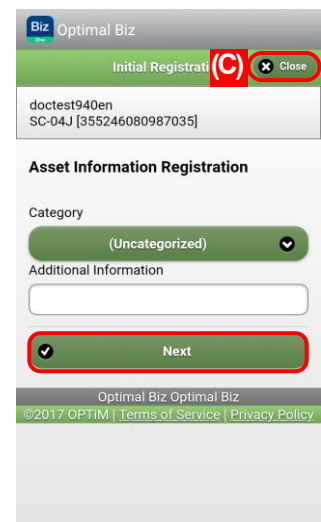
✎ Tap [Next] (B).

✎ If you do not want to register the device information, tap [Close] (C).

✎ If the Android portal settings in the management site are set to hidden and if entry customization has not been registered, the initial registration screen does not appear.
The content displayed for device information registration will vary depending on the setting.

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

🔍 "Asset" – "Customizing input items" in <Management
Site Reference Manual>



- [7] Registration is complete. Tap [OK].**

