



Android Enterprise Zero-Touch integration guide

Date: 22/03/2023



1- What is Android Enterprise zero-touch?

Android Enterprise zero-touch allows enterprise to enroll company's devices to an EMM system without a necessity of going through the manual enrollment procedure. Android Enterprise zero-touch integration with Essentials MDM gives a possibility to auto-enroll all devices with Android 8 and newer.

For more information visit Android Enterprise zero-touch page:

<https://www.android.com/enterprise/management/zero-touch/>

2- Integrating Essentials MDM Server with zero-touch service

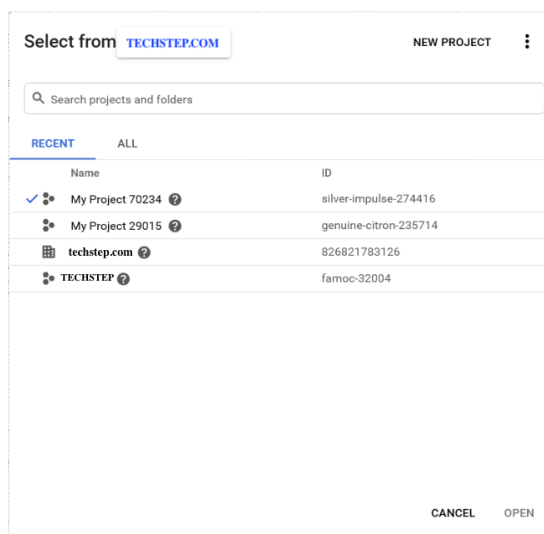
In order to be able to use Essentials MDM zero-touch integration, Essentials administrators have to integrate and authorize the whole Essentials MDM Server machine to appropriate Enterprise Google API. As an Essentials administrator you will require:

- SSH access to your Essentials application machine
- Google account

2.1 Create Google Developer Project

Using your Google account login to Google's Developer Console - <https://console.developers.google.com>

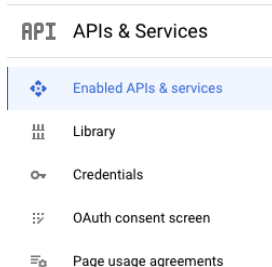
Once logged in, create a new project. It will contain all zero-touch settings for this Essentials MDM Server integration, including appropriate credentials.



Choose a name for your project. That will help you identify it in the future. When the notification icon indicates that the project is ready – you're all set to enabling Enterprise API.

2.2 Enable Enterprise API

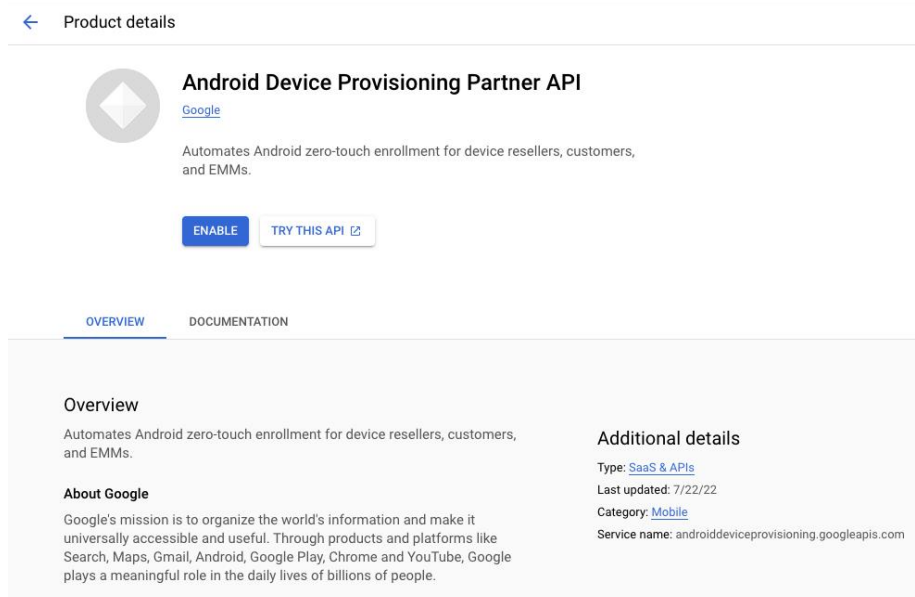
Make sure that you've selected your project, and then select from the right side menu **Library** or click "ENABLE APIS AND SERVICES"



In order to support zero-touch, the Google Project that you just created, needs the following API to be enabled:

- Android Device Provisioning Partner API
(Service name: *androiddeviceprovisioning.googleapis.com*)

Search and choose this API from Google's library and then click "ENABLE".

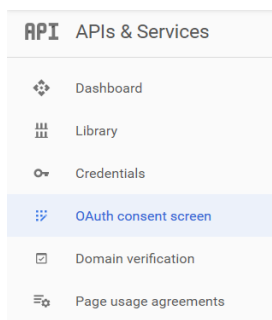


2.3 Configure API Credentials

Essentials zero-touch Integration uses OAuth 2.0 credentials for authentication and authorization. In this step we'll setup this method.

2.3.1 Configure OAuth Consent screen

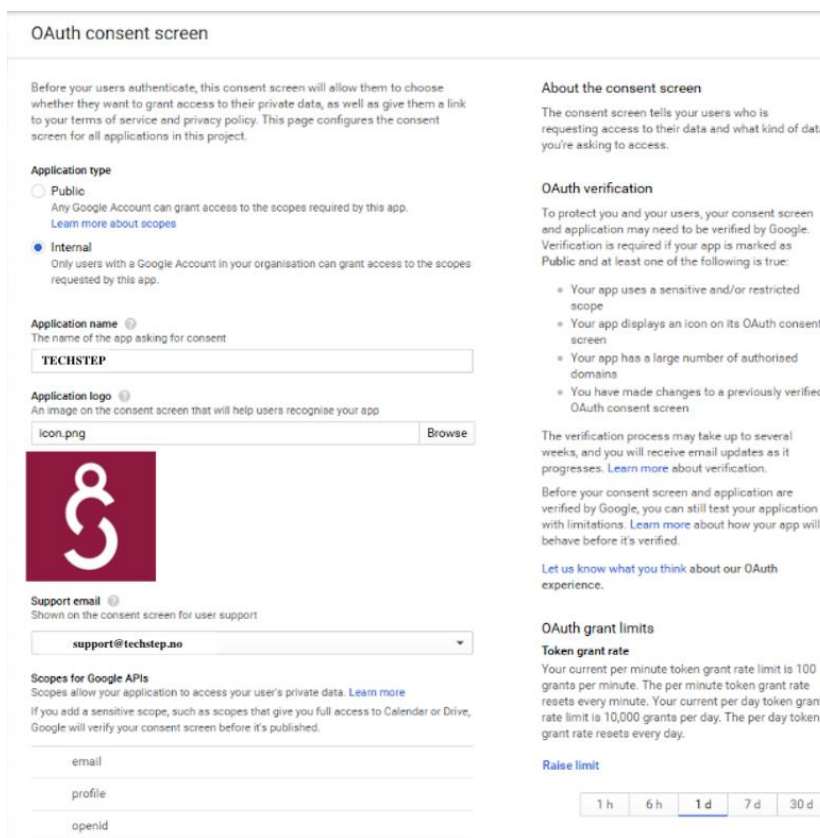
Make sure that you've selected your project, and then select from the right side menu **OAuth consent screen**.



This OAuth consent screen will be presented to an administrator that is adding a zero-touch account to an organization in Essentials MDM. First you will have to choose between Internal (Only users from your organisation) or External (Any user with Google account) user type.

Fill appropriate information accordingly, paying extra attention to fields:

- Application name (required)
- Support e-mail (required)
- Authorized domains (required) - it has to be top level domain on which your Essentials MDM Server is hosted (e.g. if machine is hosted on 'emm.company.com', the top level domain will be 'company.com')
- Application logo (optional) required if you want to use the logo, otherwise - optional
- Application Homepage link, Application Privacy Policy link



OAuth consent screen

Before your users authenticate, this consent screen will allow them to choose whether they want to grant access to their private data, as well as give them a link to your terms of service and privacy policy. This page configures the consent screen for all applications in this project.


Application type

☐ Public
Any Google Account can grant access to the scopes required by this app.
[Learn more about scopes](#)

☒ Internal
Only users with a Google Account in your organisation can grant access to the scopes requested by this app.

Application name ⓘ
The name of the app asking for consent

Application logo ⓘ
An image on the consent screen that will help users recognise your app



Support email ⓘ
Shown on the consent screen for user support

Scopes for Google APIs
Scopes allow your application to access your user's private data. [Learn more](#)
If you add a sensitive scope, such as scopes that give you full access to Calendar or Drive, Google will verify your consent screen before it's published.

About the consent screen
The consent screen tells your users who is requesting access to their data and what kind of data you're asking to access.

OAuth verification
To protect you and your users, your consent screen and application may need to be verified by Google. Verification is required if your app is marked as Public and at least one of the following is true:

- Your app uses a sensitive and/or restricted scope
- Your app displays an icon on its OAuth consent screen
- Your app has a large number of authorised domains
- You have made changes to a previously verified OAuth consent screen

The verification process may take up to several weeks, and you will receive email updates as it progresses. [Learn more](#) about verification.

Before your consent screen and application are verified by Google, you can still test your application with limitations. [Learn more](#) about how your app will behave before it's verified.

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

OAuth grant limits
Token grant rate
Your current per minute token grant rate limit is 100 grants per minute. The per minute token grant rate resets every minute. Your current per day token grant rate limit is 10,000 grants per day. The per day token grant rate resets every day.

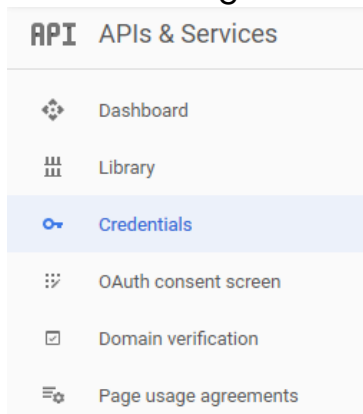
[Raise limit](#)

No data for this time interval

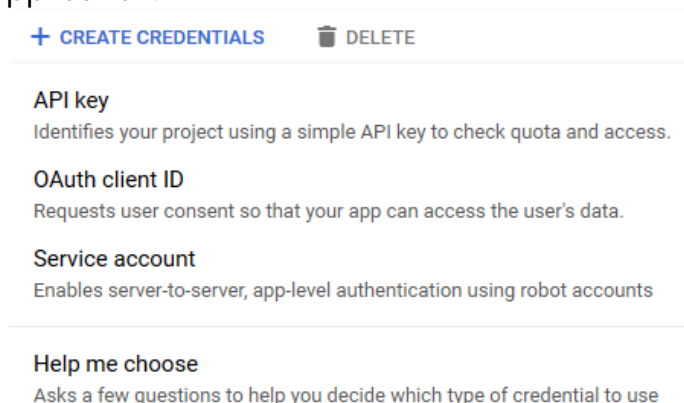
When configured, click SAVE at the bottom of the page

2.3.2 Configure OAuth client ID

Once you've configured OAuth consent screen you can generate credentials for your Essentials MDM Server. Make sure that you've selected your project, and then select from the right side menu **Credentials**.



Click CREATE CREDENTIALS and from the dropdown menu, choose OAuth Client ID and select Web application:



Fill appropriate information accordingly, paying most details to fields:

- Name (required) - Internal name for credentials (will not be displayed to users)
- Authorized JavaScript origins (required) - Address of your Essentials MDM Server machine, in format: <https://emm.yourcompany.com>. It has to match authorized top level domain in the configured OAuth consent screen.
- Authorized redirect URIs (required) - Return address used during zero-touch enrollment. It has format: <https://emm.yourcompany.com/ui/devices/enrollment/zeroTouch>. It has to match authorized top level domain in the configured OAuth consent screen.

Android Enterprise Zero-Touch integration guide

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.

Application type *
Web application

[Learn more](#) about OAuth client types

Name *
Web client 3

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 [authorised domains](#).

Authorised JavaScript origins **?**

For use with requests from a browser

+ ADD URI

Authorised redirect URIs **?**

For use with requests from a web server

+ ADD URI

CREATE

CANCEL

When configured, click CREATE at the bottom on the page. You will see a confirmation box with your client ID and your client secret.

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 published. This may require a verification process that can take several days.


Your Client ID
711782125315-k1b5rcnop29qan6o20c28h1eqs719rbt.apps.gc

Your Client Secret
kb0Tcnhrzx-04tCJJWdQqLtW

OK

Download your credentials by clicking Download JSON button next to credentials that you have just configured.

OAuth 2.0 Client IDs

<input type="checkbox"/>	Name	Creation date ↓	Type	Client ID				
<input type="checkbox"/>	Web client 3	12 May 2020	Web application	711782125315-k1b5...				

2.4 Add Credentials to your Essentials MDM Server machine

The final step to integrating zero-touch with your Essentials MDM Server machine is adding the credentials from the previous step to your server machine. In order to do so, first log in to your Essentials MDM Server via SSH to user with root privileges. Once authorized edit this file with editor of your choice, e.g.:

```
[root@famoc-app /]# nano /var/www/aplikacje/config.php
```

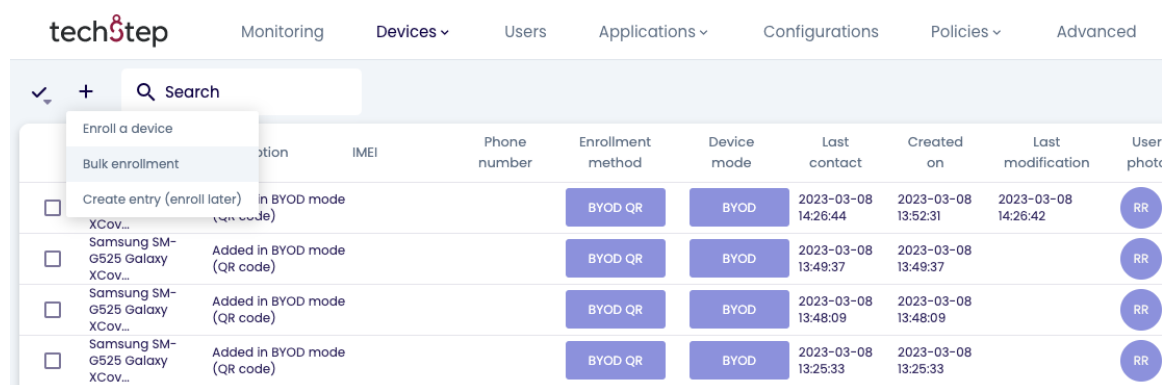
In the file, please find section that begins with: `'/*--BEGIN CUSTOM GLOBAL--*/'` and add the content of the downloaded file accordingly:

```
/*--BEGIN CUSTOM GLOBAL--*/
$cons_zt_json='CONTENT_OF_JSON_CREDENTIALS_FILE';
/*--END CUSTOM GLOBAL--*/
```

Save the file and close the SSH session. Your Essentials MDM Server is all set and your administrators may start using benefits of zero-touch integration.

3- Adding zero-touch account to Essentials MDM organization

In order to start adding zero-touch devices to your Essentials MDM organization, you need to add your company zero-touch account to your Essentials MDM organization. You can do that using our bulk enrollment wizard in the devices view. When you logged in as administrator to your organization, go to the DEVICES tab, then hover over the **+** icon and choose Bulk enrollment.

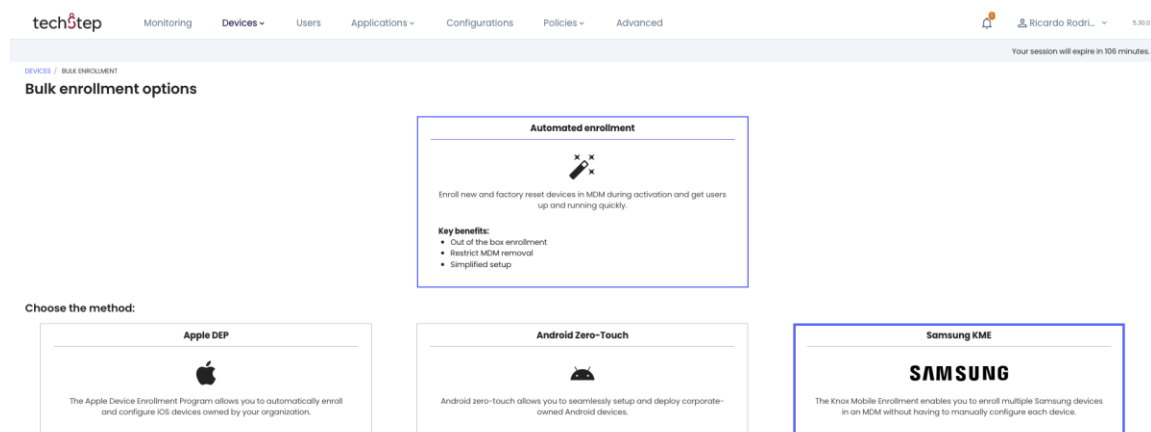


The screenshot shows the 'techStep' MDM interface. The top navigation bar includes 'Monitoring', 'Devices' (selected), 'Users', 'Applications', 'Configurations', 'Policies', and 'Advanced'. Below the navigation bar, there is a search bar and a dropdown menu. The dropdown menu is open, showing options: 'Enroll a device', 'Bulk enrollment', and 'Create entry (enroll later)'. The main table displays a list of devices with columns: 'Device name', 'IMEI', 'Phone number', 'Enrollment method', 'Device mode', 'Last contact', 'Created on', 'Last modification', and 'User photo'. The table contains four rows of Samsung SM-G525 Galaxy devices, all enrolled in BYOD mode using QR codes.

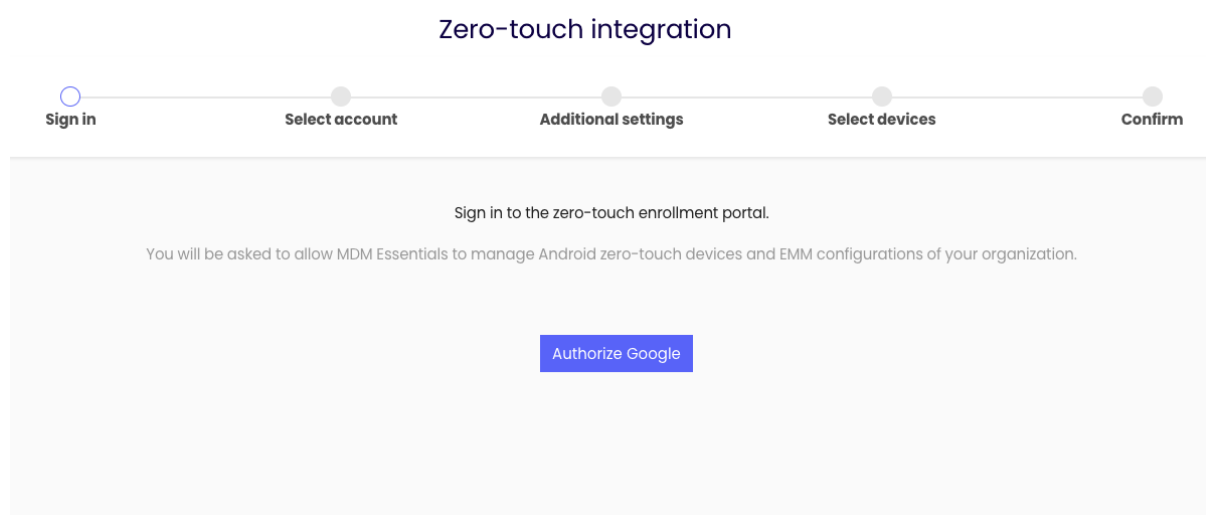
Device name	IMEI	Phone number	Enrollment method	Device mode	Last contact	Created on	Last modification	User photo
XCov... Samsung SM-G525 Galaxy	Added in BYOD mode (QR code)		BYOD QR	BYOD	2023-03-08 14:26:44	2023-03-08 13:52:31	2023-03-08 14:26:42	RR
XCov... Samsung SM-G525 Galaxy	Added in BYOD mode (QR code)		BYOD QR	BYOD	2023-03-08 13:49:37	2023-03-08 13:49:37		RR
XCov... Samsung SM-G525 Galaxy	Added in BYOD mode (QR code)		BYOD QR	BYOD	2023-03-08 13:48:09	2023-03-08 13:48:09		RR
XCov... Samsung SM-G525 Galaxy	Added in BYOD mode (QR code)		BYOD QR	BYOD	2023-03-08 13:25:33	2023-03-08 13:25:33		RR

Android Enterprise Zero-Touch integration guide

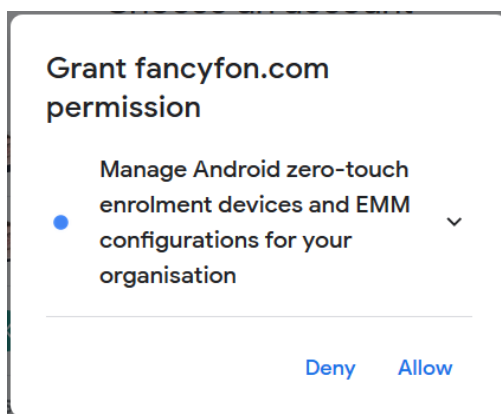
And then select Android zero-touch method:



To add new zero-touch integration, use Start now button. It will open a modal that will guide you through the authorization process. Choose Authorize Google:



Log in with your zero-touch administrator account and grant appropriate permissions to Essentials MDM:



Android Enterprise Zero-Touch integration guide

Once successfully authorized, Essentials MDM will be able to manage your zero-touch integration. From the dropdown list choose the desired zero-touch account to integrate with (if your administrator account is connected with more than one company at zero-touch console). Then choose the default user of the devices at Essentials MDM and assign Device Groups. You can also decide if you wish to demand credentials from user for enrollment. There is also a possibility to enroll devices in BYOD mode (in that mode only Work Profile part of the device is managed by the Essentials MDM administrator).

Zero-touch integration

Sign in

Select account

Additional settings

Select devices

Confirm

Select zero-touch account to be integrated with MDM Essentials

Account name
Techstep Lab

Admin email ⓘ

Default user of imported devices
Rodriguez Ricardo (ricardo.rodriguez@techstep.io)

Enrollment method

Fully managed device (COBO)

Corporate-owned device with work profile (WPC)

Dedicated device (COSU)

Shared device BETA

Authentication method ⓘ

No authentication

User credentials

Enrollment code

Device groups
Select group

Next

On the next screen, provide your company details that will be presented to the user, during the device enrollment process:

Zero-touch integration

Sign in

Select account

Additional settings

Select devices

Confirm

Client name
Techstep AS

Support phone number
+4723172350

Support email address
support@techstepdemo.com

Additional information
Essentials

This device is managed.
Techstep AS has configured this device to be fully managed. If you believe this is an error, please contact them through the following means:
📞 +4723172350
✉ support@techstepdemo.com

Message from Techstep AS
Essentials

Device information

Back Next

Finally, select the device that you want to import to Essentials. You can select required devices manually or choose Autoimport option that will periodically (30 min interval) synchronize new devices from zero-touch to Essentials MDM. If you wish to demand user authorization for enrollment for a specific device select option Require credentials.

The device can be in one of the 3 states, based on it's zero-touch configuration assignment:

1. UNASSIGNED - the device has no zero-touch configuration (and will receive one if selected, or if autoimport is chosen)
2. CURRENT - the device has current zero-touch configuration assigned (and will not receive a new configuration during synchronizations)
3. OTHER - the device has already assigned a different EMM zero-touch configuration. By default it will not receive new zero-touch profile during autoimport. To override other EMM profile you must select the required devices on this step.

Zero-touch integration

● Sign in

● Select account

● Additional settings

○ Select devices

● Confirm

Select the devices to import or let MDM Essentials auto-import all unassigned devices

If you have devices assigned to other EMM configurations, you must select them manually to import them

Auto-import ☐ Select all (4) ☐ < >

	IMEI	Device vendor	Serial number	Authentication method	Enroll into WPC mode	Enroll into COSU	Enroll into Shared devi...	Status
<input type="checkbox"/>	8672	5		Default	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	OTHER
<input type="checkbox"/>	3543	9		Default	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	OTHER
<input type="checkbox"/>	3543	7		Default	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	OTHER
<input type="checkbox"/>	863	2		Default	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	OTHER

Back

Next

Once you've selected your configuration, click Synchronize to add the devices to your Essentials MDM account. It will redirect you to the summary screen.

Zero-touch integration

● Sign in

● Select account

● Additional settings

● Select devices

○ Confirm

Make sure synchronization details are correct and proceed by clicking Synchronize button

Devices to import: 0

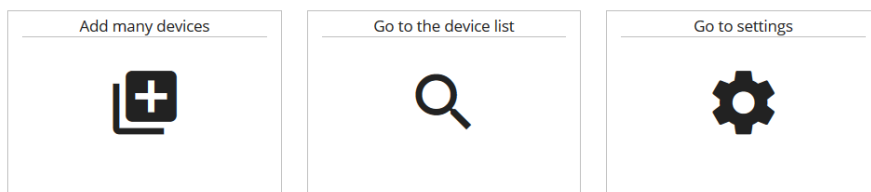
Devices to detach: 0

Back

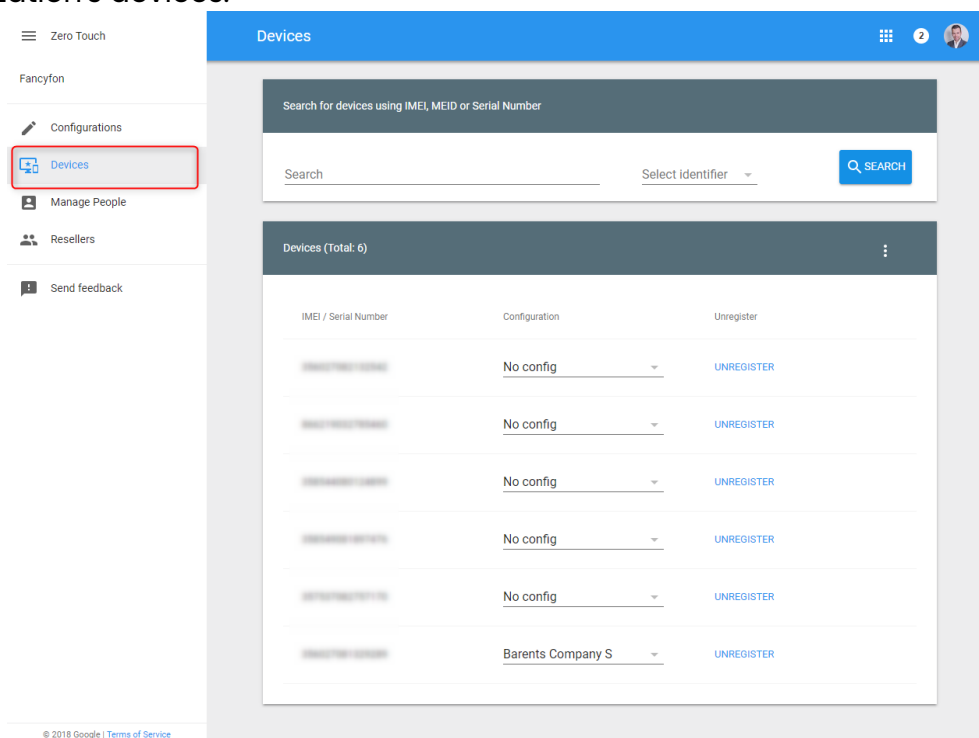
Synchronize



What do you want to do next?



Go to the Zero-Touch portal in your browser and log in to your account (<https://partner.android.com/zerotouch>). Go to the tab: Devices. You'll see your organization's devices.



The Available devices provides you with information: number of successfully imported devices / number of selected devices. In case of any problems with import go and see system log for more details.

Once the synchronization is complete - you're all set! The devices will enroll to Essentials MDM once turned on.