

FAMOC®

SafetyNet configuration



www.famoc.com

PUBLISHED BY

Famoc Software Limited

Atrium Business Centre

The Atrium, Blackpool Park

Cork, Ireland

Copyright© 2008-2020 by Famoc Software Limited

All rights reserved. No part of the contents of this document may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

Famoc™ and FAMOC™ are either registered trademarks or trademarks of Famoc Software Limited.

This publication may contain the trademarks and service marks of third parties and such trademarks and service marks are the property of their respective owners.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS AND SERVICES IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS AND SERVICES. THE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT AND SERVICES ARE SET FORTH IN THE Famoc TERMS AND CONDITIONS AND ARE INCORPORATED HEREIN BY THIS REFERENCE.



Table of contents

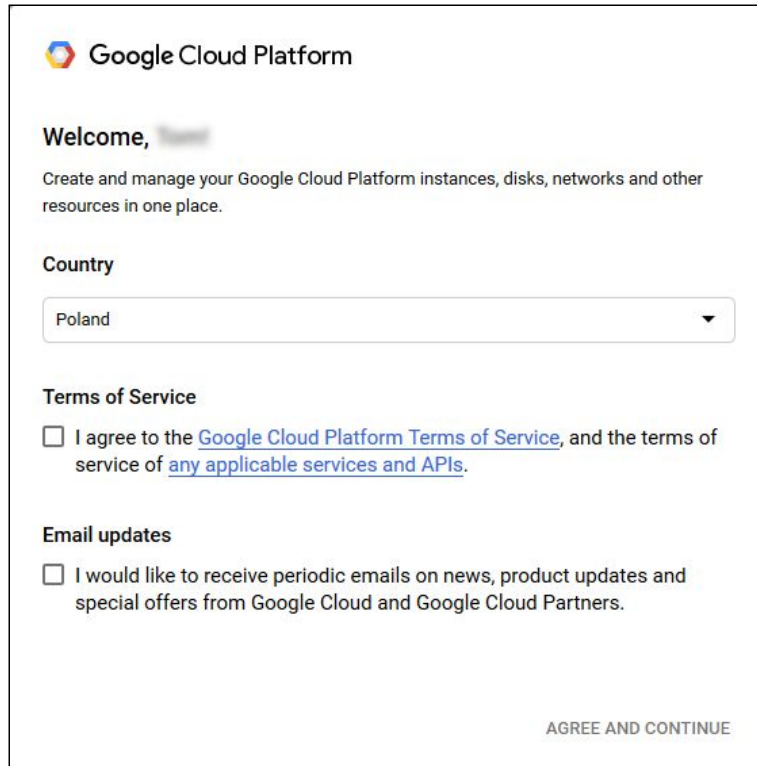
Obtaining the SafetyNet API key	3
Activation of SafetyNet in the FAMOC system	8

1 Obtaining the SafetyNet API key

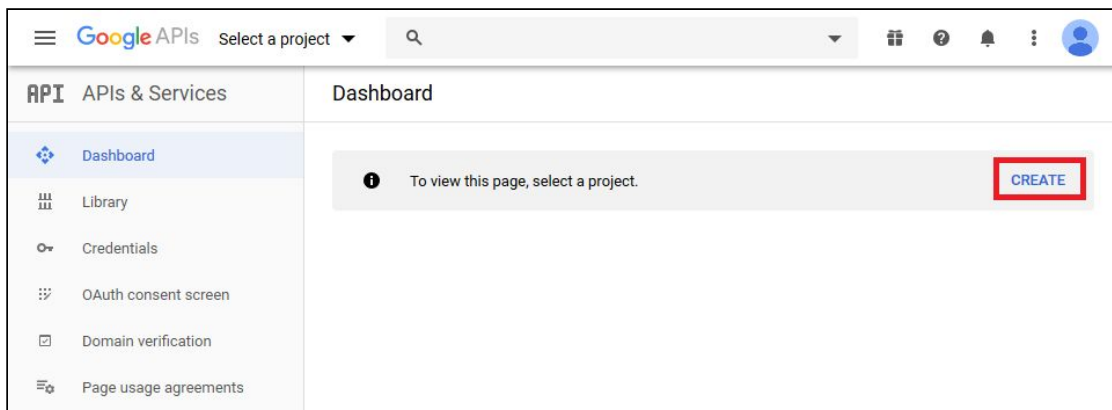
Requirements:

- active Google account:


To generate the SafetyNet API key, please visit <https://console.developers.google.com/> and log in to your Google account. Then accept the Google Cloud Platform terms of use and terms of service for the relevant services and APIs.




Create a new project, enter its name ('No organization' can be set in Location).




New Project

 You have 12 projects remaining in your quota. Request an increase or delete projects. [Learn more](#)

[MANAGE QUOTAS](#)

Project name *
My Project 54421 

Project ID: wise-brook-266609. It cannot be changed later. [EDIT](#)

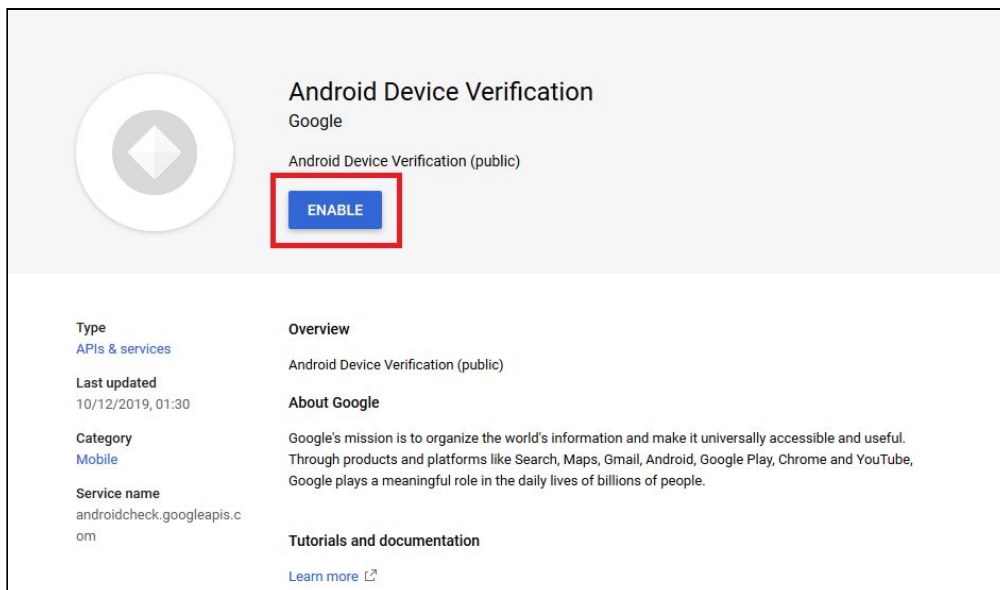
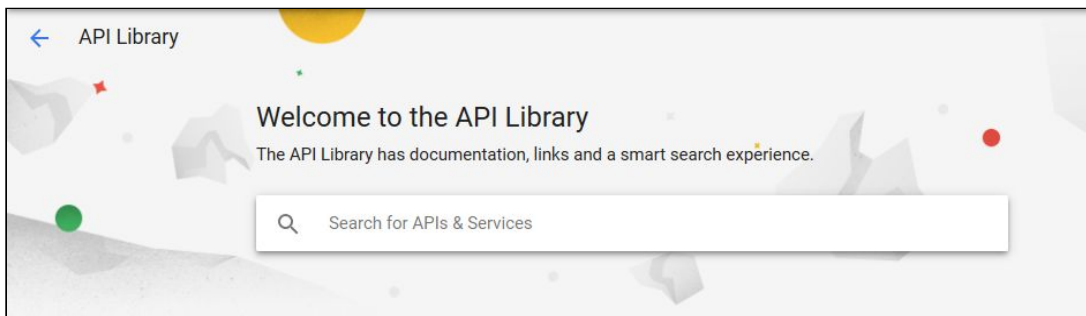
Location *
 No organisation [BROWSE](#)

Parent organisation or folder

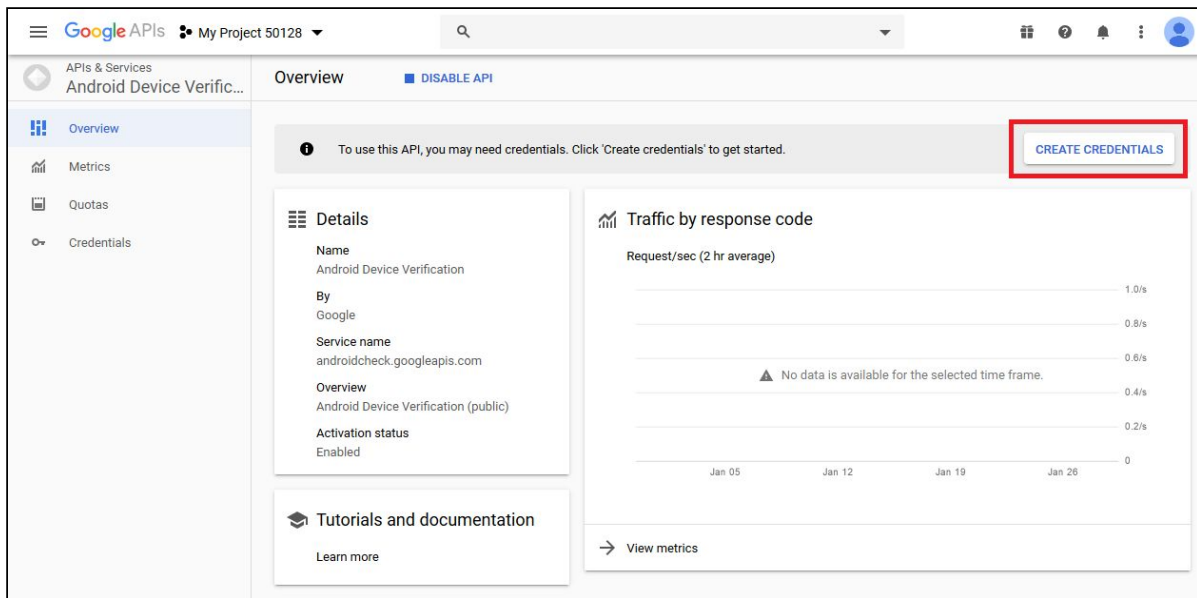
[CREATE](#) [CANCEL](#)

Go to <https://console.developers.google.com/apis/library>

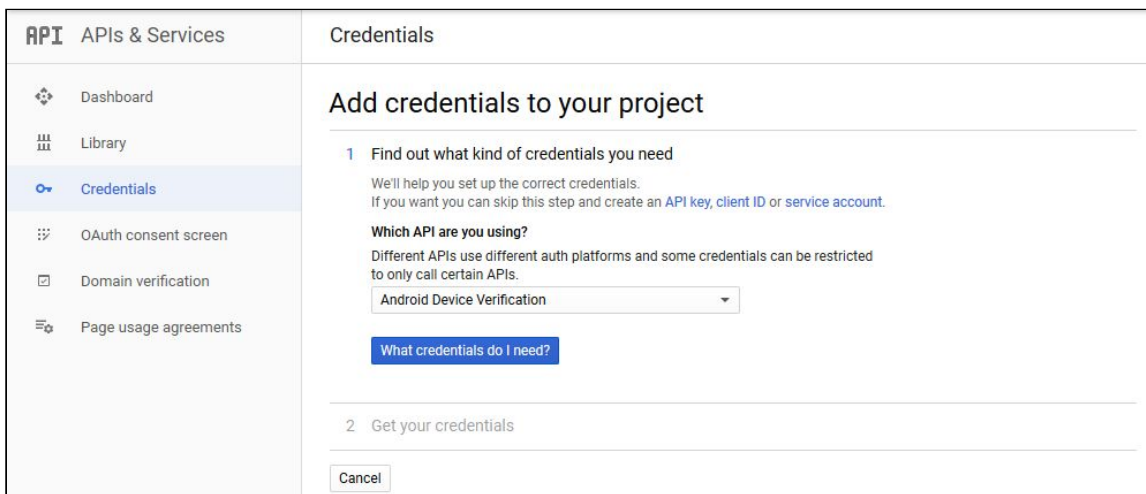
On the page, search for Android Device Verification API and click 'Enable'



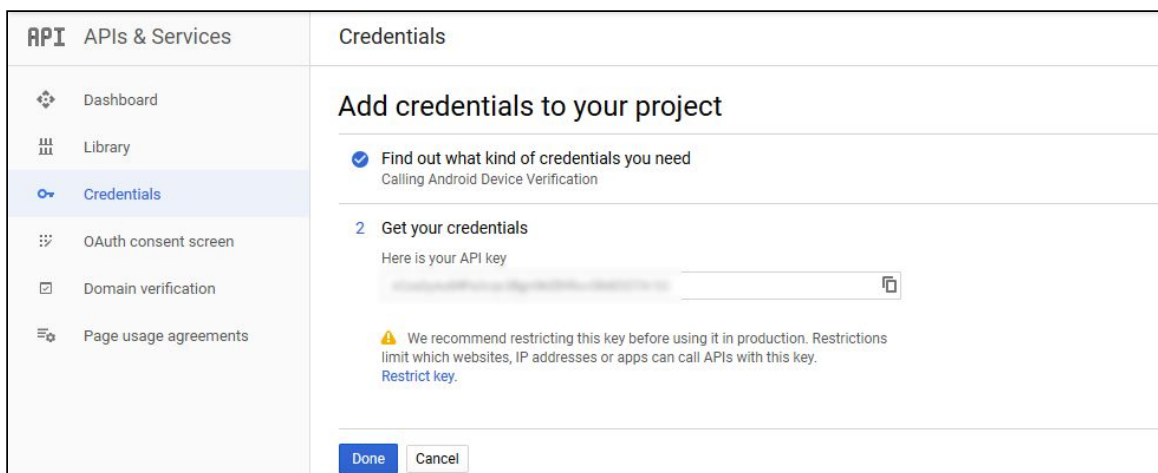
You will be taken to a new page where you must create your login details.




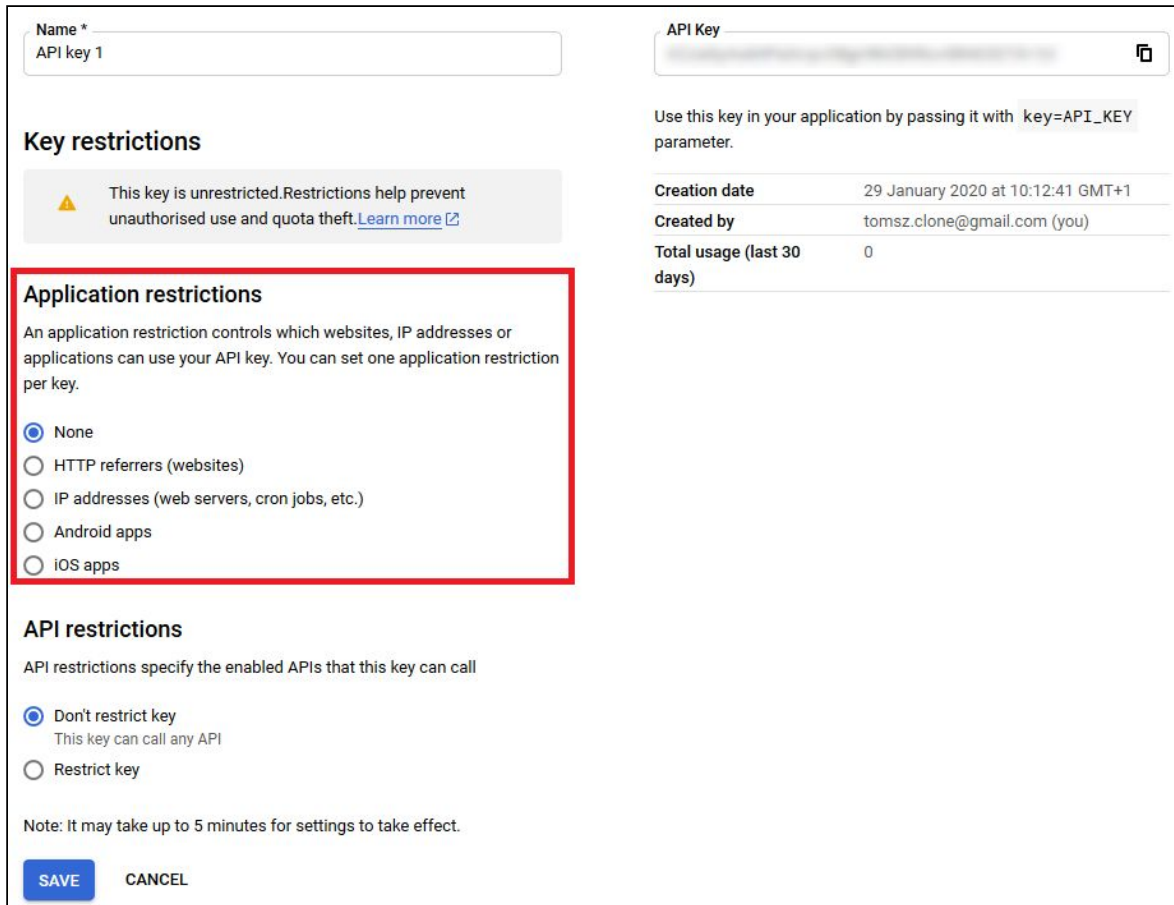
Select 'Android Device Verification' and then click 'What credentials do I need?'



An API key will be generated, copy it and click 'Done'.




Click the edit icon () in the credentials tab next to the name of your API key. In the key restrictions, make sure that 'Application restrictions' are set to 'None'



Name *
API key 1

API Key
[Redacted]

Key restrictions

 This key is unrestricted. Restrictions help prevent unauthorised use and quota theft. [Learn more](#)

Application restrictions

An application restriction controls which websites, IP addresses or applications can use your API key. You can set one application restriction per key.

- None
- HTTP referrers (websites)
- IP addresses (web servers, cron jobs, etc.)
- Android apps
- iOS apps

API restrictions

API restrictions specify the enabled APIs that this key can call

- Don't restrict key
This key can call any API
- Restrict key

Note: It may take up to 5 minutes for settings to take effect.

SAVE **CANCEL**

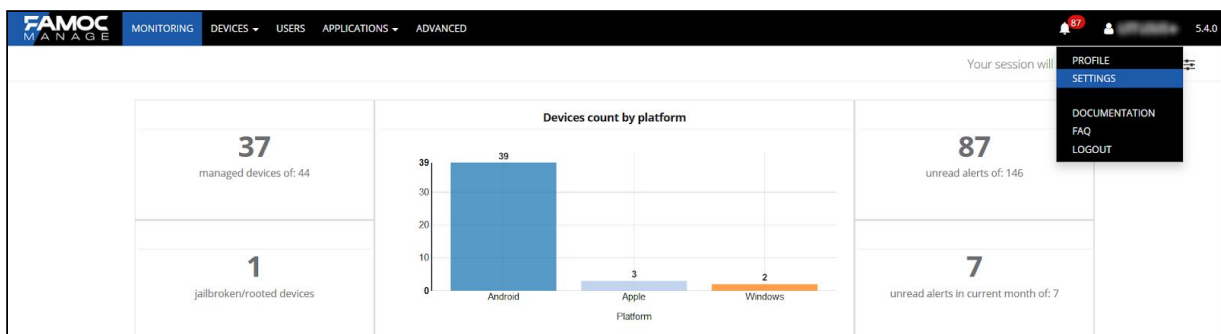
Creation date 29 January 2020 at 10:12:41 GMT+1

Created by tomsz.clone@gmail.com (you)

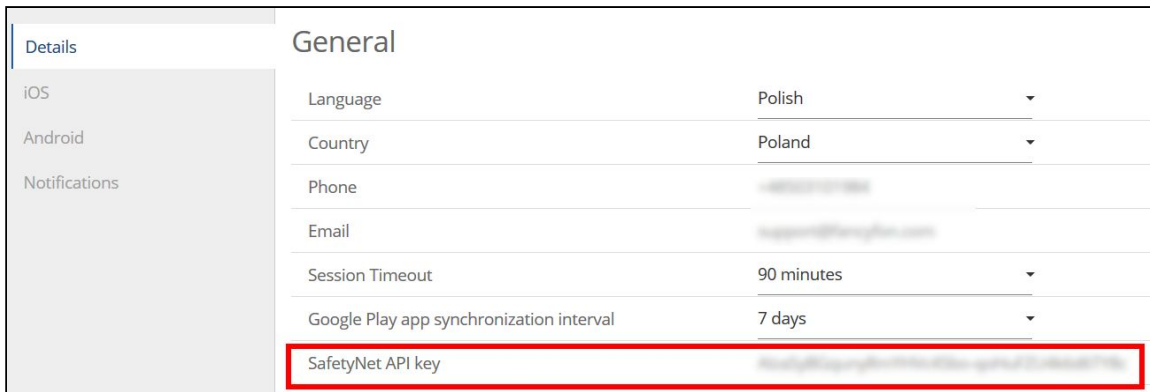
Total usage (last 30 days) 0

2 Activation of SafetyNet in the FAMOC system

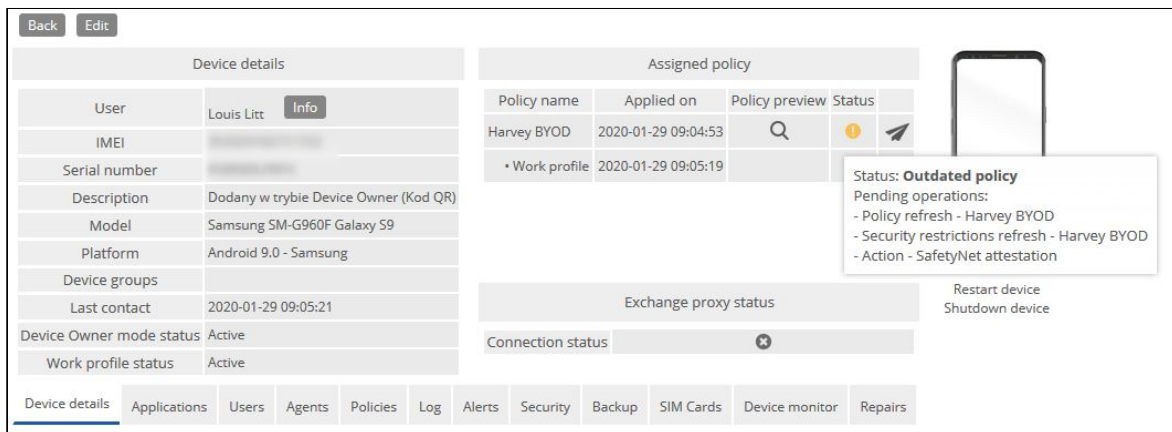
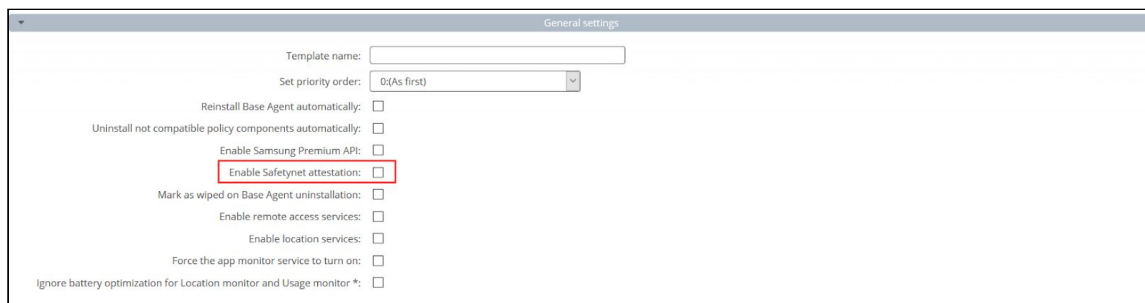
After logging in to FAMOC, select the organization settings.



In the 'Details' tab, in the 'SafetyNet API Key' field, paste the generated key.



In the General Settings of the policy (**Advanced** -> **Settings**) the option 'Enable SafetyNet attestation' has appeared - after enabling it and saving the general policy, a new operation 'SafetyNet Attestation' will appear during enrollment. For devices that were previously added to FAMOC, the policy status will change to 'Obsolete' and the next time the policy is refreshed, the validation operation will be performed.





During enrollment, if the result of the validation is negative, the components of the general policy and work profile will not be installed. The result of the validation depends on the status of the device (e.g. whether it is rooted, has an unlocked bootloader), possible cases are listed below (there must be at least one 'false' for the validation not to pass):

Table 1. Examples of how device status could affect the values of `basicIntegrity` and `ctsProfileMatch`

Device Status	Value of <code>ctsProfileMatch</code>	Value of <code>basicIntegrity</code>
Certified, genuine device that passes CTS	<code>true</code>	<code>true</code>
Certified device with unlocked bootloader	<code>false</code>	<code>true</code>
Genuine but uncertified device, such as when the manufacturer doesn't apply for certification	<code>false</code>	<code>true</code>
Device with custom ROM (not rooted)	<code>false</code>	<code>true</code>
Emulator	<code>false</code>	<code>false</code>
No device (such as a protocol emulating script)	<code>false</code>	<code>false</code>
Signs of system integrity compromise, one of which may be rooting	<code>false</code>	<code>false</code>
Signs of other active attacks, such as API hooking	<code>false</code>	<code>false</code>

Each project has its limits on the number of API queries, by default by default, the values shown below are set. (these are maximum values):

Quota Name	Limit	
Queries per day	10,000	
Queries per 100 seconds per user	1,000	
Queries per 100 seconds	1,000	

Quota Name	Limit	
Queries to verify endpoint per day	10,000	
Queries to verify endpoint per 100 seconds per user	1,000	
Queries to verify endpoint per 100 seconds	1,000	

You can change them by visiting <https://console.developers.google.com/apis/> dashboard, then selecting 'Android Device Verification' -> Quotas tab.