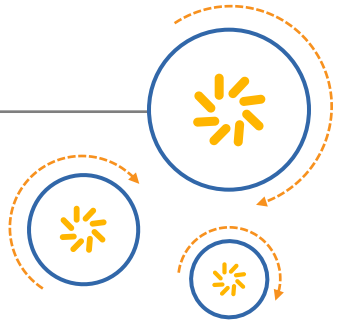
Qualcomm Technologies, Inc.



Genuine Device Detection Subsystem 1.0.0

User Guide (Authority)

GDDS-User-Guide-Authority-1.0.0

November 23, 2020

Revision history

Revision	Date	Description
A		First Release

Contents

Figures

Tables

1. Introduction

Genuine Device Detection Subsystem (GDDS) is the subsystem of Device Identification, Registration & Blocking System (DIRBS). It provides a platform for authorized entity to identify genuine device among duplicated IMEIs.

The Device Identification, Registration & Blocking System (DIRBS) is a country-wide system deployed in cooperation between the country regulator, operators in that country, and a technology partner that supports deployment. The system checks, identifies, and discourages non-compliant devices by verifying the installed base of devices currently active in a market and continuing to monitor as new devices are activated.

DIRBS can verify that:

- Devices have properly allocated identifiers and type approval
- Devices are not duplicated or stolen
- Device importation takes place through legal channels

1.1. Purpose

This document is intended to give assistance to the user to use the Genuine Device Detection Subsystem (GDDS).

1.2. Supported Desktop Browsers

Table 1 - Supported Desktop Browsers

Name	Version
Internet Explorer	11.0
Firefox	82.0.3
Chrome	86.0
Safari	13.1.2
Edge	86.0

1.3. Supported Mobile Browsers

Table 2 - Supported Mobile Browsers

Name	Version
Chrome	86.0.4
UC Browser	13.3.3
Opera (Android)	60.3
Opera Touch (iOS)	2.5.1
Safari	13.1.2
Samsung Internet	13.0.1
Android	10

1.4. Definitions, Acronyms, and Abbreviations

Table 3 - Definition, Acronyms, and Abbreviations

Term	Definition
DIRBS	Device Identification Registration and Blocking System
IAM	Identity Access Management System
GDDS	Genuine Device Detection Subsystem
MSISDN	Mobile Subscriber Integrated Services Directory Number
IMEI	International Mobile Equipment Identity
TAC	Type Allocation Code

2. System Description

Table 4 - System Description

Feature/Sections	Explanation
Login Screen	• To access the system, authorized user first needs to enter his/her credentials on login page. This login page authenticates user from IAM and redirects user to GDDS.
Portal Sections	The portal is divided into the following sections. • **Header** Header section displays name of the system and it contains following features. • **Language** Displays language of the system i.e. English, Spanish and Indonesian. • **User Profile Drop-down** Displays the user name with logout functionality. • **Navigation Panel** Navigation Panel contains main navigation menu through which user can navigate the whole system. • **Main Content Area** Main Content Area contains all the content to be displayed for respective feature. • **Breadcrumbs** Breadcrumbs allow user to keep track of their location within the system. • **Footer** Footer contains the software version and copyrights statement.
Dashboard	• The dashboard displays total count of Approved Logins, Pending Logins, Unique Brands and Total TACs. It also displays the recent pending login requests along with their details.

Account Approval	• Facilitates user to assign required brands to respective OEM(s).
Upload TAC Database File	• Facilitates user to upload file containing TAC details into the system.
Upload Duplication List	• Facilitates user to upload list of duplicated IMEIs into the system.
Send SMS to Duplicated IMEIs	• Allows user to send SMS to all device holders (Genuine and Duplicate).
Detect and Notify Genuine Device	• Facilitates user to identify genuine device among duplicated IMEIs and notify genuine device holders accordingly.
Notify Duplicated IMEIs	• Facilitates user to notify device holder(s) whose IMEIs have been marked as duplicated IMEI(s).
Create Black List	• Facilitates user to create a black list which contains IMEIs that have been marked as duplicate by the system.

3. System Navigation

3.1. Login Screen

1. Enter your credentials i.e. Username and Password.
2. Click on the “Log in” button.

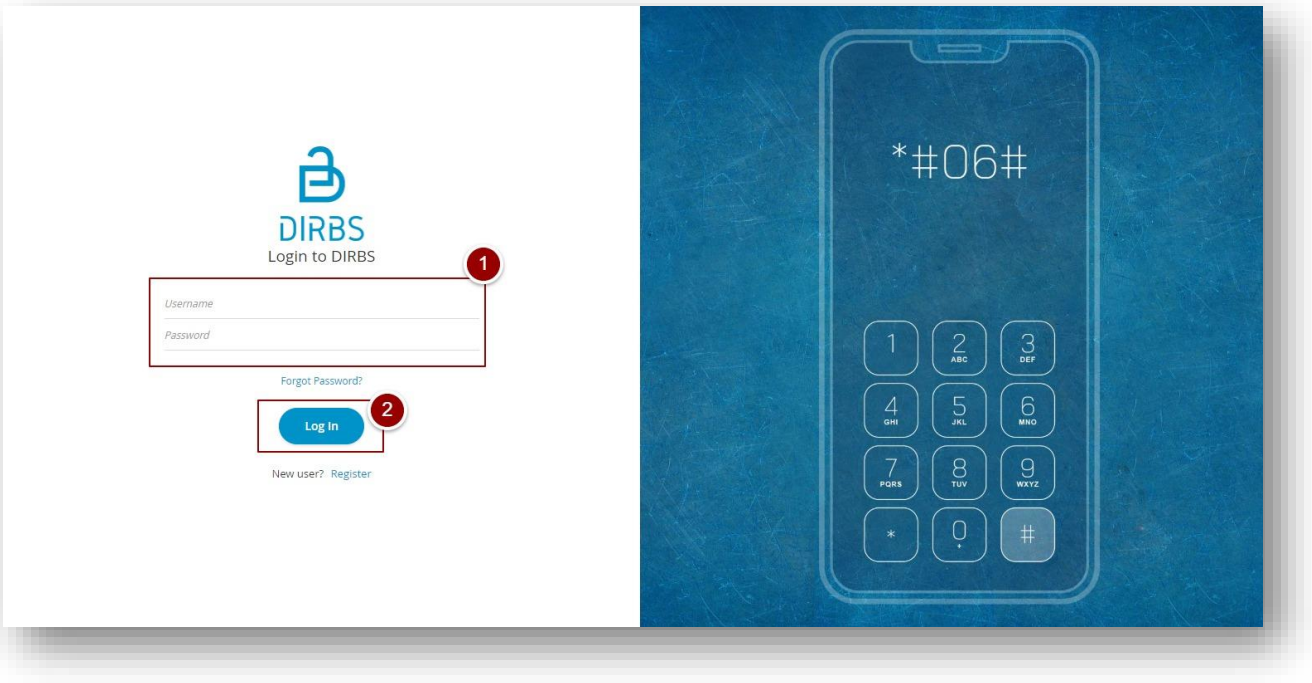


Figure 1 - Login Screen

3.2. Portal Sections

The portal screen is divided into following sections.

1. **Header** section displays name, language of the system and name of logged in user with logout functionality.
2. **Main Navigation Panel** helps user to navigate the system.
3. **Breadcrumbs** is a navigational aid in UI.
4. **Main Content Area** contains all relevant information related to the respective feature/option.
5. **Footer** contains version and copyrights of the system.

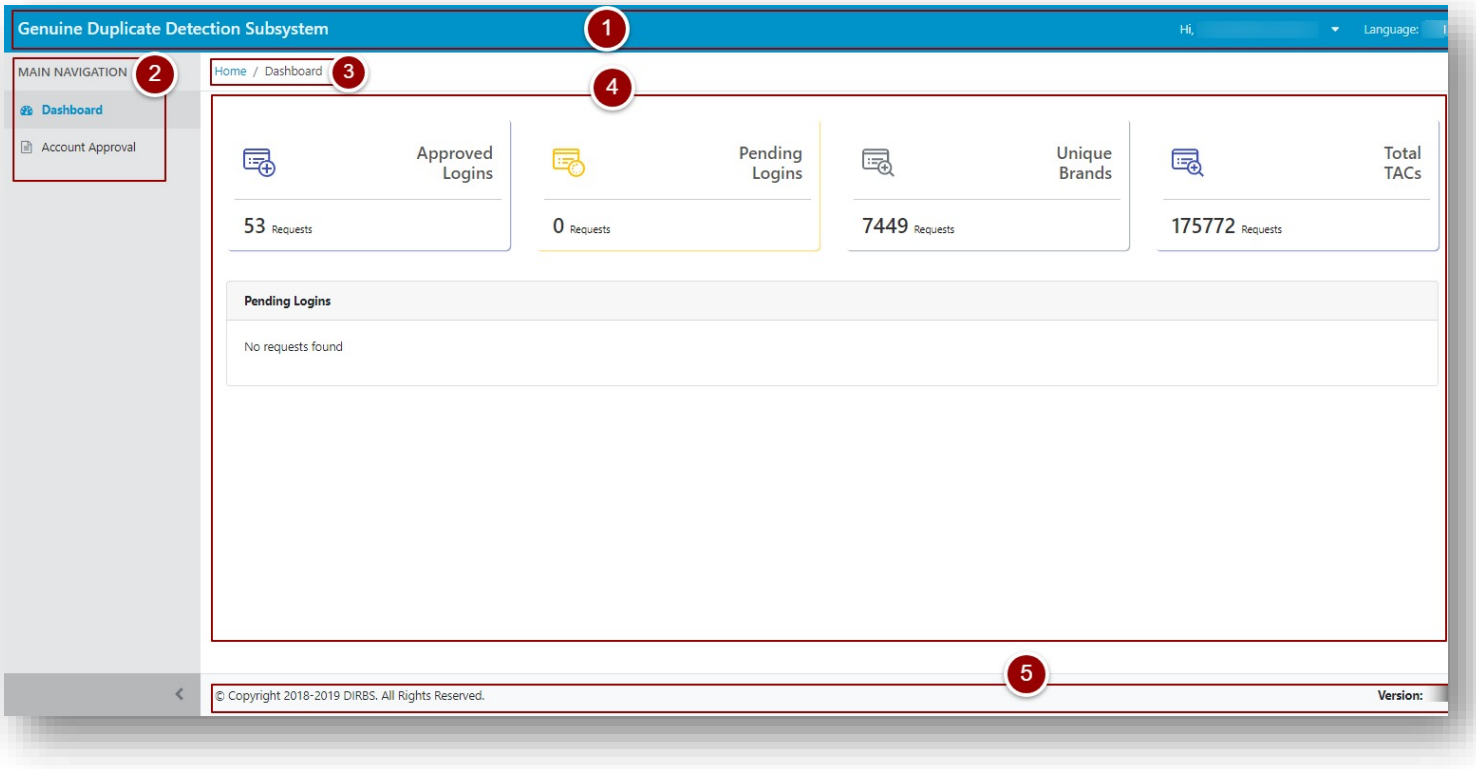


Figure 2 - Portal Sections

3.3. Dashboard

By clicking on “login” button, user will be redirected to dashboard screen that displays the total count of “Approved Logins”, “Pending Logins”, “Unique Brands” and “Total TACs”. It also displays recent pending login requests along with their details.

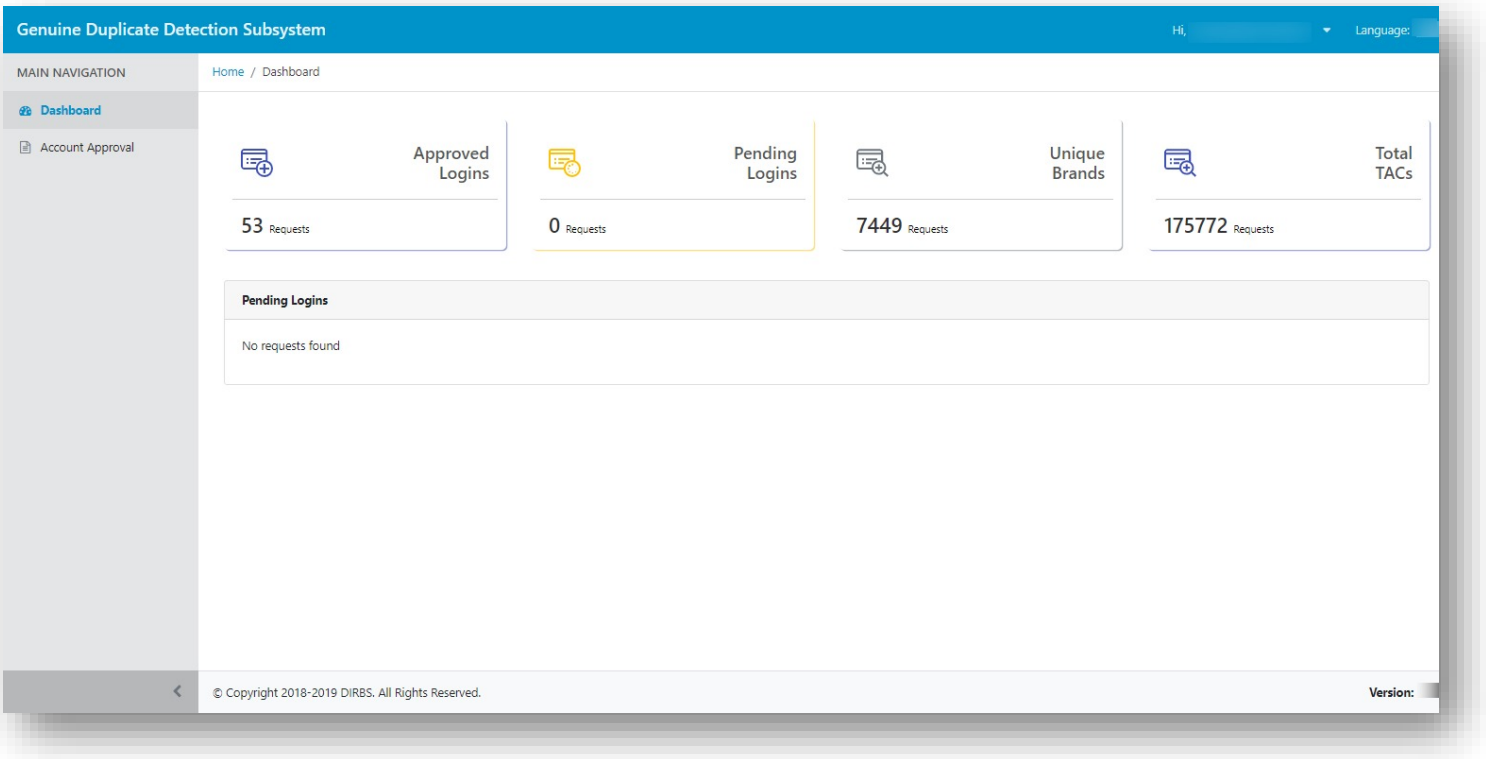


Figure 3 - Dashboard Screen

3.4. Upload TAC Database File

To upload brand names in the system, user needs to upload TAC database file from command line.

1. Go to GDDS_BACKEND directory.
2. Activate virtual environment and upload GSMA TAC database file.

```
source venv/bin/activate

update-gsma-tacs /home/Filename.txt
```

System will display total number of newly added brands in the system.

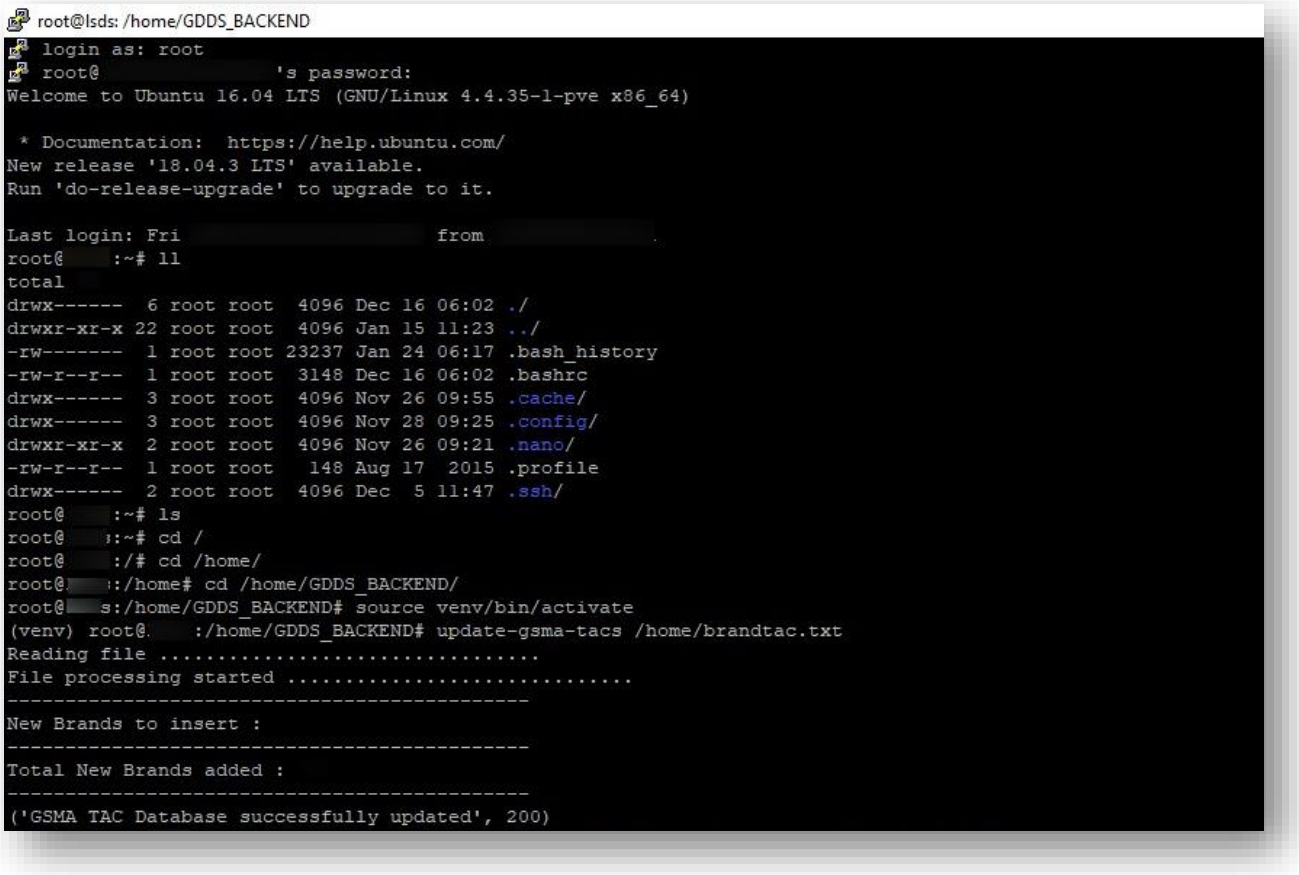


Figure 4 - Upload TAC Database File

3.5. Brand Association

To approve OEM(s) account, user needs to associate brands with respective OEM.

1. Click on “Account Approval” tab.
2. Select required OEM.
3. All available brands will be displayed under “Available Brands”.

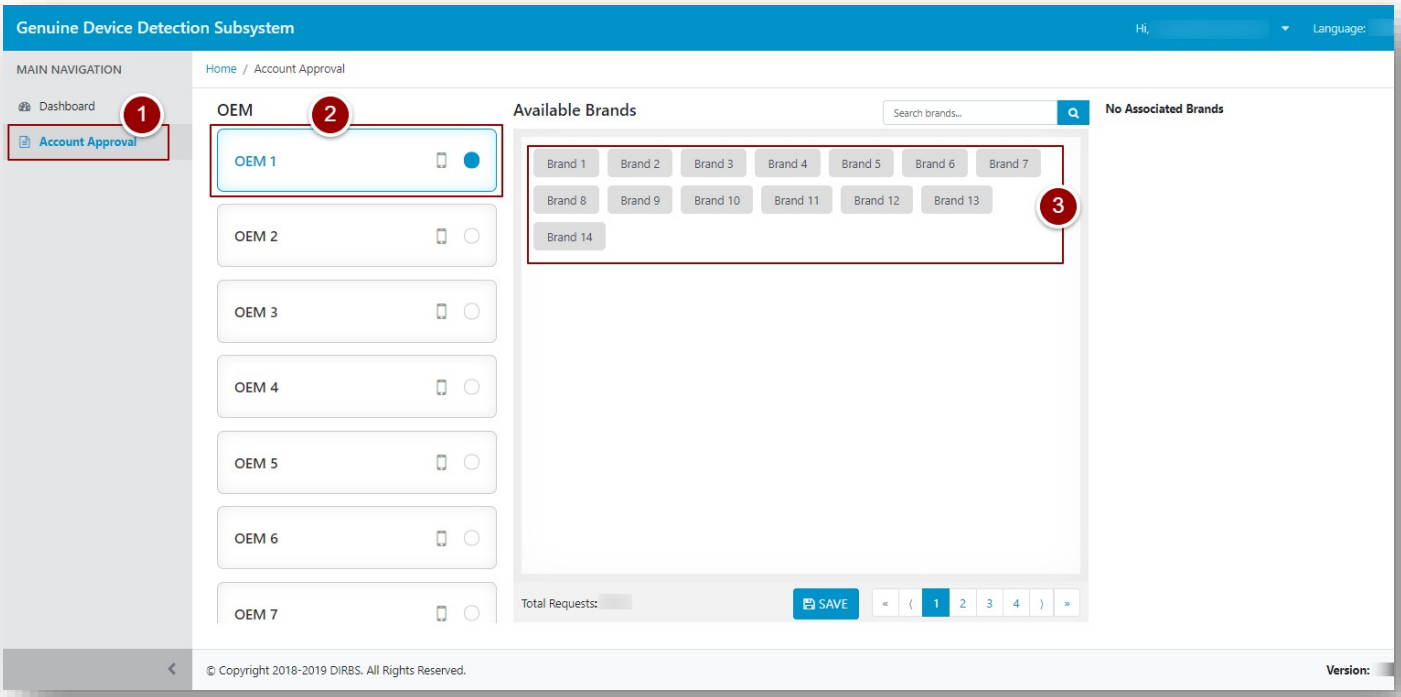


Figure 5 - Brand Association (i)

4. To associate any brand to OEM, click on required brand name.

   If any brand is already assigned then it will be displayed on right side under “Associated Brands”.

   To de-associate any brand, click on brand name displayed under “Associated Brands” and follow step 6.

5. Selected brand name will be displayed on right side under “Associated Brands”.
6. Click on “Save” button.

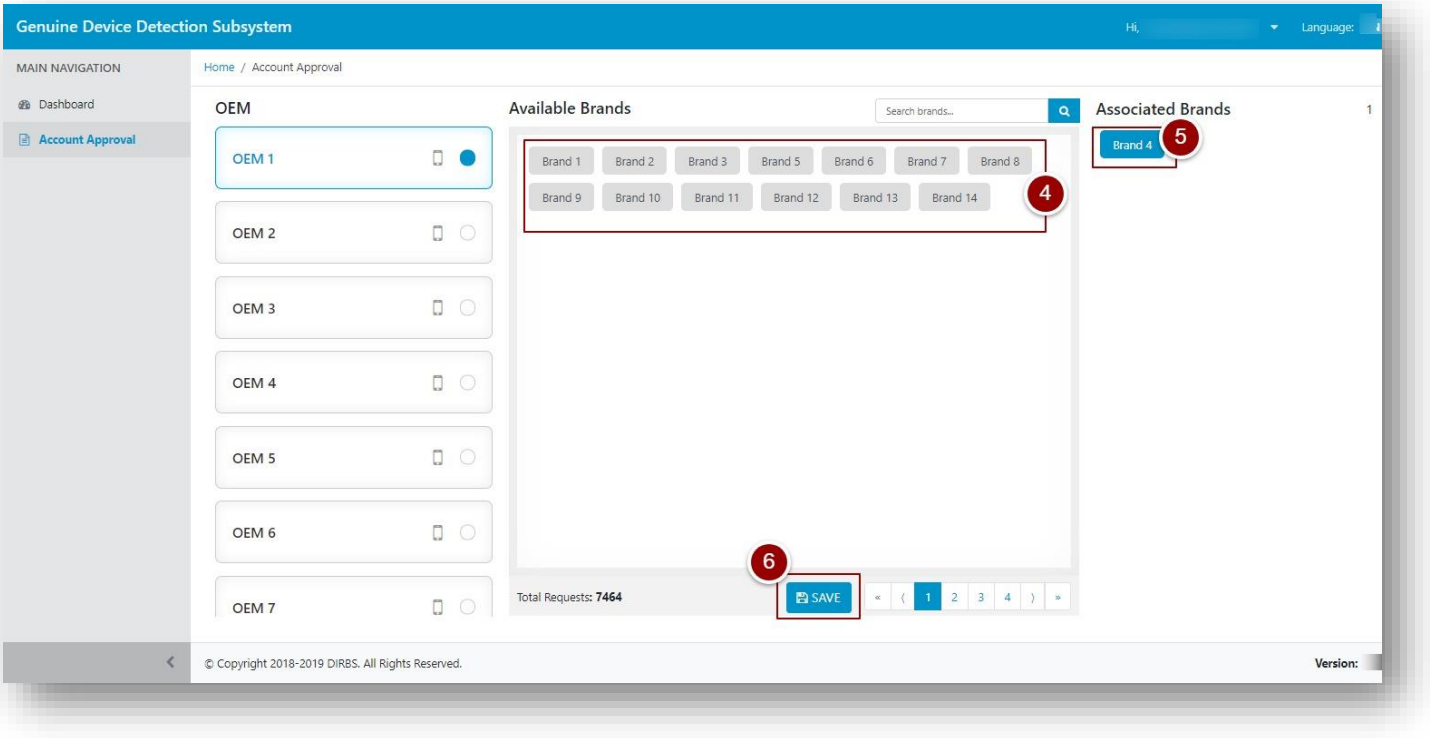


Figure 6 - Brand Association (ii)

A popup will appear for confirmation.

7. Click on “OK” button.

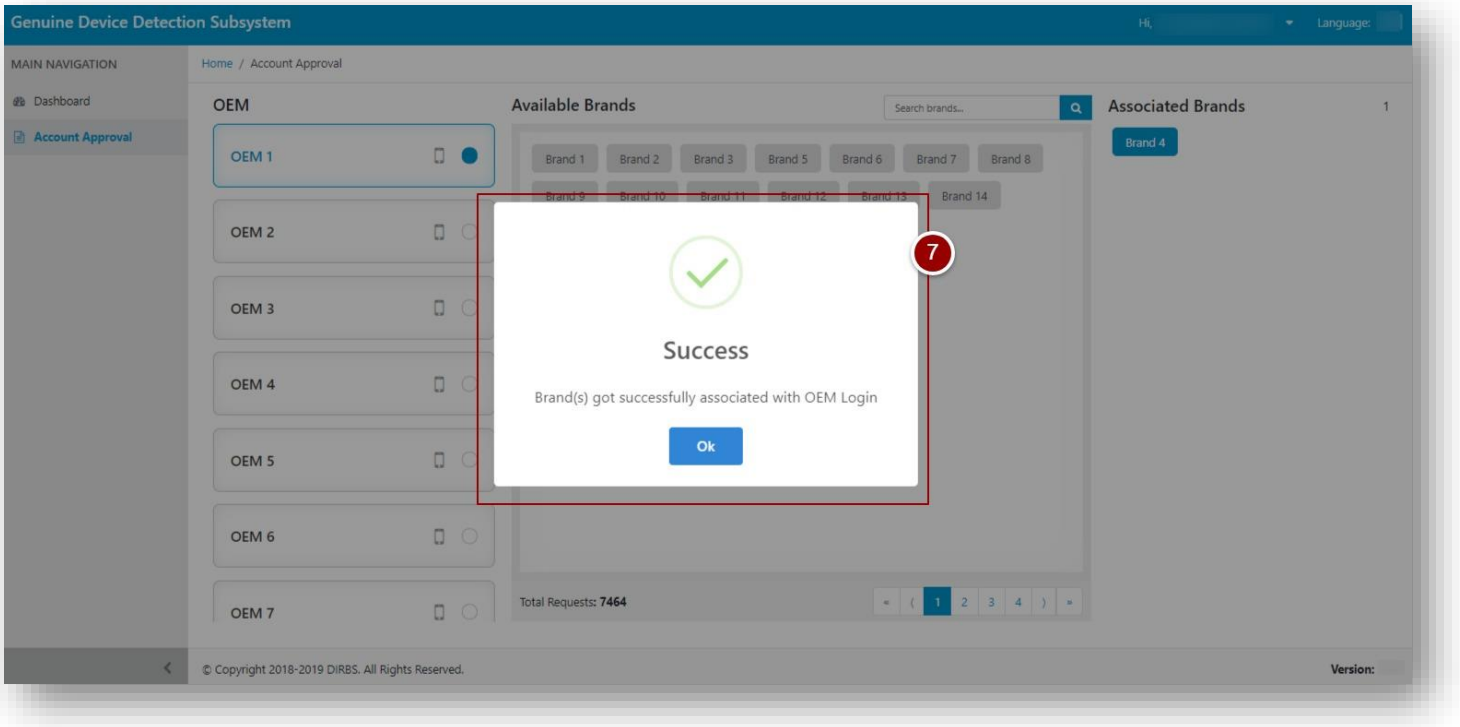


Figure 7 - Brand Association (iii)

3.6. Upload Duplicate IMEIs List

To send list of duplicated IMEIs to respective OEM, user needs to first upload file of duplicated IMEIs in the system.

1. Go to GDDS_BACKEND directory.
2. Activate virtual environment and upload list of duplicated IMEIs.

```
source venv/bin/activate

import duplication_list /home/duplicationlist.txt
```

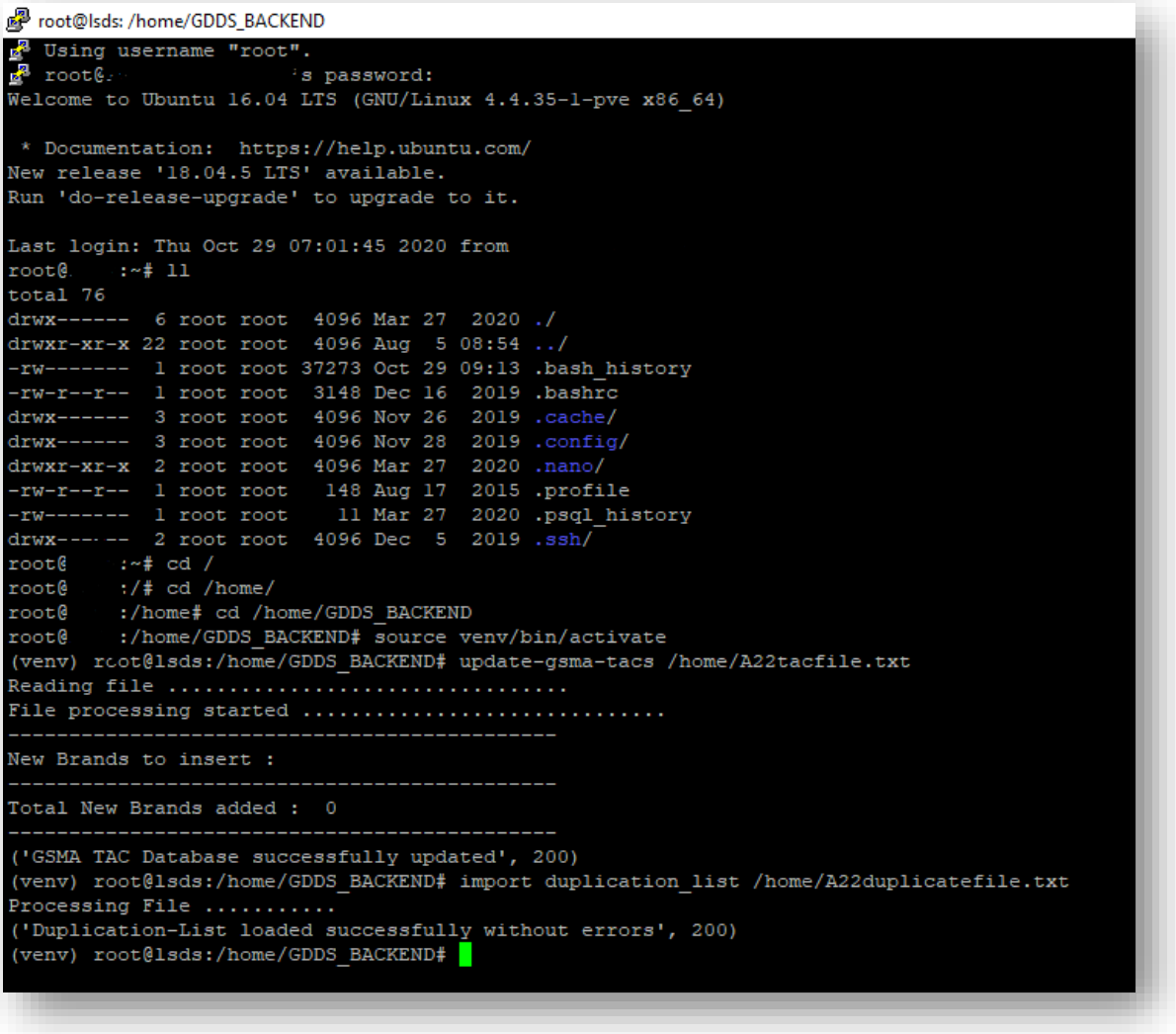


Figure 8 - Upload Duplicate list

3.7. Send SMS to All Users Using Duplicate IMEIs

To send SMS to all users who are using duplicated IMEIs to provide their info, run the following commands.

1. Go to GDDS_BACKEND directory.
2. Activate virtual environment and send SMS to all MSISDNS against duplicated IMEIs.

```
source venv/bin/activate

send-request-sms all
```

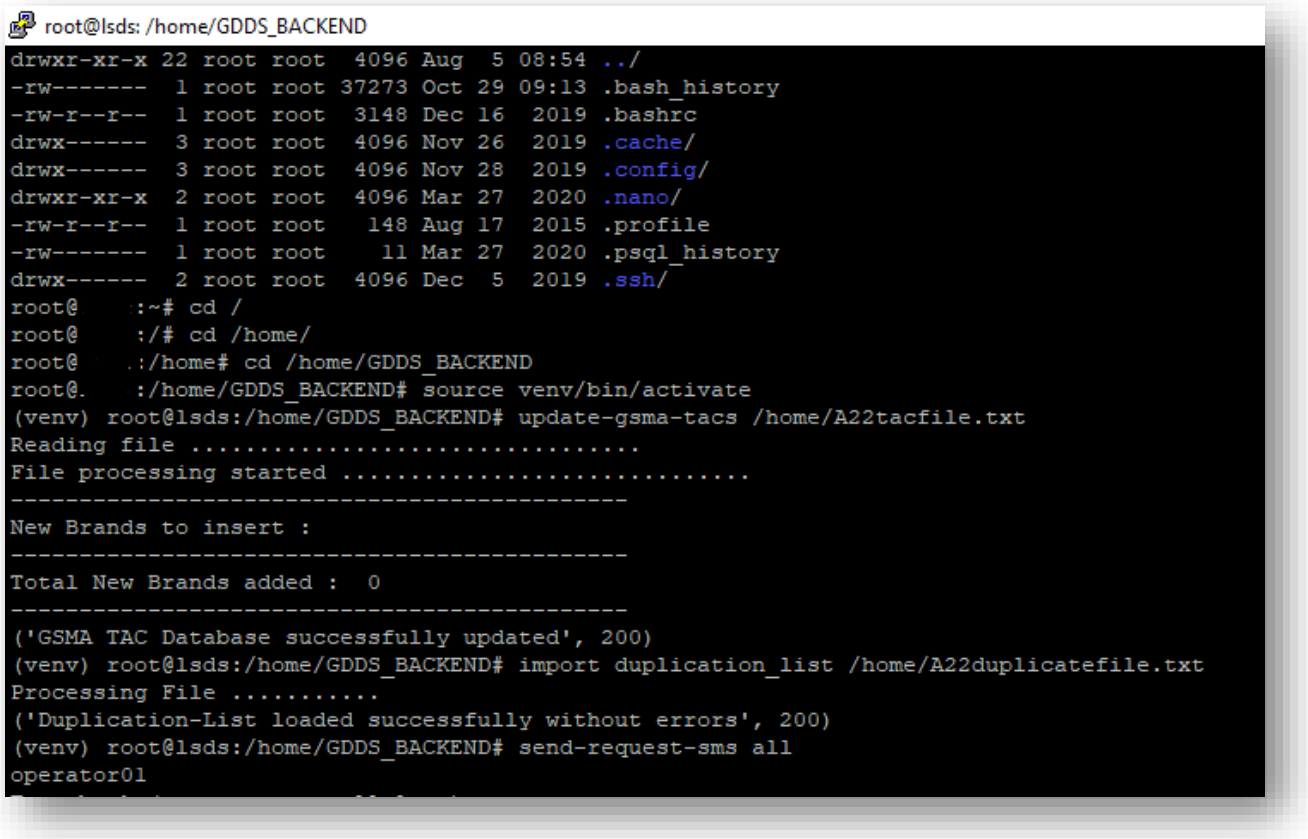


Figure 9 - SMS to All Duplicate IMEIs

3.8. Send SMS to All Un-notified Users using Duplicate IMEIs

To send SMS to all un-notified users using duplicated IMEIs to provide their info, run the following commands.

3. Go to GDDS_BACKEND directory.
4. Activate virtual environment and send SMS to all MSISDNS against duplicated IMEIs.

```
source venv/bin/activate

send-request-sms unnotified
```

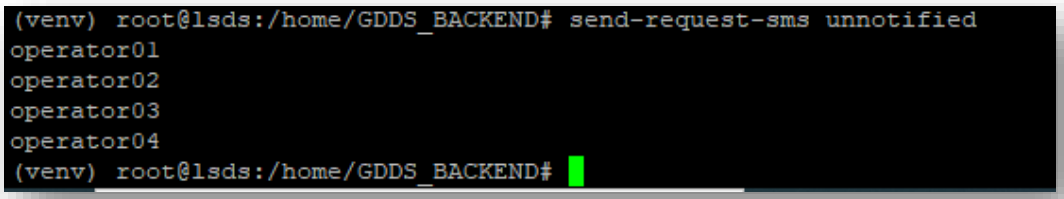


Figure 10 - SMS to All Un-notified Duplicate IMEIs

3.9. Detect and notify genuine device

To detect and notify genuine device user, run the following commands.

1. Go to GDDS_BACKEND directory.
2. Activate virtual environment and compare data coming from OEM and Device holder by running below mentioned commands.

```
source venv/bin/activate

run-comparison

send-intimation-sms genuine
```

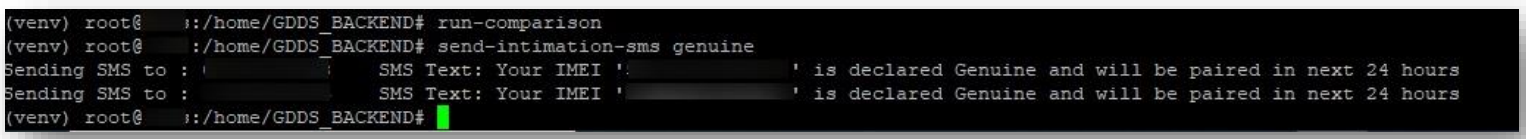


Figure 11 - Detect and Notify Genuine Device

3.10. Notify Duplicated IMEIs

System will notify non-genuine device holders.

1. Go to GDDS_BACKEND directory.
2. Activate virtual environment and send SMS to non-genuine device holder(s).

```
source venv/bin/activate

send-intimation-sms duplicated
```

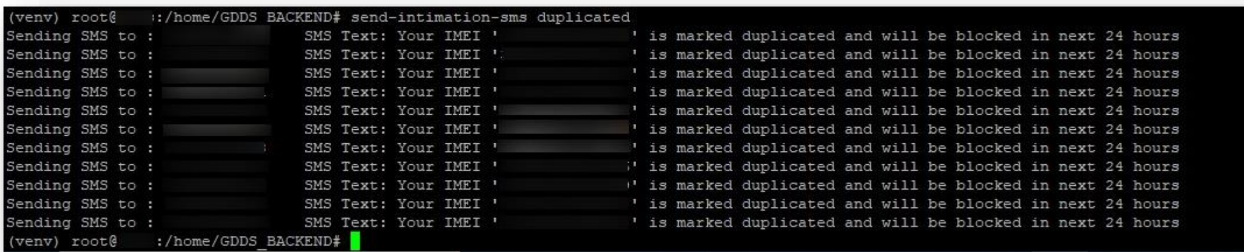


Figure 12 - Notify Duplicated IMEIs

3.11.Create Pairing & Black list

System will create a list of IMEIs which are being marked as duplicate.

1. Go to GDDS_BACKEND directory.
2. Activate virtual environment and run below mentioned command to create a Pairing & black list.

```
source venv/bin/activate

generate-lists
```

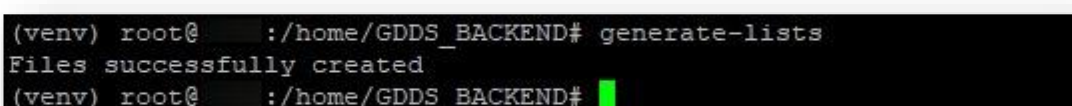


Figure 13 - Create Black List

3.12. Integration with DPS

System will generate a pair code and send that Pair code to users who are marked as Genuine.

1. Go to GDDS_BACKEND directory.
2. Activate virtual environment and run below mentioned command to generate a pair code.

```
source venv/bin/activate

register-with-dps
```

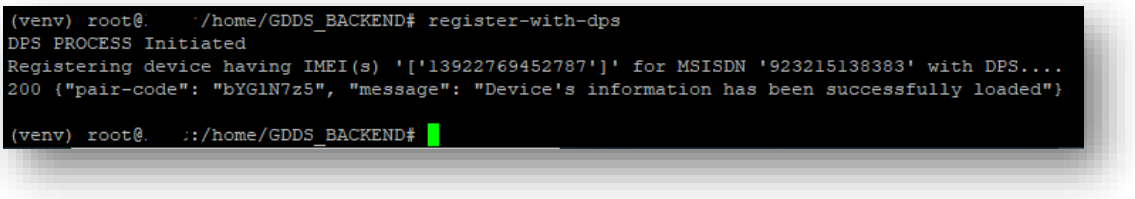


Figure 14 - Integration with DPS

