ve

**Lawful Agency User Manual v 1.0**

* **Central Equipment Identity Register Portal**

Document Change History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Change Type | Description | Date |
| Draft |  | Submitted for internal review | February 2020 |

Contents

Document Change History i

Contents ii

Figures iii

1 Overview 1

1.1 Scope 1

1.2 Acronyms & Abbreviations 1

1.3 Conventions 1

2 Operations 3

2.1 Application Overview 3

2.2 Logging into the Application 3

2.3 Application User Interface 11

2.3.1 Dashboard 13

2.4 Stolen/Recovery Devices 18

2.4.1 Individual Device Stolen 18

2.4.2 Company Device Stolen 24

2.4.3 Individual Device Recovery 28

2.4.4 Bulk Device Recovery 31

2.5 Edit Stolen/Recovery Device Requests 33

2.6 Filter Stolen/Recovery Device Requests 35

2.7 Export Stolen/Recovery Device Requests 36

2.8 Grievance Management 37

2.9 Filter Grievances 41

2.10 Export Grievances 42

Figures

Figure 1: DMC Home Page 3

Figure 2: Lawful Agency Registration 4

Figure 3: Verify OTP 6

Figure 4: Enter OTP 7

Figure 5: Login 8

Figure 6: Home Page 9

Figure 7: Forgot Password 9

Figure 8: Set New Password 10

Figure 9: Home Page 11

Figure 10: Edit Information 12

Figure 11: Change Password 12

Figure 12: Manage Account 13

Figure 13: Home Page 14

Figure 14: Stolen/Recovery Devices 15

Figure 15: Stolen/Recovery Devices 16

Figure 16: Grievance Management 16

Figure 17: Home Page 17

Figure 18: Home Page 18

Figure 19: Stolen/Recovery Devices 19

Figure 20: Report Stolen 19

Figure 18: Home Page 24

Figure 19: Stolen/Recovery Devices 25

Figure 20: Report Stolen 25

Figure 21: Report Stolen 29

Figure 22: Stolen/Recovery Devices 29

Figure 23: Report Stolen 30

Figure 21: Report Recovery 31

Figure 22: Stolen/Recovery Devices 32

Figure 23: Report Recovery 32

Figure 24: Stolen/Recovery Devices 34

Figure 25: Edit Stolen Device (Individual Device) 34

Figure 26: Edit Stolen Device (Bulk Device) 35

Figure 25: Edit Recovery Device (Individual Device) 35

Figure 27: Stolen/Recovery Devices 36

Figure 28: Filtered Device Stolen/Recovery Requests 37

Figure 29: Stolen/Recovery Devices 38

Figure 30: Open or Save Exported Stolen/Recovery Devices File 38

Figure 31: Exported Stolen/Recovery Devices 39

Figure 46: Home Page 40

Figure 47: Grievance Management 40

Figure 48: Report Grievance 40

Figure 49: Grievance Management 41

Figure 50: Filter Grievances 43

Figure 51: Filtered Grievances 43

Figure 52: Grievance Management 44

Figure 53: Open or Save Exported Grievance File 44

Figure 54: Exported Grievances 44

# Overview

## Scope

The objective of this manual is to help Lawful Agency to report stolen and recovered devices (IMEIs/MEIDs/ESNs) and report grievances.

## Acronyms & Abbreviations

| **Acronym** | **Full Form** |
| --- | --- |
| CEIR | Central Equipment Identity Register |
| EIR | Equipment Identity Register |
| ESN | Electronic Serial Number |
| FIR | First Information Report |
| IMEI | International Mobile Equipment Identity |
| MEID | Mobile Equipment Identifier |
| PDA | Personal Digital Assistant |
| TAC | Type Allocation Code |
| TRC | Telecom Regulator of Cambodia |

## Conventions

| **Information** | **Convention** |
| --- | --- |
| UI elements  (such as names of windows, buttons, and fields) | Bold |
| References  (such as names of files, sections, paths, and  parameters) | *Italics* |
| **\*** | Indicates a mandatory field or column |

# Operations

## Application Overview

The CEIR (Central Equipment Identity Register) Lawful Agency Portal application is used to report stolen/recovered devices as reported by the device end user in the network.. The devices that are stolen can be marked as recovered as well using the application. Lawful Agency can raise grievances to the CEIR administrator whenever there is any problem.

Lawful Agency can use the application to perform the following tasks:

* Report Stolen devices
* Report Recovered devices
* Report grievances

## Logging into the Application

Before login, Lawful Agency needs to register in the application. Employee or Lawful Agency personnel register on the CEIR portal on behalf of a Lawful Agency.

To register:

1. Enter the DMC home portal page URL in the browser address bar. This opens the following page.

A screenshot of a cell phone

Description automatically generated

Figure 1: DMC Home Page

1. Select **Lawful Agency** from the **Registration** list.

A screenshot of a cell phone

Description automatically generated

The **Lawful Agency Registration** page appears. The Lawful Agency needs to enter the following information.

A screenshot of a computer

Description automatically generated

Figure 2: Lawful Agency Registration

1. **\*First Name**: Enter the first name.
2. **Middle Name**: Enter the middle name (if any).
3. **\*Last Name**: Enter the last name.
4. **Address**: Enter the Lawful Agency’s address:
   * Street Number
   * Village
   * Locality
   * District
   * Commune
   * Province
   * Country
5. **\*National ID:** Enter the national ID of Lawful Agency personnel.
6. **\*Upload National ID**: Upload the image of the original national ID of Lawful Agency personnel. This can be a pdf or image (.jpeg) of size not more than 5 MB.
7. **Upload Photo**: Upload the photograph of the Lawful Agency personnel. The photograph can be a pdf or image (.jpeg) of size not more than 5 MB.
8. **Employee ID**: Enter the employee ID of the Lawful Agency.
9. **Upload ID Card**: Upload the image of the ID card. The photograph can be a pdf or image (.jpeg) of size not more than 5 MB.
10. **Nature of Employment**: Select the type of employment of the Lawful Agency personnel:
    * Permanent
    * Temporary
    * Contract
11. **Designation and Title**: Enter the designation of the Lawful Agency’s personnel.
12. **Reporting Authority Name**: Enter the name of the officer to whom the Lawful Agency’s personnel reports.
13. **Reporting Authority Email ID**: Enter the mail ID of the officer to whom the Lawful Agency’s personnel reports to.
14. **Reporting Authority Contact Number**: Enter the contact number of the officer to whom the Lawful Agency personnel reports to.
15. **Email**: Enter the mail ID of Lawful Agency’s personnel. This mail ID would be used for communication with the Lawful Agency.
16. **\*Contact Number**: Enter the mobile number of Lawful Agency’s personnel. Lawful Agency receives notifications at this mobile number.
17. **\*Password**: Enter a login password. This is the password that would be used to log into the CEIR Lawful Agency Portal application.
18. **\*Confirm Password**: Re-enter the password for confirmation.
19. **\***Select three security questions and enter an answer for each question. This is required by the system when the Lawful Agency forgets the login password. In such a situation, the system requires some type of identification to authenticate the Lawful Agency. The security questions are used to identify and authenticate the Lawful Agency.
20. **\***Enter the captcha shown on the page. This is required to prove to the system that the Lawful Agency is not a robot.
21. **\***Select the declaration check box.
22. Click **SUBMIT**.

An OTP is sent to the Lawful Agency’s mail ID and contact number.

A screenshot of a cell phone

Description automatically generated

Figure 3: Verify OTP

The Lawful Agency is prompted to enter both the OTPs in the page for verification.

A screenshot of a cell phone

Description automatically generated

Figure 4: Enter OTP

If the two OTPs match, the following message appears. If the OTPs do not match, an error message is displayed. In case the OTP is not received, click **Resend OTP** to request the CEIR system to resend the OTP. The two OTPs are resent, one to the contact number and the other to the mail account.

A screenshot of a social media post

Description automatically generated

After the OTPs are verified successfully, the registration request is sent for approval to the CEIR administrator. The approval turnaround time is 2-3 days. After approval from the CEIR administrator, an e-mail containing a registration ID is sent to the Lawful Agency’s personnel mail account. The registration ID is a unique automatically generated ID. The ID is the login username for access to the CEIR Lawful Agency Portal application. This concludes the registration process.

To start using the application, log into the application.

To login:

1. Open the browser and enter the DMC home portal URL in the address bar. The login screen appears.

A screenshot of a cell phone

Description automatically generated

Figure 5: Login

On the top right corner of the login screen is the **Language** option. The application supports two languages: **English** and **Khmer**. On selecting a given language, all the field and column labels in the application appear in the selected language. All user inputs are, however, in English.

A screenshot of a cell phone

Description automatically generated

1. Next, enter the assigned login username and password.

Username is the registration ID that is sent on mail to the Lawful Agency after successful registration in the system. Username is a unique ID that is automatically generated by the system. The login password is the password that the Lawful Agency enters in the registration page. Refer to during *Figure 2: Lawful Agency Registration*.

1. Enter the captcha.
2. Click **LOGIN**.

If the login and password are incorrect or the captcha is not correct, an error message appears, and the Lawful Agency is prompted to re-enter the login details.

On entering correct information, the application Home page appears.

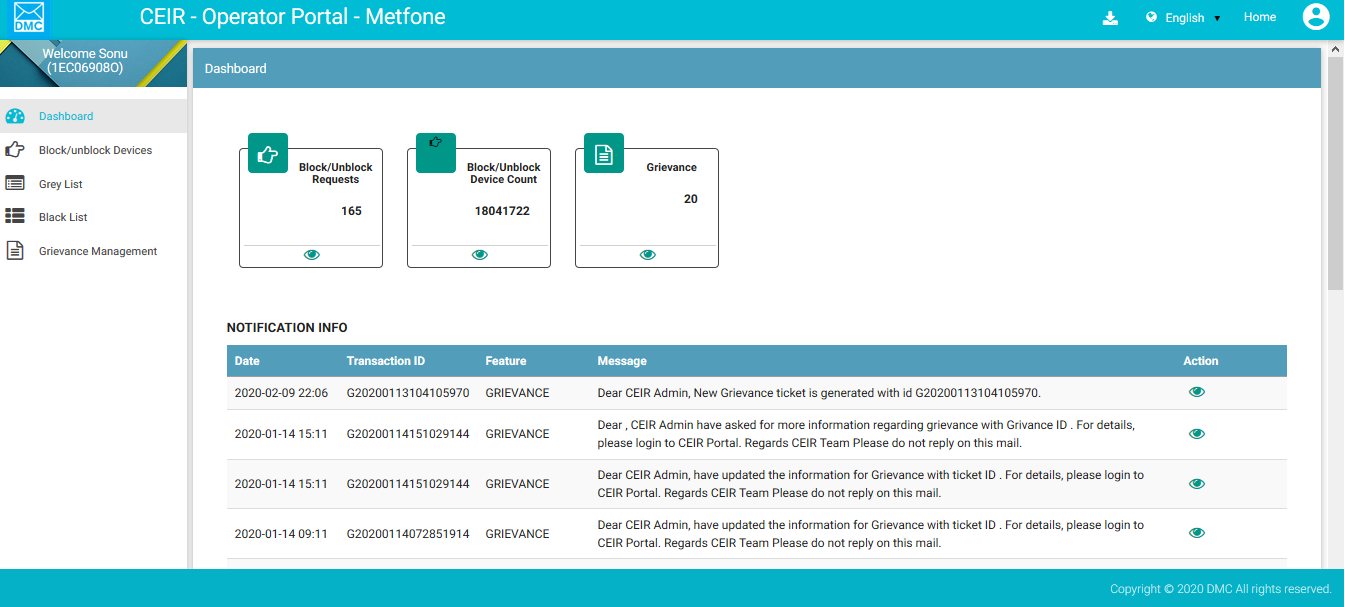


Figure 6: Home Page

If the Lawful Agency forgets the assigned password, click the **Forgot Password** link on the **Login** page. The **Forgot Password** page appears.

A screenshot of a cell phone

Description automatically generated

Figure 7: Forgot Password

1. Enter the login username.
2. Select a security question from the list. Select any one of the security questions that were selected during registration.
3. Enter the answer to the selected security question. This should match the answer given at the time of registration.
4. Click **SUBMIT**.

The **Set New Password** page appears.

A screenshot of a cell phone

Description automatically generated

Figure 8: Set New Password

1. Enter a new password. Click  to see the password characters being entered. Click on it again to hide the password characters. This works like a toggle key.
2. Re-enter the password.
3. Click **Save**.

## Application User Interface

On logging into the application successfully, the CEIR Lawful Agency Portal Home page appears.

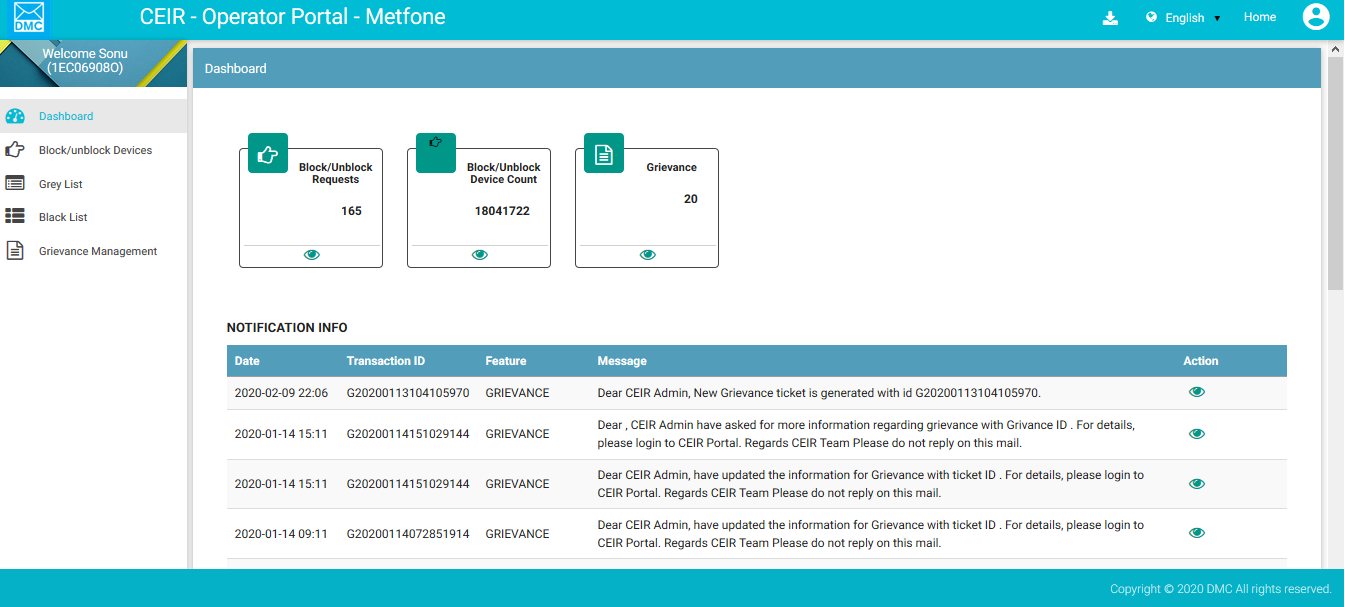


Figure 9: Home Page

The Home page has all the feature menus on the left panel.

The center of the page is the Dashboard.

The top right corner of the screen displays the following menu options:

* **Download** : Click to download this user manual.
* **English** : Select **English** or **Khmer**. All the field and column labels appear in the selected language. User inputs are, however, in English.

A close up of a logo

Description automatically generated

* **Home**: Click on it to go to the **DMC Home Portal** page.
* A close up of a logo

  Description automatically generated (**User profile**): Click on it to see the following menu:

A screenshot of a cell phone

Description automatically generated

* **** (**Edit Info**): Click on it to modify the registered information. The **Edit Information** page opens.

A screenshot of a cell phone

Description automatically generated

Figure 10: Edit Information

1. Make the required changes.
2. Click **Submit** to save the changes.

* **** (**Change Password**): Click on it change the login password.

A screenshot of a cell phone

Description automatically generated

Figure 11: Change Password

1. **Old Password**: Enter the existing password. Click  to see the password characters being entered. Click on it again to hide the password characters. This works like a toggle key.
2. **New Password**: Enter a new password.
3. **Confirm Password**: Re-enter the new password to confirm the password.
4. Click **SUBMIT**.

* **** (**Enable/Disable Account**): Lawful Agency can deactivate their account or disable/enable their account.
  + Deactivating an account means deleting the login account. After the Lawful Agency’s account is deleted, he/she can raise a grievance to reactivate it when required. The grievance is sent to the CEIR administrator who reactivates the account. After reactivation, the Lawful Agency can use the same login username and password to log into the application.
  + When the account is disabled, the Lawful Agency can only view information and not add or modify information in the application. After the account is disabled, they can enable it using the same menu.

A screenshot of a cell phone

Description automatically generated

Figure 12: Manage Account

1. Select **Deactivate** or **Disable**.
2. Click **SUBMIT**.

### Dashboard

The Dashboard provides a quick display and access to the following information:

* Stolen/Recovered Requests
* Stolen / Recovered IMEI Count
* Grievances

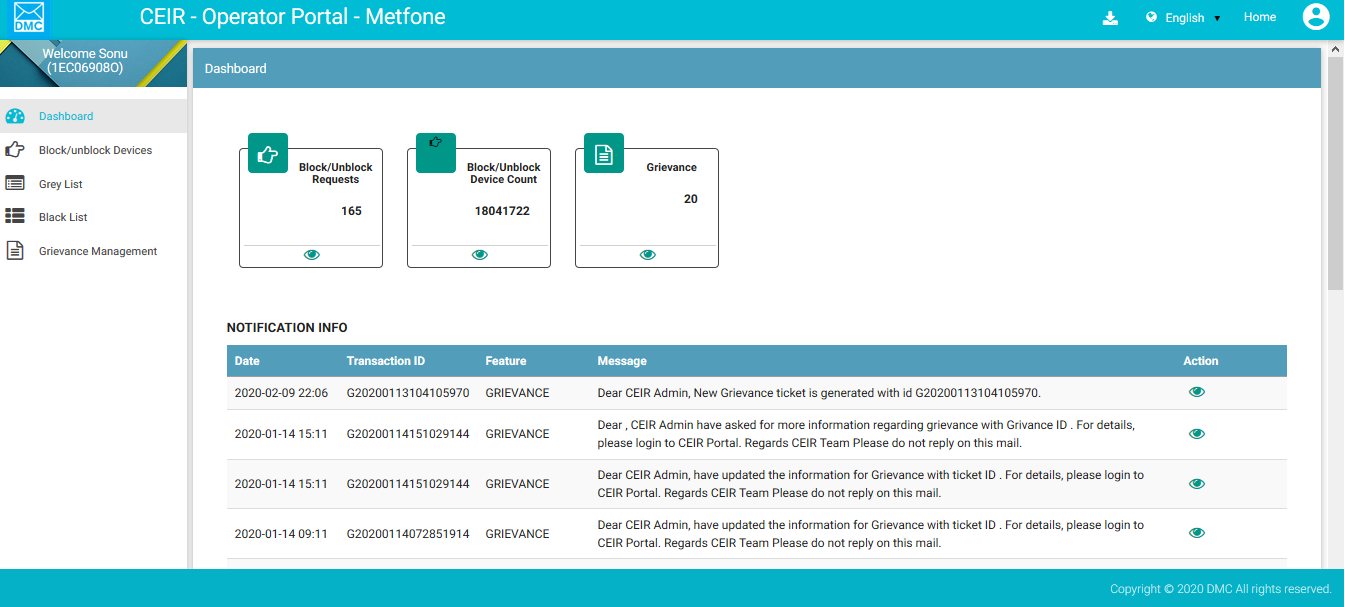


Figure 13: Home Page

**Stolen /Recovery Requests**

The box displays the total number of stolen and recovery requests.

A screenshot of a cell phone

Description automatically generated

Click  (**View**) to go to the **Stolen/Recovery Devices** dashboard. Refer to *Stolen/Recovery Devices* for more information.

**A screenshot of a computer

Description automatically generated**

Figure 14: Stolen/Recovery Devices

**Stolen/Recovery Device Count**

The box displays the total number of devices (IMEIs/MEIDs/ESNs) for which Stolen and Recovery requests have been registered.

A screenshot of a cell phone

Description automatically generated

Click  (**View**) to go to the **Stolen/Recovery Devices** dashboard. Refer to *Stolen/Recovery Devices* for more information.

**A screenshot of a computer

Description automatically generated**

Figure 15: Stolen/Recovery Devices

**Grievance**

This box displays the total number of grievances raised.

A screenshot of a cell phone

Description automatically generated

Click  (**View)** to go to the *Grievance Management* dashboard.

**A screenshot of a computer

Description automatically generated**

Figure 16: Grievance Management

**Notification Information**

This section displays the ten most recent notifications.

A screenshot of a social media post

Description automatically generated

Figure 17: Home Page

Notifications are of two types.

1. Notifications that provide only information. For example, a notification informing the Lawful Agency about the account status is an information only notification because it requires no action. The **View** icon () is disabled in such notifications.
2. Notifications that require some action by the Lawful Agency. For example, a notification about the Stolen device rejection by the CEIR administrator requires the Lawful Agency to take some action. The **View** icon () is enabled in such notifications. Click  (**View)** to access the relevant page of the notification.

The notification panel has the following columns:

* **Date**: Date of sending the notification
* **Transaction ID**: Transaction ID for which the notification is sent. If the notification is related to the Lawful Agency account, the login username is shown instead of any transaction ID.
* **Feature**: This is the name of the feature for which the notification is sent. For example, if the notification is for a grievance, the feature name **Grievance** is shown.
* **Message**: This is the message of the notification. An example is shown below.
* **Action**: This shows the **View** icon. It is activated  if the Lawful Agency can click on it else it is disabled .

## Stolen/Recovery Devices

Lawful Agency reports stolen devices (IMEI/MEID/ESN) when there the same is reported to lawful agency by end user. Lawful Agency validates that the user is the valid owner of the device. Once the Lawful Agency is satisfied, then the Lawful Agency can report devices as stolen in the CEIR system.

Whenever a device is reported as stolen, the IMEI/MEID/ESN of the device is kept in a grey-list. This is done for a given duration after which the device IMEI/MEID/ESN is moved to the blacklist. Moving the information to the blacklist indicates permanent blocking.

### Individual Device Stolen

To report stolen of a individual device:

1. Select **Stolen/Recovery Devices** in the left panel of the Home page.

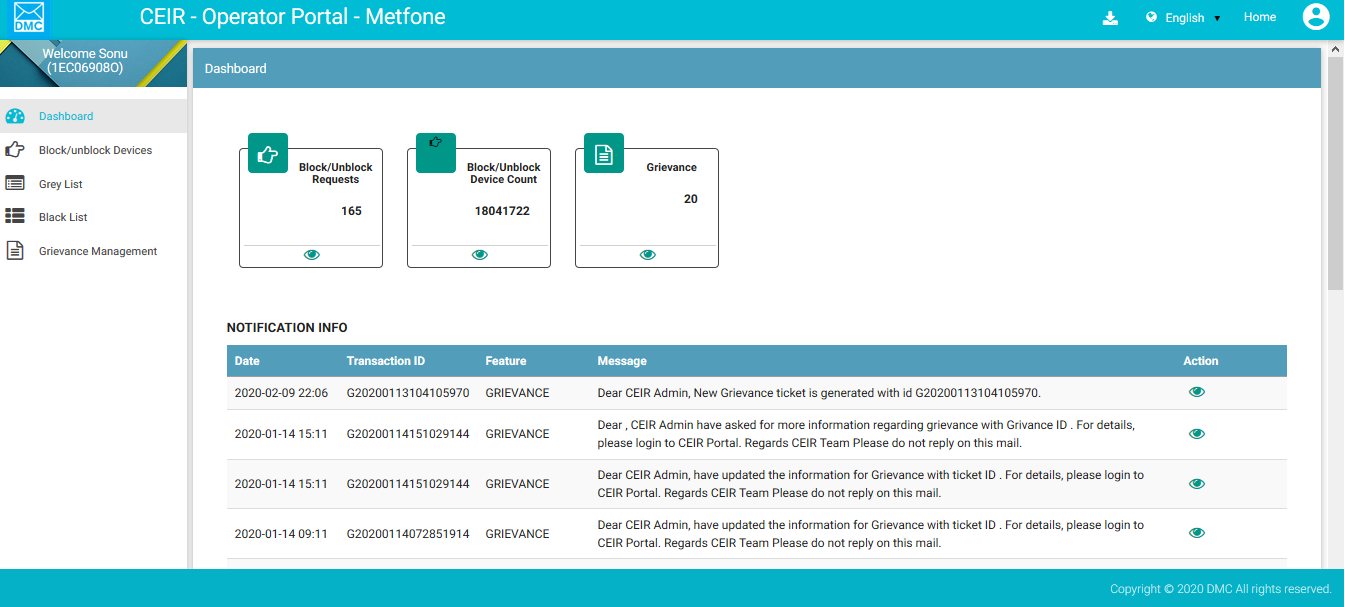


Figure 18: Home Page

The **Stolen/Recovery Devices** dashboard appears.

A screenshot of a computer

Description automatically generated

Figure 19: Stolen/Recovery Devices

1. Click **Report Stolen/Recovery** (seen on the top right corner of the menu bar).



1. Select **Stolen** as per the action to be taken.

A screenshot of a cell phone

Description automatically generated

Figure 20: Report Stolen

The screen has two sections: **Individual** and **Company/Organization/Company**.

By default, the **Individual** section appears.

1. Enter the following information:

* **\*First Name**: Enter the first name.
* **Middle Name**: Enter the middle name (if any).
* **\*Last Name**: Enter the last name.
* **\*National ID/Passport Number:** Enter the national ID of Lawful Agency personnel.
* **\*Upload National ID/Passport Image**: Upload the image of the original national ID / Passport of Device owner. This can be a pdf or image (.jpeg) of size not more than 5 MB.
* **Email**: Enter the mail ID of user. This mail ID would be used for communication with the user.
* **\*Contact Number**: Enter the mobile number of user.
* **Address**: Enter the User’s address:
  + Property Location
  + Street Number
  + Village
  + Locality
  + District
  + Commune
  + Province
  + Country
  + Postal Code
* **\*Device Brand Name:** Select the brand of the device
* **Type**: Select the type of device.
* **Device ID Type**: Select the device ID type:
  + IMEI
  + MEID
  + ESN
* **Model Name:** Select the model of the device.
* **Multiple SIM Status**: Select whether the device supports multiple SIM slots.
  + Yes
  + No
* **Contact Number:** Enter the mobile number in the device when it was stolen
* **Operator**: Select the operator.
* **\*Remarks**: Enter details about device being Stolen.
* **\*Complaint Type**: Select the reason for the device to be stolen:
  + Lost
  + Stolen
* **Blocking Type**: Select the Blocking mode. This is applicable only to Blocking:
  + Immediate: The device is instantly blacklisted.
  + Default: The device is sent to the blacklist after a given duration. The duration is configurable by the CEIR administrator.
  + Later: The device is sent to the blacklist at the specified date. Select the date using the calendar A picture containing clock, door, drawing

    Description automatically generated.
* **IMEI/MEID/ESN**: Enter the value of the IMEIs or MEIDs or ESNs of the device which are to be marked as Stolen
* **\*Place of Stolen:**
  + Property Location
  + Street Number
  + Village
  + Locality
  + District
  + Commune
  + Province
  + Country
  + Postal Code
* \*Device Stolen Date: Select the date from the calender
* Upload FIR: Upload the copy of FIR Report
* Remark: Enter the Remarks

1. Click **Submit**.

A unique transaction ID is generated, and the Blocking request is processed internally. The request can be seen on top of the dashboard.

A screenshot of a social media post

Description automatically generated

For each request, the dashboard displays the following information:

| **Column** | **Description** |
| --- | --- |
| Date | Date of registering the request to be marked as Stolen |
| Transaction ID | Transaction ID assigned to the request. |
| Block Type | Blocking Type: Immediate, Default or Later |
| Request Type | The request type can be Stolen or Recovery depending on the action taken. |
| Mode | This indicates whether the transaction is for a individual device (Individual) or for bulk devices (Company). |
| Status | * The request goes through the following status modes:   + New: When a request is raised, the status is New.   + Processing: The request is verified internally.   + Rejected by System: If the request has an error, an error file is generated. The error file can be downloaded. The error could be in the file format, size or request specifications.   + Pending Approval from CEIR Admin: If the request is successfully verified by the system, the request is shared with the CEIR administrator for review.   + Rejected by CEIR Admin: The CEIR administrator reviews the details and rejects the request if there is a problem. The Lawful Agency can view the error file and fix the errors in the request.   + Approved by CEIR Admin: When the CEIR administrator approves the request, the status changes to Approved by CEIR Admin.   + Withdrawn by CEIR Admin: When the CEIR administrator withdraws the request, the status changes to Withdrawn by CEIR Admin. This could be done when the Lawful Agency has wrongly marked a device as stolen, which has been rightly claimed by another user. * Withdrawn by User: The Lawful Agency can withdraw the request when the status is New or Rejected by System. |
| Quantity | If the request is for a bulk device request, this refers to the number of IMEIs/MEIDs/ESNs in the **.csv** file else it refers to the IMEIs/MEIDs/ESNs in the individual device being marked as Stolen. |
| Action | This displays different actions that can be performed on the request.   * Error : This is seen when there is an error file generated because of invalid information in the request. Click on the icon to download the error file. * Download A circuit board    Description automatically generated: This is used to take a dump of the request that is uploaded to the system. This is enabled only for bulk requests. Click on it download the file. * View : This is used to view the request. Click on it view the request details. * Edit A close up of a logo    Description automatically generated: This is used to modify the request. This is allowed when the status is New or Rejected by System or Rejected by CEIR Admin. Click on it to modify the request details. * Delete : This is used to delete the request. This is allowed only when the request status is New or Rejected by System. Click on it to delete the request. |

### Company Device Stolen

This feature is used in cases when there is a theft in the warehouse/shop of any stakeholder like distributor, retailer, importer etc and want those reports to be marked as stolen.

To report stolen of devices in company scenario:

1. Select **Stolen/Recovery Devices** in the left panel of the Home page.

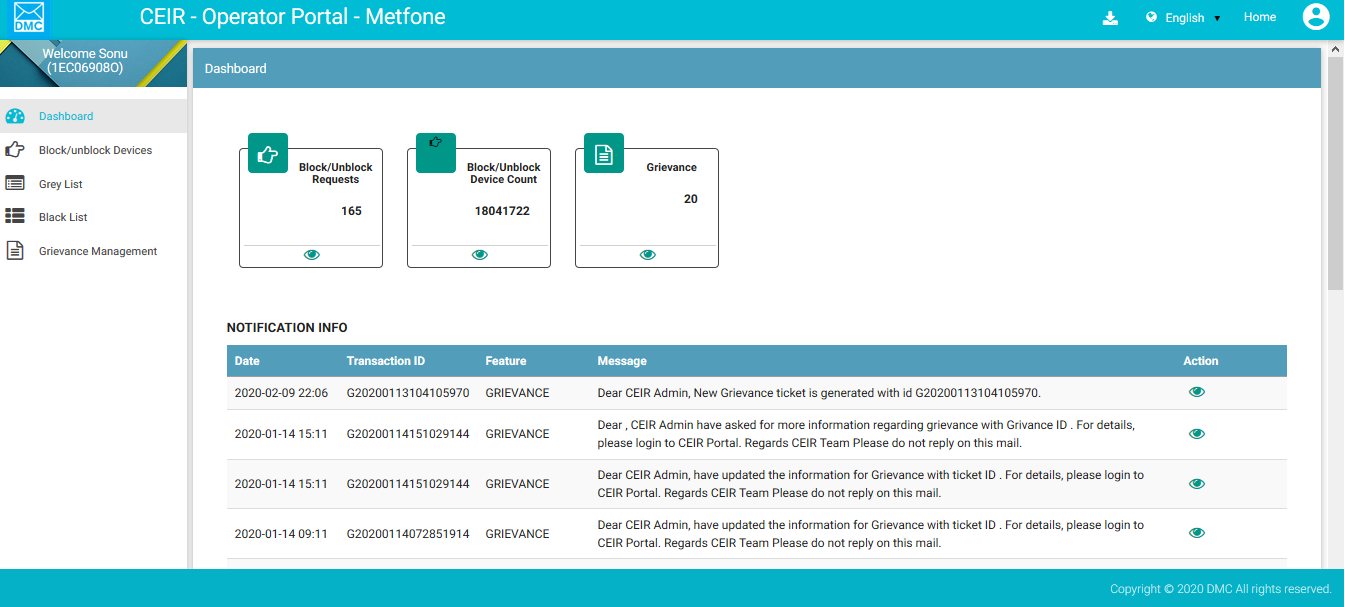


Figure 18: Home Page

The **Stolen/Recovery Devices** dashboard appears.

A screenshot of a computer

Description automatically generated

Figure 19: Stolen/Recovery Devices

1. Click **Report Stolen/Recovery** (seen on the top right corner of the menu bar).



1. Select **Stolen** as per the action to be taken.

A screenshot of a cell phone

Description automatically generated

Figure 20: Report Stolen

The screen has two sections: **Individual** and **Company/Organization/Company**.

By default, the **Individual** section appears. Select **Company/Organization/Company**

1. Enter the following information:

* **\*First Name**: Enter the first name.
* **Middle Name**: Enter the middle name (if any).
* **\*Last Name**: Enter the last name.
* **Email**: Enter the mail ID of user. This mail ID would be used for communication with the user.
* **\*Contact Number**: Enter the mobile number of user.
* **\* Company Name**: Name of the Company
* **Address**: Enter the User’s address:
  + Property Location
  + Street Number
  + Village
  + Locality
  + District
  + Commune
  + Province
  + Country
  + Postal Code.
* **\*Remarks**: Enter details about device being Stolen.
* **\*Complaint Type**: Select the reason for the device to be stolen:
  + Lost
  + Stolen
* **Upload Device List**: Select the file to be uploaded.
* **\*Quantity**: Enter the quantity of IMEI/ESN/MEID in the file
* **Blocking Type**: Select the Blocking mode. This is applicable only to Blocking:
  + Immediate: The device is instantly blacklisted.
  + Default: The device is sent to the blacklist after a given duration. The duration is configurable by the CEIR administrator.
  + Later: The device is sent to the blacklist at the specified date. Select the date using the calendar A picture containing clock, door, drawing

    Description automatically generated.
* **\*Place of Stolen:**
  + Property Location
  + Street Number
  + Village
  + Locality
  + District
  + Commune
  + Province
  + Country
  + Postal Code
* \*Device Stolen Date: Select the date from the calender
* Upload FIR: Upload the copy of FIR Report
* Remark: Enter the Remarks
* **\*** Click **Download Sample Format** to save the format of the **.csv** file in which to enter the details of the devices to be marked as Stolen or Recovery.

A screenshot of a social media post

Description automatically generated

1. Enter the details under each column for each device to be mark as Stolen. The file size should not exceed 2 MB. The file name should not exceed 30 characters.

The file has the following columns:

* + **Device type**: The device can be a handheld phone, mobile phone, feature phone, smart phone, Vehicle, Portable (include PDA), Module, Dongle, WLAN router, modem, connected computer, tablet, e- Book.
  + **\*Device ID type**: Type can be IMEI or ESN or MEID.
  + **Multiple SIM Status**: Whether the device supports multiple SIM slots (Y/N).
  + **S/N of Device**: Device serial number
  + **\*IMEI/ESN/MEID**: Value of IMEI or ESN or MEID
  + **Device launch date**: Launch date or manufacturing date of the device (in the format, DDMMYYYY).
  + **Device status**: Whether the device is new or used (New/Used)

A screenshot of a computer

Description automatically generated

1. Save the file.
2. Click **File** to upload the saved file to the system.
3. Click **Submit**.

A unique transaction ID is generated, and the Stolen request is processed internally. The request can be seen on top of the dashboard.

The request is saved, and a unique transaction ID is generated and assigned to the request. This transaction ID is used to track and identify the request.

The request appears on top of the dashboard.

For each request, the dashboard displays information in a table as shown in *Individual Device Blocking*.

### Individual Device Recovery

To recover a single device, Lawful Agency are required to enter the device information in a **.csv** file and upload it to the system. The format of the file and a sample are shown later in this section.

To Stolen or Recovery multiple devices:

1. Select **Stolen/Recovery Devices** in the left panel of the Home page.

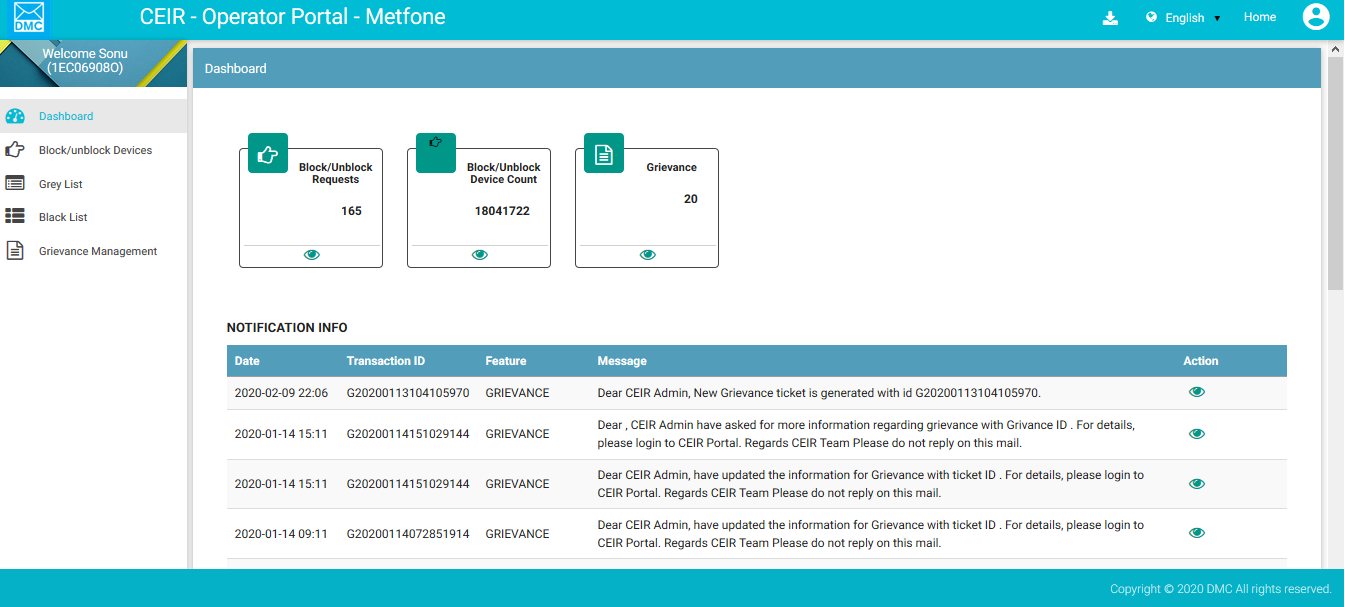


Figure 21: Report Stolen

The **Stolen/Recovery Devices** dashboard appears.

A screenshot of a computer

Description automatically generated

Figure 22: Stolen/Recovery Devices

1. Click **Report Stolen/Recovery**.



1. Select **Stolen** or **Recovery**.
2. On selecting **Stolen**, the **Report Stolen** page appears. Select **Bulk**.

A screenshot of a social media post

Description automatically generated

Figure 23: Report Stolen

1. Enter the following information:

* **\*Device Brand Name:** Select the brand of the device
* **Device Type**: Select the type of device.
* **Device ID Type**: Select the device ID type:
  + IMEI
  + MEID
  + ESN
* **Model Name:** Select the model of the device.
* **Device Serial Number:** Serial Number of the device
* **Multiple SIM Status**: Select whether the device supports multiple SIM slots.
  + Yes
  + No
* **IMEI/MEID/ESN**: Enter the value of the IMEIs or MEIDs or ESNs of the device which are to be marked as recovered
* **\*Place of Recovery:**
  + Property Location
  + Street Number
  + Village
  + Locality
  + District
  + Commune
  + Province
  + Country
  + Postal Code
* \*Device Recovery Date: Select the date from the calendar
* Remark: Enter the Remarks

1. Click **Submit**.

The request is saved, and a unique transaction ID is generated and assigned to the request. This transaction ID is used to track and identify the request.

The request appears on top of the dashboard.

For each request, the dashboard displays information in a table as shown in *Individual Device Blocking*.

### Bulk Device Recovery

This feature is applicable for scenarios where the stakeholder of CEIR system like retailer has lost all their stock from warehouse due to theft. In this case, this feature can be used.

To recover bulk device:

1. Select **Stolen/Recovery Devices** in the left panel of the Home page.

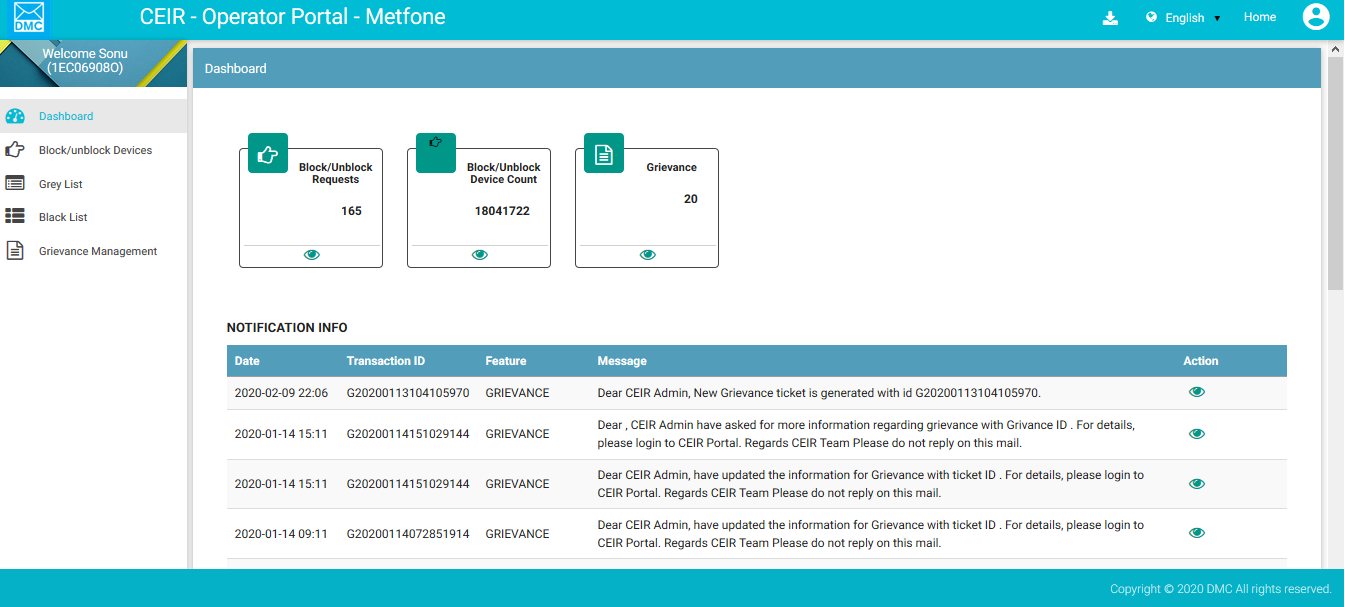


Figure 21: Report Recovery

The **Stolen/Recovery Devices** dashboard appears.

A screenshot of a computer

Description automatically generated

Figure 22: Stolen/Recovery Devices

1. Click **Report Stolen/Recovery**.



1. Select **Recovery**.
2. On selecting **Recovery**, the **Report Recovery** page appears. Select **Company/Individual/Organization**.

A screenshot of a social media post

Description automatically generated

Figure 23: Report Recovery

1. Enter the following information:

* **Upload Device List**: Select the file to be uploaded.
* **\*Quantity**: Enter the quantity of IMEI/ESN/MEID in the file
* **\*Place of Recovery:**
  + Property Location
  + Street Number
  + Village
  + Locality
  + District
  + Commune
  + Province
  + Country
  + Postal Code
* \*Device Recovery Date: Select the date from the calendar
* Remark: Enter the Remarks

1. Click **Submit**.

The request is saved, and a unique transaction ID is generated and assigned to the request. This transaction ID is used to track and identify the request.

The request appears on top of the dashboard.

For each request, the dashboard displays information in a table as shown in *Individual Device Blocking*

For file format, refer to information as shown in *Bulk Device Blocking.*

## Edit Stolen/Recovery Device Requests

Lawful Agency can change the Stolen/Recovery request details registered in the system. This can be done only when the request status is New or Rejected by System.

To modify request details:

1. Click **Edit (**A close up of a logo

   Description automatically generated**)**  against the request to be modified.

A screenshot of a cell phone

Description automatically generated

Figure 24: Stolen/Recovery Devices

The **Edit** page appears. The edit page would appear as per the applicable flow. There are 4 flows:

1. Single Device Stolen Flow
2. Bulk Device Stolen Flow
3. Single Device Recovery Flow
4. Bulk Device Recovery Flow

A screenshot of a cell phone

Description automatically generated

Figure 25: Edit Stolen Device (Individual Device)

The **Edit** page is different for bulk devices (Stolen and Recovery).

A screenshot of a cell phone

Description automatically generated

Figure 26: Edit Stolen Device (Bulk Device)

The **Edit** page is different for single devices (Recovery).

A screenshot of a cell phone

Description automatically generated

Figure 25: Edit Recovery Device (Individual Device)

The **Edit** page is different for bulk devices (Recovery).

A screenshot of a cell phone

Description automatically generated

**Figure 25: Edit Recovery Device (Bulk Device)**

1. Make the required changes
2. Click **UPDATE**.

The status of the request changes to **New** and is submitted for reprocessing.

## Filter Stolen/Recovery Device Requests

Lawful Agency can view selective Stolen/Recovery device requests after specifying the required filters. For example, Lawful Agency can view requests that are pending approval from the CEIR administrator.

To filter Stolen/Recovery device requests:

A screenshot of a cell phone

Description automatically generated

Figure 27: Stolen/Recovery Devices

1. Enter data in one or more of the listed fields:

* **Start** **Date** and **End** **Date**: This refers to the registering Stolen/Recovery device requests in the system.
* **Transaction ID**: Each request is assigned a unique transaction ID. Lawful Agency can view a specific request by entering its transaction ID.
* **Request Type**: This refers to the type of request: Stolen or Recovery.
* **Status**: This refer to various state of the stolen/recovery request in bulk/single cases
* **Mode**: This refers to whether the request is for a individual device or bulk devices: Individual or Bulk.

1. Click **FILTER**.

The requests that match the filter values are shown in the dashboard.

A screenshot of a cell phone

Description automatically generated

Figure 28: Filtered Device Stolen/Recovery Requests

## Export Stolen/Recovery Device Requests

Lawful Agency can download all the uploaded requests in a **.csv** file. This is done using an export utility.

To export the uploaded requests:

1. On the **Stolen/Recovery Devices** page, click **Export**.

A screenshot of a cell phone

Description automatically generated

Figure 29: Stolen/Recovery Devices

The following page appears.

A screenshot of a cell phone

Description automatically generated

Figure 30: Open or Save Exported Stolen/Recovery Devices File

1. Click **Open with** to view the **.csv** as an Excel file.

A screenshot of a computer

Description automatically generated

Figure 31: Exported Stolen/Recovery Devices

Filtered data can also be exported. To do this, filter specific data by defining filter values. Refer to *Filter Stolen/Recovery Device Requests* for information and then use the export feature to export the filtered data.

## Grievance Management

Lawful Agency can register complaints or grievances when there is a problem in the portal. For example, there could be situations when the Blocking/Recovery, grey list, or black list features are not functional.

When an Lawful Agency raises a grievance, the grievance goes through the following stages:

1. A notification is sent to the CEIR administrator. The notification appears on the CEIR administrator portal. A mail is also sent to the registered mail of the CEIR administrator.
2. The CEIR administrator responds to the grievance. A response notification is sent to the Lawful Agency portal, and the Lawful Agency’s registered mail ID.
3. Steps 1 to 2 are repeated until the grievance is closed. The administrator closes the grievance.

There are situations when the grievance is automatically closed. A grievance is automatically closed when the status of the grievance changes to **Pending with User**, but there is no response from the Lawful Agency for a specified period.

To raise a grievance

1. Select **Grievance Management** in the left panel.

A screenshot of a social media post

Description automatically generated

Figure 46: Home Page

1. The **Grievance Management** page appears. Click **Report Grievance**.

A screenshot of a computer

Description automatically generated

Figure 47: Grievance Management

The **Report Grievance** page appears.

A screenshot of a cell phone

Description automatically generated

Figure 48: Report Grievance

1. Enter the following information:
   1. **Transaction ID**: Enter the transaction ID of the Stolen/Recovery request if the grievance is related to Blocking/Recovery or the ID of the grey ID list if related to the grey list or the ID of the blacklist if related to blacklist.
   2. **\*Category**: Select the category of the grievance. The options are:

* Stolen/Recovery Related
* Other
  1. **Document Type:** Select the type of identification or another document that is to be uploaded.
  2. **Upload Supporting Document:** Click **Select File** to upload the document selected in **Document Type**.
  3. To upload more documents,click **+Add More Files.**

This adds two more fields: **Document Type** and **Select File**.

* 1. **\*Remarks:** Enter information about the grievance raised. This helps the administrator to understand the problem in detail.

1. Click **SUBMIT**.

A grievance ID is generated and assigned to the registered grievance. The registered grievance appears on top of the dashboard.

A screenshot of a social media post

Description automatically generated

The new grievance appears on the top of the page.

A screenshot of a social media post

Description automatically generated

Figure 49: Grievance Management

For each grievance added, the following information is displayed on the page.

| **Column** | **Description** |
| --- | --- |
| Raised Date | Date of raising a grievance. |
| Last Update Date | The date when the grievance was modified. |
| Transaction ID | The transaction ID of request for which a grievance was raised. |
| Grievance ID | This is the ID that is automatically assigned to the grievance. |
| Grievance Status | The uploaded grievance goes through different status modes.   * New: When a grievance is raised. * Pending with CEIR Administrator: When a response is awaited from the CEIR administrator. * Pending with User: When a response is awaited from the Lawful Agency. * Closed: When the CEIR administrator closes the grievance. |
| Action | This displays different actions that can be performed on a grievance.   * Reply : This is used to respond to the grievance. The response is given by the CEIR administrator or Lawful Agency. The exchange of responses is done until the grievance is closed. * View A close up of a logo    Description automatically generated: This is used to view the grievance response history. The importer can see all the responses exchanged for any grievance. |

## Filter Grievances

The Lawful Agency can view selective grievances depending on specific filter values. For example, the Lawful Agency can view only those grievances that are pending with the CEIR administrator. Similarly, one can view only those grievances that are closed.

To filter grievances:

A screenshot of a cell phone

Description automatically generated

Figure 50: Filter Grievances

1. Specify the required value in one or more of the fields listed:

* **Start Date** and **End Date**: Period of raising grievances.
* **Transaction ID**: This is the ID of the transaction for which the grievance is raised.
* **Grievance ID**: This is the ID assigned to the grievance.
* **Grievance Status**: The status can be:
  + New
  + Pending with CEIR Administrator
  + Pending with User
  + Closed

1. Click **Filter**.

The filtered grievances are shown on the page.

A screenshot of a social media post

Description automatically generated

Figure 51: Filtered Grievances

## Export Grievances

All the uploaded grievances can be downloaded in a **.csv** file. This is done using an export utility.

To export the grievances:

1. Click **Export** (seen on the top right corner of the **Grievance Management** page).

A screenshot of a cell phone

Description automatically generated

Figure 52: Grievance Management

The following page appears.

A screenshot of a cell phone

Description automatically generated

Figure 53: Open or Save Exported Grievance File

1. Click **Open with** to view the file.

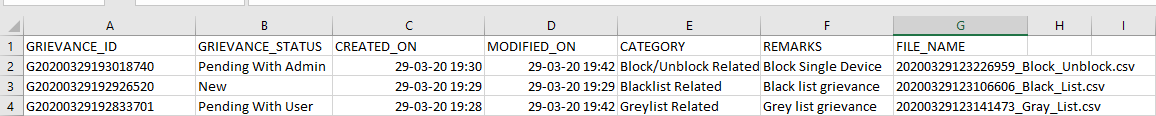


Figure 54: Exported Grievances

Instead of exporting all the grievances, Lawful Agency can export filtered grievances. First, filter the grievance data based on specific filters (refer to *Filter Grievances*) and then export the filtered grievances using the export utility.