Central Equipment Identity Register Portal

Lawful Agency User Manual v 2.0

Document Change History

Version	Change Type	Description	Date
Draft		Submitted for internal review	June 2020

Copyright @ 2020 DMC All Rights Reserved

Contents

Copyright @ 2020 DMC All Rights Reserved

Figures

Copyright @ 2020 DMC All Rights Reserved

1 Overview

1.1 Scope

The objective of this manual is to help lawful agency personnel report stolen and recovered devices (IMEIs) and report grievances.

1.2 Acronyms & Abbreviations

Acronym	Full Form
CEIR	Central Equipment Identity Register
EIR	Equipment Identity Register
IMEI	International Mobile Equipment Identity
PDA	Personal Digital Assistant
TAC	Type Allocation Code
TRC	Telecom Regulator of Cambodia

1.3 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

Copyright @ 2020 DMC All Rights Reserved

2 Operations

2.1 Application Overview

The CEIR Lawful Agency Portal application enables agency personnel to report devices (IMEIs) that are stolen and report devices (IMEIs) that are recovered. This includes devices owned by individuals, companies, organizations, and government.

Lawful agency personnel can use the application to perform the following tasks:

- Report stolen devices (IMEIs)
- Report recovered devices (IMEIs)
- Report grievances

2.2 Logging into the Application

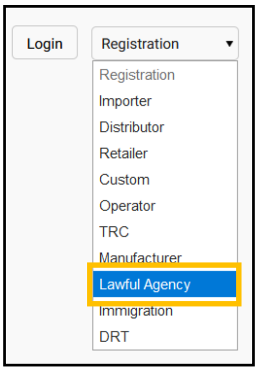
Before login, personnel need to register in the application.

To register:

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

Figure 1: DMC Home Page

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



Copyright @ 2020 DMC All Rights Reserved

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

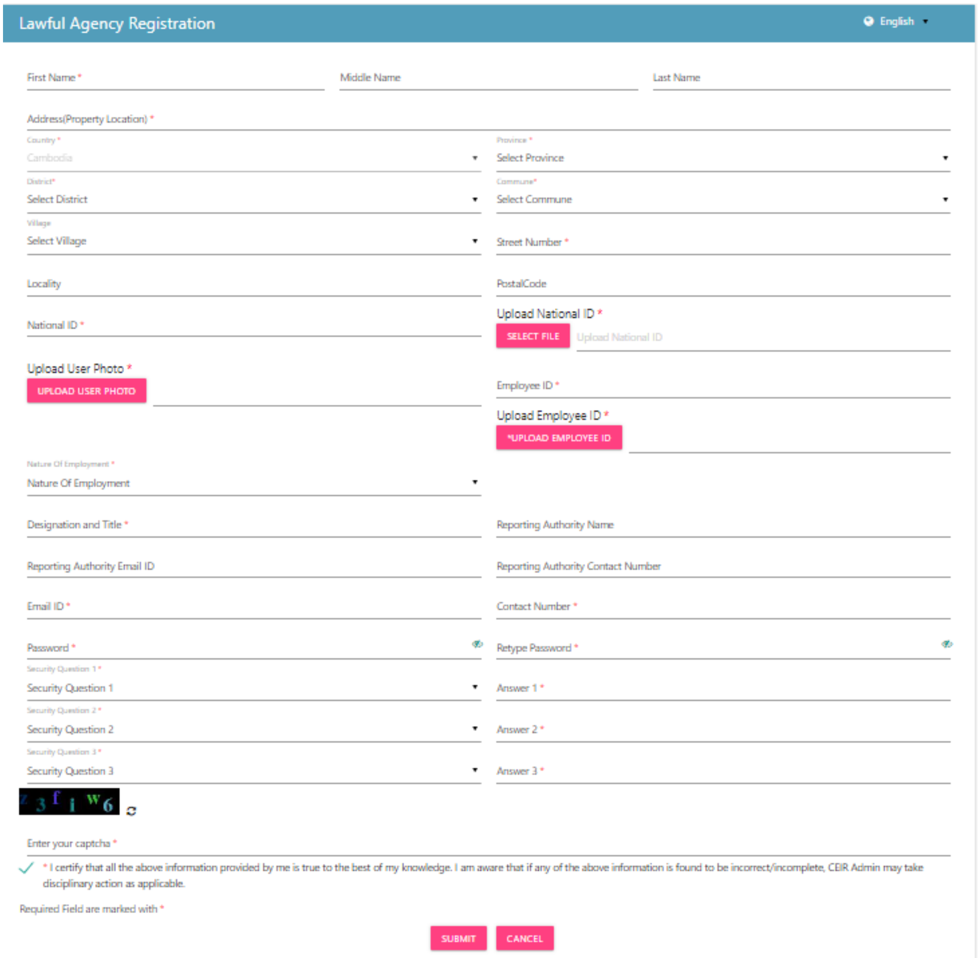


Figure 2: Lawful Agency Registration

3. ***First Name**: Enter the first name.
4. **Middle Name**: Enter the middle name (if any).
5. ***Last Name**: Enter the last name.
6. **Address**: Enter the address:
   - *Street Number
   - Village
   - Locality

Copyright @ 2020 DMC All Rights Reserved

- *District
- *Commune
- Postal Code
- *Country
- *Province

7. ***National ID:** Enter the national ID of the agency personnel.
8. ***Upload National ID**: Upload the image of the original national ID of the personnel. This can be a pdf or image (.jpeg) of size not more than 2 MB.
9. ***Upload Photo**: Upload the photograph of the personnel. The photograph can be a pdf or image (.jpeg) of size not more than 2 MB.
10. ***Employee ID**: Enter the employee ID.
11. ***Upload Employee ID**: Upload the image of the Employee ID card. The photograph can be a pdf or image (.jpeg) of size not more than 2 MB.
12. **Nature of Employment**: Select the type of employment of the personnel:
    - Permanent
    - Temporary
    - Contract
13. ***Designation and Title**: Enter the designation of the agency personnel.
14. **Reporting Authority Name**: Enter the name of the officer to whom the personnel reports to.
15. **Reporting Authority Email ID**: Enter the mail ID of the officer to whom the personnel reports to.
16. **Reporting Authority Contact Number**: Enter the contact number of the officer to whom the personnel reports to.
17. ***Email**: Enter the mail ID of the personnel. This mail ID would be used for communication with the agency
18. ***Contact Number**: Enter the mobile number of the personnel. The agency would receive notifications at this mobile number.
19. ***Password**: Enter a login password. This is the password that would be used to log into the Lawful Agency Portal application.

Copyright @ 2020 DMC All Rights Reserved

20. ***Retype Password**: Re-enter the password for confirmation.
21. *Select three security questions and enter an answer for each question. This is required by the system when the agency personnel forget the login password. In such a situation, the system requires some type of identification to authenticate the personnel. The security questions are used to identify and authenticate the personnel.
22. *Enter the captcha shown on the page. This is required to prove to the system that the personnel are not a robot.
23. *Select the declaration check box.
24. Click **SUBMIT**.

An OTP is sent to the personnel's mail ID and contact number.

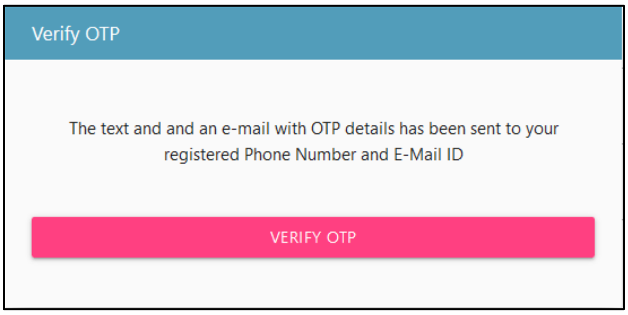


Figure 3: Verify OTP

The personnel are prompted to enter both the OTPs in the page for verification.

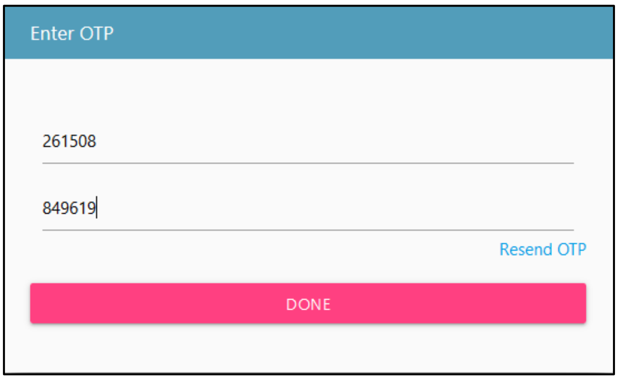
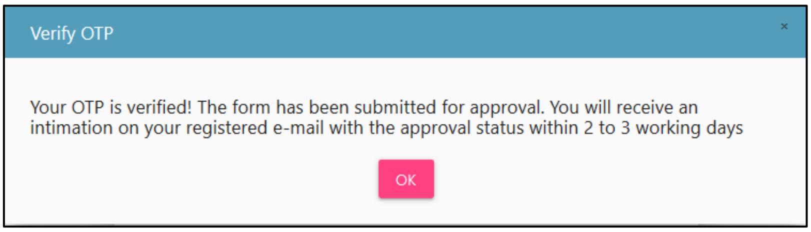


Figure 4: Enter OTP

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.

Copyright @ 2020 DMC All Rights Reserved



After the OTPs are verified successfully, the registration request is sent for approval to the CEIR Admin. The approval turnaround time is 2-3 days. After approval from the CEIR Admin, an e-mail containing a registration ID is sent to the 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.

<u>To login:</u>

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

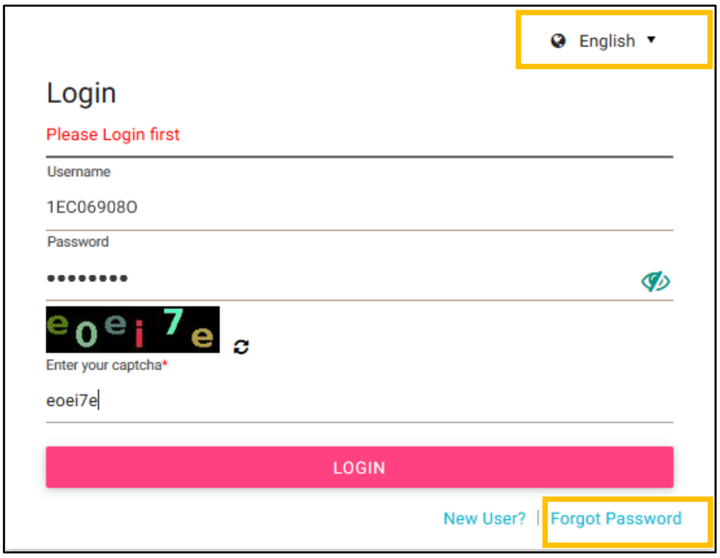
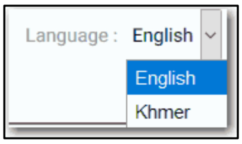


Figure 5: Login

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.



Copyright @ 2020 DMC All Rights Reserved

2. Next, enter the assigned login user ID and password.

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

3. Enter the captcha.

4. Click **LOGIN**.

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

On entering correct information, the application home page appears.

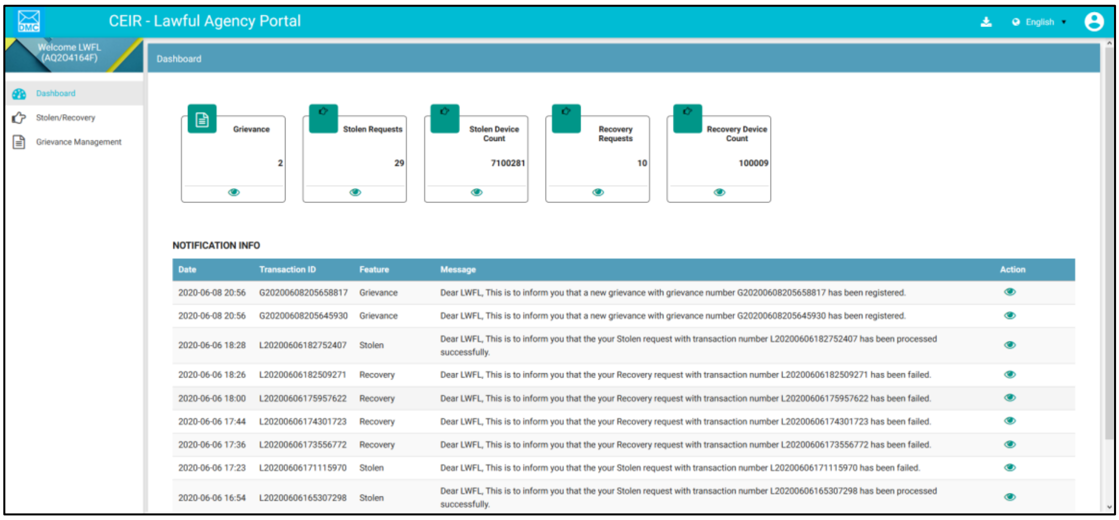
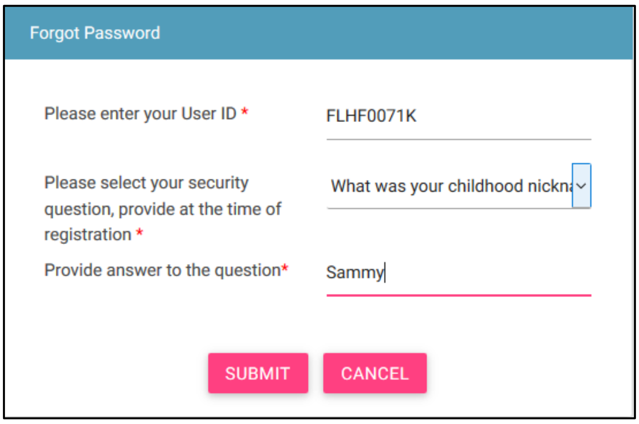


Figure 6: Home Page

If the personnel forget the assigned password, click the **Forgot Password** link on the **Login** page. The **Forgot Password** page appears.



Copyright @ 2020 DMC All Rights Reserved

Figure 7: Forgot Password

1. Enter the login user ID.
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.

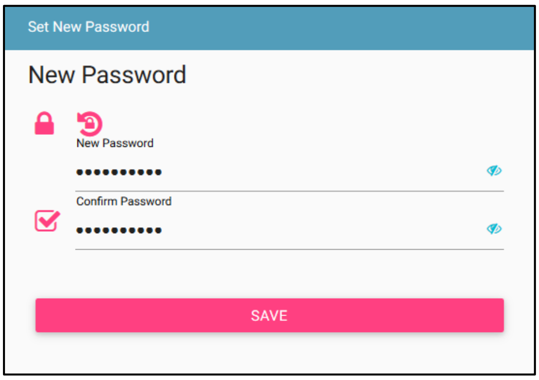


Figure 8: Set New Password

5. 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.
6. Re-enter the password.
7. Click **Save**.

Copyright @ 2020 DMC All Rights Reserved

2.3 Application User Interface

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

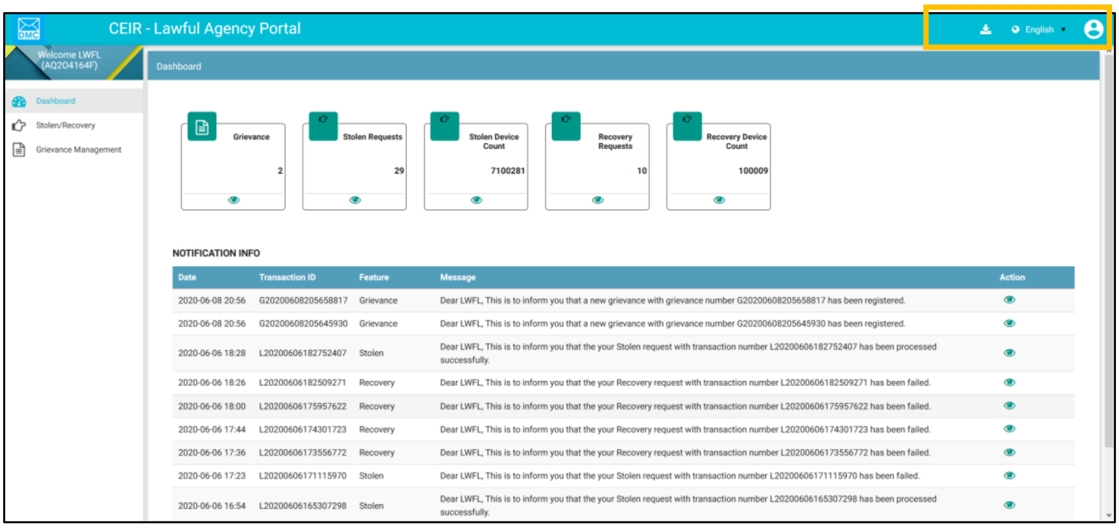


Figure 9: Home Page

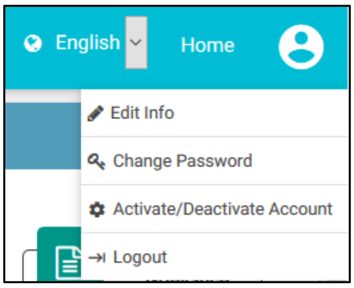
The Home page has all the feature menus on the left panel.

The center of the page is the Dashboard.

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

- **Download Manual** : 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.

- (**User profile**): Click on it to see the following menu:



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

Copyright @ 2020 DMC All Rights Reserved

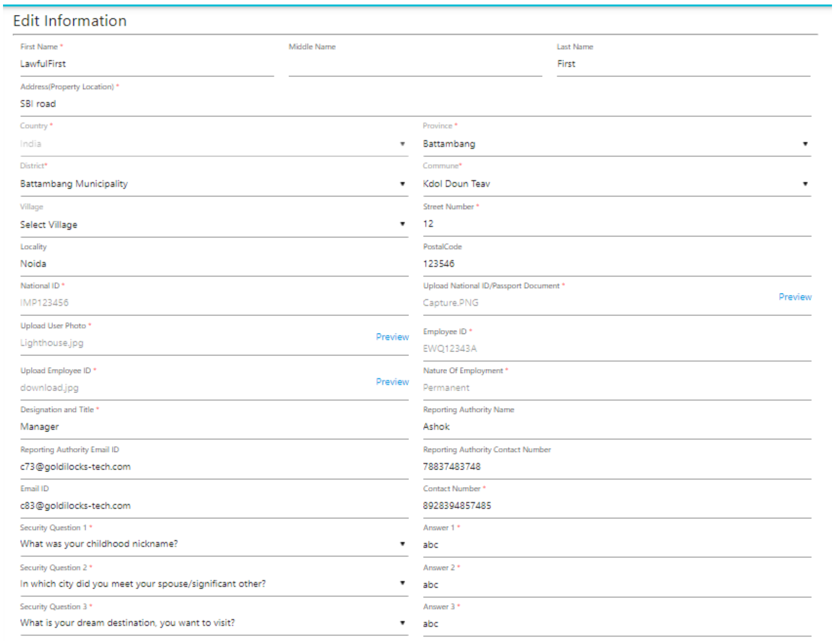


Figure 10: Edit Information

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

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

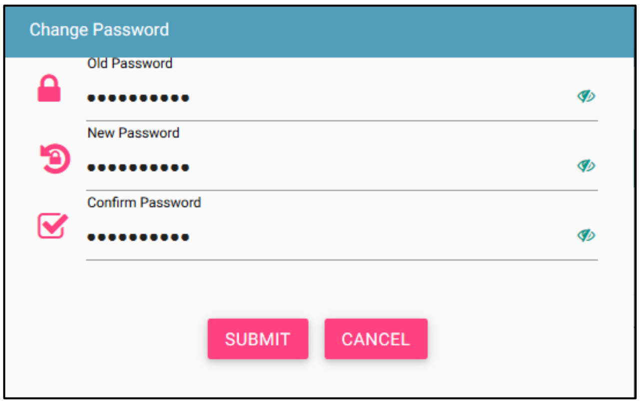


Figure 11: Change Password

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**.

Copyright @ 2020 DMC All Rights Reserved

- (**Enable/Disable Account**): Personnel can deactivate their account or disable/enable their account.
  - Deactivating an account means deleting the login account. After the account is deleted, he/she can raise a grievance to reactivate it when required. The grievance is sent to the CEIR Admin who reactivates the account. After reactivation, the personnel can use the same login username and password to log into the application.
  - When the account is disabled, the personnel 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.

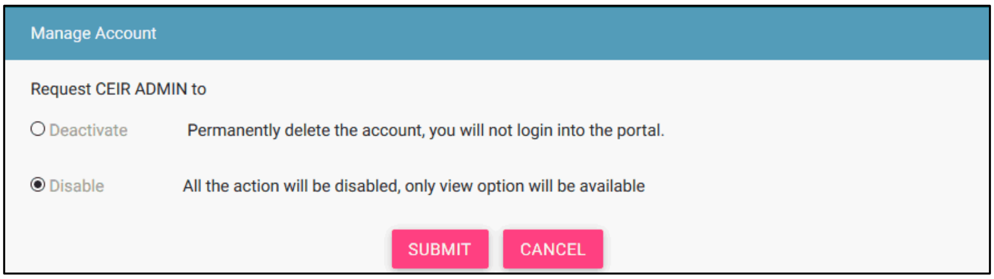


Figure 12: Manage Account

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

2.3.1 Dashboard

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

- Stolen/Recovery
- Grievance Management

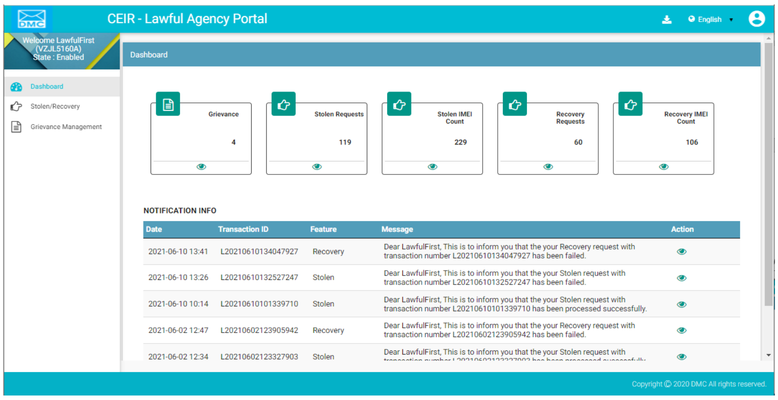
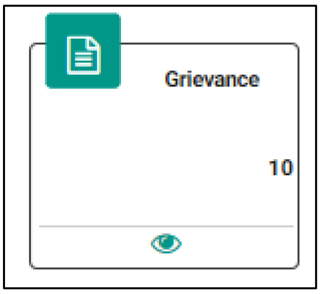


Figure 13: Home Page

Copyright @ 2020 DMC All Rights Reserved

Grievance

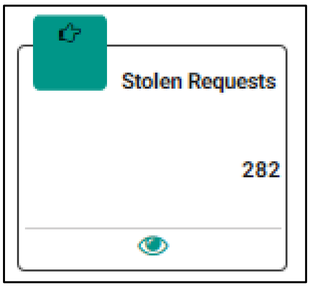
The box displays the total number of grievances registered by the personnel.



Click (**View**) to go to the **Grievance Management** dashboard. Refer to *Grievance Management* for more information.

Stolen Requests

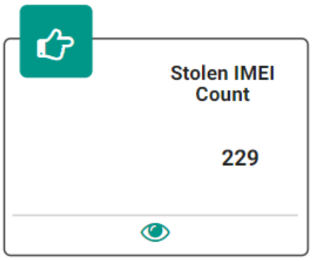
This box displays the total number of requests reported for stolen devices (IMEIs).



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

Stolen Device Count

This box displays the total number of devices (IMEIs) that have been reported as stolen.

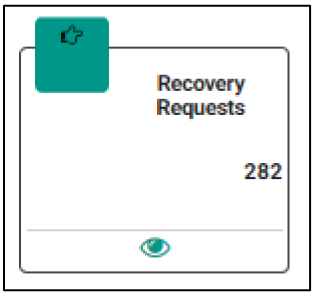


Click (**View)** to go to the *Stolen/Recovery* dashboard.

Recovery Requests

Copyright @ 2020 DMC All Rights Reserved

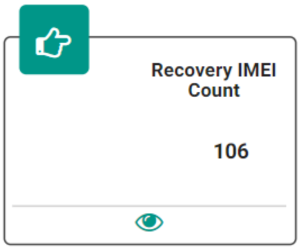
This box displays the total number of device recovery requests that have been reported by the personnel.



Click (**View)** to go to the *Stolen/Recovery* dashboard.

Recovery Device Count

This box displays the total number of devices (IMEIs) that have been recovered.



Click (**View)** to go to the *Stolen/Recovery* dashboard.

Notification Information

This section displays the most recent notifications. System Admin can configure the number of notifications that are displayed on user dashboard.

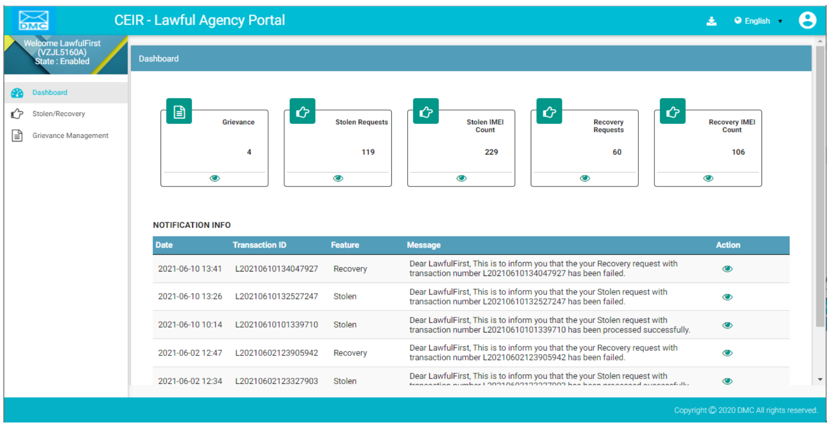


Figure 14: Home Page

Copyright @ 2020 DMC All Rights Reserved

Notifications are of two types.

1. Notifications that provide only information. For example, a notification informing the personnel 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 personnel. For example, a notification about a rejection of a stolen device request requires the personnel to take some action. The **View** icon ( ) is enabled in such notifications. Click (**View)** to access the relevant request details.

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 personnel account (activation, deactivation), 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.
- **Action**: This shows the **View** icon. It is activated if the personnel can click on it else it is disabled .

2.4 Reporting Stolen/Recovered Devices

Lawful agency personnel report devices that have been stolen and recovered. The device could belong to an individual or a company/organization/government.

2.4.1 Reporting Individual Stolen Devices

<u>To report an individual stolen device:</u>

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

Copyright @ 2020 DMC All Rights Reserved

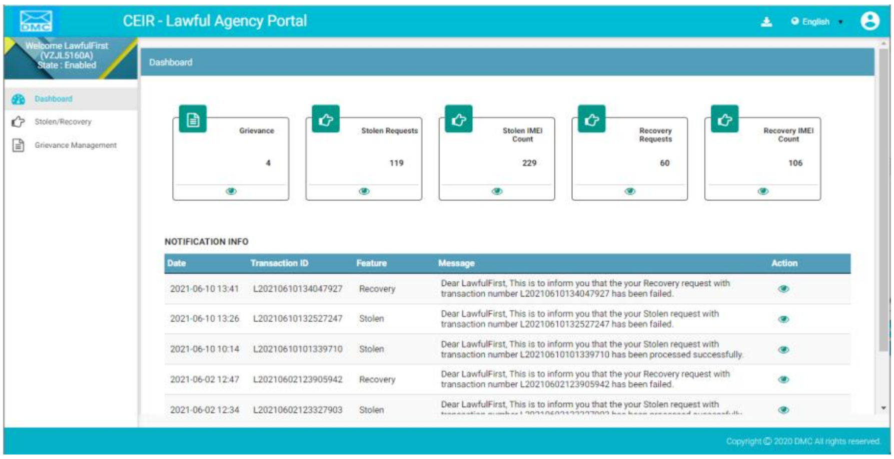


Figure 15: Home Page

The **Stolen/Recovery** dashboard appears.

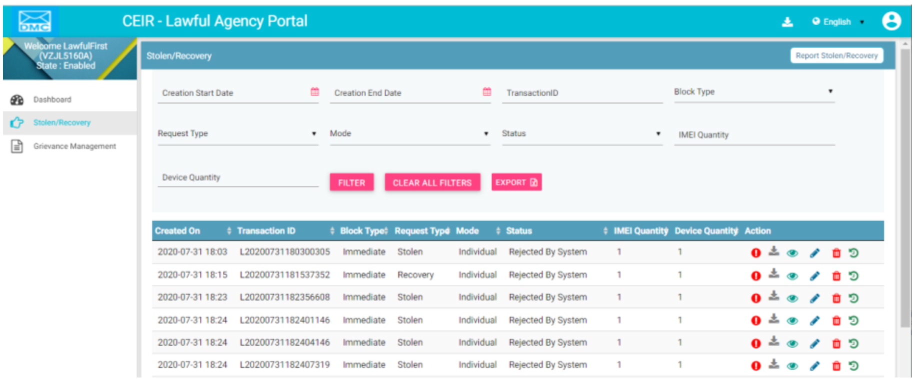
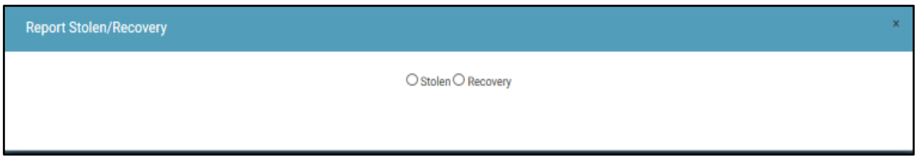


Figure 16: Stolen/Recovery

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



3. Select **Stolen**.

Copyright @ 2020 DMC All Rights Reserved

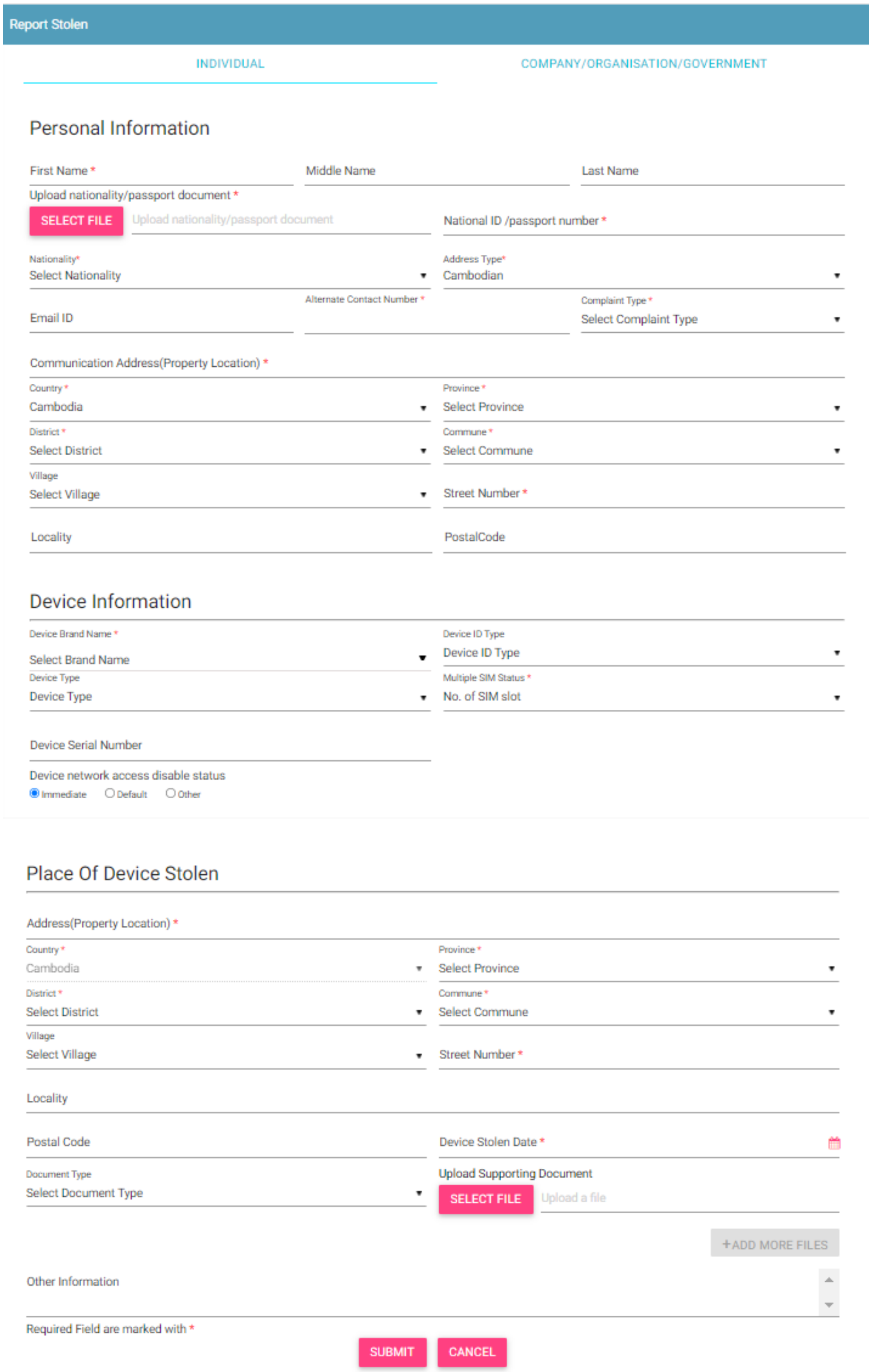


Figure 17: Report Stolen (Individual)

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

By default, the **Individual** section appears. Here, the devices that are stolen from an individual are reported.

Copyright @ 2020 DMC All Rights Reserved

4. Enter the following information:

Personal Information: Enter the personal details of the person whose stolen device is reported.

- *First Name
- Middle Name
- Last Name
- *Upload Nationality/Passport document: Click **Select** to upload an image or pdf of the document.
- *National ID/Passport Number: Enter the NID or passport number.
- *Nationality: Select Nationality
- *Address type: Specify if the address of the individual is Cambodian/International
- Email: Enter the email ID.
- *Alternate Contact Number: Enter the mobile number.
- ***Complaint Type**: Select the type of complaint (Lost, Stolen) from the list.
- *Communication Address (Property Location)
- *Street Number
- Village
- Locality
- *District
- *Commune
- Postal Code
- *Country
- *Province

Device Information: Enter details of the stolen device.

- *Device Brand Name: Select the brand of the device from the list.
- *Device ID Type: Select the type of ID to be entered for the device:
    - IMEI
- **Device Type**: Select the type of device from the list.

Copyright @ 2020 DMC All Rights Reserved

- *Multiple SIM Status**: Number of SIM slots the device supports(1-4)
- **Device Serial Number** : Serial Number of the device stolen/lost.

Place of Device Stolen: Enter the address of the place where the device was stolen or lost.

- *Address (Property Location)
- *Street Number
- Village
- Locality
- *District
- *Commune
- Postal Code
- *Country
- *Province
- *Device Stolen Date**: Click on the calendar to select the date.
- Document Type : Select the type of document to upload
- **Upload Supporting Document**: Click **Select** to upload the FIR file.
- **Other Information:** Remarks (if any)

5. Click **Submit**.

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

For each request, the dashboard displays the following information:

Column	Description
Date	Date of registering the request.
Transaction ID	Transaction ID assigned to the request.
Request Type	Type of request generated is Stolen.

Copyright @ 2020 DMC All Rights Reserved

Column	Description
Mode	Indicates whether the request is for an individual or company (Individual or Company). In this case, it is Individual.
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, policy violation or request specifications. ○ Pending Approval from CEIR Admin: If the request is successfully verified by the system, the request is shared with the CEIR Admin for review. ○ Rejected by CEIR Admin: The CEIR Admin reviews the details and rejects the request if there is a problem. The operator can view the error file and fix the errors in the request. ○ Approved by CEIR Admin: When the CEIR Admin approves the request, the status changes to Approved by CEIR Admin. ○ Withdrawn by CEIR Admin: When the CEIR Admin withdraws the request, the status changes to Withdrawn by CEIR Admin. For example, this could be done when the personnel have wrongly marked

Copyright @ 2020 DMC All Rights Reserved

Column	Description
	a device as stolen, which has been recovered. ○ Withdrawn by User: The personnel can withdraw the request only when the status is New or Rejected by System.
IMEI Quantity	Refers to the number of IMEIs reported stolen or recovered.
Device Quantity	Refers to the number of devices reported stolen or recovered. A device can have multiple IMEIs.
Action	This displays different actions that can be performed on the request. • Error : An error file is generated if there is any problem in the request(s) submitted. Click to download the error file. Refer to *Figure 18* for a sample error file. • Download : This is applicable only when the request is for company/organization/government stolen devices. This opens the input device file that is uploaded to the system. • View : This is used to view the request. Click on it view the request details. • Edit : This is used to modify the request. This is allowed only 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.

Copyright @ 2020 DMC All Rights Reserved

Column	Description
	• History : This is used to view the history of the transaction. It shows the various status modes through which the transaction has gone through.

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	DEVICETYPE	DeviceIdType	MultipleS	S/NofDev	IMEI/ESN/	Devicelau	DeviceSta	Error Cod	Error Message				
2	null	IMEI	null	null	1E+15	null	null	Error Description : IMEI does not pass the Checksum algorithm					
3													

Figure 18: Error File

2.4.2 Reporting Company/Organization/Government Stolen/Lost Devices

<u>To report a stolen device:</u>

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

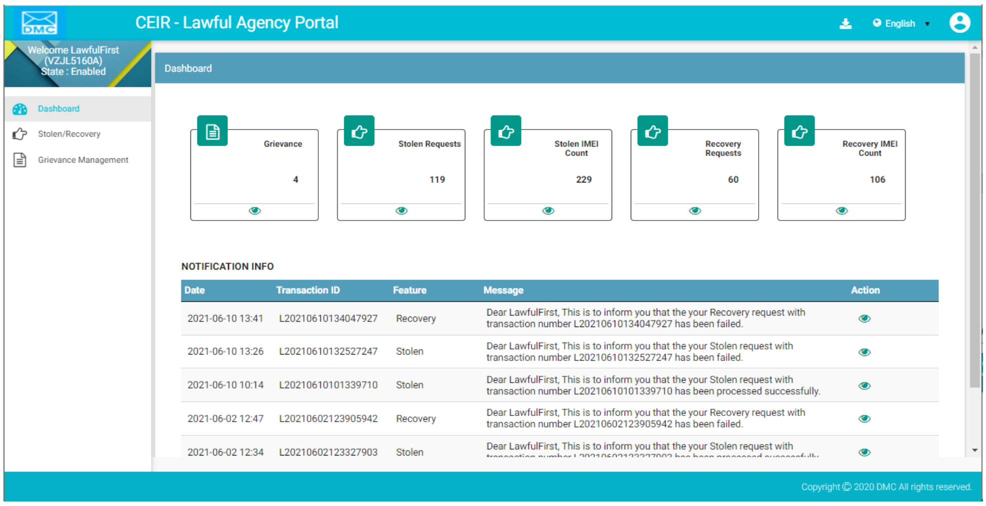


Figure 19: Home Page

The **Stolen/Recovery** dashboard appears.

Copyright @ 2020 DMC All Rights Reserved

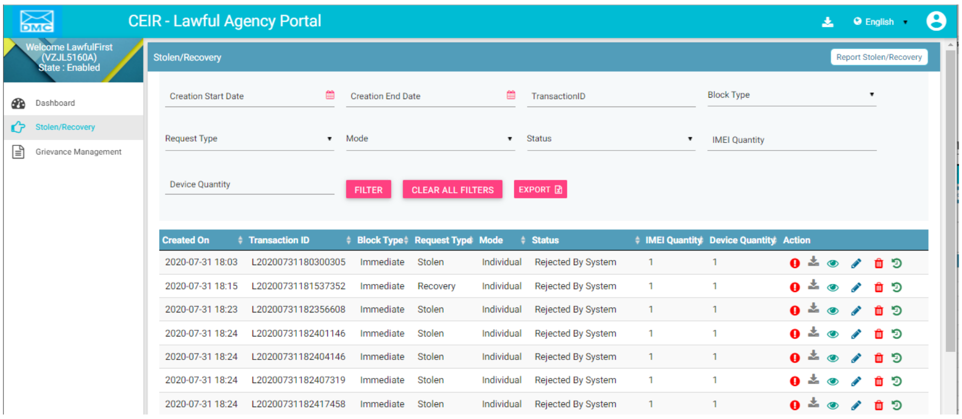
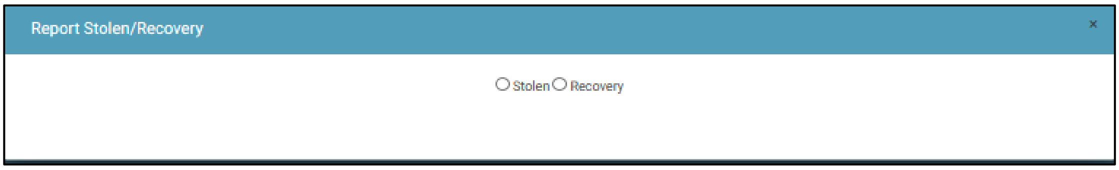


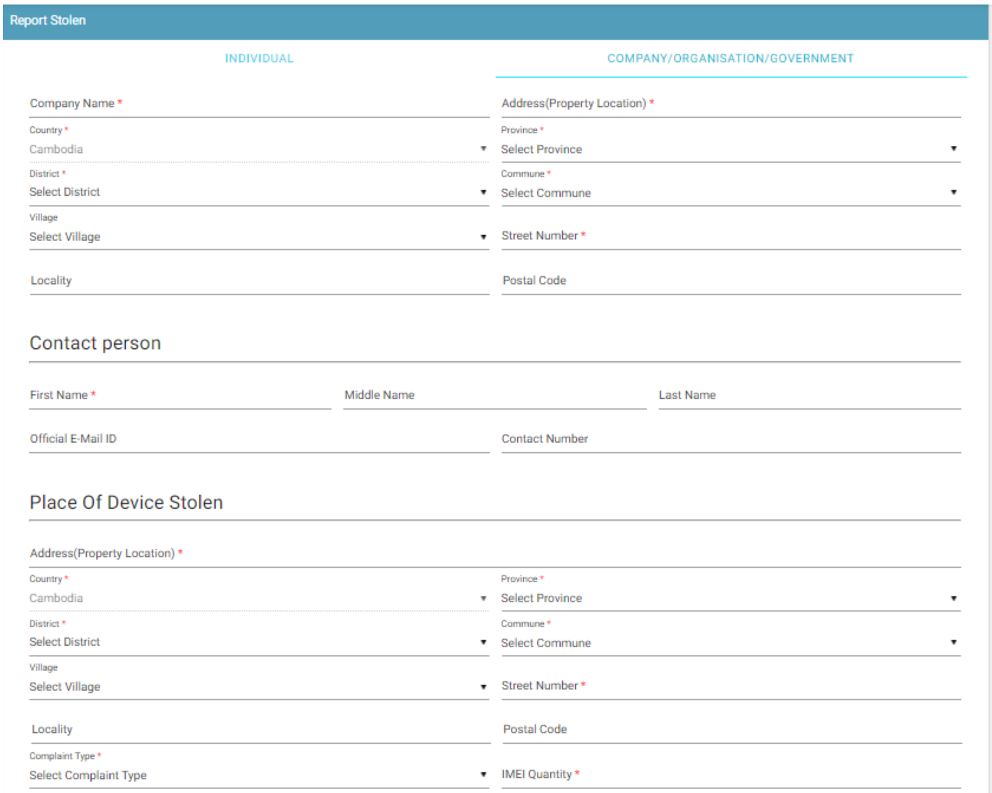
Figure 20: Stolen/Recovery

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



3. Select **Stolen**.

Select the **Company/Organization/Government** tab.



Copyright @ 2020 DMC All Rights Reserved

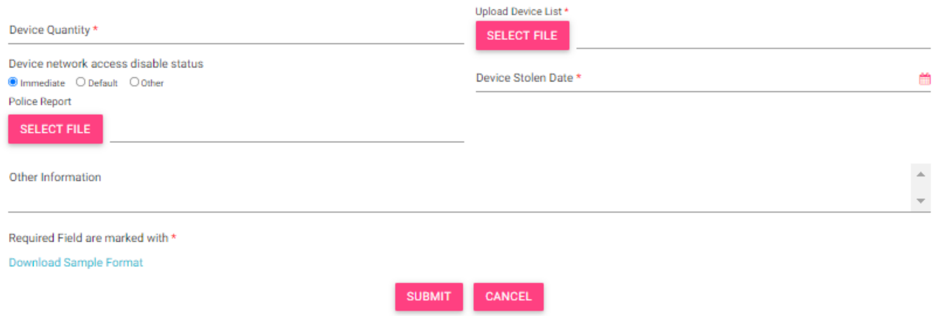


Figure 21: Report Stolen (Company/Organization/Government)

4. Enter the following information:

- ***Company Name**
- ***Address (Property Location)**
- ***Street Number**
- **Village**
- **Locality**
- ***District**
- ***Commune**
- **Postal Code**
- ***Country**
- ***Province**

Contact Person: Enter the personal details of the authorized person in the company/organization/government.

- *First Name
- Middle Name
- Last Name
- Official E-Mail ID
- Contact Number

Place of Device Stolen: Enter the address of the place where the device(s) was stolen/lost.

- *Address(Property Location)
- *Street Number

Copyright @ 2020 DMC All Rights Reserved

- Village
- Locality
- *District
- *Commune
- Postal Code
- *Country
- *Province
- ***Complaint Type**: The complaint type has two values:
    - Stolen
    - Lost
- ***IMEI Quantity**: This is the total count of the IMEIs in the stolen/lost devices.
- ***Device Quantity**: This is the total number of devices stolen/lost. A device can have multiple IMEIs.
- ***Upload Device List**: Enter the stolen/recovered device details in a **.csv** file and upload it.

	A	B	C	D	E	F	G
1	DEVICETYPE	DeviceIdType	MultipleSIMStatus	S/NofDevice	IMEI	Devicelaunchdate	DeviceStatus
2	Handheld	IMEI	4	34562	999339988776608	22-05-2020	New
3	Handheld	IMEI	4	34562	999339988776609	22-05-2020	New
4	Handheld	IMEI	1	98126	999339988776610	22-05-2020	New
5	Handheld	IMEI	4	34562	999339988776611	22-05-2020	New
6	Handheld	IMEI	1	34523	999339988776612	22-05-2020	New
7	Handheld	IMEI	4	34562	999339988776613	22-05-2020	New
8	Handheld	IMEI	1	98126	999339988776614	22-05-2020	New
9	Handheld	IMEI	1	34523	999339988776615	22-05-2020	New
10	Handheld	IMEI	1	98126	999339988776616	22-05-2020	New

- **Device Network access disable status**
    - Immediate: The device(s) is instantly blacklisted.
    - Default: The device(s) is sent to the blacklist after a given duration. The duration is configurable by the CEIR Admin.
    - Later: The device(s) is sent to the blacklist at the specified date. Select the date using the calendar .
- **Device Stolen Date**: Select device stolen date.
- **Other Information**

Copyright @ 2020 DMC All Rights Reserved

7. Click **Submit**.

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

8. For each request, the dashboard displays the following information:

Column	Description
Date	Date of registering the request.
Transaction ID	Transaction ID assigned to the request.
Request Type	Type of request generated is Stolen.
Mode	Indicates whether the request is for an individual or company (Individual or Company). In this case, it is 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, policy violation or request specifications. ○ Pending Approval from CEIR Admin: If the request is successfully verified by the system, the request is shared with the CEIR Admin for review. ○ Rejected by CEIR Admin: The CEIR Admin reviews the details and rejects the request if there is a problem. The personnel can view the error file and fix the errors in the request.

Copyright @ 2020 DMC All Rights Reserved

Column	Description
	○ Approved by CEIR Admin: When the CEIR Admin approves the request, the status changes to Approved by CEIR Admin. ○ Withdrawn by CEIR Admin: When the CEIR Admin withdraws the request, the status changes to Withdrawn by CEIR Admin. For example, this could be done when the personnel have wrongly marked a device as stolen, which has been recovered. ○ Withdrawn by User: The personnel can withdraw the request only when the status is New or Rejected by System.
IMEI Quantity	Refers to the number of IMEIs reported stolen.
Device Quantity	Refers to the number of devices reported stolen. A device can have multiple IMEIs.
Action	This displays different actions that can be performed on the request. • Error : An error file is generated if there is any problem in the request(s) submitted. Click to download the error file. Refer to *Figure 18* for a sample error file. • Download : This is used to take a dump of the **.csv** file that is uploaded to the system. This file is uploaded when the request is for stolen company/organization/government devices. This is enabled when the request is rejected by the system or CEIR Admin. Click on it download the file. • View : This is used to view the request. Click on it view the request details.

Copyright @ 2020 DMC All Rights Reserved

Column	Description
	• Edit : This is used to modify the request. This is allowed only 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. • History : This is used to view the history of the transaction. It shows the various status modes through which the transaction has gone through.

2.5 Reporting Recovered Devices

Lawful agency personnel can report devices that have been recovered. The device could belong to an individual or a company/organization/government.

2.5.1 Reporting Individual Recovered Devices

<u>To report an individual recovered device:</u>

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

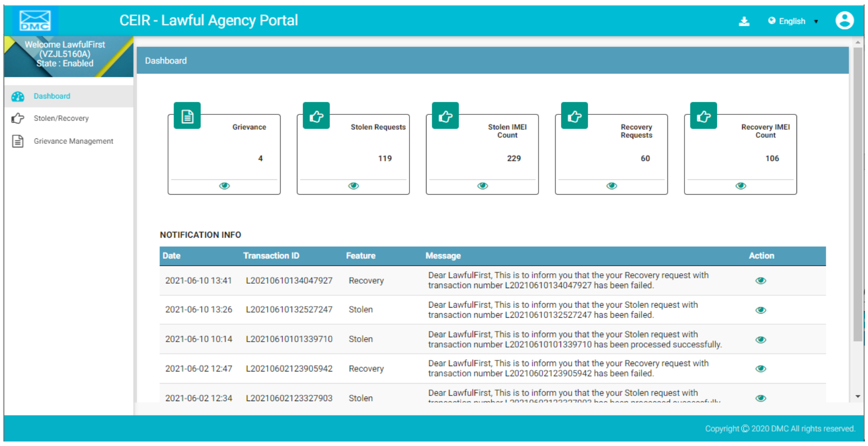


Figure 22: Home Page

Copyright @ 2020 DMC All Rights Reserved

The **Stolen/Recovery** dashboard appears.

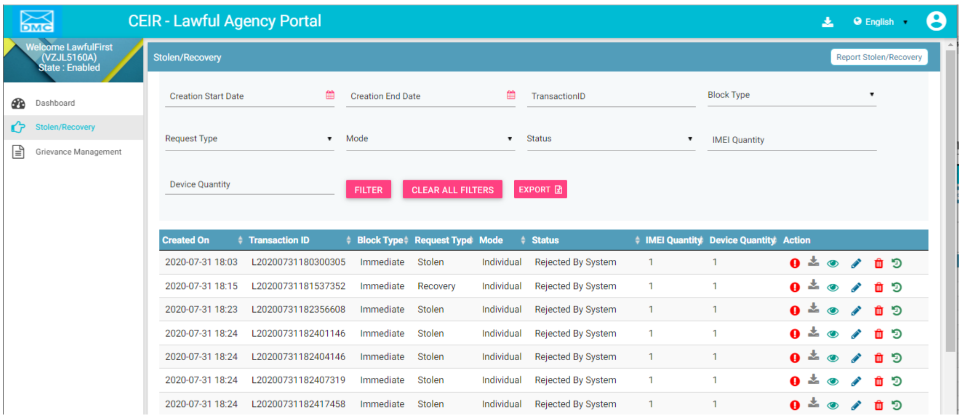
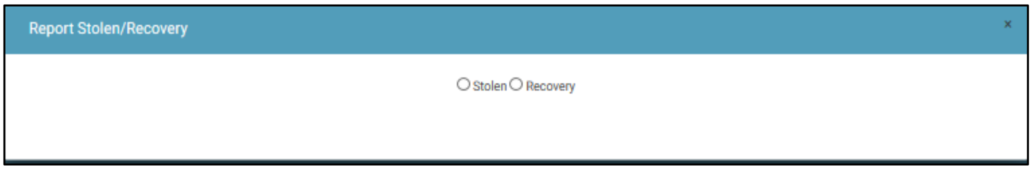


Figure 23: Stolen/Recovery

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



3. Select **Recovery**.

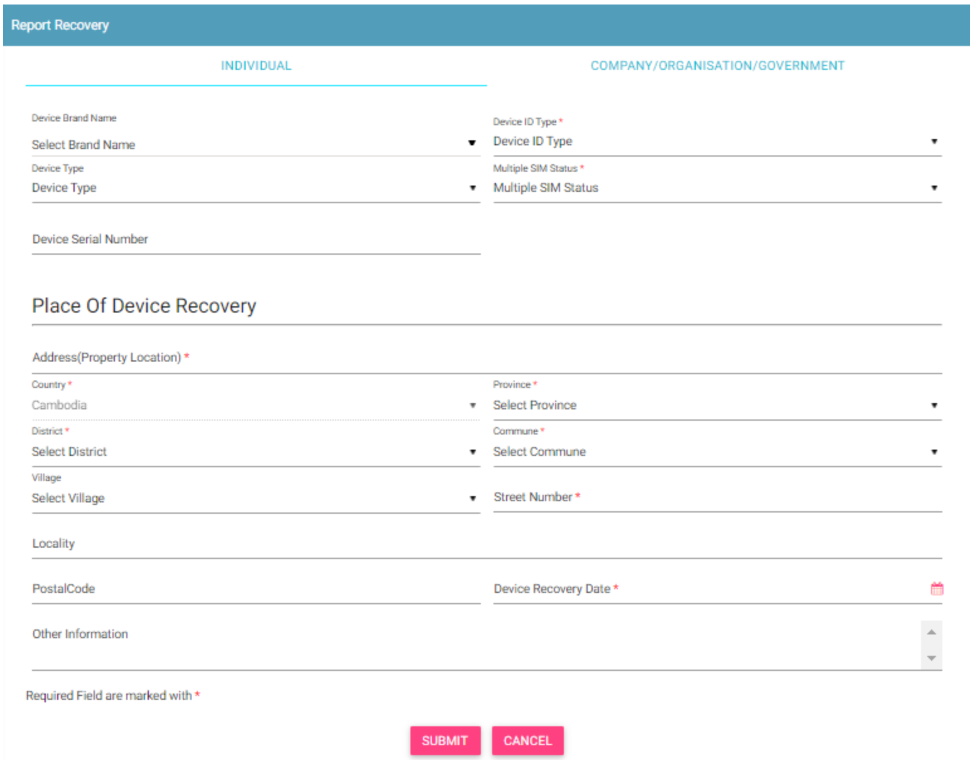


Figure 24: Report Recovery (Individual)

Copyright @ 2020 DMC All Rights Reserved

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

By default, the **Individual** section appears. Here, the devices that have been recovered for an individual are reported.

4. Enter the following information:

Personal Information: Enter the personal details of the person whose stolen device has been recovered.

- **Device Brand Name**: Select the brand name from the list.
- ***Device ID Type**: Select the ID type to be entered for the device:
    - IMEI
- **Device Type**: Select the type of device recovered.
    - ***Multiple SIM Status**: Number of multiple SIM the device supports (1-4)
- **Device Serial Number**: Enter the device serial number.
- *IMEI: Enter the IMEI number(s) of the device recovered.

Place of Recovery

- *Address (Property Location)
- *Street Number
- *Village
- *Locality
- *District
- *Commune
- *Postal Code
- *Country
- *Province
- ***Device Recovery Date**: Click the calendar to select the date when the device was recovered.
- **Remarks**

5. Click **Submit**.

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

Copyright @ 2020 DMC All Rights Reserved

For each request, the dashboard displays the following information:

Column	Description
Date	Date of registering the request to recover the device.
Transaction ID	Transaction ID assigned to the request.
Request Type	The request type here is Recovery.
Mode	Indicates whether the request is for an individual or company (Individual or Company). In this case, it is Individual.
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, policy violation or request specifications. This is applicable only for company/organization/government recovered devices. ◦ Pending Approval from CEIR Admin: If the request is successfully verified by the system, the request is shared with the CEIR Admin for review. ◦ Rejected by CEIR Admin: The CEIR Admin reviews the details and rejects the request if there is a problem. The personnel can view the error file and fix the errors in the request.

Copyright @ 2020 DMC All Rights Reserved

Column	Description
	○ Approved by CEIR Admin: When the CEIR Admin approves the request, the status changes to Approved by CEIR Admin. ○ Withdrawn by CEIR Admin: When the CEIR Admin withdraws the request, the status changes to Withdrawn by CEIR Admin. For example, this could be done when the personnel have wrongly marked a device as stolen, which has been recovered. ○ Withdrawn by User: The personnel can withdraw the request only when the status is New or Rejected by System.
IMEI Quantity	Refers to the number of IMEIs recovered.
Quantity	Refers to the number of devices recovered. A single device can have multiple IMEIs.
Action	This displays different actions that can be performed on the request. • Error : An error file is generated when there is a problem in the request(s) submitted. Click on the icon to download the error file. • Download : This is applicable when the request is for company/organization/government recovered devices. This downloads the device file that is uploaded to the system. • View : This is used to view the request. Click on it view the request details. • Edit : This is used to modify the request. This is allowed only when the status is New or Rejected by

Copyright @ 2020 DMC All Rights Reserved

Column	Description
	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. • History : This is used to view the history of the transaction. It shows the various status modes through which the transaction has gone through.

2.5.2 Reporting Company/Organization/Government Recovered Devices

To report recovered company/organization/government devices:

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

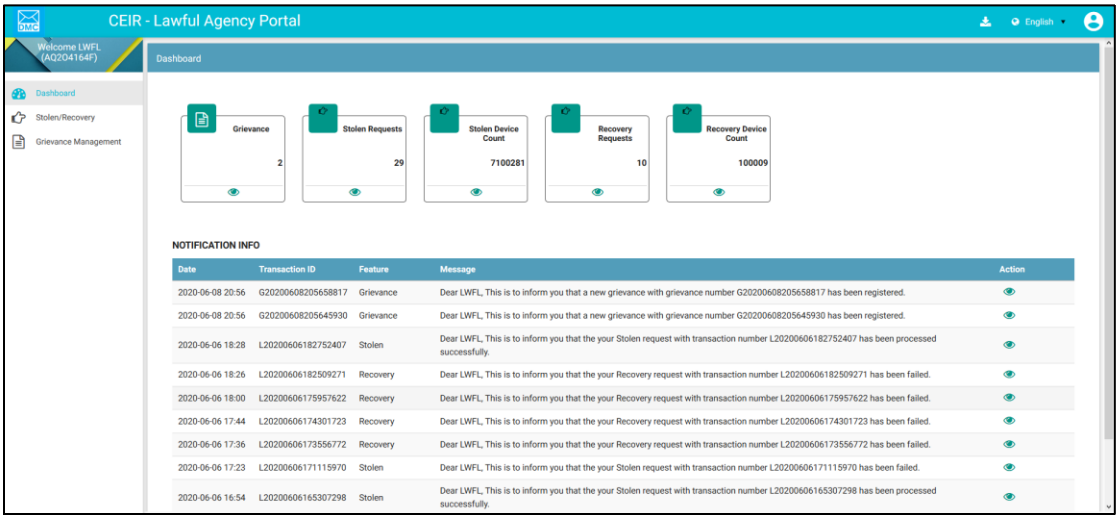


Figure 25: Home Page

The **Stolen/Recovery** dashboard appears.

Copyright @ 2020 DMC All Rights Reserved

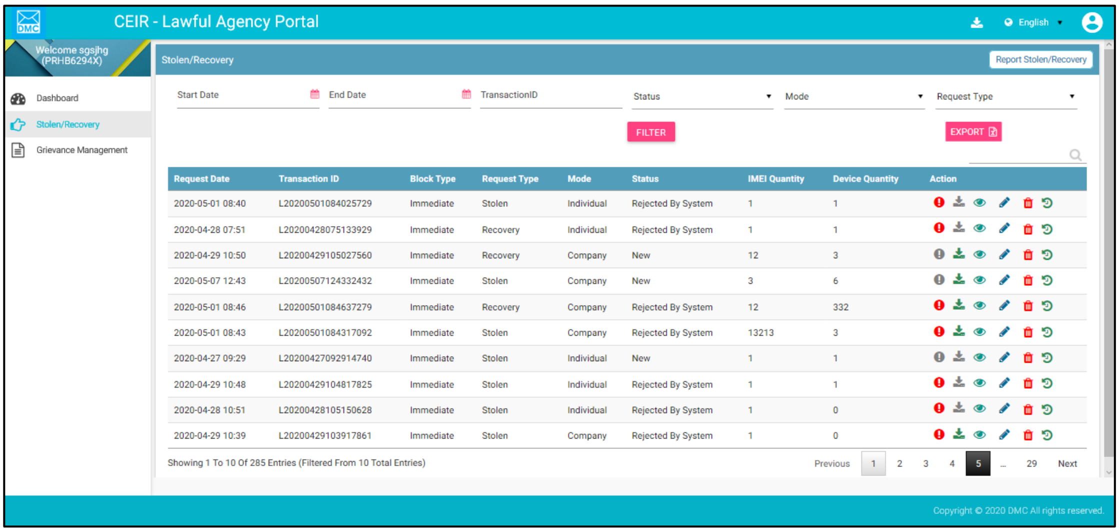
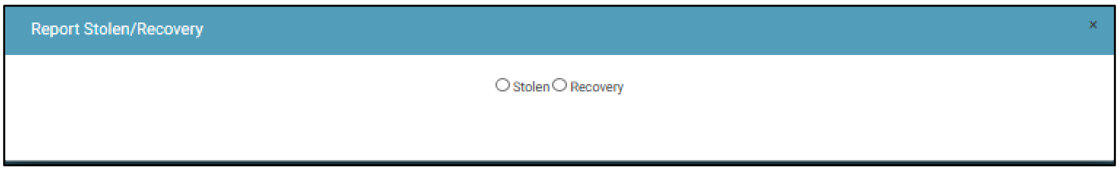


Figure 26: Stolen/Recovery

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



3. Select **Recovery**.

Select the **Company/Organization/Government** tab.

Copyright @ 2020 DMC All Rights Reserved

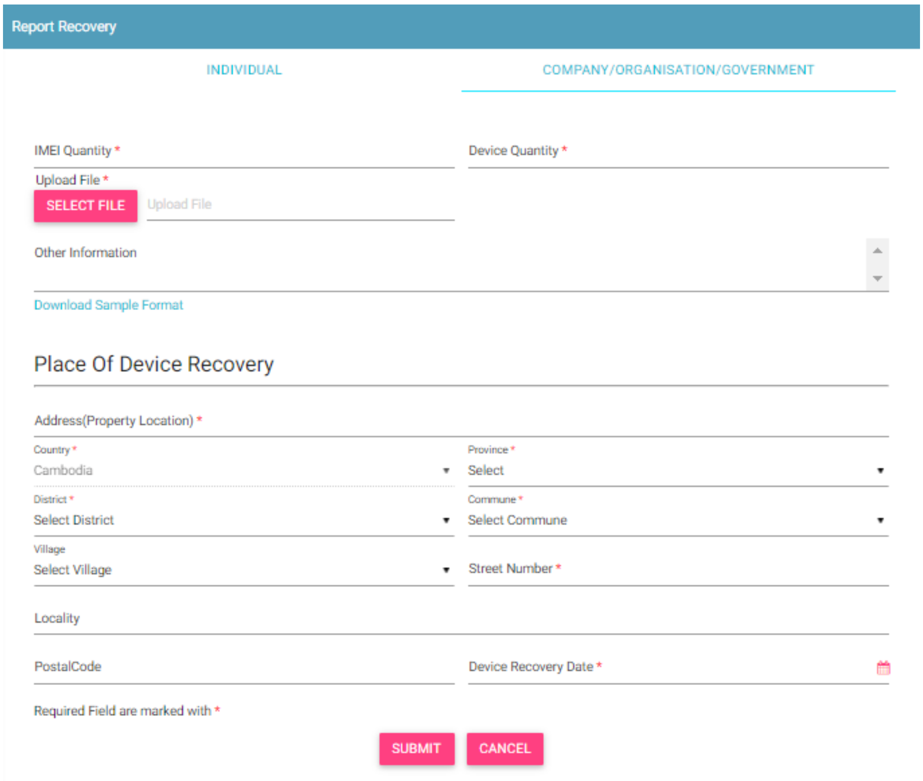


Figure 27: Report Recovery (Company/Organization/Government)

4. Enter the following information:

- ***IMEI Quantity**: Enter the number of IMEIs recovered.
- *Device Quantity: Enter the number of devices recovered. A device can have multiple IMEIs.
- ***Upload File**: Enter the recovered device details. To enter the device details, click **Download Sample Format** and save the format file. Enter the device details in the specified format. Click **Select** to upload the file.
- **Other Information**

Place of Device Recovery: Enter the address of the place where the devices were recovered.

- *Address (Property Location)
- *Street Number
- Village
- Locality
- *District

Copyright @ 2020 DMC All Rights Reserved

- *Commune
- Postal Code
- *Country
- *Province
- ***Device Recovery Date**: Click the calendar to select the recovery date.

9. Click **Submit**.

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

10. For each request, the dashboard displays the following information:

Column	Description
Date	Date of registering the request.
Transaction ID	Transaction ID assigned to the request.
Request Type	The request type is Recovery.
Mode	Indicates whether the request is for an individual or company (Individual or Company). In this case, it is 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, policy violation or request specifications. ○ Pending Approval from CEIR Admin: If the request is successfully verified by the

Copyright @ 2020 DMC All Rights Reserved

Column	Description
	system, the request is shared with the CEIR Admin for review. ◦ Rejected by CEIR Admin: The CEIR Admin reviews the details and rejects the request if there is a problem. The operator can view the error file and fix the errors in the request. ◦ Approved by CEIR Admin: When the CEIR Admin approves the request, the status changes to Approved by CEIR Admin. ◦ Withdrawn by CEIR Admin: When the CEIR Admin withdraws the request, the status changes to Withdrawn by CEIR Admin. For example, this could be done when the personnel have wrongly marked a device as stolen, which has been recovered. ◦ Withdrawn by User: The personnel can withdraw the request only when the status is New or Rejected by System.
Quantity	Refers to the number of IMEIs recovered.
Quantity	Refers to the number of devices recovered. A device can have multiple IMEIs.
Action	This displays different actions that can be performed on the request. • Error : This is enabled when there is an error file generated because of a problem in the request(s) submitted. Click on the icon to download the error file. • Download : This is used to take a dump of the **.csv** file that is uploaded to the system. This file is

Copyright @ 2020 DMC All Rights Reserved

Column	Description
	uploaded when the request is for company/organization/government recovered devices. This is enabled when the request is rejected by the system or CEIR Admin. Click on it download the file. • View : This is used to view the request. Click on it view the request details. • Edit : This is used to modify the request. This is allowed only 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. • History : This is used to view the history of the transaction. It shows the various status modes through which the transaction has gone through.

2.6 Editing Stolen or Recovered Device Requests

Lawful agency personnel can change the 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 ()** against the request to be modified.

Copyright @ 2020 DMC All Rights Reserved

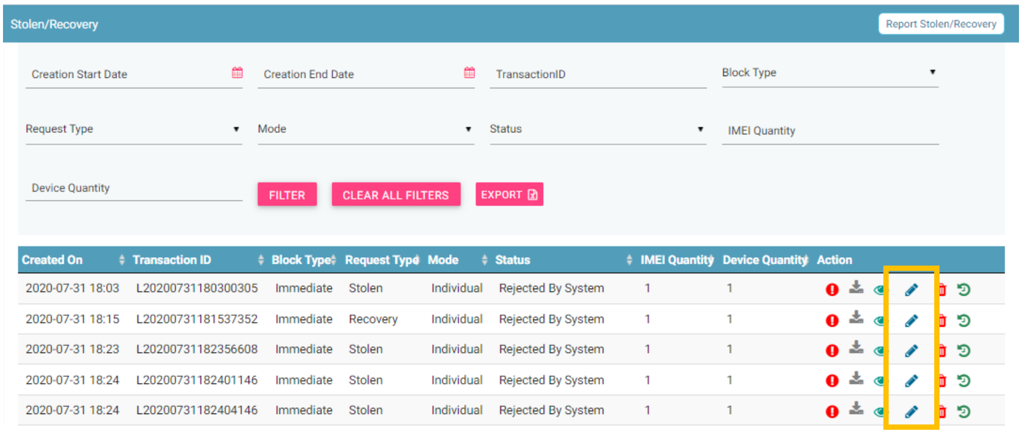


Figure 28: Stolen/Recovery

The **Edit** page appears. The page has the same fields as seen in the page when reporting individual or company/organization/government stolen or recovered devices.

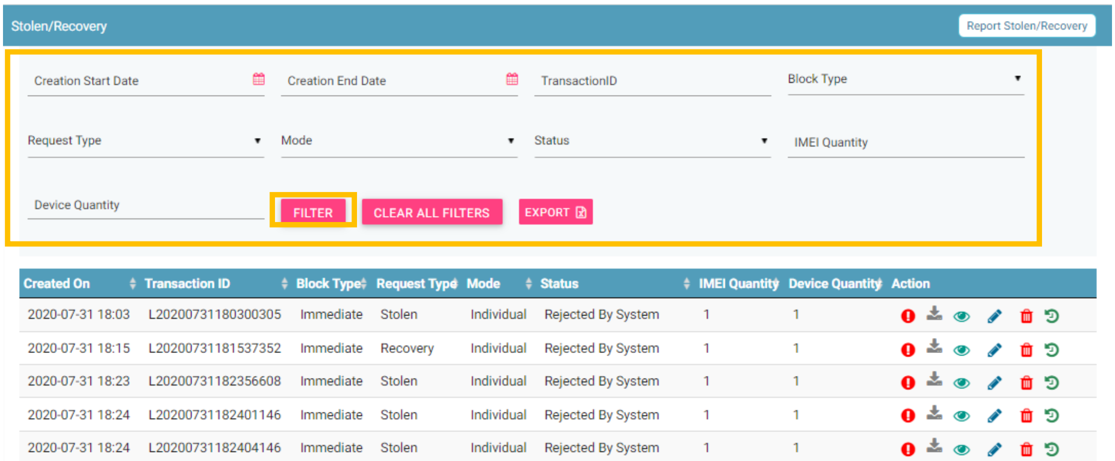
2. Make the required changes
3. Click **UPDATE**.

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

2.7 Filtering Stolen or Recovered Device Requests

Lawful agency personnel can view selective device requests after specifying the required filters. For example, they can view requests that are pending approval from the CEIR Admin.

<u>To filter device requests:</u>



Copyright @ 2020 DMC All Rights Reserved

Figure 29: Stolen/Recovery

1. Enter data in one or more of the listed fields:
    - **Start Date** and **End Date**: This refers to the period of reporting stolen/lost or recovered devices.
    - **Transaction ID**: Each request is assigned a unique transaction ID.
    - **Status**: This refers to the status of the request:
        - New
        - Processing
        - Rejected by System
        - Rejected CEIR Admin
        - Approved CEIR Admin
        - Withdrawn CEIR Admin
        - Withdrawn User
    - **Mode**: This refers to whether the request for a stolen or recovered device is: Individual or Company.
    - **Request Type**: This refers to the type of request: Stolen or Recovered.
2. Click **FILTER**.

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

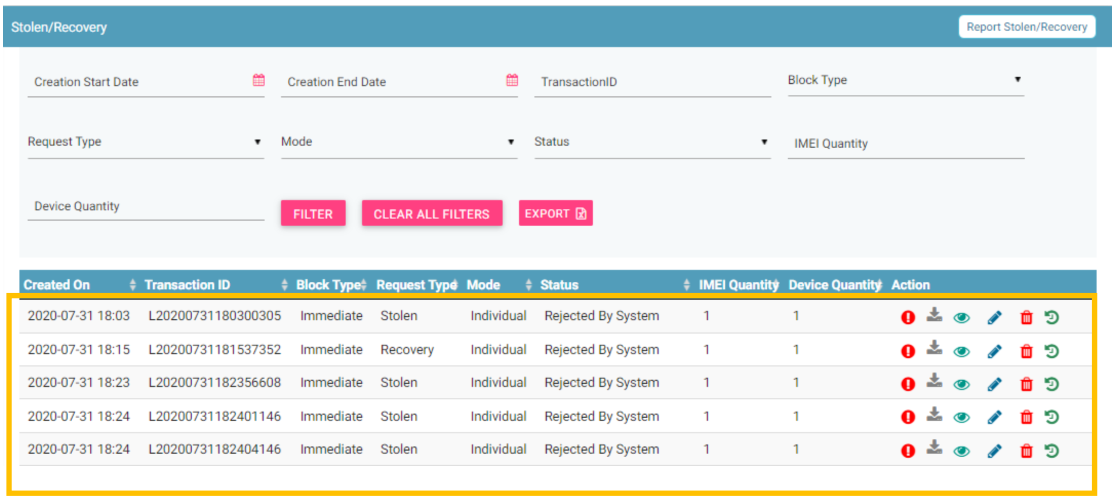


Figure 30: Filtered Requests

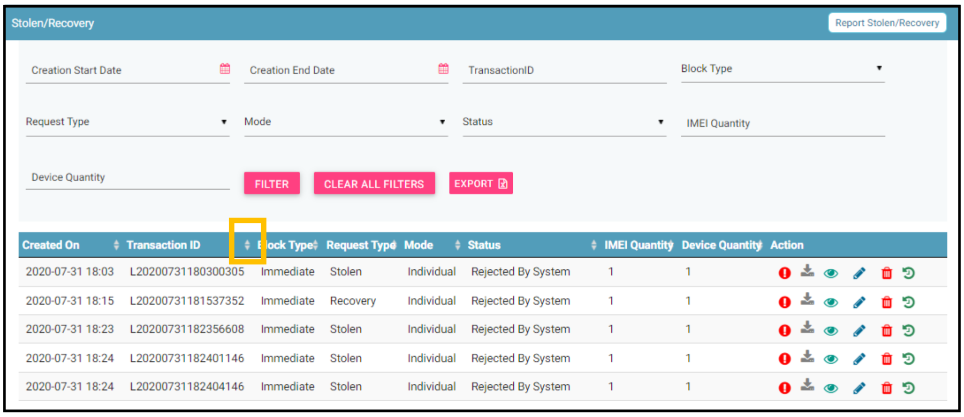
The user can clear all filters using the "**Clear All Filters**" button. This will reset all the filter values applied on the page and the data table will be refreshed.

Copyright @ 2020 DMC All Rights Reserved

2.1 Sorting Stolen/Recovery Device Requests

By default, all records displayed are sorted based on modified date. User can sort the records by clicking the arrow button on header in the table displayed.

On first click, the records are sorted in ascending order. When user clicks the arrow buttons again, records are sorted in descending order.



2.2 Exporting Stolen or Recovered Device Requests

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

<u>To export the uploaded requests:</u>

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

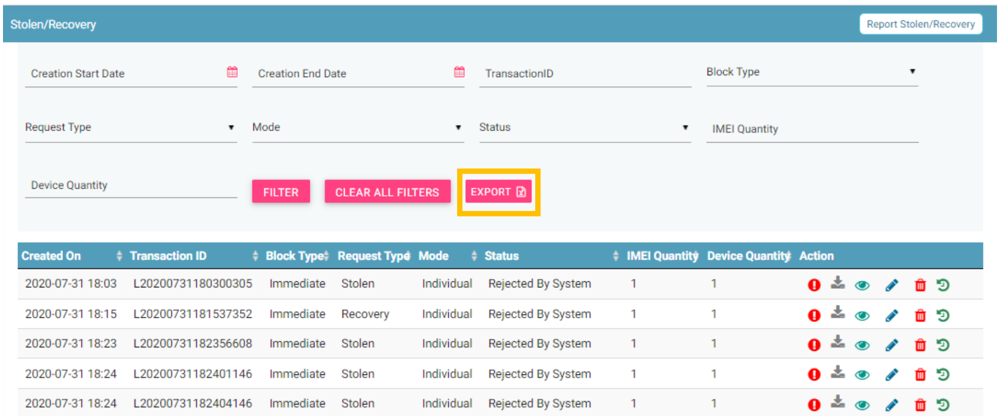


Figure 31: Stolen/Recovery

The following page appears.

Copyright @ 2020 DMC All Rights Reserved

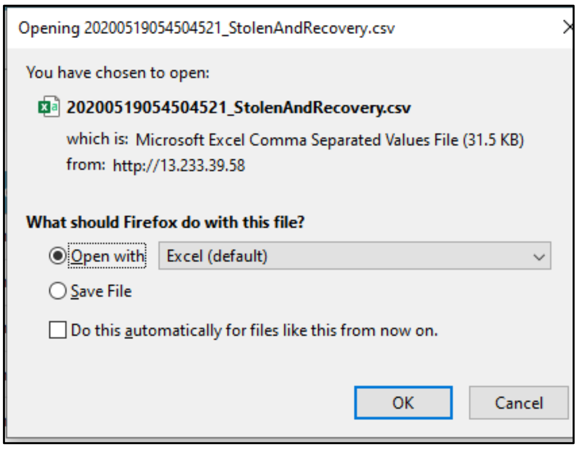


Figure 32: Open or Save Stolen/Recovery File

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

	A	B	C	D	E	F	G	H	I	J
1	Modified On	Created On	Transaction ID	Block Type	Request Type	Mode	Status	IMEI Quantity	Device Quantity	Filename
2	31-07-2020 18:42	31-07-2020 18:24	L20200731182439652	Immediate	Stolen	Individual	Rejected By System	1	2	Stock (24).csv
3	01-08-2020 13:28	31-07-2020 19:33	L20200731193329107	Immediate	Stolen	Individual	Rejected by CEIR Admin	1	2	example15.csv
4	14-08-2020 13:26	14-08-2020 13:25	L20200814132523037	Immediate	Stolen	Individual	Rejected By System	2	3	example15.csv
5	14-08-2020 15:05	14-08-2020 15:04	L20200814150450334	Immediate	Recovery	Individual	Rejected By System	1	2	example15.csv
6	14-08-2020 15:21	14-08-2020 15:20	L20200814152051062	Immediate	Recovery	Individual	Rejected By System	10	10	consignmentReport.csv
7	17-08-2020 19:26	17-08-2020 19:04	L20200817190449045	Immediate	Recovery	Individual	Rejected by CEIR Admin	1	1	
8	17-08-2020 19:43	17-08-2020 19:41	L20200817194131008	Immediate	Stolen	Individual	Rejected by CEIR Admin	1	1	

Figure 33: Exported Stolen/Recovery File

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

2.3 Grievance Management

Lawful agency personnel can register complaints or grievances when there is a problem in the portal. For example, there could be situations when the stolen/recovery feature is not working.

When the personnel raise a grievance, the grievance goes through the following stages:

1. A notification is sent to the CEIR Admin. The notification appears on the CEIR Admin portal. A mail is also sent to the registered mail of the CEIR Admin.
2. The CEIR Admin responds to the grievance. A response notification is sent to the lawful agency portal, and the registered mail ID.
3. Steps 1 to 2 are repeated until the grievance is closed. CEIR Admin closes the grievance.

Copyright @ 2020 DMC All Rights Reserved

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 personnel for a specified period.

To raise a grievance

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

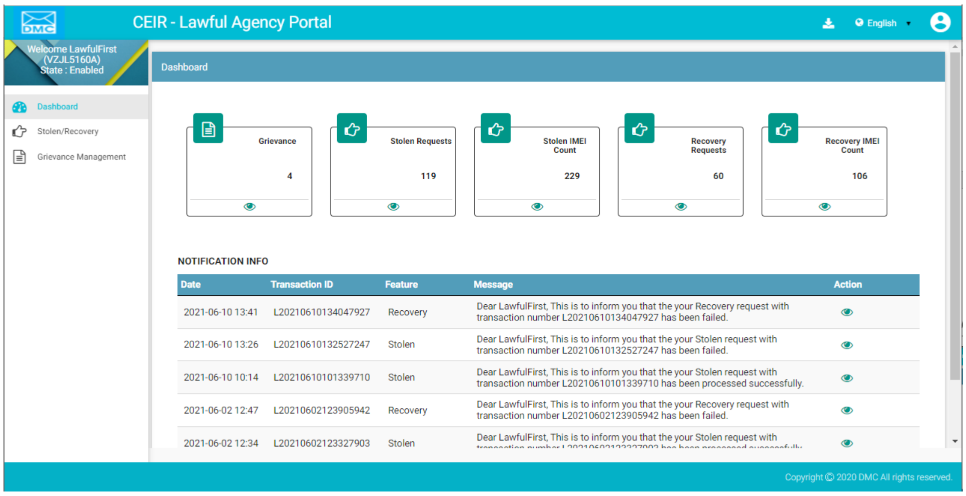


Figure 34: Home Page

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

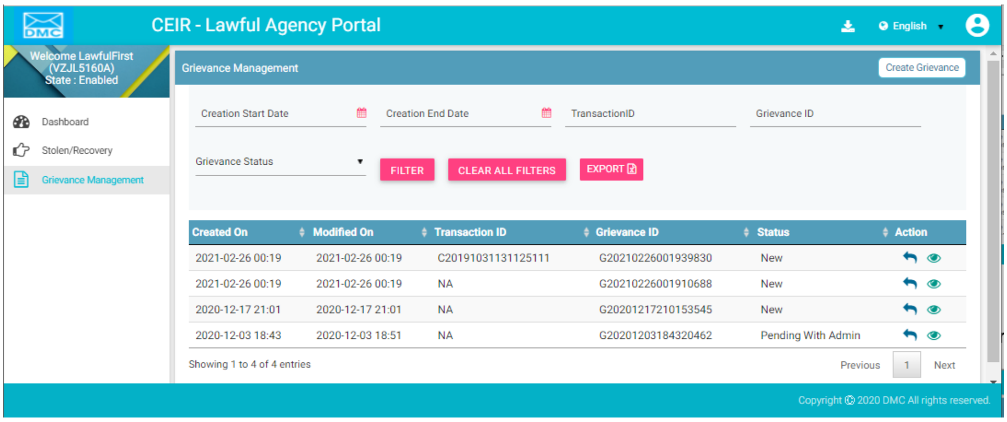


Figure 35: Grievance Management

The **Report Grievance** page appears.

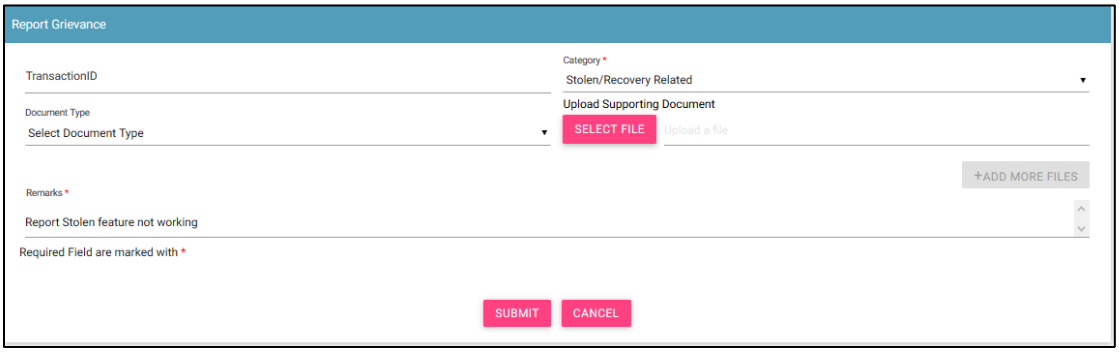


Figure 36: Report Grievance

3. Enter the following information:

    a. **Transaction ID**: Enter the transaction ID of the stolen/recovery request if the grievance is related it.

    b. ***Category**: Select the category of the grievance. The options are:

    - Stolen/Recovery Related
    - Other

    c. **Document Type:** Select the type of identification or another document that is to be uploaded.

    - FIR Document
    - National ID Document
    - Other

    d. **Upload Supporting Document:** Click **Select File** to upload the document selected in **Document Type**.

    e. To upload more documents, click **+Add More Files.**

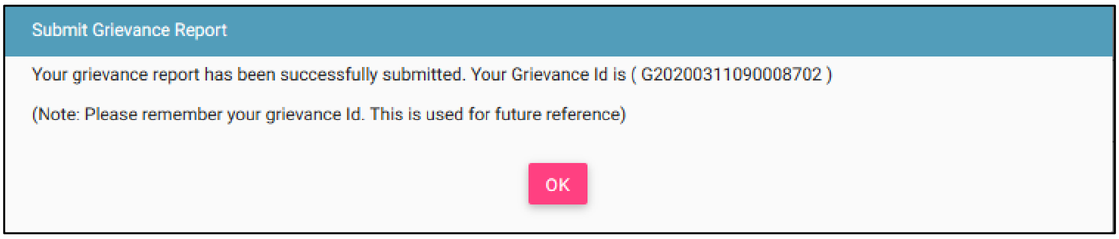
    This adds two more fields: **Document Type** and **Select File**.

    f. ***Remarks:** Enter information about the grievance raised. This helps CEIR Admin to understand the problem in detail.

4. Click **SUBMIT**.

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

Copyright @ 2020 DMC All Rights Reserved



The new grievance appears on the top of the page.

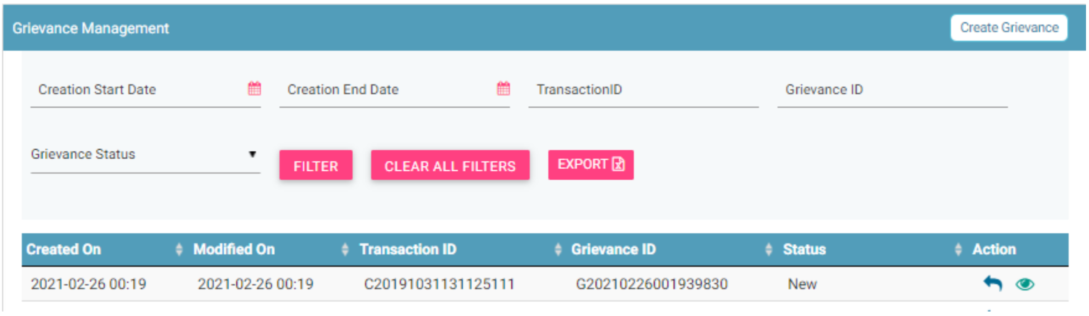


Figure 37: Grievance Management

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

Column	Description
Created On	Date of raising a grievance.
Modified On	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 Admin: When a response is awaited from the CEIR Admin. • Pending with User: When a response is awaited from the lawful agency personnel.

Copyright @ 2020 DMC All Rights Reserved

Column	Description
	• Closed: When the CEIR Admin 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 Admin or agency personnel. The exchange of responses is done until the grievance is closed. • View : This is used to view the grievance response history. The agency personnel can see all the responses exchanged for any grievance.

2.4 Filtering Grievances

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

<u>To filter grievances:</u>

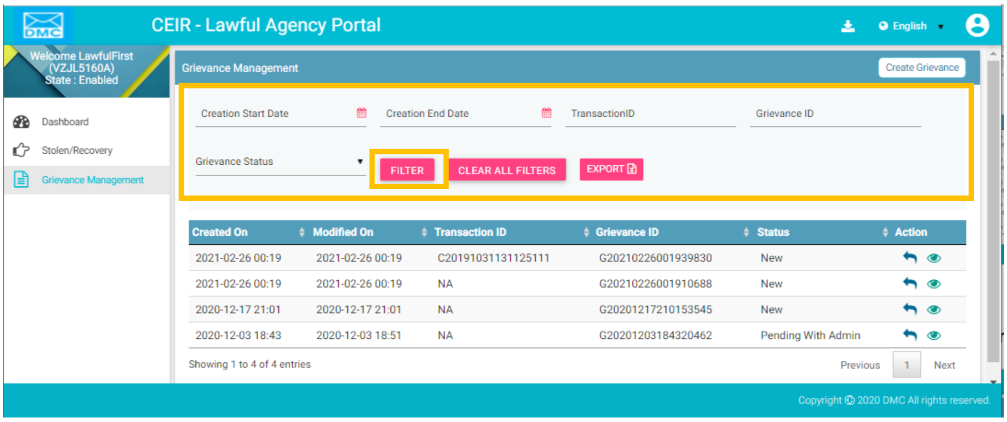


Figure 38: Filter Grievances

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

Copyright @ 2020 DMC All Rights Reserved

- **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 Admin
    - Pending with User
    - Closed

2. Click **Filter**.

The filtered grievances are shown on the page.

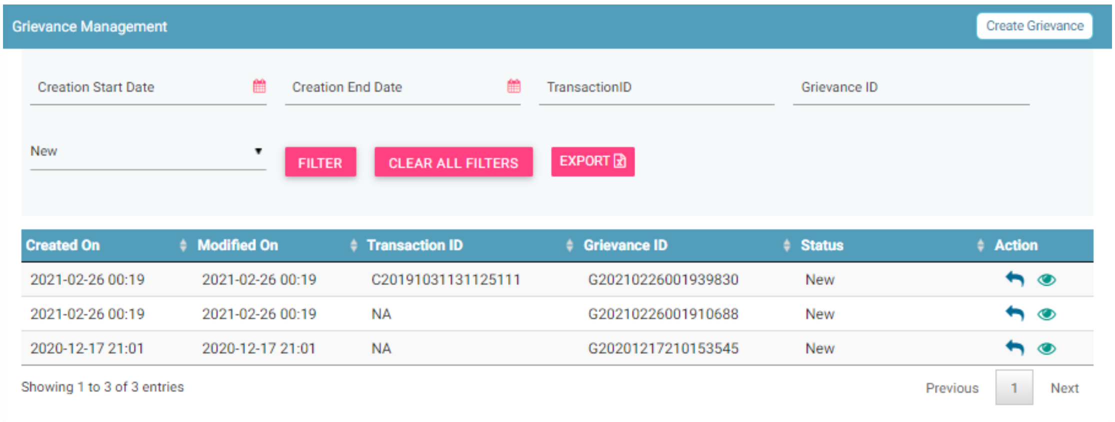


Figure 39: Filtered Grievances

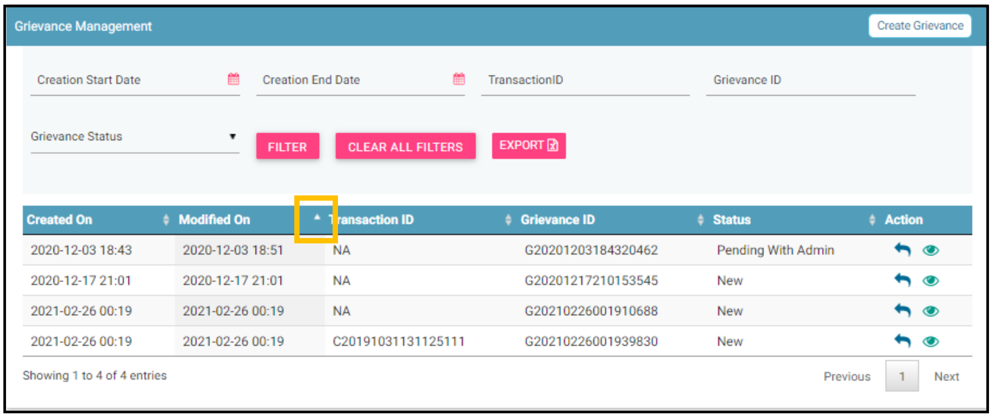
The user can clear all filters using the "**Clear All Filters**" button. This will reset all the filter values applied on the page and the data table will be refreshed.

2.5 Sorting Grievances

By default, all records displayed are sorted based on modified date. User can sort the records by clicking the arrow button on header in the table displayed.

On first click, the records are sorted in ascending order. When user clicks the arrow buttons again, records are sorted in descending order.

Copyright @ 2020 DMC All Rights Reserved



2.6 Exporting Grievances

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

<u>To export the grievances:</u>

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

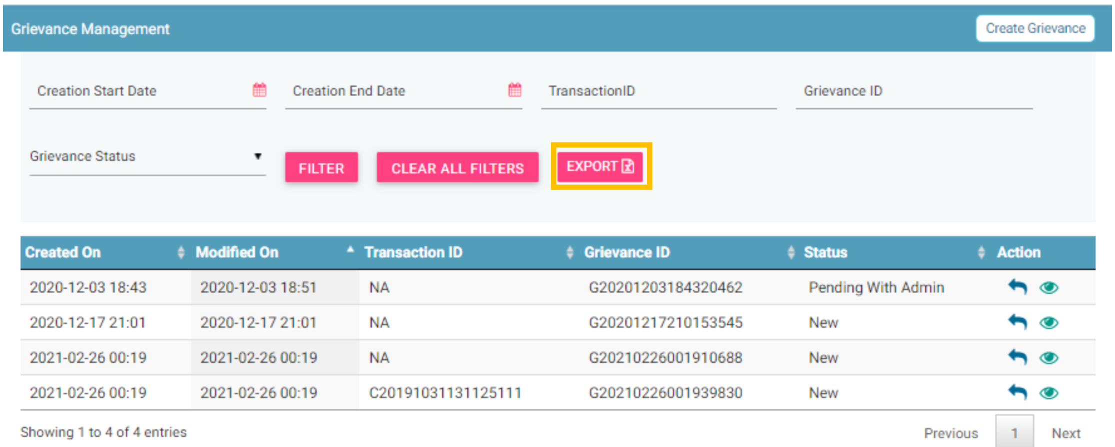


Figure 40: Grievance Management

Copyright @ 2020 DMC All Rights Reserved

The following page appears.

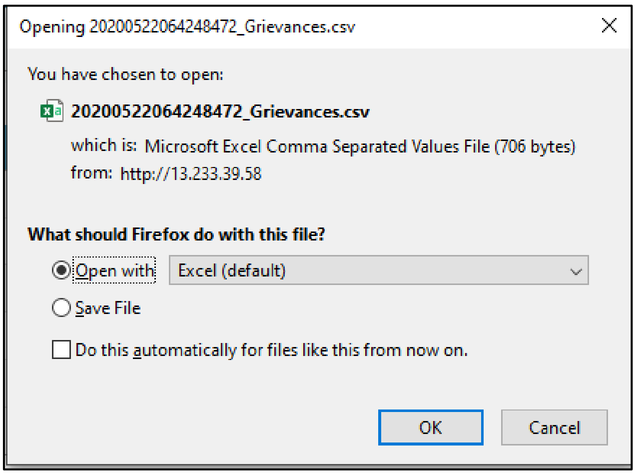
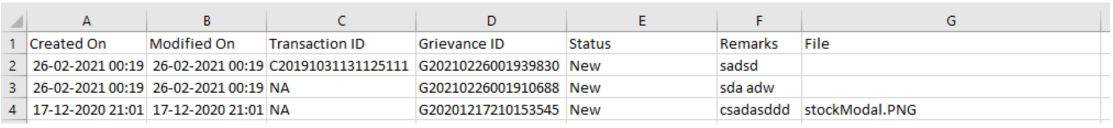


Figure 41: Open or Save Exported Grievance File

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



	A	B	C	D	E	F	G
1	Created On	Modified On	Transaction ID	Grievance ID	Status	Remarks	File
2	26-02-2021 00:19	26-02-2021 00:19	C20191031131125111	G20210226001939830	New	sadsd	
3	26-02-2021 00:19	26-02-2021 00:19	NA	G20210226001910688	New	sda adw	
4	17-12-2020 21:01	17-12-2020 21:01	NA	G20201217210153545	New	csadasddd	stockModal.PNG

Figure 42: Exported Grievances

Instead of exporting all the grievances, personnel 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.

Copyright @ 2020 DMC All Rights Reserved