



Central Equipment Identity Register Portal

Lawful Agency User Manual v 1.0



Document Change History

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



Contents

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.....	10
2.3.1	Dashboard.....	12
2.4	Reporting Stolen/Recovered Devices.....	16
2.4.1	Reporting Individual Stolen Devices	16
2.4.2	Reporting Company/Organization/Government Stolen/Lost Devices	23
2.5	Reporting Recovered Devices	30
2.5.1	Reporting Individual Recovered Devices	30
2.5.2	Reporting Company/Organization/Government Recovered Devices.....	35
2.6	Editing Stolen or Recovered Device Requests.....	40
2.7	Filtering Stolen or Recovered Device Requests.....	41
2.8	Exporting Stolen or Recovered Device Requests.....	42
2.9	Grievance Management	43
2.10	Filtering Grievances	47
2.11	Exporting Grievances	48



Figures

Figure 1: DMC Home Page	3
Figure 2: Lawful Agency Registration	4
Figure 3: Verify OTP	6
Figure 4: Enter OTP	6
Figure 5: Login	7
Figure 6: Home Page	8
Figure 7: Forgot Password	8
Figure 8: Set New Password	9
Figure 9: Home Page	10
Figure 10: Edit Information	11
Figure 11: Change Password	11
Figure 12: Manage Account	12
Figure 13: Home Page	13
Figure 14: Home Page	15
Figure 15: Home Page	16
Figure 16: Stolen/Recovery	17
Figure 17: Report Stolen (Individual)	18
Figure 18: Error File	23
Figure 19: Home Page	23
Figure 20: Stolen/Recovery	24
Figure 21: Report Stolen (Company/Organization/Government)	25
Figure 22: Home Page	30
Figure 23: Stolen/Recovery	30
Figure 24: Report Recovery (Individual)	31
Figure 25: Home Page	35
Figure 26: Stolen/Recovery	36
Figure 27: Report Recovery (Company/Organization/Government)	36
Figure 28: Stolen/Recovery	40
Figure 29: Stolen/Recovery	41
Figure 30: Filtered Requests	42
Figure 31: Stolen/Recovery	42
Figure 32: Open or Save Stolen/Recovery File	43
Figure 33: Exported Stolen/Recovery File	43
Figure 34: Home Page	44
Figure 35: Grievance Management	44
Figure 36: Report Grievance	45
Figure 37: Grievance Management	46
Figure 38: Filter Grievances	47
Figure 39: Filtered Grievances	48
Figure 40: Grievance Management	49
Figure 41: Open or Save Exported Grievance File	49
Figure 42: Exported Grievances	49



1 Overview

1.1 Scope

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

1.2 Acronyms & Abbreviations

Acronym	Full Form
CEIR	Central Equipment Identity Register
EIR	Equipment Identity Register
ESN	Electronic Serial Number
IMEI	International Mobile Equipment Identity
MEID	Mobile Equipment Identifier
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)	<i>Italics</i>



Information	Convention
*	Indicates a mandatory field or column



2 Operations

2.1 Application Overview

The CEIR Lawful Agency Portal application enables agency personnel to report devices (IMEIs/MEIDs/ESNs) that are stolen and report devices (IMEIs/MEIDs/ESNs) 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/MEIDs/ESNs)
- Report recovered devices (IMEIs/MEIDs/ESNs)
- 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.

Welcome To Central Equipment Identity Register						
Login	Registration ▼	Register Grievance ▼	Stock ▼	Check Device	Register Device	Update Visa Validity

Figure 1: DMC Home Page

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



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
 - 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 ID Card:** Upload the image of the 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.
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.

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 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.



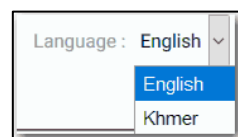
To start using the application, log into the application.

To login:

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

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.



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 enters 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.

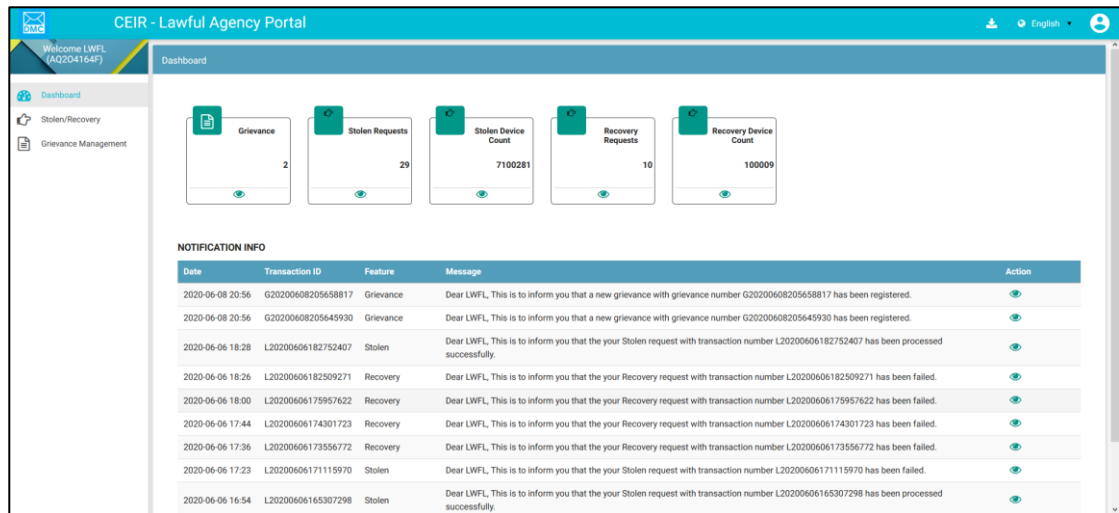


Figure 6: Home Page

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

Forgot Password

Please enter your User ID * FLHF0071K

Please select your security question, provide at the time of registration * What was your childhood nickname

Provide answer to the question* Sammy

SUBMIT **CANCEL**

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.



Set New Password


New Password

New Password

Confirm Password

SAVE

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**.



2.3 Application User Interface

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

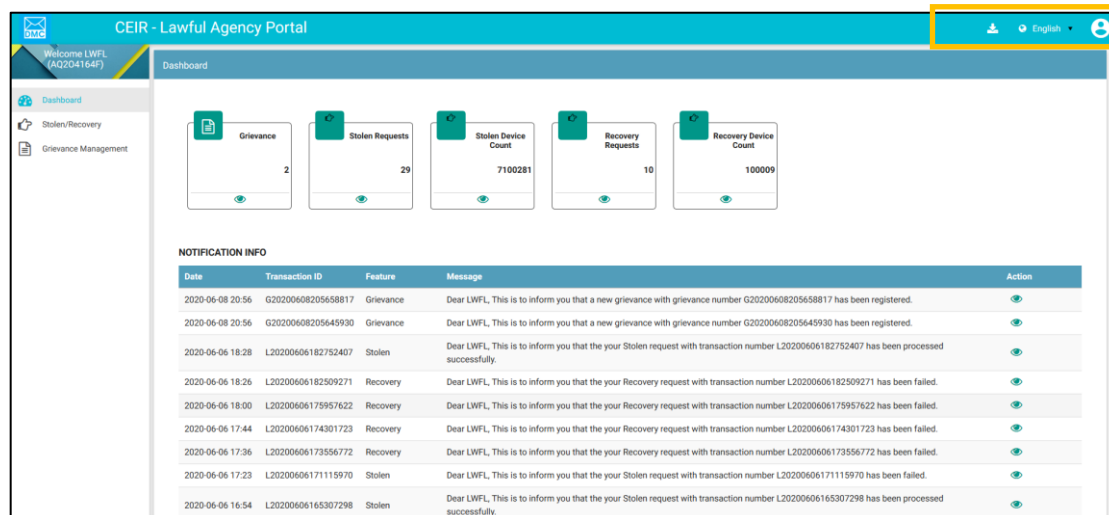


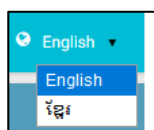
Figure 9: Home Page

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

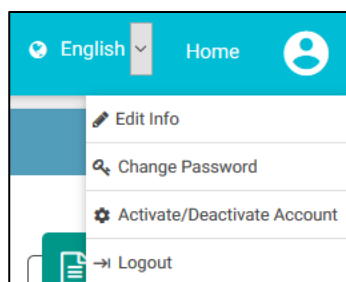
The center of the page is the Dashboard.


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

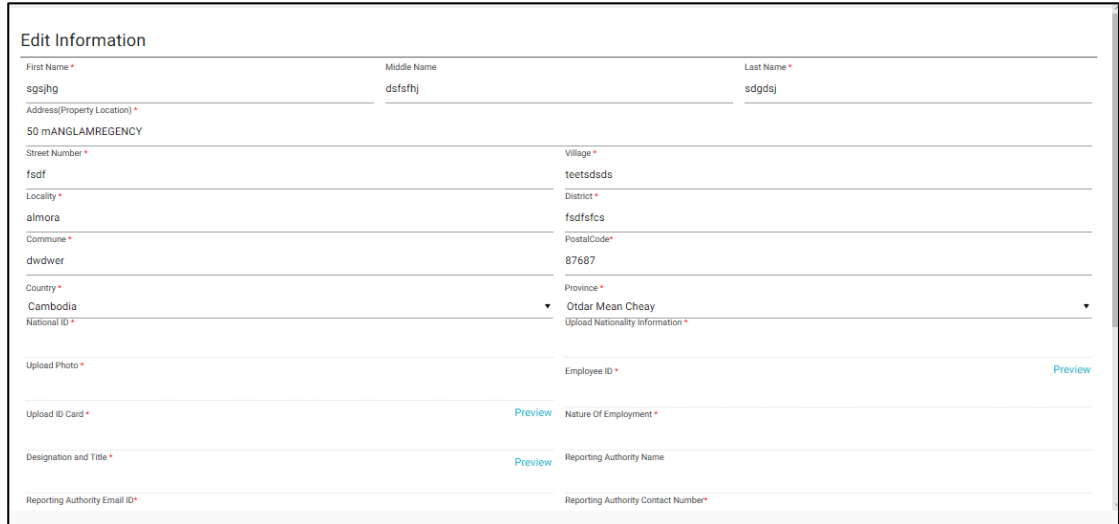
- **Download Manual** : Click to download this user manual.
- **English** : Select **English** or **Khmer**. All the field and column labels appear in the selected language. User inputs are, however, in English.



- **Home**: Click on it to go to the **DMC Home Portal** page.
- (**User profile**): Click on it to see the following menu:




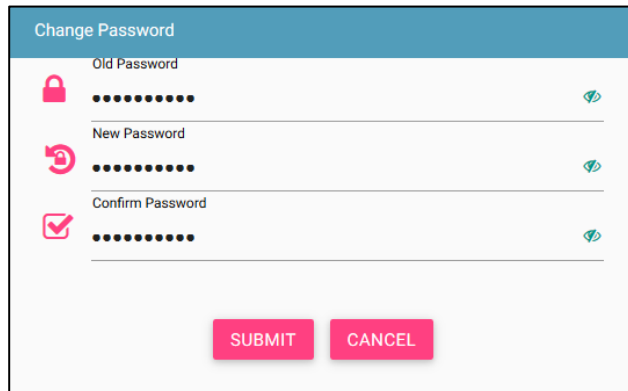
-  (**Edit Info**): Click on it to modify the registered information. The **Edit Information** page opens.



The 'Edit Information' form is a structured layout for updating user details. It includes fields for personal information (First Name, Middle Name, Last Name), address (Address/Property Location, Street Number, Village, Locality, District, Commune, Postal Code), and identification (Country, National ID, Province, Employee ID). There are also sections for photo upload, ID card upload, and reporting authority details (Designation and Title, Reporting Authority Name, Reporting Authority Email ID, Reporting Authority Contact Number). Each field has a red asterisk indicating it is required. Some fields have a 'Preview' link next to them.


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.




The 'Change Password' form is a simple interface with three input fields: 'Old Password', 'New Password', and 'Confirm Password'. Each field has a red lock icon on the left and a green eye icon on the right, indicating a password toggle. Below the fields are two buttons: 'SUBMIT' and 'CANCEL'.

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):** 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 administrator 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.

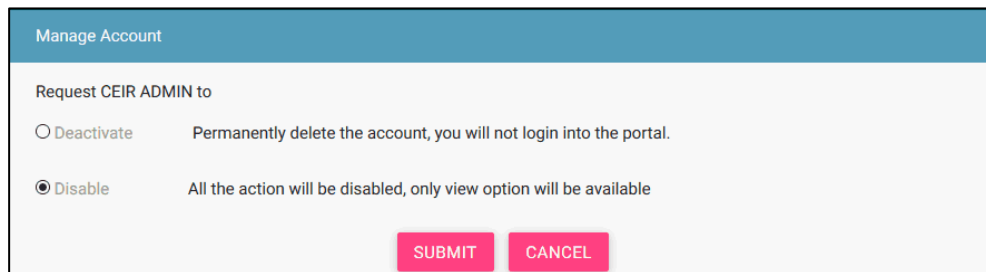


Figure 12: Manage Account

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

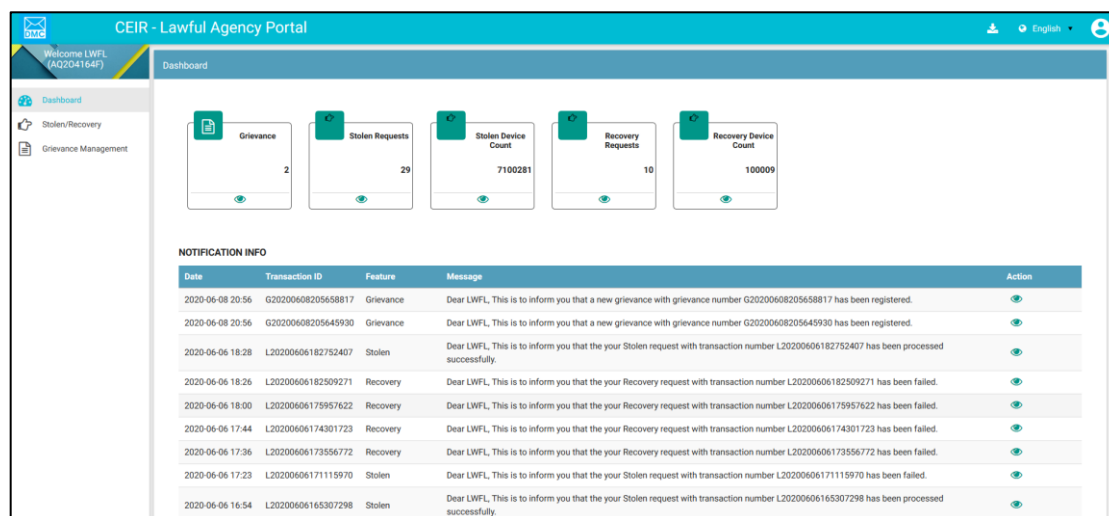
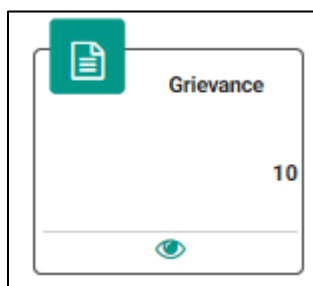


Figure 13: Home Page

Grievance

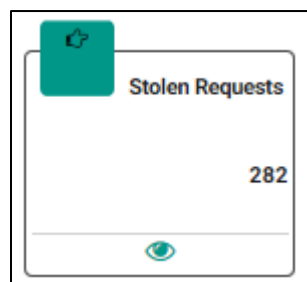
The box displays the total number of grievances registered by the personnel.



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/MEIDs/MSNs).

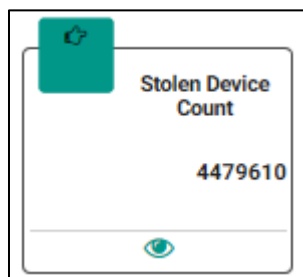


Click (**View**) to go to the **Stolen/Recovery** dashboard. Refer to *Stolen/Recovery Devices* for more information.



Stolen Device Count

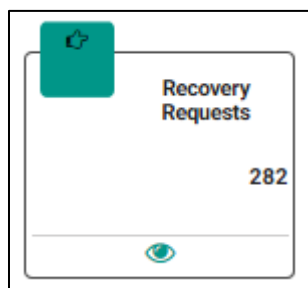
This box displays the total number of devices (IMEIs/MEIDs/MSNs) that have been reported as stolen.



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

Recovery Requests

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/MEIDs/MSNs) that have been recovered.



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

Notification Information

This section displays the ten most recent notifications.

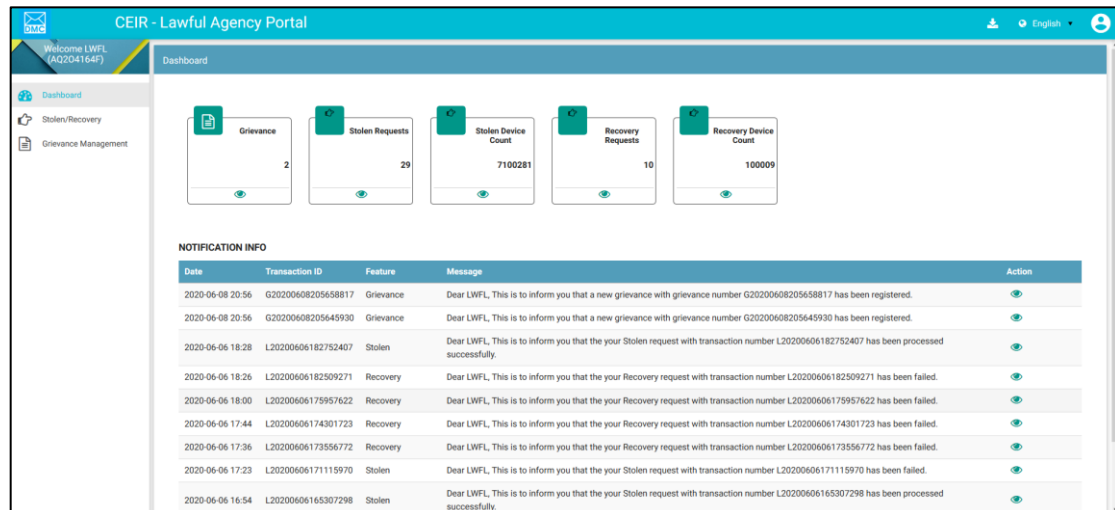


Figure 14: Home Page



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

To report an individual stolen device:

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

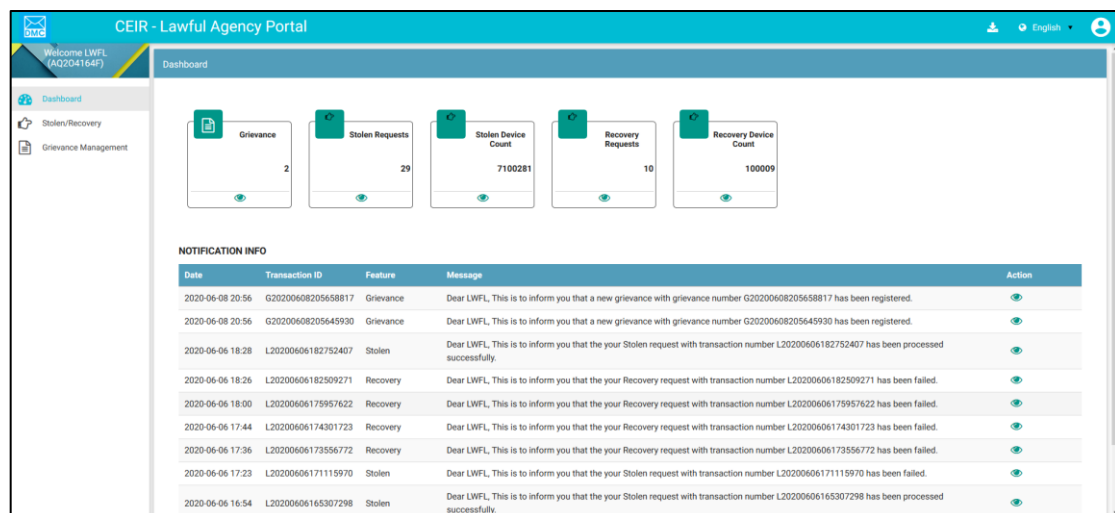


Figure 15: Home Page

The **Stolen/Recovery** dashboard appears.



Request Date	Transaction ID	Block Type	Request Type	Mode	Status	IMEI Quantity	Device Quantity	Action
2020-05-01 08:40	L20200501084025729	Immediate	Stolen	Individual	Rejected By System	1	1	
2020-04-28 07:51	L20200428075133929	Immediate	Recovery	Individual	Rejected By System	1	1	
2020-04-29 10:50	L20200429105027560	Immediate	Recovery	Company	New	12	3	
2020-05-07 12:43	L20200507124332432	Immediate	Stolen	Company	New	3	6	
2020-05-01 08:46	L20200501084637279	Immediate	Recovery	Company	Rejected By System	12	332	
2020-05-01 08:43	L20200501084317092	Immediate	Stolen	Company	Rejected By System	13213	3	
2020-04-27 09:29	L20200427092914740	Immediate	Stolen	Individual	New	1	1	
2020-04-29 10:48	L20200429104817825	Immediate	Stolen	Individual	Rejected By System	1	1	
2020-04-28 10:51	L20200428105150628	Immediate	Stolen	Individual	Rejected By System	1	0	
2020-04-29 10:39	L20200429103917861	Immediate	Stolen	Company	Rejected By System	1	0	

Figure 16: Stolen/Recovery

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

Report Stolen/Recovery

☒ Stolen ☐ Recovery

- Select **Stolen**.

Personal Information

First Name *
aaa

Middle Name
yadav

Last Name *
ss

Upload NID/Passport Image
 status.PNG

NID/Passport Number *
ZXCZCZCZCXCXZC

Email
ysharad2@gmail.com

Alternate Contact Number *
9675475886

Address(Property Location) *
aa, aa

Street Number *
aa

Village *
khatima

Locality *
delhi

District *
USN

Commune *
aa

Postal Code *
262308

Country *
Bahamas

Province *
Marsh Harbour



Device Information

Device Brand Name *

Apple

Device ID Type

Device ID Type

Device Type

Device Type

Contact Number *

1111111111111111

Contact Number 2

Contact Number 3

Contact Number 4

Multiple Sim Status

Multiple Sim Status

IMEI/MEID/ESN Number

1

123213213131231

3

Blocking Type

☒ Immediate ☐ Default ☐ Other

Model Number

i10

Operator *

Smart

Operator 2

Select Operator

Operator 3

Select Operator

Operator 4

Select Operator

Complaint Type *

Lost

Place Of Device Stolen

Address(Property Location) *

a

Street Number *

a

Locality *

a

Commune *

a

Country *

Qatar

Device Stolen Date *

2020-04-14

Remarks

Village *

a

District *

a

Postal Code *

123213

Province *

Ad Dawhah

Upload FIR

SELECT FILE

Required Field are marked with *

SUBMIT

CANCEL

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.

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 NID/Passport Image: Click **Select** to upload an image or pdf of the document.
- *NID/Passport Number: Enter the NID or passport number.




- *Email: Enter the mail ID.
- *Alternate Contact Number: Enter the mobile number.
- *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
 - MEID
 - ESN
- *Device Type: Select the type of device from the list.
- *Model Number: Enter the model number of the device.
- *Contact Number: Enter the contact number of the operator.
- *Operator: Select the operator name from the list.
- **Multiple SIM Status:** Select whether the device supports multiple SIM slots.
 - Yes
 - No
- *Complaint Type: Select the type of complaint (Lost, Stolen) from the list.
- **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 .
- **IMEI/MEID/ESN:** Enter the value of the IMEIs or MEIDs or ESNs 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.
- **Upload FIR:** Click **Select** to upload the FIR file.
- **Remark**

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.



Column	Description
Mode	Indicates whether the request is for an individual or company (Individual or Company). In this case, it is Individual.
Status	<ul style="list-style-type: none">• The request goes through the following status modes:<ul style="list-style-type: none">○ 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 administrator for review.○ Rejected by CEIR Admin: The CEIR administrator 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 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. For example, this could be done when the personnel have wrongly marked



Column	Description
	<p>a device as stolen, which has been recovered.</p> <ul style="list-style-type: none">○ 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.
Quantity	Refers to the number of devices reported stolen or recovered. A device can have multiple IMEIs/MEIDs/ESNs.
Action	<p>This displays different actions that can be performed on the request.</p> <ul style="list-style-type: none">• Error : An error file is generated if there is any problem in the request(s) submitted. Click to download the error file. Refer to <i>Figure 18</i> 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.



Column	Description
	<ul style="list-style-type: none">View 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/DeviceId	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

To report a stolen device:

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

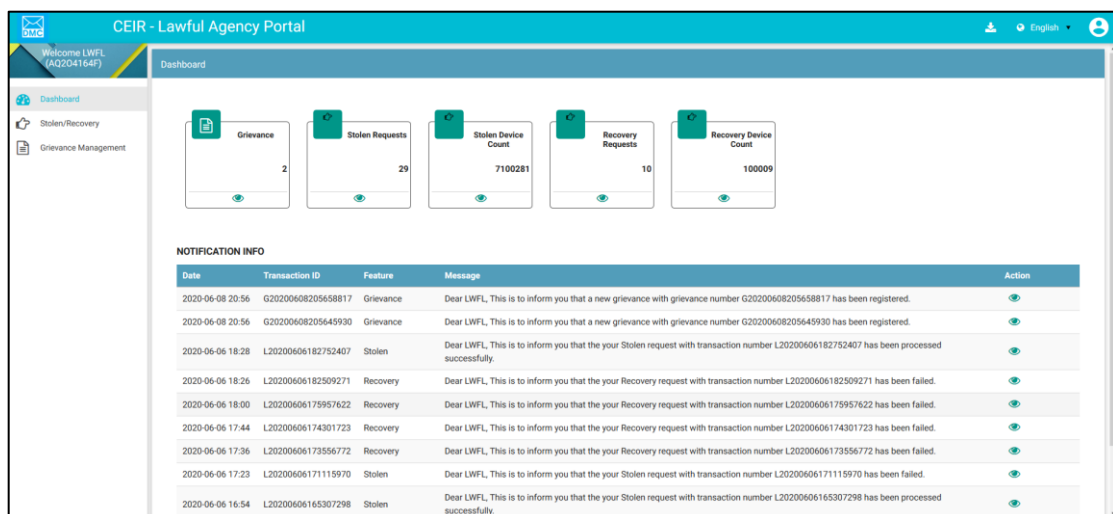


Figure 19: Home Page

The **Stolen/Recovery** dashboard appears.



Request Date	Transaction ID	Block Type	Request Type	Mode	Status	IMEI Quantity	Device Quantity	Action
2020-05-01 08:40	L20200501084025729	Immediate	Stolen	Individual	Rejected By System	1	1	[Action Icons]
2020-04-28 07:51	L20200428075133929	Immediate	Recovery	Individual	Rejected By System	1	1	[Action Icons]
2020-04-29 10:50	L20200429105027560	Immediate	Recovery	Company	New	12	3	[Action Icons]
2020-05-07 12:43	L20200507124332432	Immediate	Stolen	Company	New	3	6	[Action Icons]
2020-05-01 08:46	L20200501084637279	Immediate	Recovery	Company	Rejected By System	12	332	[Action Icons]
2020-05-01 08:43	L20200501084317092	Immediate	Stolen	Company	Rejected By System	13213	3	[Action Icons]
2020-04-27 09:29	L20200427092914740	Immediate	Stolen	Individual	New	1	1	[Action Icons]
2020-04-29 10:48	L20200429104817825	Immediate	Stolen	Individual	Rejected By System	1	1	[Action Icons]
2020-04-28 10:51	L20200428105150628	Immediate	Stolen	Individual	Rejected By System	1	0	[Action Icons]
2020-04-29 10:39	L20200429103917861	Immediate	Stolen	Company	Rejected By System	1	0	[Action Icons]

Figure 20: Stolen/Recovery

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

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

- Select **Stolen**.

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

INDIVIDUAL	COMPANY/ORGANISATION/GOVERNMENT
Company Name *	Address (Property Location) *
HCL	Noida
Street Number *	Village *
A101	Noida
Locality *	District *
Green Avenue	Noida
Commune *	Postal Code *
Noida	110033
Country *	Province *
India	Uttar Pradesh



Authorized personnel

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

Place Of Device Stolen

Address(Property Location) *	
Delhi	
Street Number *	Village *
Safdarjung	Delhi
Locality *	District *
Safdarjung	Delhi
Commune *	Postal Code *
Delhi	110089
Country *	Province *
India	Delhi
Complaint Type *	IMEI Quantity *
Stolen	1
Device Quantity *	Upload Device List *
1	<div>SELECT FILE Stock.csv</div>
Blocking Type	Device Stolen Date *
<input checked="" type="radio"/> Immediate <input type="radio"/> Default <input type="radio"/> Other	2020-04-01
Upload FIR	
<div>SELECT FILE</div>	

Upload FIR

SELECT FILE

Remark

Required Field are marked with *

[Download Sample Format](#)

SUBMIT

CANCEL

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

6. Enter the following information:

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



Authorized Personnel: 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
- Street Number
- 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	DeviceId	MultipleS	S/NofDevice	IMEI/ESN/MEID	DeviceLaunchdate	DeviceStatus
2	Smartphone	IMEI	Yes	3212	234562875785875	20-12-15	New
3	Smartphone	IMEI	Yes	43521	234562875785876	21-12-15	New
4	Smartphone	IMEI	Yes	414121	234562875785877	22-12-15	New
5	Smartphone	IMEI	Yes	8968687	234562875785878	23-12-15	New
6	Smartphone	IMEI	Yes	576476	234562875785879	24-12-15	New
7							

- **Blocking Type**

- 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 administrator.
- Later: The device(s) is sent to the blacklist at the specified date. Select the date using the calendar .

- **Upload FIR:** Click **Select** to upload the FIR file.

- **Remark**

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	<ul style="list-style-type: none">• The request goes through the following status modes:<ul style="list-style-type: none">○ New: When a request is raised, the status is New.○ Processing: The request is verified internally.



Column	Description
	<ul style="list-style-type: none">○ 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 administrator for review.○ Rejected by CEIR Admin: The CEIR administrator 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.○ 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. 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.
Quantity	Refers to the number of devices reported stolen. A device can have multiple IMEIs/MEIDs/ESNs.



Column	Description
Action	<p>This displays different actions that can be performed on the request.</p> <ul style="list-style-type: none">• Error : An error file is generated if there is any problem in the request(s) submitted. Click to download the error file. Refer to <i>Figure 18</i> 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.• 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.• View 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

To report an individual recovered device:

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

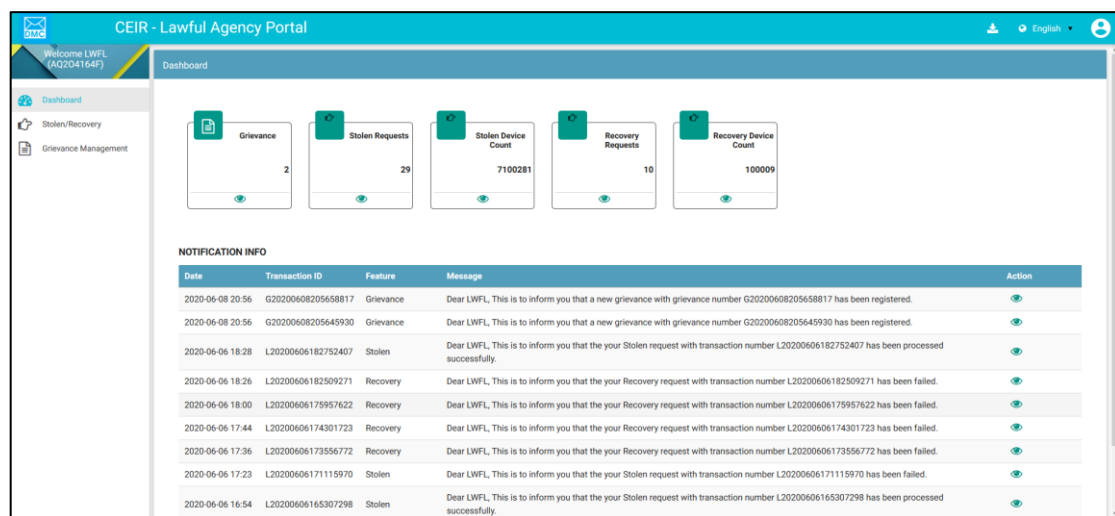


Figure 22: Home Page

The **Stolen/Recovery** dashboard appears.

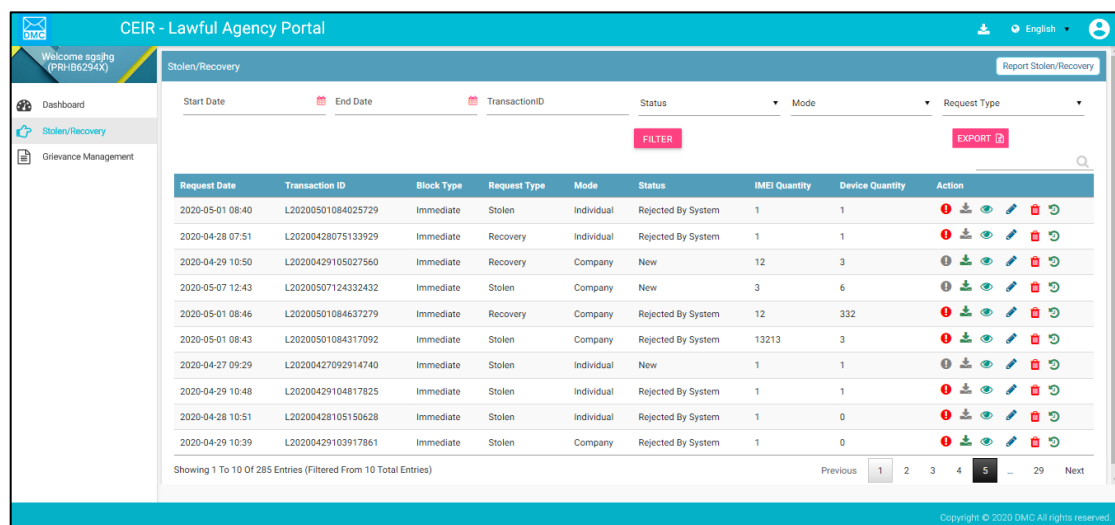


Figure 23: Stolen/Recovery



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

Report Stolen/Recovery

☐ Stolen ☐ Recovery

3. Select **Recovery**.

Device Brand Name
Select Brand Name

Model Number
Select Model Number

Device ID Type *
MEID

Device Type
Device Type

Multiple Sim Status
Multiple Sim Status

Device Serial Number

IMEI/MEID/ESN Number
1
8888888888888888

2

3

4

Place Of Device Recovery

Address(Property Location) *

a

Street Number *

a

Village *

a

Locality *

a

District *

a

Commune *

a

PostalCode *

111111

Country *

Afghanistan

Province *

Badakhshan

Remarks

Device Recovery Date *

2020-04-23

Required Field are marked with *

SUBMIT CANCEL

Figure 24: Report Recovery (Individual)

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.
- **Model Number:** Enter the device model number.
- ***Device ID Type:** Select the ID type to be entered for the device:
 - IMEI



- MEID
 - ESN
- **Device Type:** Select the type of device recovered.
- **Multiple SIM Status:** Select whether the device supports multiple SIM slots:
 - Yes
 - No
- **Device Serial Number:** Enter the device serial number.
- ***IMEI/MEID/ESN:** Enter the IMEI or MEID or ESN 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.





For each request, the dashboard displays the following information:

Column	Description
Date	Date of registering the request to recover the device.




Column	Description
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	<ul style="list-style-type: none">• The request goes through the following status modes:<ul style="list-style-type: none">○ 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 administrator for review.○ Rejected by CEIR Admin: The CEIR administrator 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.○ Approved by CEIR Admin: When the CEIR administrator approves the request,



Column	Description
	<p>the status changes to Approved by CEIR Admin.</p> <ul style="list-style-type: none">○ Withdrawn by CEIR Admin: When the CEIR administrator 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/MEIDs/ESNs.
Action	<p>This displays different actions that can be performed on the request.</p> <ul style="list-style-type: none">• 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 System or Rejected by CEIR Admin. Click on it to modify the request details.



Column	Description
	<ul style="list-style-type: none">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.View 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.

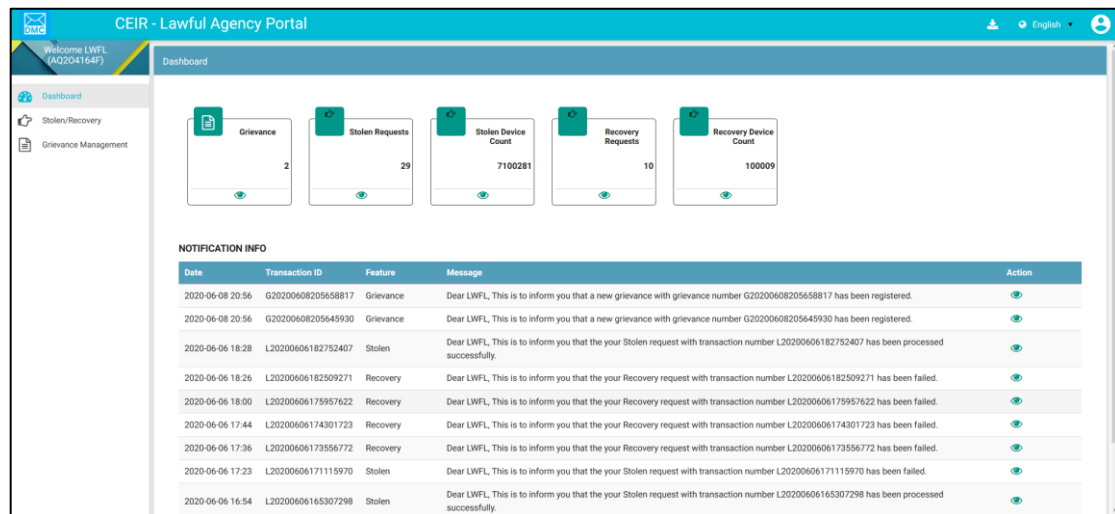


Figure 25: Home Page

The **Stolen/Recovery** dashboard appears.



Request Date	Transaction ID	Block Type	Request Type	Mode	Status	IMEI Quantity	Device Quantity	Action
2020-05-01 08:40	L20200501084025729	Immediate	Stolen	Individual	Rejected By System	1	1	[Icons]
2020-04-28 07:51	L20200428075133929	Immediate	Recovery	Individual	Rejected By System	1	1	[Icons]
2020-04-29 10:50	L20200429105027560	Immediate	Recovery	Company	New	12	3	[Icons]
2020-05-07 12:43	L20200507124332432	Immediate	Stolen	Company	New	3	6	[Icons]
2020-05-01 08:46	L20200501084637279	Immediate	Recovery	Company	Rejected By System	12	332	[Icons]
2020-05-01 08:43	L20200501084317092	Immediate	Stolen	Company	Rejected By System	13213	3	[Icons]
2020-04-27 09:29	L20200427092914740	Immediate	Stolen	Individual	New	1	1	[Icons]
2020-04-29 10:48	L20200429104817825	Immediate	Stolen	Individual	Rejected By System	1	1	[Icons]
2020-04-28 10:51	L20200428105150628	Immediate	Stolen	Individual	Rejected By System	1	0	[Icons]
2020-04-29 10:39	L20200429103917861	Immediate	Stolen	Company	Rejected By System	1	0	[Icons]

Figure 26: Stolen/Recovery

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

- Select **Recovery**.

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

Quantity * 12
Device Quantity * 3
Remarks
Upload File
SELECT FILE con_2_rec (1) (1).csv
Download Sample Format

Place Of Device Recovery
Address(Property Location) * sharad
Street Number * new ashok nagar, del
Locality * kk
Commune * delhi
Country * India
Device Recovery Date * 2020-04-23
Village * village
District * sdsadf
Postal Code * 110096
Province * Delhi

Required Field are marked with *

SUBMIT CANCEL

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


- 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/MEIDs/ESNs.
- **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.

- **Remarks**

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

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



Column	Description
Mode	Indicates whether the request is for an individual or company (Individual or Company). In this case, it is Company.
Status	<ul style="list-style-type: none">• The request goes through the following status modes:<ul style="list-style-type: none">○ 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 administrator for review.○ Rejected by CEIR Admin: The CEIR administrator 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 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. For example, this could be done when the personnel have wrongly marked



Column	Description
	<p>a device as stolen, which has been recovered.</p> <ul style="list-style-type: none">○ 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 device can have multiple IMEIs/MEIDs/ESNs.
Action	<p>This displays different actions that can be performed on the request.</p> <ul style="list-style-type: none">• 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 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.



Column	Description
	<ul style="list-style-type: none">View 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.

The screenshot shows the 'Stolen/Recovery' portal interface. At the top, there are filters for Start Date, End Date, TransactionID, Rejected By System, Mode, and Request Type, along with 'FILTER' and 'EXPORT' buttons. Below the filters is a table with the following columns: Request Date, Transaction ID, Block Type, Request Type, Mode, Status, IMEI Quantity, Device Quantity, and Action. The table contains several rows of data. In the 'Action' column, there are icons for 'View', 'Edit', 'Cancel', and 'Refresh'. The 'Edit' icon (a blue pencil) is highlighted with a yellow box in the first row of the table.

Request Date	Transaction ID	Block Type	Request Type	Mode	Status	IMEI Quantity	Device Quantity	Action
2020-05-01 08:40	L20200501084025729	Immediate	Stolen	Individual	Rejected By System	1	1	
2020-04-28 07:51	L20200428075133929	Immediate	Recovery	Individual	Rejected By System	1	1	
2020-04-29 10:50	L20200429105027560	Immediate	Recovery	Company	New	12	3	
2020-05-07 12:43	L20200507124332432	Immediate	Stolen	Company	New	3	6	
2020-05-01 08:46	L20200501084637279	Immediate	Recovery	Company	Rejected By System	12	332	
2020-05-01 08:43	L20200501084317092	Immediate	Stolen	Company	Rejected By System	13213	3	
2020-04-27 09:29	L20200427092914740	Immediate	Stolen	Individual	New	1	1	
2020-04-29 10:48	L20200429104817825	Immediate	Stolen	Individual	Rejected By System	1	1	
2020-04-28 10:51	L20200428105150628	Immediate	Stolen	Individual	Rejected By System	1	0	

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 administrator.

To filter device requests:

The screenshot shows a web interface titled "Stolen/Recovery" with a "Report Stolen/Recovery" button. Below the header is a filter bar with fields for "Start Date", "End Date", "TransactionID", "Rejected By System", "Mode", and "Request Type". There are "FILTER" and "EXPORT" buttons. Below the filter bar is a table with the following columns: Request Date, Transaction ID, Block Type, Request Type, Mode, Status, IMEI Quantity, Device Quantity, and Action. The table contains 10 rows of data.

Request Date	Transaction ID	Block Type	Request Type	Mode	Status	IMEI Quantity	Device Quantity	Action
2020-05-01 08:40	L20200501084025729	Immediate	Stolen	Individual	Rejected By System	1	1	[Icons]
2020-04-28 07:51	L20200428075133929	Immediate	Recovery	Individual	Rejected By System	1	1	[Icons]
2020-04-29 10:50	L20200429105027560	Immediate	Recovery	Company	New	12	3	[Icons]
2020-05-07 12:43	L20200507124332432	Immediate	Stolen	Company	New	3	6	[Icons]
2020-05-01 08:46	L20200501084637279	Immediate	Recovery	Company	Rejected By System	12	332	[Icons]
2020-05-01 08:43	L20200501084317092	Immediate	Stolen	Company	Rejected By System	13213	3	[Icons]
2020-04-27 09:29	L20200427092914740	Immediate	Stolen	Individual	New	1	1	[Icons]
2020-04-29 10:48	L20200429104817825	Immediate	Stolen	Individual	Rejected By System	1	1	[Icons]
2020-04-28 10:51	L20200428105150628	Immediate	Stolen	Individual	Rejected By System	1	0	[Icons]

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.

Request Date	Transaction ID	Block Type	Request Type	Mode	Status	IMEI Quantity	Device Quantity	Action
2020-05-01 08:40	L20200501084025729	Immediate	Stolen	Individual	Rejected By System	1	1	[Icons]
2020-04-28 07:51	L20200428075133929	Immediate	Recovery	Individual	Rejected By System	1	1	[Icons]
2020-05-01 08:46	L20200501084637279	Immediate	Recovery	Company	Rejected By System	12	332	[Icons]
2020-05-01 08:43	L20200501084317092	Immediate	Stolen	Company	Rejected By System	13213	3	[Icons]
2020-04-29 10:48	L20200429104817825	Immediate	Stolen	Individual	Rejected By System	1	1	[Icons]
2020-04-28 10:51	L20200428105150628	Immediate	Stolen	Individual	Rejected By System	1	0	[Icons]
2020-04-29 10:39	L20200429103917861	Immediate	Stolen	Company	Rejected By System	1	0	[Icons]
2020-04-28 10:44	L20200428104426899	Immediate	Stolen	Individual	Rejected By System	1	0	[Icons]
2020-04-28 08:51	L20200428085143242	Immediate	Recovery	Individual	Rejected By System	1	0	[Icons]

Figure 30: Filtered Requests

2.8 Exporting Stolen or Recovered Device Requests

Personnel 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** page, click **Export**.

Request Date	Transaction ID	Block Type	Request Type	Mode	Status	IMEI Quantity	Device Quantity	Action
2020-05-01 08:40	L20200501084025729	Immediate	Stolen	Individual	Rejected By System	1	1	[Icons]
2020-04-28 07:51	L20200428075133929	Immediate	Recovery	Individual	Rejected By System	1	1	[Icons]
2020-04-29 10:50	L20200429105027560	Immediate	Recovery	Company	New	12	3	[Icons]
2020-05-07 12:43	L20200507124332432	Immediate	Stolen	Company	New	3	6	[Icons]
2020-05-01 08:46	L20200501084637279	Immediate	Recovery	Company	Rejected By System	12	332	[Icons]
2020-05-01 08:43	L20200501084317092	Immediate	Stolen	Company	Rejected By System	13213	3	[Icons]
2020-04-27 09:29	L20200427092914740	Immediate	Stolen	Individual	New	1	1	[Icons]
2020-04-29 10:48	L20200429104817825	Immediate	Stolen	Individual	Rejected By System	1	1	[Icons]
2020-04-28 10:51	L20200428105150628	Immediate	Stolen	Individual	Rejected By System	1	0	[Icons]

Figure 31: Stolen/Recovery

The following page appears.

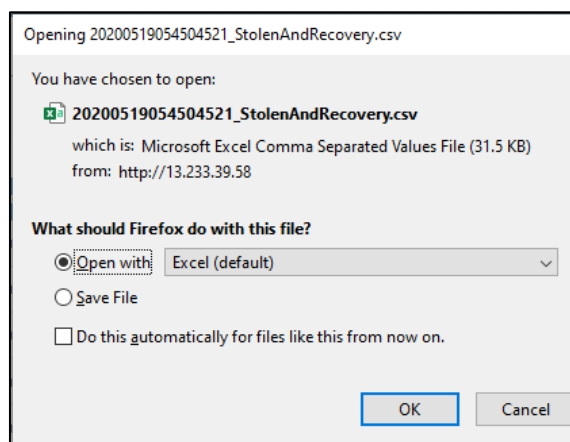


Figure 32: Open or Save Stolen/Recovery File

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

	A	B	C	D	E	F	G	H
1	Created On	Modified On	Txn Id	Request Type	Mode	Status	Filename	Device Quantity
2	16-06-20 14:47	16-06-20 14:48	L20200616144746002	Stolen	Company	Rejected By Sy	con_1_rec.csv	1
3	16-06-20 15:38	16-06-20 15:39	L20200616153846891	Stolen	Company	Rejected By Sy	stk_1_rec.csv	1
4	16-06-20 18:43	16-06-20 18:44	L20200616184306919	Recovery	Company	Rejected By Sy	stk_1_rec.csv	1
5	17-06-20 15:41	17-06-20 15:41	L20200617154115232	Recovery	Company	Rejected By Sy	Stock (22).csv	2
6	15-06-20 16:46	15-06-20 17:00	L20200615164651727	Recovery	Company	Rejected By Sy	100k IMEI 999995	60454

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.

2.9 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 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 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 personnel for a specified period.

To raise a grievance

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

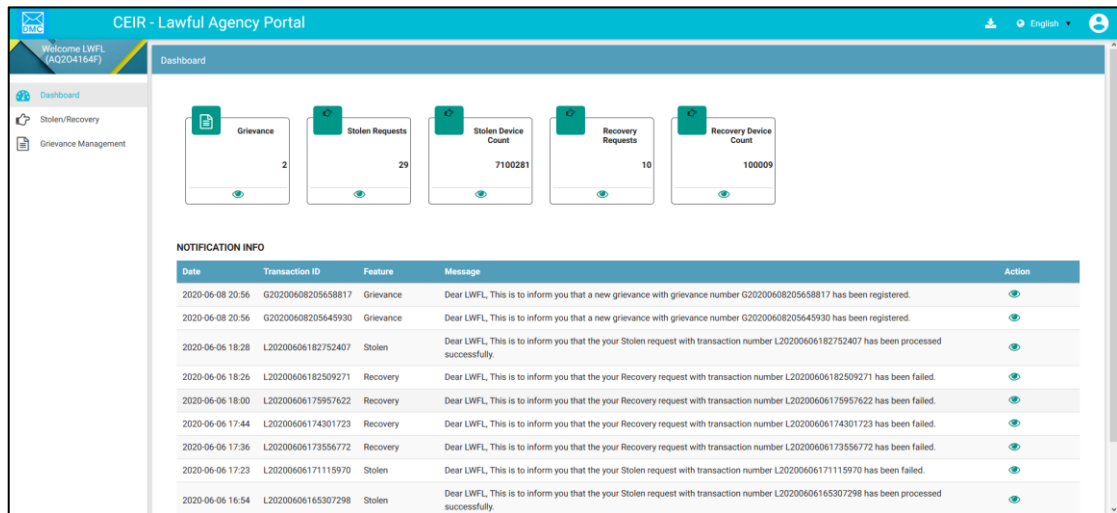


Figure 34: Home Page

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

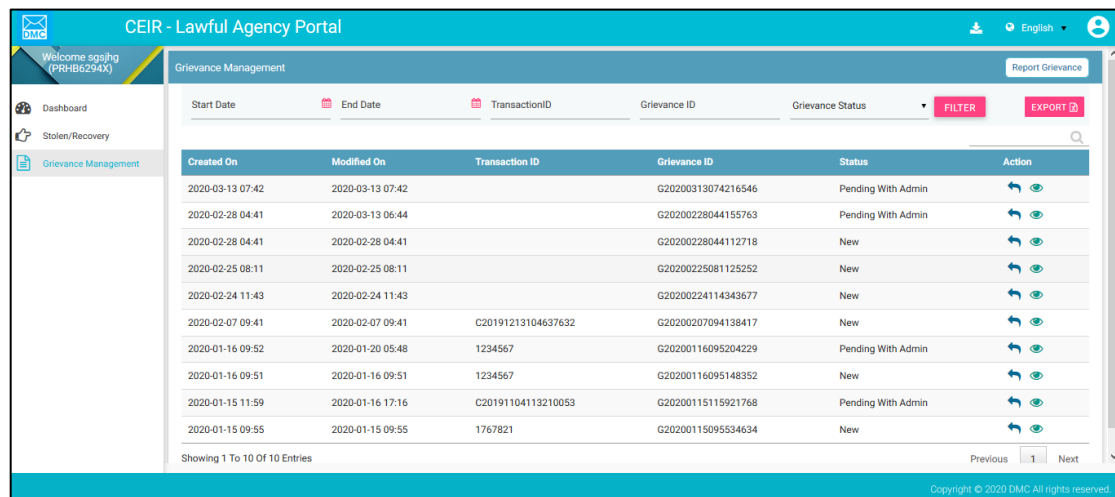


Figure 35: Grievance Management



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 the administrator 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.



Submit Grievance Report

Your grievance report has been successfully submitted. Your Grievance Id is (G20200311090008702)

(Note: Please remember your grievance Id. This is used for future reference)

OK

The new grievance appears on the top of the page.



Grievance Management						Report Grievance
Start Date	End Date	TransactionID	Grievance ID	Grievance Status		FILTER EXPORT
						Q
Raised Date	Modified On	Transaction ID	Grievance ID	Grievance Status	Action	
2020-03-11 09:00	2020-03-11 09:00		G20200311090008702	New		

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	<p>The uploaded grievance goes through different status modes.</p> <ul style="list-style-type: none">• 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 personnel.• Closed: When the CEIR administrator closes the grievance.



Column	Description
Action	<p>This displays different actions that can be performed on a grievance.</p> <ul style="list-style-type: none">Reply : This is used to respond to the grievance. The response is given by the CEIR administrator 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.

2.10 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 administrator. Similarly, one can view only those grievances that are closed.

To filter grievances:

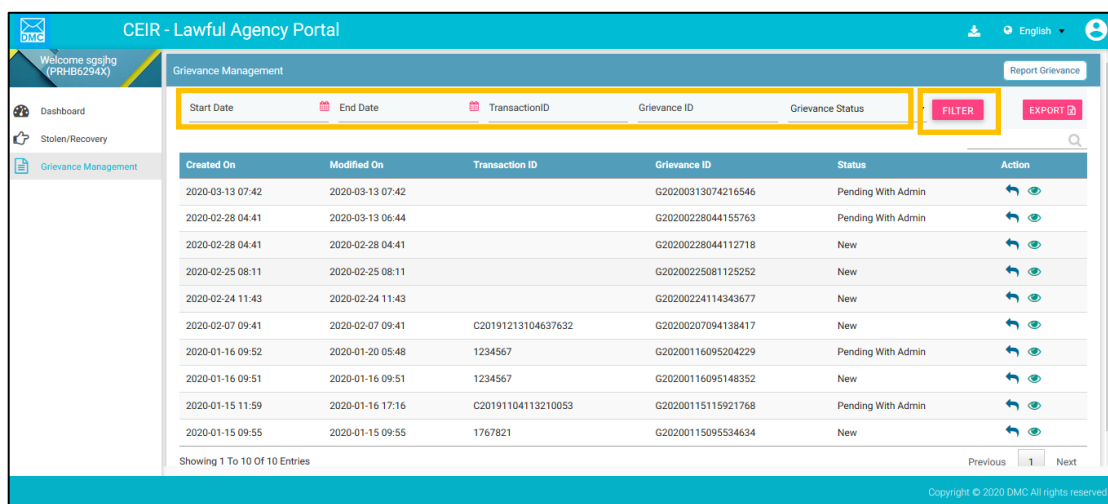


Figure 38: Filter Grievances

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

2. Click **Filter**.

The filtered grievances are shown on the page.

The screenshot shows the 'Grievance Management' interface. At the top, there are filters for 'Start Date' (2020-02-01), 'End Date' (2020-05-01), 'TransactionID', 'Grievance ID', and 'Grievance Status'. There are 'FILTER' and 'EXPORT' buttons. Below the filters is a table with the following data:

Created On	Modified On	Transaction ID	Grievance ID	Status	Action
2020-03-13 07:42	2020-03-13 07:42		G20200313074216546	Pending With Admin	
2020-02-28 04:41	2020-03-13 06:44		G20200228044155763	Pending With Admin	
2020-02-28 04:41	2020-02-28 04:41		G20200228044112718	New	
2020-02-25 08:11	2020-02-25 08:11		G20200225081125252	New	
2020-02-24 11:43	2020-02-24 11:43		G20200224114343677	New	
2020-02-07 09:41	2020-02-07 09:41	C20191213104637632	G20200207094138417	New	

Showing 1 To 6 Of 6 Entries

Previous 1 Next

Figure 39: Filtered Grievances

2.11 Exporting 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).



Created On	Modified On	Transaction ID	Grievance ID	Status	Action
2020-03-13 07:42	2020-03-13 07:42		G20200313074216546	Pending With Admin	↶ 👁
2020-02-28 04:41	2020-03-13 06:44		G20200228044155763	Pending With Admin	↶ 👁
2020-02-28 04:41	2020-02-28 04:41		G20200228044112718	New	↶ 👁
2020-02-25 08:11	2020-02-25 08:11		G20200225081125252	New	↶ 👁
2020-02-24 11:43	2020-02-24 11:43		G20200224114343677	New	↶ 👁
2020-02-07 09:41	2020-02-07 09:41	C20191213104637632	G20200207094138417	New	↶ 👁
2020-01-16 09:52	2020-01-20 05:48	1234567	G20200116095204229	Pending With Admin	↶ 👁
2020-01-16 09:51	2020-01-16 09:51	1234567	G20200116095148352	New	↶ 👁
2020-01-15 11:59	2020-01-16 17:16	C20191104113210053	G20200115115921768	Pending With Admin	↶ 👁
2020-01-15 09:55	2020-01-15 09:55	1767821	G20200115095534634	New	↶ 👁

Figure 40: Grievance Management

The following page appears.

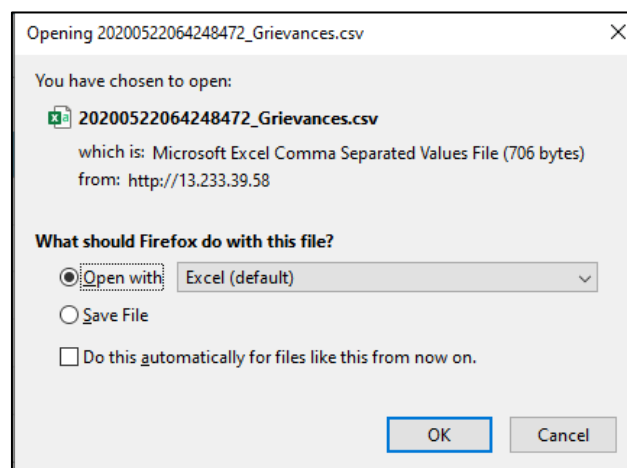


Figure 41: Open or Save Exported Grievance File

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

	A	B	C	D	E	F	G
1	GRIEVANCE_ID	GRIEVANCE_STATUS	CREATED_ON	MODIFIED_ON	CATEGORY	REMARKS	FILE_NAME
2	G20200616103003674	Pending With Admin	16-06-20 10:30	16-06-20 10:31	Stolen/Recovery Related	cc	Consignment (34).csv
3	G20200615081405453	Pending With User	15-06-20 8:14	15-06-20 8:21	Stolen/Recovery Related	Testing 2	null
4	G20200615081354318	Pending With User	15-06-20 8:13	15-06-20 8:19	Stolen/Recovery Related	Testing	null

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.