Central Equipment Identity Register Portal

Operator User Manual v 2.0

Document Change History

Version	Change Type	Description	Date
Draft		Submitted for internal review	February 2020
Final		Final version	April 2020

Copyright @ 2020 DMC All Rights Reserved

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 11

2.3.1 Dashboard 13

2.4 Block/Unblock Devices 17

2.4.1 Single Device Blocking/Unblocking 17

2.4.2 Bulk Device Blocking/Unblocking 22

2.5 Edit Block/Unblock Device Requests 25

2.6 Filter Block/Unblock Device Requests 27

2.7 Export Block/Unblock Device Requests 28

2.8 Greylist 29

2.9 Filter Greylist 32

2.10 Export Greylist 34

2.11 Blacklist 35

2.12 Filter Blacklist 38

2.13 Export Blacklist 40

2.14 Grievance Management 41

2.15 Filter Grievances 45

2.16 Export Grievances 46

Copyright @ 2020 DMC All Rights Reserved

Figures

Figure 1: DMC Home Page 3
Figure 2: Operator Registration 4
Figure 3: Verify OTP 6
Figure 4: Enter OTP 7
Figure 5: Login 8
Figure 6: Home Page 9
Figure 7: Forgot Password 9
Figure 8: Set New Password 10
Figure 9: Home Page 11
Figure 10: Edit Information 12
Figure 11: Change Password 12
Figure 12: Manage Account 13
Figure 13: Home Page 14
Figure 14: Block/Unblock Devices 14
Figure 15: Block/Unblock Devices 15
Figure 16: Grievance Management 16
Figure 17: Home Page 16
Figure 18: Home Page 18
Figure 19: Block/Unblock Devices 18
Figure 20: Report Block 19
Figure 21: Report Block 23
Figure 22: Block/Unblock Devices 23
Figure 23: Report Block 24
Figure 24: Block/Unblock Devices 26
Figure 25: Edit Block Device (Single Device) 26
Figure 26: Edit Block Device (Bulk Device) 26
Figure 27: Block/unblock Devices 27
Figure 28: Filtered Device Block/Unblock Requests 27
Figure 29: Block/Unblock Devices 28
Figure 30: Open or Save Exported Block/Unblock Devices File 29
Figure 31: Exported Block/Unblock Devices 29
Figure 32: Home Page 30
Figure 33: Grey List 30
Figure 34: Grey List 32
Figure 35: Filtered Greylists 33
Figure 36: Grey List 34
Figure 37: Open or Save Exported Greylists 34
Figure 38: Exported Greylists 35
Figure 39: Home Page 35
Figure 40: Black List 36
Figure 41: Black List 38
Figure 42: Filtered Blacklists 39
Figure 43: Black List 40
Figure 44: Open or Save Exported Blacklist File 40
Figure 45: Exported Blacklists 41
Figure 46: Home Page 42
Figure 47: Grievance Management 42
Figure 48: Report Grievance 42
Figure 49: Grievance Management 43
Figure 50: Filter Grievances 45
Figure 51: Filtered Grievances 46
Figure 52: Grievance Management 47
Figure 53: Open or Save Exported Grievance File 47

Copyright @ 2020 DMC All Rights Reserved

Figure 54: Exported Grievances 47

Copyright @ 2020 DMC All Rights Reserved

1 Overview

1.1 Scope

The objective of this manual is to help operators block and unblock devices (IMEIs/MEIDs/ESNs), download greylisted and blacklisted numbers, update their internal EIR systems, 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)	*Italics*

Copyright @ 2020 DMC All Rights Reserved

Information	Convention
*	Indicates a mandatory field or column

Copyright @ 2020 DMC All Rights Reserved

2 Operations

2.1 Application Overview

The CEIR (Central Equipment Identity Register) Operator Portal application is used to block devices that violate the operator contract agreement. The devices that are blocked can be unblocked as well using the application. Operators can raise grievances to the CEIR administrator whenever there is any problem.

Operators can use the application to perform the following tasks:

- Block devices
- Unblock devices
- Download greylists for monitoring devices
- Download blacklists for blocking devices
- Report grievances

2.2 Logging into the Application

Before login, operators need to register in the application. Employee or operator personnel register on the CEIR portal on behalf of an operator.

To register:

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

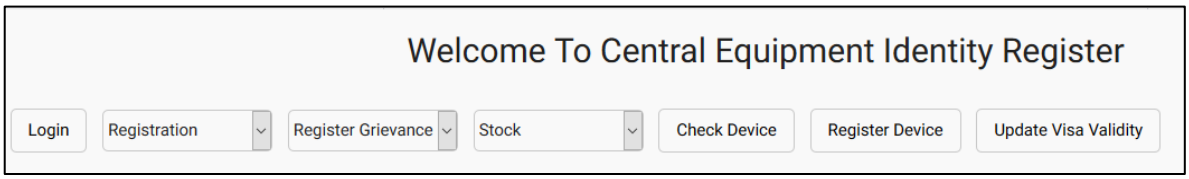
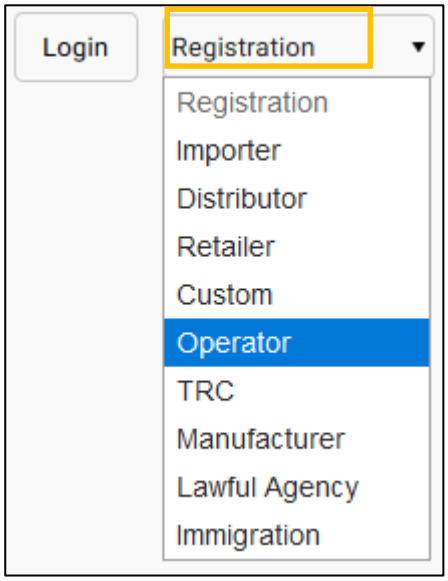


Figure 1: DMC Home Page

2. Select **Operator** from the **Registration** list.

Copyright @ 2020 DMC All Rights Reserved



The **Operator Registration** page appears. The operator needs to enter the following information.

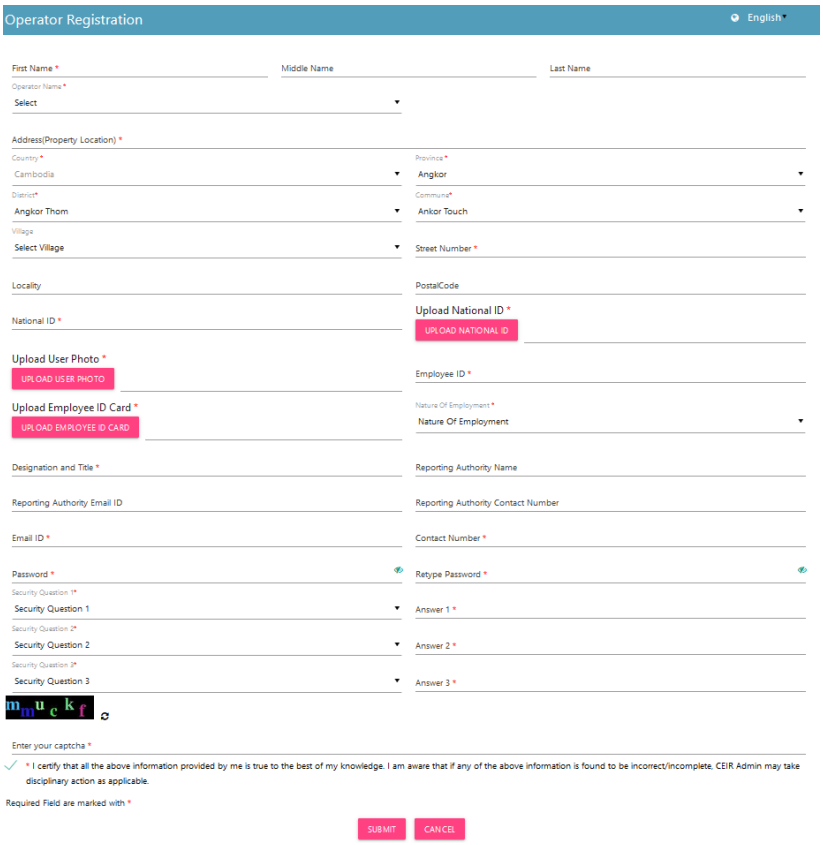


Figure 2: Operator Registration

3. ***First Name**: Enter the first name.
4. **Middle Name**: Enter the middle name (if any).

Copyright @ 2020 DMC All Rights Reserved

5. ***Last Name**: Enter the last name.
6. ***Type**: Select the operator type:
    - Metfone
    - Smart
    - Seatel
    - Cellcard
7. **Address**: Enter the operator's address:
    - Street Number
    - Village
    - Locality
    - District
    - Commune
    - Province
    - Country
8. ***National ID:** Enter the national ID of operator personnel.
9. ***Upload National ID**: Upload the image of the original national ID of operator personnel. This can be a pdf or image (.jpeg) of size not more than 2 MB.
10. **Upload Photo**: Upload the photograph of the operator personnel. The photograph can be a pdf or image (.jpeg) of size not more than 2 MB.
11. **Employee ID**: Enter the employee ID of the operator.
12. **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.
13. **Nature of Employment**: Select the type of employment of the operator personnel:
    - Permanent
    - Temporary
    - Contract
14. **Designation and Title**: Enter the designation of the operator's personnel.
15. **Reporting Authority Name**: Enter the name of the officer to whom the operator's personnel reports to.

Copyright @ 2020 DMC All Rights Reserved

16. **Reporting Authority Email ID**: Enter the mail ID of the officer to whom the operator's personnel reports to.
17. **Reporting Authority Contact Number**: Enter the contact number of the officer to whom the operator personnel reports to.
18. **Email**: Enter the mail ID of operator's personnel. This mail ID would be used for communication with the operator.
19. ***Contact Number**: Enter the mobile number of operator's personnel. Operators receive notifications at this mobile number.
20. ***Password**: Enter a login password. This is the password that would be used to log into the CEIR Operator Portal application.
21. ***Confirm Password**: Re-enter the password for confirmation.
22. *Select three security questions and enter an answer for each question. This is required by the system when the operator forgets the login password. In such a situation, the system requires some type of identification to authenticate the operator. The security questions are used to identify and authenticate the operator.
23. *Enter the captcha shown on the page. This is required to prove to the system that the operator is not a robot.
24. *Select the declaration check box.
25. Click **SUBMIT**.

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

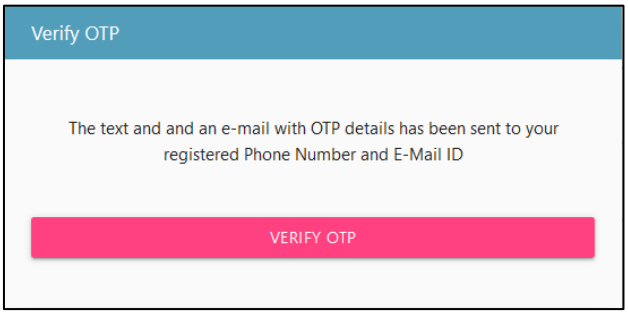


Figure 3: Verify OTP

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

Copyright @ 2020 DMC All Rights Reserved

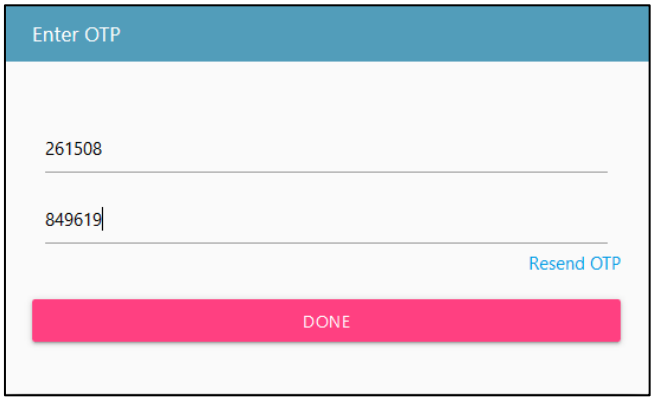
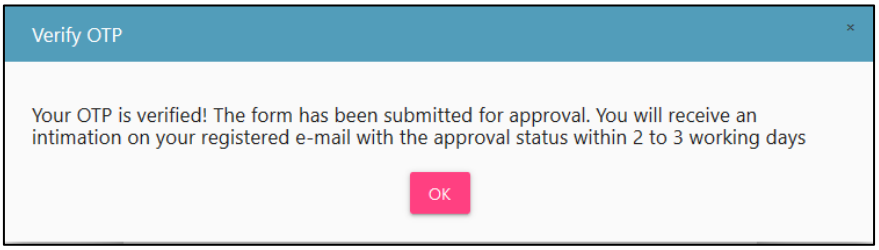


Figure 4: Enter OTP

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 operator's personnel mail account. The registration ID is a unique automatically generated ID. The ID is the login username for access to the CEIR Operator 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.

Copyright @ 2020 DMC All Rights Reserved

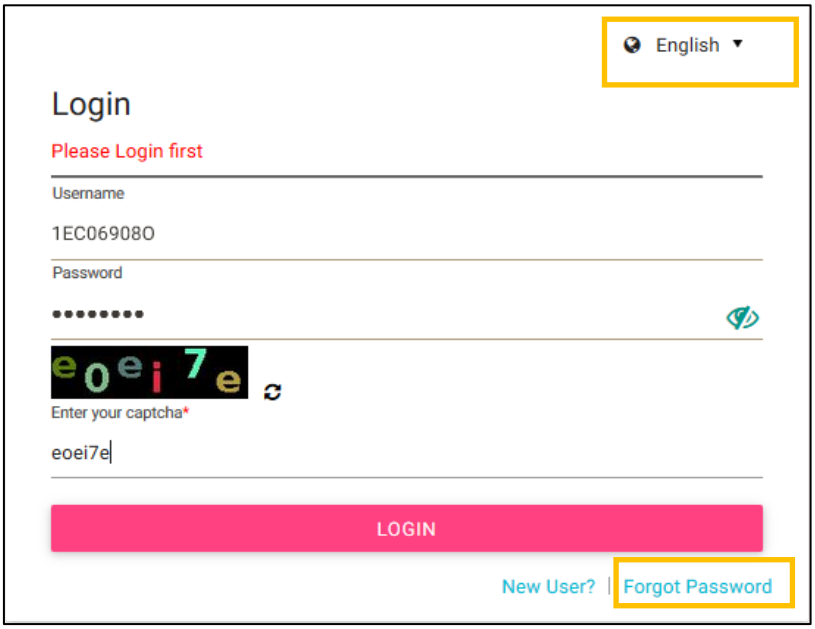
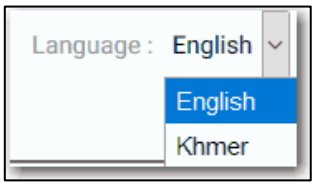


Figure 5: Login

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 username and password.

Username is the registration ID that is sent on mail to the operator after successful registration in the system. Username is a unique ID that is automatically generated by the system. The login password is the password that the operator enters in the registration page. Refer to during *Figure 2: Operator 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 operator is prompted to re-enter the login details.

On entering correct information, the application Home page appears.

Copyright @ 2020 DMC All Rights Reserved

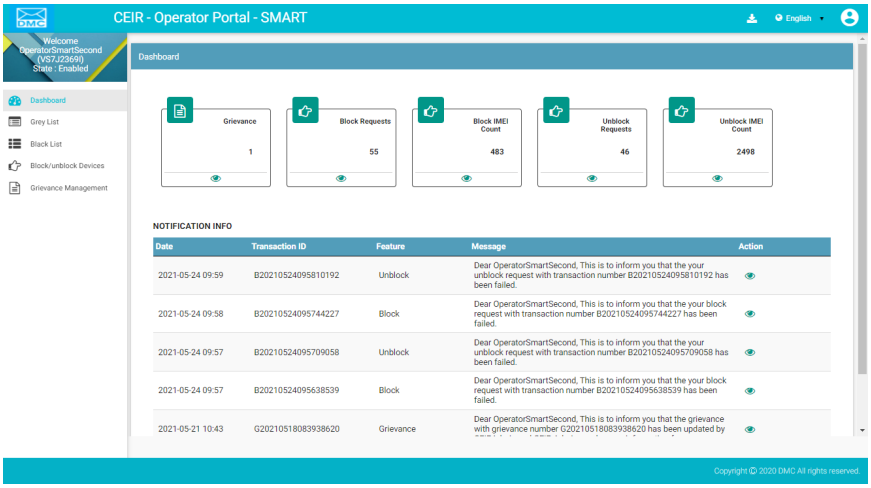


Figure 6: Home Page

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

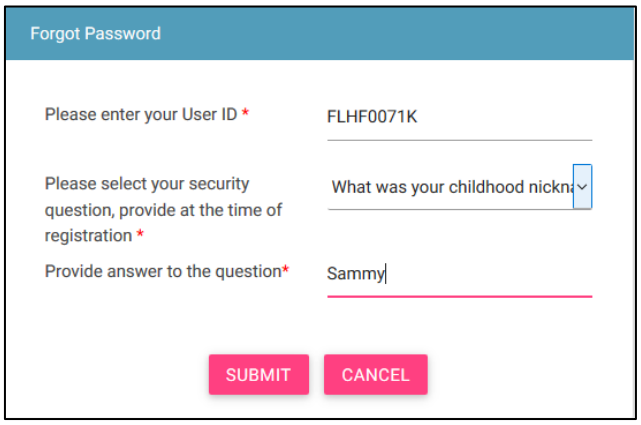


Figure 7: Forgot Password

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

The **Set New Password** page appears.

Copyright @ 2020 DMC All Rights Reserved

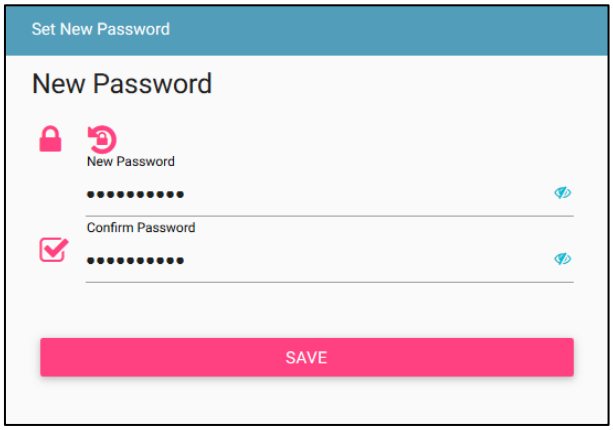


Figure 8: Set New Password

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 Operator Portal Home page appears.

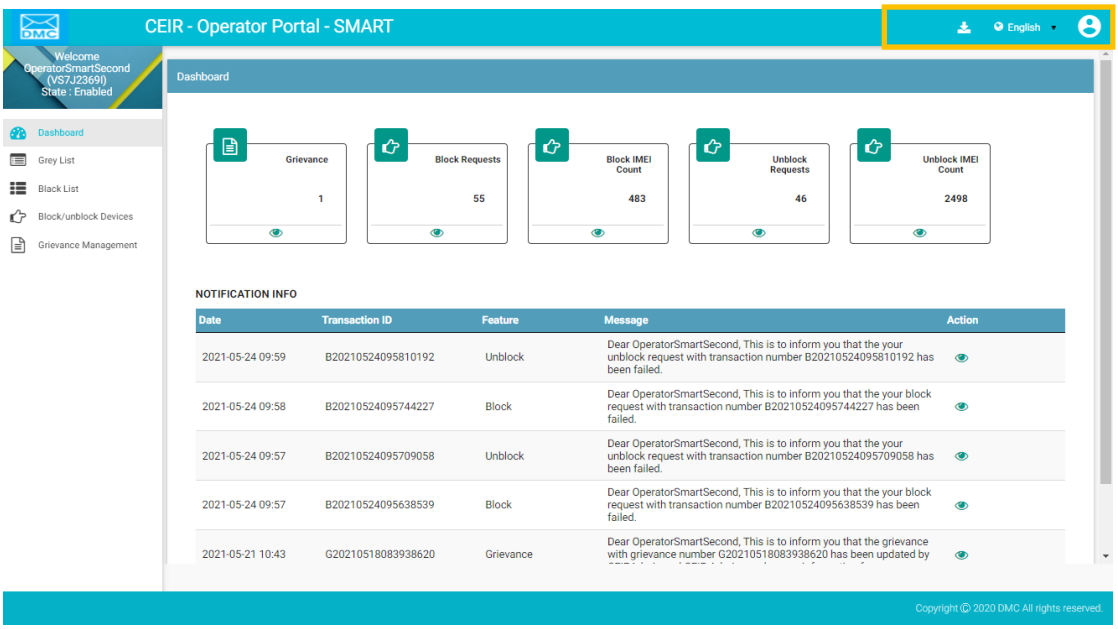


Figure 9: Home Page

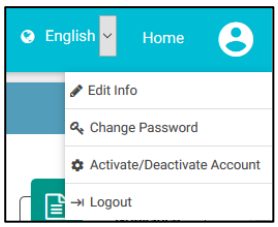
The Home page has all the feature menus on the left panel.

The center of the page is the Dashboard.

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

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

- (**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.

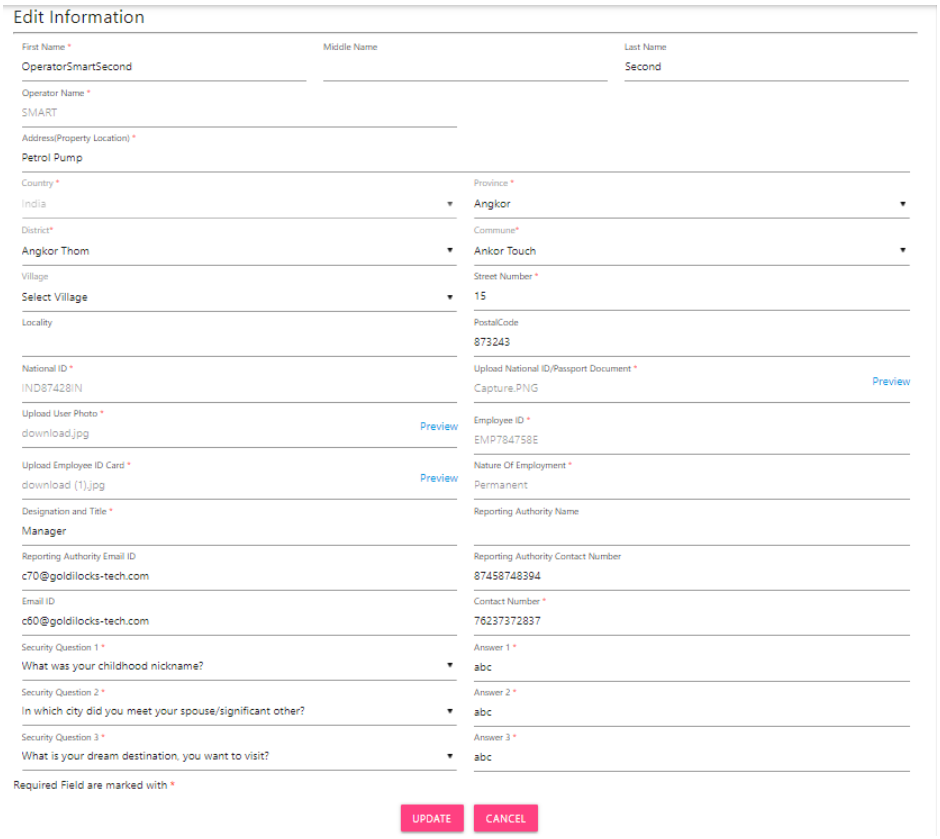


Figure 10: Edit Information

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

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

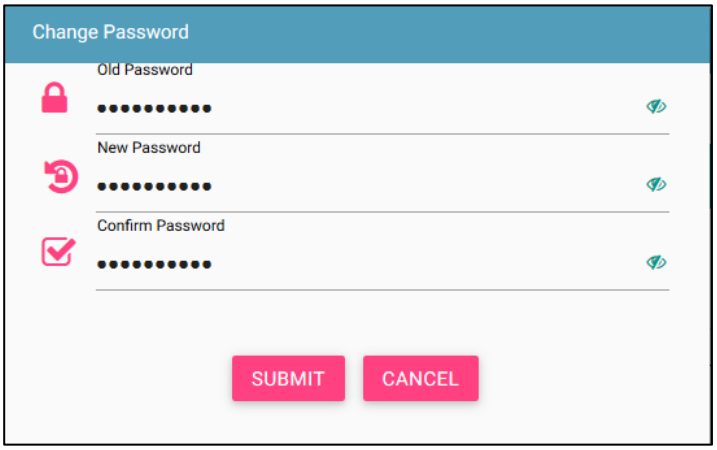


Figure 11: Change Password

Copyright @ 2020 DMC All Rights Reserved

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

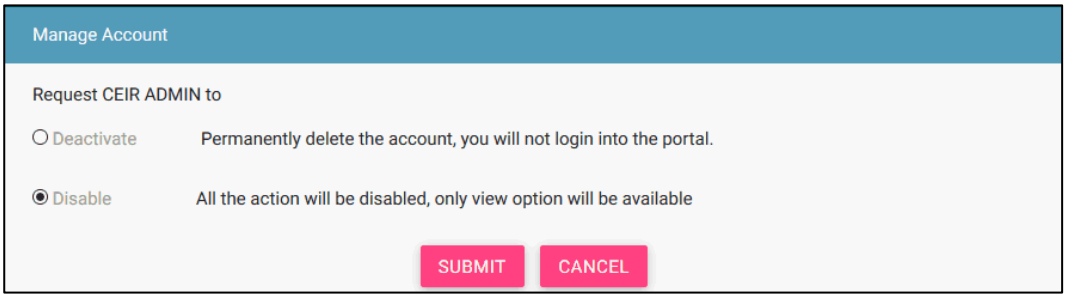


Figure 12: Manage Account

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

2.4 Dashboard

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

- Block/Unblock Requests
- Block/Unblock Device Count

Copyright @ 2020 DMC All Rights Reserved

- Grievances

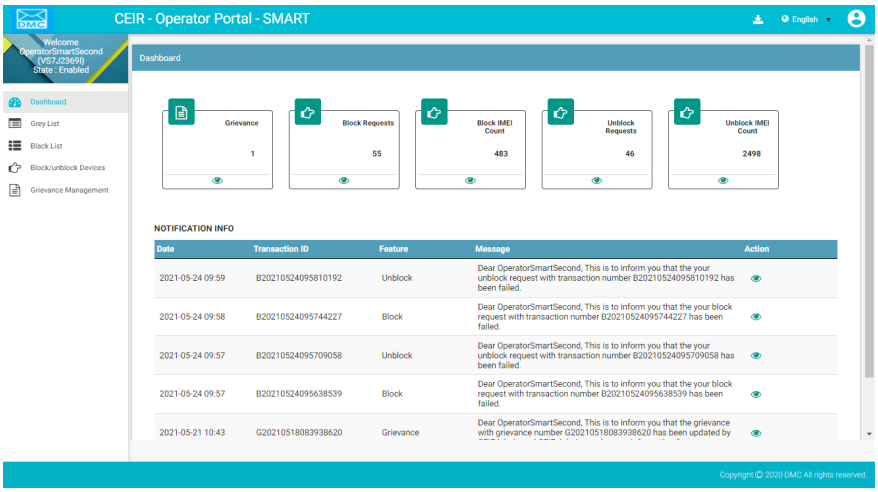
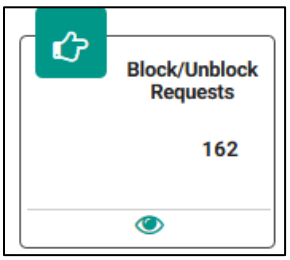


Figure 13: Home Page

Block/Unblock Requests

The box displays the total number of block and unblock requests.



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

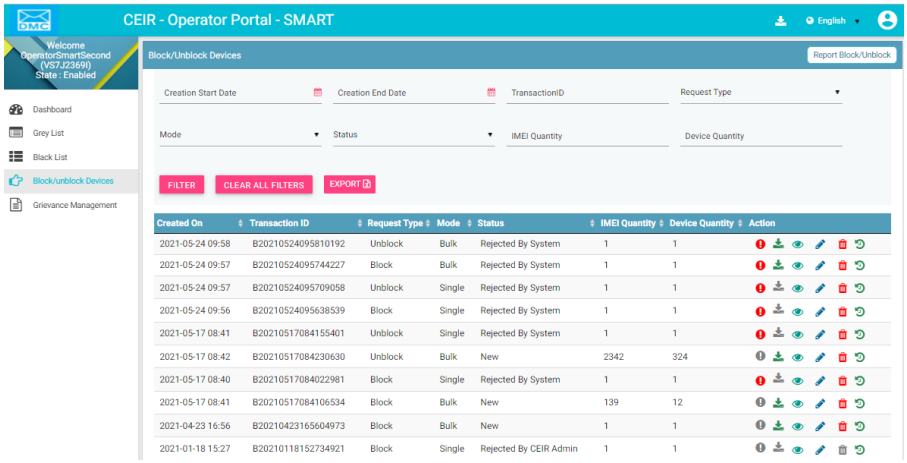
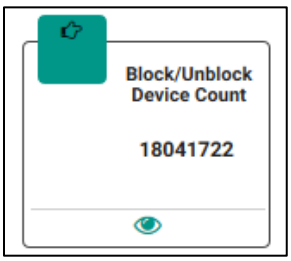


Figure 14: Block/Unblock Devices

Block/Unblock Device Count

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



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

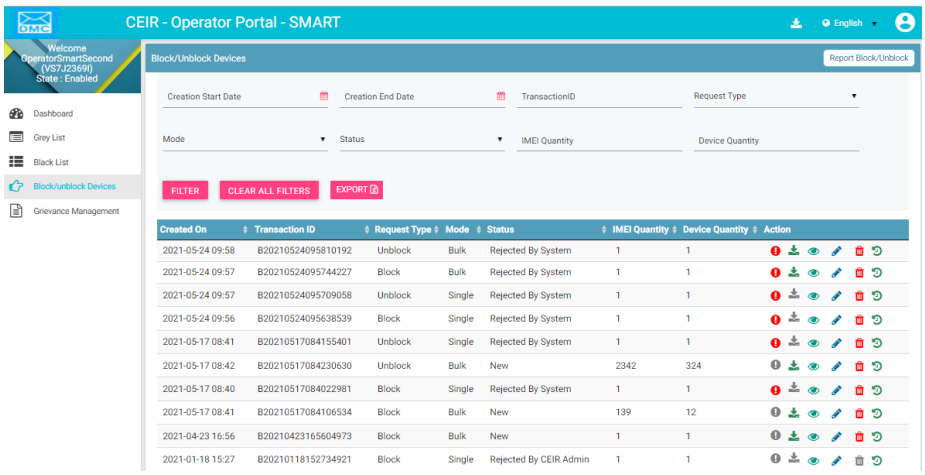
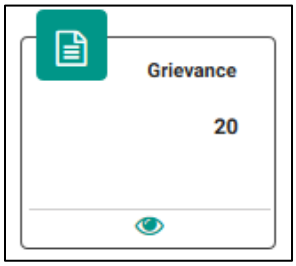


Figure 15: Block/Unblock Devices

Grievance

This box displays the total number of grievances raised.



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

Copyright @ 2020 DMC All Rights Reserved

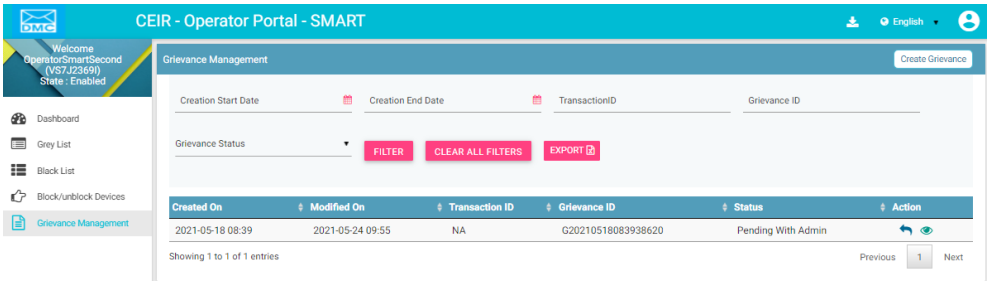


Figure 16: Grievance Management

Notification Information

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

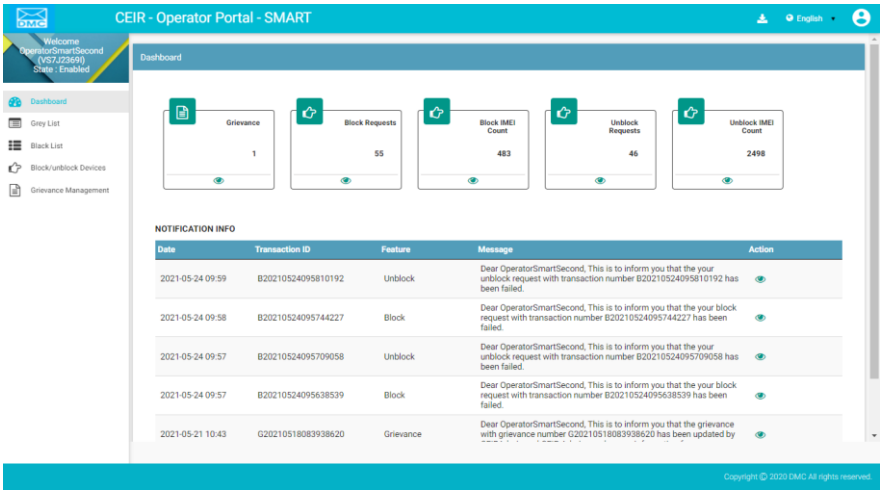


Figure 17: Home Page

Notifications are of two types.

1. Notifications that provide only information. For example, a notification informing the operator 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 operator. For example, a notification about the block device rejection by the CEIR administrator requires the operator 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

Copyright @ 2020 DMC All Rights Reserved

- **Transaction ID**: Transaction ID for which the notification is sent. If the notification is related to the operator account, the login username is shown instead of any transaction ID.
- **Feature**: This is the name of the feature for which the notification is sent. For example, if the notification is for a grievance, the feature name **Grievance** is shown.
- **Message**: This is the message of the notification. An example is shown below.

- **Action**: This shows the **View** icon. It is activated if the operator can click on it else it is disabled .

2.5 Block/Unblock Devices

Operators block devices (IMEI/MEID/ESN) when there is a contract violation. The operator can block or unblock a single device at a time or multiple devices at a time.

Whenever a device is blocked, the IMEI/MEID/ESN of the device is kept in a greylist. This is done for a given duration after which the device IMEI/MEID/ESN is moved to the blacklist. Moving the information to the blacklist indicates permanent blocking.

2.5.1 Single Device Blocking/Unblocking

To block or unblock a single device:

1. Select **Block/Unblock Devices** in the left panel of the Home page.

Copyright @ 2020 DMC All Rights Reserved

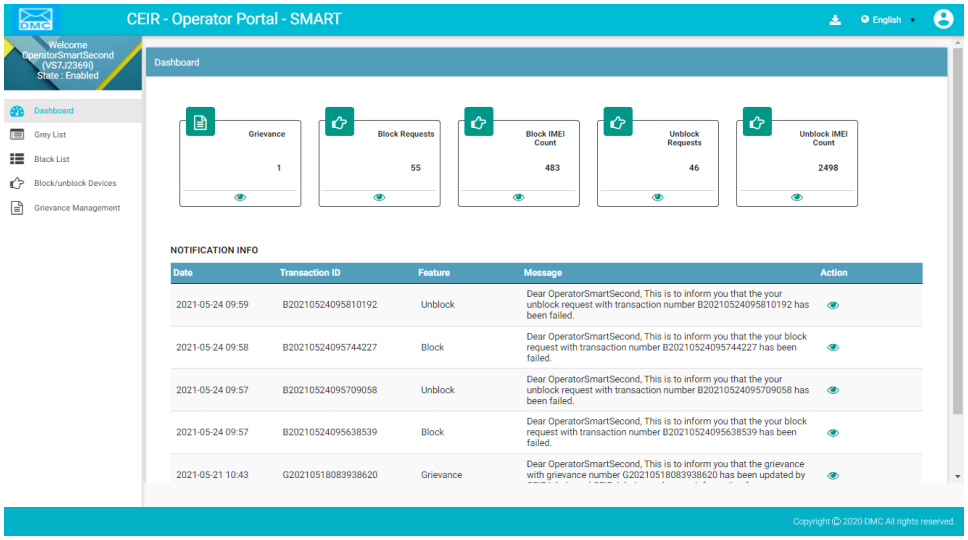


Figure 18: Home Page

The **Block/Unblock Devices** dashboard appears.

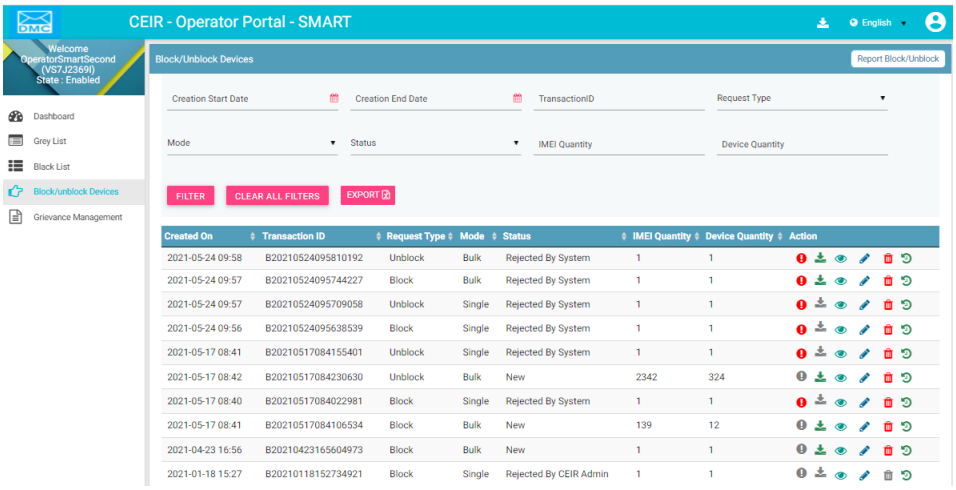


Figure 19: Block/Unblock Devices

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

3. Select **Block** or **Unblock** as per the action to be taken.

Copyright @ 2020 DMC All Rights Reserved

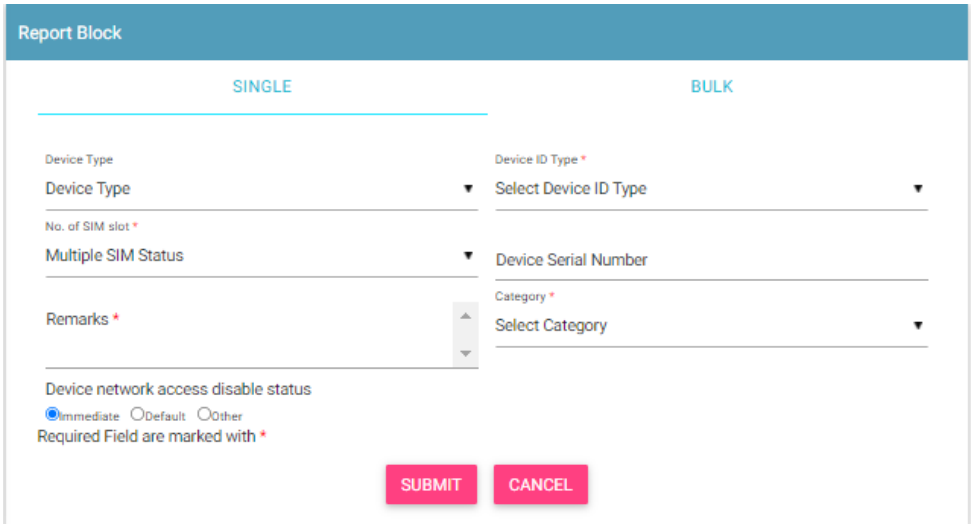


Figure 20: Report Block

The screen has two sections: **Single** and **Bulk**.

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

4. Enter the following information:

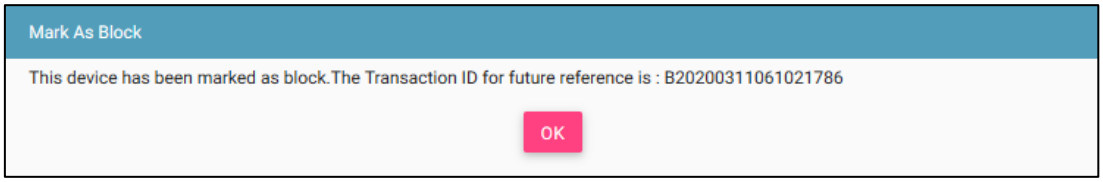
- ***Device Type**: Select the type of device to be blocked or unblocked.
- **Device ID Type**: Select the type of ID to be entered for the device that is being blocked or unblocked:
    - IMEI
- **No. of SIM slots**: Number of slots the device supports (1-4)
- **Device Serial Number**: Enter the device serial number.
- ***Remarks**: Enter details about device being blocked or unblocked.
- ***Category**: Select the reason for blocking the device:
    - Contract Violation
    - Other
- **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 .

Copyright @ 2020 DMC All Rights Reserved

- **IMEI**: Enter the value of the IMEIs of the device to be blocked.

5. Click **Submit**.

A unique transaction ID is generated, and the blocking or unblocking 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 block or unlock the device.
Transaction ID	Transaction ID assigned to the request.
Request Type	The request type can be block or unblock depending on the action taken.
Mode	This indicates whether the transaction is for a single device (Single) or for bulk devices (Bulk).
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 administrator for review.

Copyright @ 2020 DMC All Rights Reserved

Column	Description
	○ 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 operator has wrongly marked a device as stolen, which has been rightly claimed by another user. ○ Withdrawn by User: The operator can withdraw the request only when the status is New or Rejected by System.
Quantity	If the request is for a bulk device request, this refers to the number of IMEIs in the **.csv** file else it refers to the IMEIs in the single device being blocked or unblocked.
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 any problem with the file format or policy violation. 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 is enabled only for bulk requests. Click on it download the file.

Copyright @ 2020 DMC All Rights Reserved

Column	Description
	• 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 request.

2.5.2 Bulk Device Blocking/Unblocking

Instead of blocking or unblocking one device at a time, operators can block or unblock multiple devices at a time. This saves time and speeds up the processing.

To block or unblock multiple devices, operators are required to enter the device information in a **.csv** file and upload it to the system. The format of the file and a sample are shown later in this section.

To block or unblock multiple devices:

1. Select **Block/Unblock Devices** in the left panel of the Home page.

Copyright @ 2020 DMC All Rights Reserved

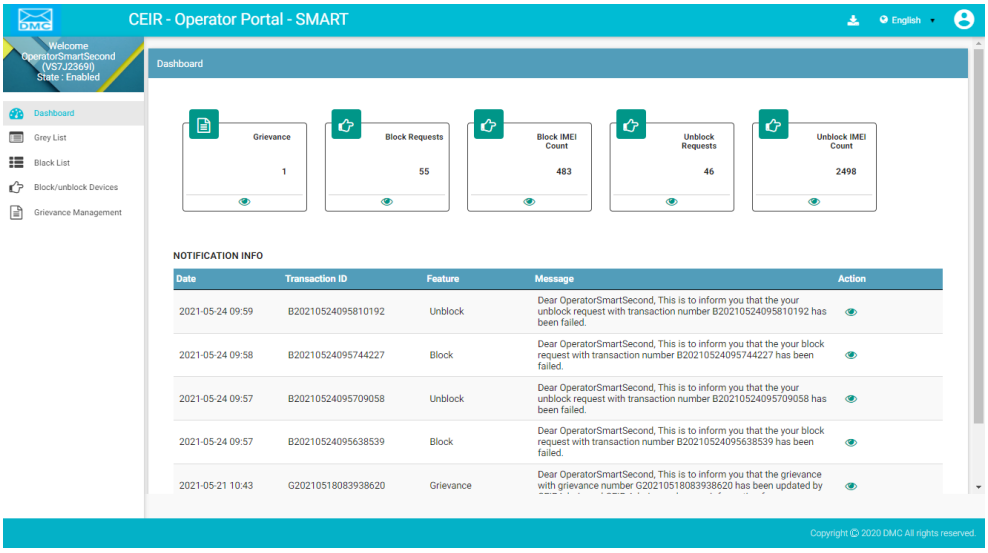


Figure 21: Report Block

The **Block/Unblock Devices** dashboard appears.

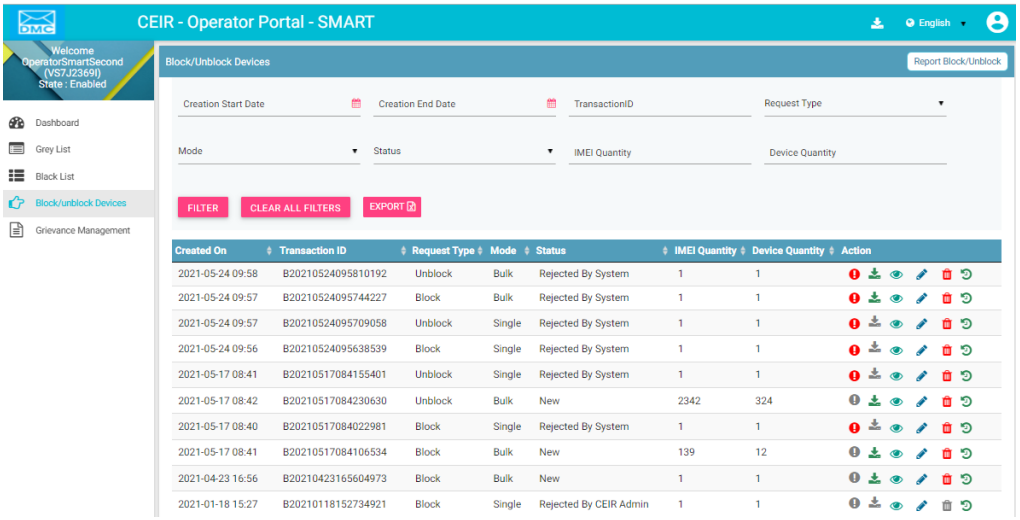
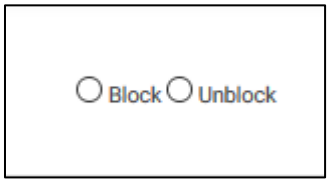


Figure 22: Block/Unblock Devices

2. Click **Report Block/Unblock**.



3. Select **Block** or **Unblock**.

4. On selecting **Block**, the **Report Block** page appears. Select **Bulk**.

Copyright @ 2020 DMC All Rights Reserved

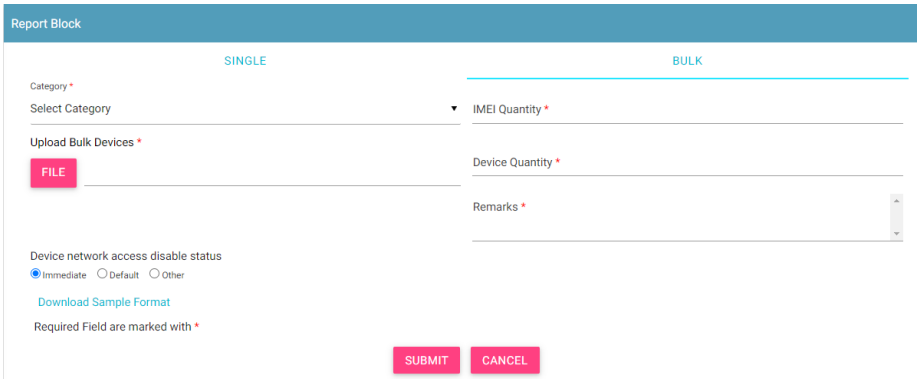


Figure 23: Report Block

Enter the following information:

- ***Category**: Select the reason for blocking or unblocking devices:
  - Contract Violation
  - Other
- ***Remarks**: Enter information about the bulk blocking or unblocking.
- ***** **IMEI Quantity**: The number of IMEIs to be blocked or unblocked.
- ***** **Device Quantity**: The number of Devices to be blocked or unblocked.
- ***** **Upload Bulk devices**: Enter the IMEI details in a file. This is a **.csv** file with defined column names. You need to enter device information in this file. First, download the file format, if required.

Click **Download Sample Format** to save the format of the **.csv** file in which to enter the details of the devices to be blocked or unblocked.

	A	B	C	D	E	F	G
1	DeviceType	DeviceIdType	MultipleSIMStatus	S/NofDevice	IMEI	Devicelaunchdate	DeviceStatus
2							
3							

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

The file has the following columns:

- **Device type**: The device can be a handheld phone, mobile phone, feature phone, smart phone, Vehicle, Portable (include PDA), Module, Dongle, WLAN router, modem, connected computer, tablet, e- Book.
- ***Device ID type**: Type can be IMEI.

Copyright @ 2020 DMC All Rights Reserved

- **Multiple SIM Status**: No of multiple SIM slots the device supports (1-4)
- **S/N of Device**: Device serial number
- ***IMEI**: Value of IMEI
- **Device launch date**: Launch date or manufacturing date of the device (in the format, DDMMYYYY).
- **Device status**: Whether the device is new or used (New/Used)

	A	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

- Save the file and click **File** to upload the saved file to the system.
- Click **Submit**.

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

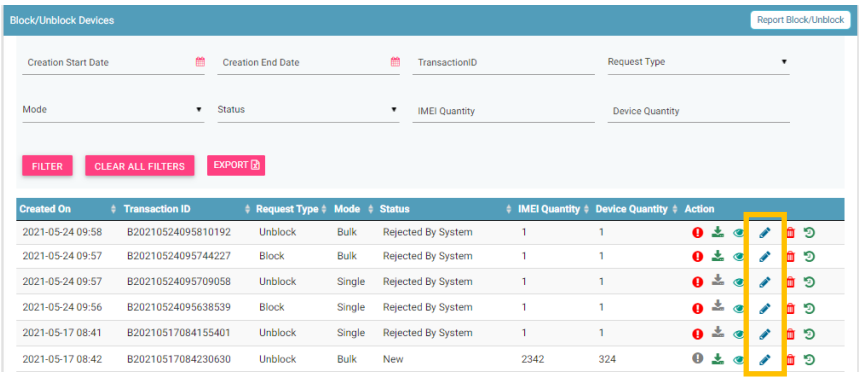
The request appears on top of the dashboard.

2.6 Edit Block/Unblock Device Requests

Operators can change the block/unblock 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 24: Block/Unblock Devices

The **Edit** page appears. The page has the same fields for block and unblock single devices.

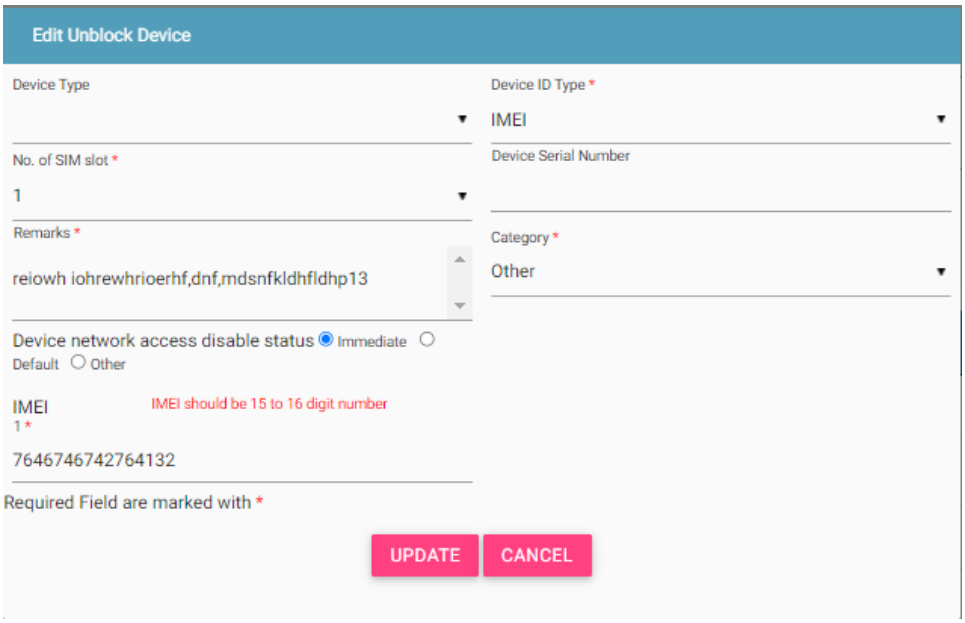


Figure 25: Edit Block Device (Single Device)

The **Edit** page is different for bulk devices (block and unblock).

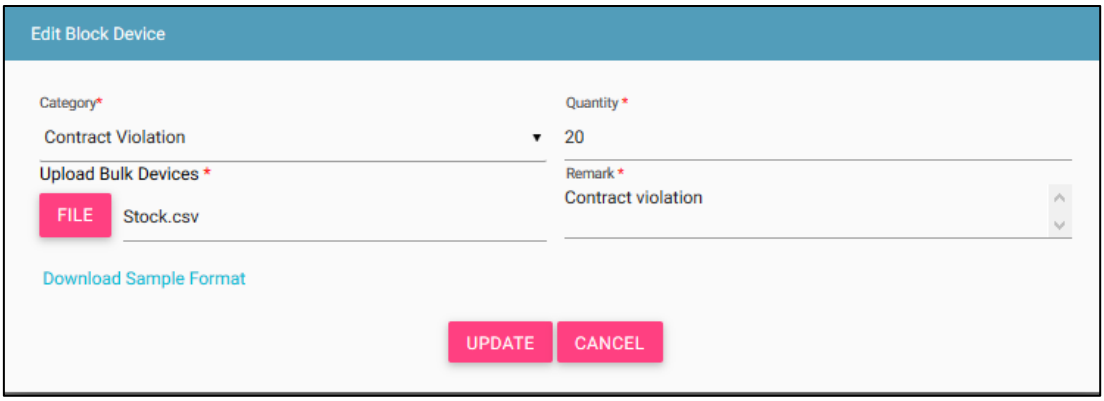


Figure 26: Edit Block Device (Bulk Device)

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

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

Copyright @ 2020 DMC All Rights Reserved

2.7 Filter Block/Unblock Device Requests

Operators can view selective block/unblock device requests after specifying the required filters. For example, operators can view requests that are pending approval from the CEIR administrator.

To filter block/unblock device requests:

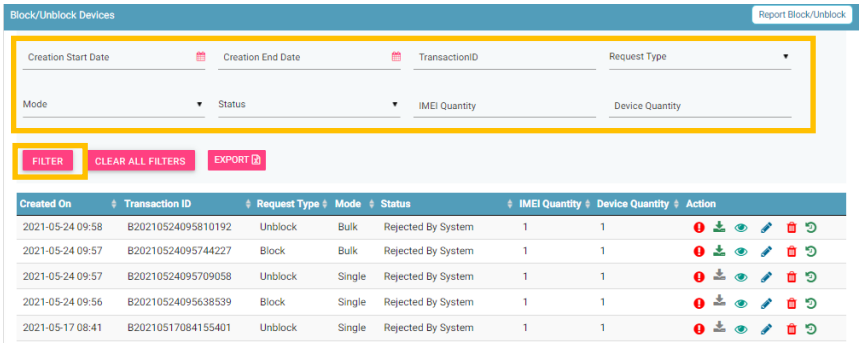


Figure 27: Block/unblock Devices

1. Enter data in one or more of the listed fields:
   - **Start Date** and **End Date**: This refers to the registering block/unblock device requests in the system.
   - **Transaction ID**: Each request is assigned a unique transaction ID. Operators can view a specific request by entering its transaction ID.
   - **Request Type**: This refers to the type of request: Block or Unblock.
   - **Mode**: This refers to whether the request is for a single device or bulk devices: Single or Bulk.
2. Click **FILTER**.

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

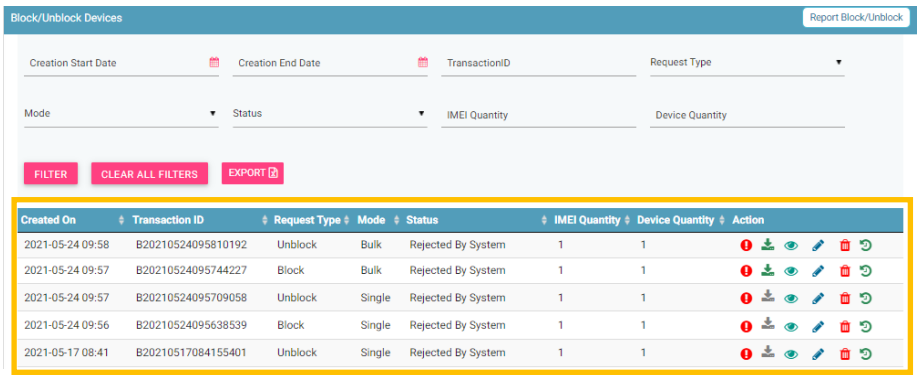


Figure 28: Filtered Device Block/Unblock Requests

Copyright @ 2020 DMC All Rights Reserved

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 is refreshed.

2.8 Sorting Block/Unblock requests

By default, all records displayed are sorted based on modified date. User can sort the records as per his convenience 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.

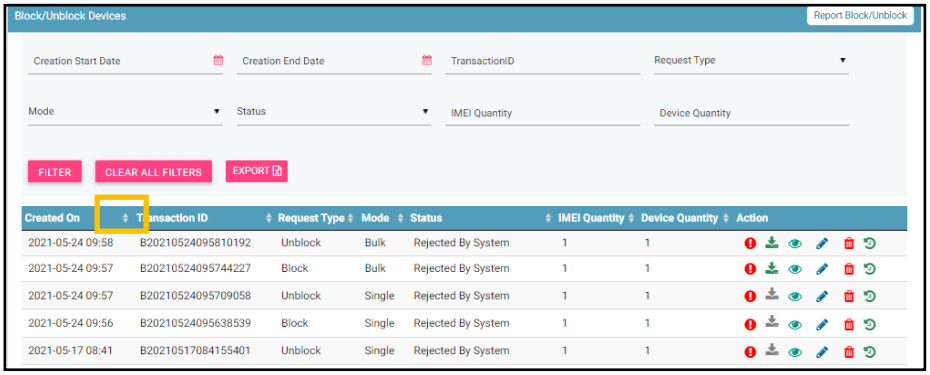


Figure 29: Sort Block/Unblock Requests

2.9 Export Block/Unblock Device Requests

Operators 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 **Block/Unblock Devices** page, click **Export**.

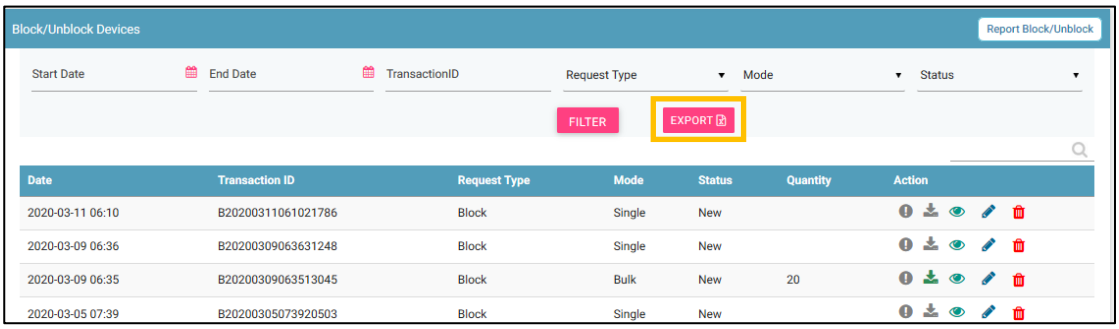


Figure 30: Block/Unblock Devices

Copyright @ 2020 DMC All Rights Reserved

The following page appears.

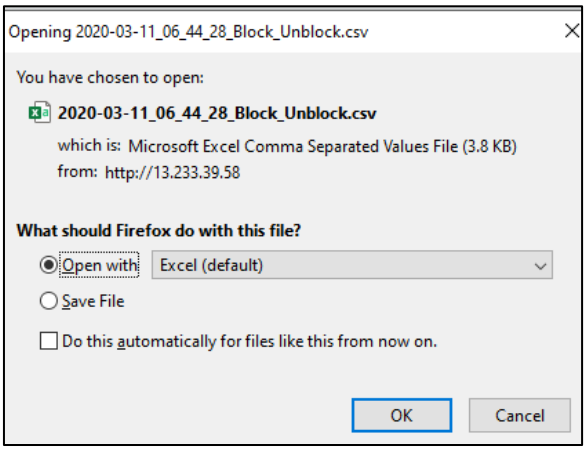


Figure 31: Open or Save Exported Block/Unblock Devices File

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

	A	B	C	D	E	F	G	
1	Created On	Modified On	Txn Id	Request Type	Mode	Status	Source	Filename
2	08-04-2020 12:07	08-04-2020 12:07	B20200408120702015	Unblock	Single	New	Metfone	
3	08-04-2020 12:07	09-04-2020 07:05	B20200408120721079	Unblock	Company	Rejected By System	Metfone	con_5_rec.csv
4	08-04-2020 14:45	09-04-2020 06:40	B20200408144546410	Block	Single	Rejected By CEIR Admin	Metfone	
5	09-04-2020 07:06	09-04-2020 07:07	B20200409070632024	Block	Single	Pending Approval From CEIR Admin	Metfone	
6	09-04-2020 07:12	09-04-2020 07:13	B20200409071244698	Block	Bulk	Pending Approval From CEIR Admin	Metfone	con_5_rec.csv
7	09-04-2020 07:24	09-04-2020 07:24	B20200409072413830	Unblock	Single	Rejected By System	Metfone	
8	09-04-2020 07:27	09-04-2020 07:27	B20200409072700865	Unblock	Bulk	Pending Approval From CEIR Admin	Metfone	con_5_rec.csv
9	09-04-2020 07:29	09-04-2020 07:30	B20200409072938039	Unblock	Single	Rejected By System	Metfone	
10	09-04-2020 13:41	09-04-2020 13:44	B20200409134113001	Block	Single	Pending Approval From CEIR Admin	Metfone	

Figure 32: Exported Block/Unblock Devices

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

2.10 Greylist

When a request to block a device is registered in the system, the IMEI of the device is moved to the greylist file. The device status is maintained in the greylist file for a given duration before it is moved to the blacklist file. The duration for which a blocked device is kept in the greylist file depends on the system configuration and type of blocking (Instant, Default, Later).

To view the greylist file:

1. Select **Grey List** in the left panel of the home page.

Copyright @ 2020 DMC All Rights Reserved

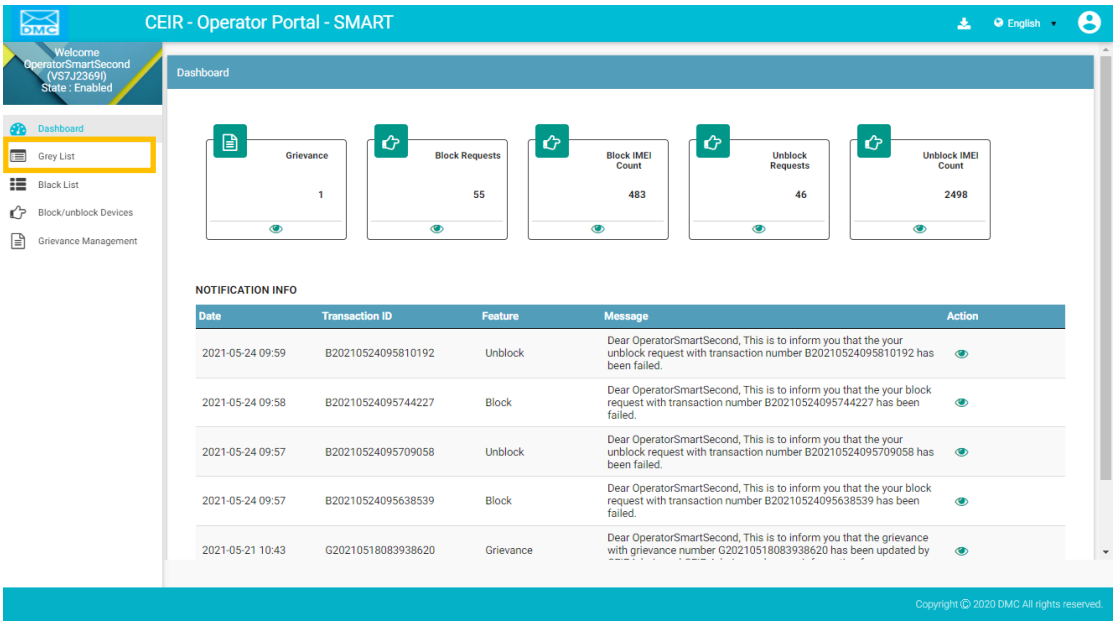


Figure 33: Home Page

The **Grey List** page appears.

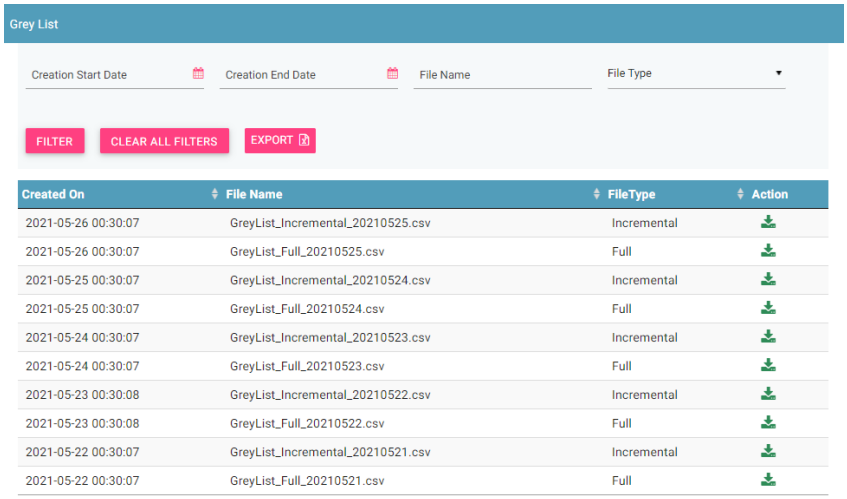


Figure 34: Grey List

For each greylisted device, the following information is shown on the dashboard.

Column	Description
Updated On	Date on which the file is created.
File Name	Name of the file. The file naming convention is:

Column	Description
	GreyList_<Type of File>_<yyyymmdd>.csv • Type of File: ○ **Full**: A full file shows all the device IDs in the grey list as on yyyymmdd. ○ **Incremental**: An incremental file shows the device IDs added or deleted on yyyymmdd. • yyyyymmdd: The date of the greylist. **Example 1:** **GreyList_Full_20200503.csv** The file is a grey list. Full: The file has the IMEIs/MEIDs/ESNs of all the devices that are in the greylist as on 5'th March 2020. **Example 2:** **GreyList_Incremental_20200703.csv** The file is a grey list. Incremental: The file has the IMEIs/MEIDs/ESNs of the devices that were added or removed from the greylist on 7'th March 2020.
File Type	A file can be: • **Full**: A full file is a list of all the devices that are in the greylist on a given date. • **Incremental**: An incremental file is a list of the devices that have been added or deleted on a given date.
Action	Download : This is used to take a dump of the file to view it.

Copyright @ 2020 DMC All Rights Reserved

A sample incremental file is shown.

	A	B
1	Device ID	Operation
2	562378129102348	Add
3	789812234323154	Delete
4	8798123423420930	Add
5	342328123492013	Delete

A sample full file is shown.

	A
1	Device ID
2	562378129102348
3	789812234323154
4	8798123423420930
5	342328123492013

2.11 Filter Greylist

Operators can view selective files by specifying the required filters. For example, operators can view a greylist file for a given period or a greylist file that is full or incremental.

To filter a greylist file:

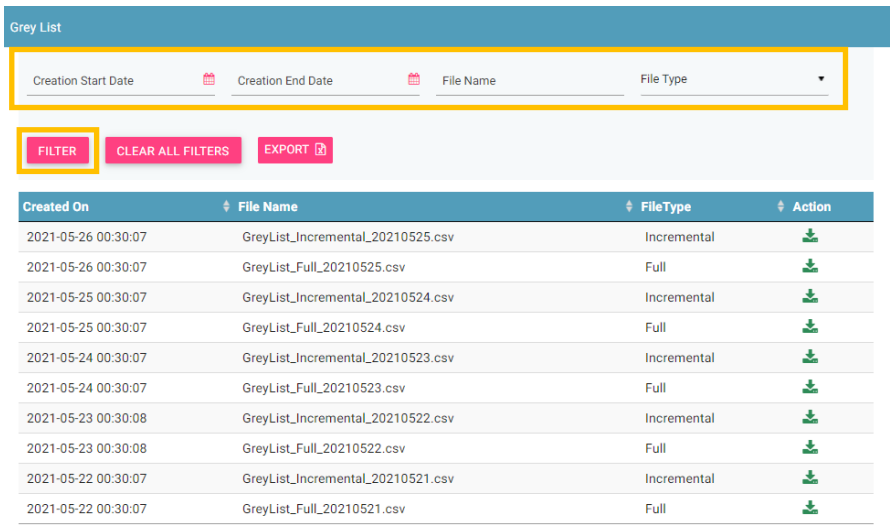


Figure 35: Grey List

1. Enter the required value in one or more of the listed fields:
   - **Start Date and End Date**: This refers to the period of generating a greylist file.

Copyright @ 2020 DMC All Rights Reserved

- **File Type**: This refers to the type of greylist file: Full or Incremental.

2. Click **FILTER**.

Greylist files that match the specified values are shown in the dashboard.

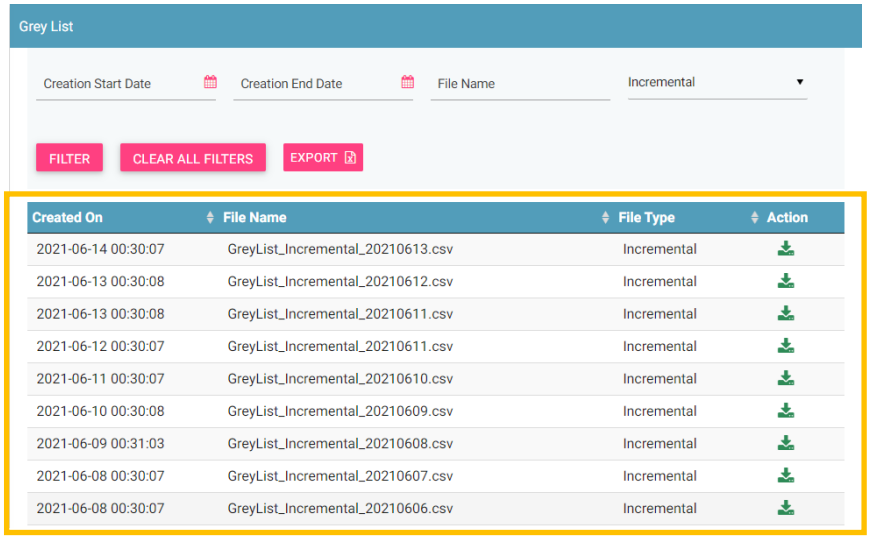


Figure 36: Filtered Greylists

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 is refreshed.

2.12 Sorting Greylists

By default, all records displayed are sorted based on modified date. User can sort the records as per his convenience 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.

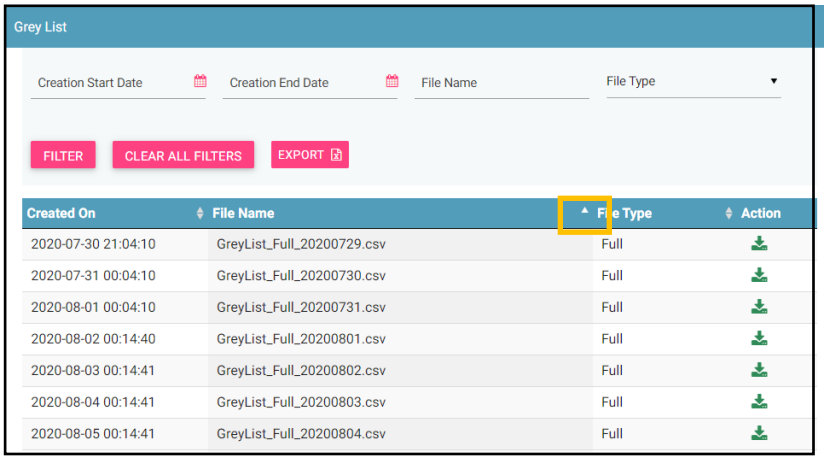


Figure 37: Sort Greylists

Copyright @ 2020 DMC All Rights Reserved

2.13 Export Greylist

Operators can download the greylist in a **.csv** file. This is done using an export utility.

To export greylist files:

1. Click **Export** (seen on the top right corner of the **Grey List** page).

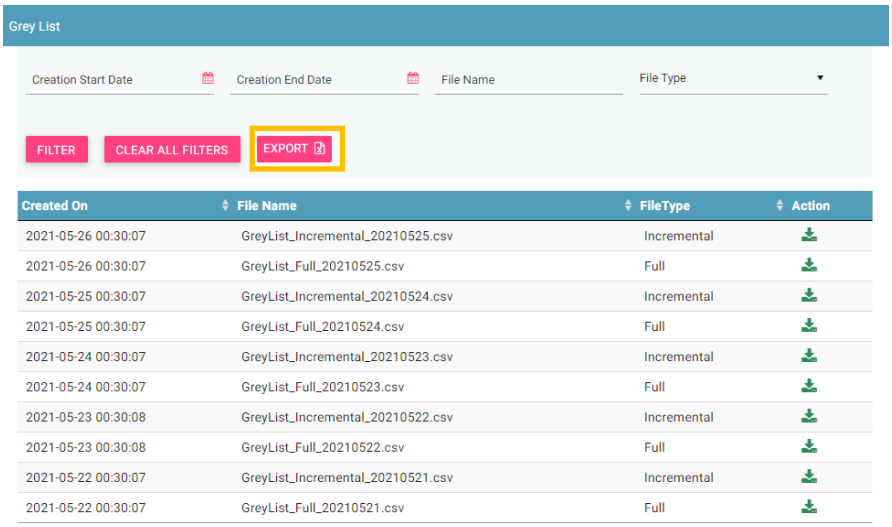


Figure 38: Grey List

The following page appears.

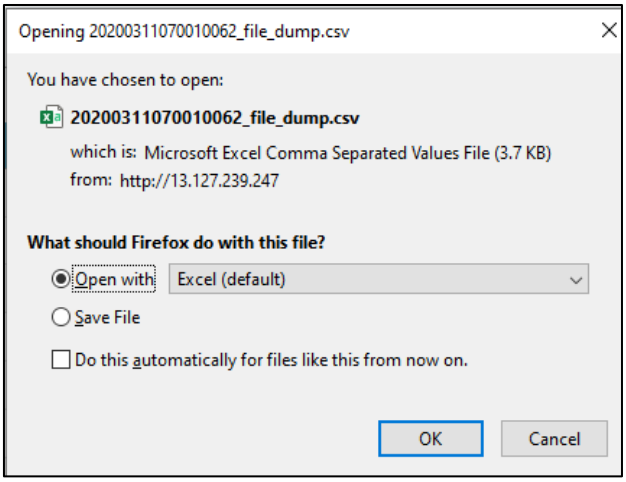


Figure 39: Open or Save Exported Greylists

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

Copyright @ 2020 DMC All Rights Reserved

	A	B	C
1	Created On	File Name	File Type
2	14-06-2021 00:30	GreyList_Incremental_20210613.csv	Incremental
3	14-06-2021 00:30	GreyList_Full_20210613.csv	Full
4	13-06-2021 00:30	GreyList_Incremental_20210612.csv	Incremental
5	13-06-2021 00:30	GreyList_Incremental_20210611.csv	Incremental
6	13-06-2021 00:30	GreyList_Full_20210612.csv	Full
7	13-06-2021 00:30	GreyList_Full_20210611.csv	Full
8	12-06-2021 00:30	GreyList_Incremental_20210611.csv	Incremental

Figure 40: Exported Greylists

Greylist files can be filtered and then exported. To filter greylist files, refer to *Filter Grey Lists* for information and then export the filtered data.

2.14 Blacklist

Device IMEIs/MEIDs/ESNs are moved from the greylist to the blacklist. The duration for which a device is kept in the greylist depends on the system configuration and the type of blocking selected at the time of blocking the device (Immediate, Default, Later).

To view blacklist files:

1. Select **Black List** in the left panel of the Home page.

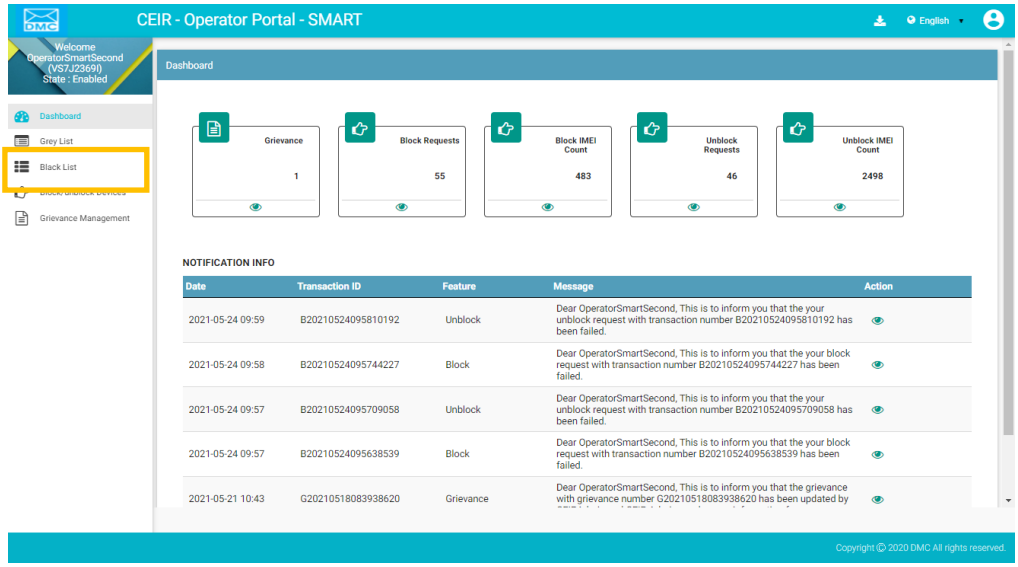


Figure 41: Home Page

2. The **Black List** page appears. The page shows the blacklist files generated on different dates.

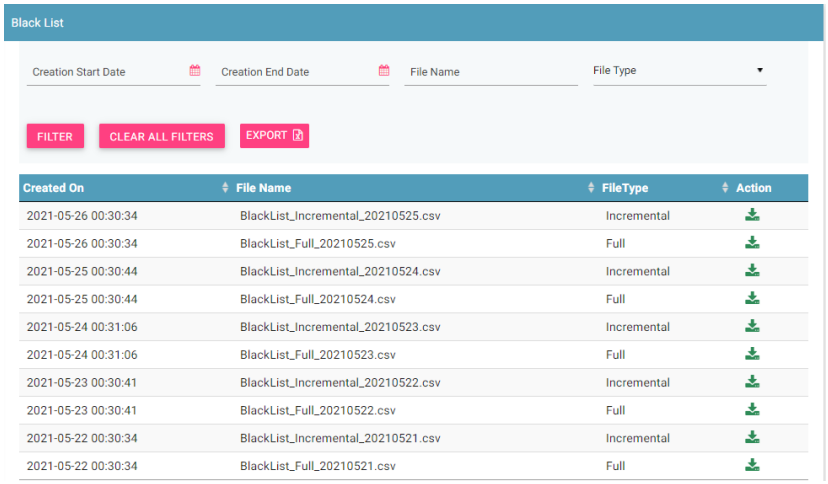


Figure 42: Black List

For each blacklist file generated, the following information is displayed on the page.

Column	Description
Updated On	Date of creating the blacklist.
File Name	Name of the file. The file naming convention is **BlackList_<Type of File>_<yyyymmdd>.csv** • **Type of File**: o Full: A full file shows all the device IDs in the blacklist as on date (yyyymmdd). o Incremental: An incremental file shows the device IDs added or deleted on the date (yyyymmdd). • **yyyyymmdd**: The date of the blacklist. **Example 1:** **BlackList_Full_20200503.csv** The file is a blacklist.

Copyright @ 2020 DMC All Rights Reserved

Column	Description
	Full: The file has the IMEIs/MEIDs/ESNs of all the devices that are in the blacklist as on 5'th March 2020. **Example 2:** **BlackList_Incremental_20200703.csv** The file is a blacklist. Incremental: The file has the IMEIs/MEIDs/ESNs of the devices that were added or removed from the blacklist on 7'th March 2020.
File Type	A file can be: • Full: A full file has a list of all the devices that are in the blacklist as on a given date. • Incremental: An incremental file has a list of the devices that have been added or deleted on a given date.
Action	Download : This is used to take a dump of the file to view it.

A sample partial blacklist file is shown.

	A	B
1	Device Id	Operation
2	978375819405983	Add
3	978375819675984	Add
4	97213131123131	Add
5	1234567890123450	Add
6	12416002672400	Add
7	1234567890123450	Add
8	9999999999999990	Add
9	68756355553	Add

A sample full blacklist file is shown.

Copyright @ 2020 DMC All Rights Reserved

	A
1	Device ID
2	997823231012234
3	672312888893324
4	889911223344789
5	567788223319009
6	8987896785657230
7	2342121234545670

2.15 Filter Blacklist

Operators can view selective blacklist files depending on specific filter values. For example, the operator can view only those files that show the number of devices added or deleted on a given date.

To filter blacklist files:

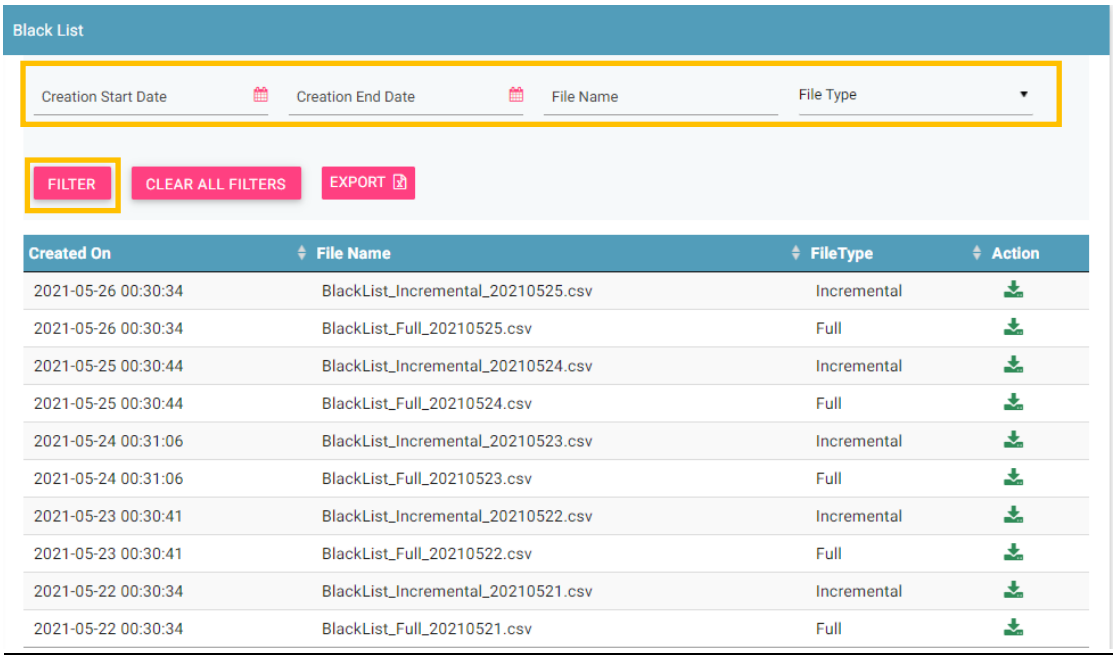


Figure 43: Black List

1. Specify the required value in one or more of the fields listed:
   - **Start Date** and **End Date**: Period of generated blacklist files.
   - **File Type**: The type can be:
     - Full
     - Incremental

Copyright @ 2020 DMC All Rights Reserved

2. Click **Filter**.

The filtered files are shown on the page.

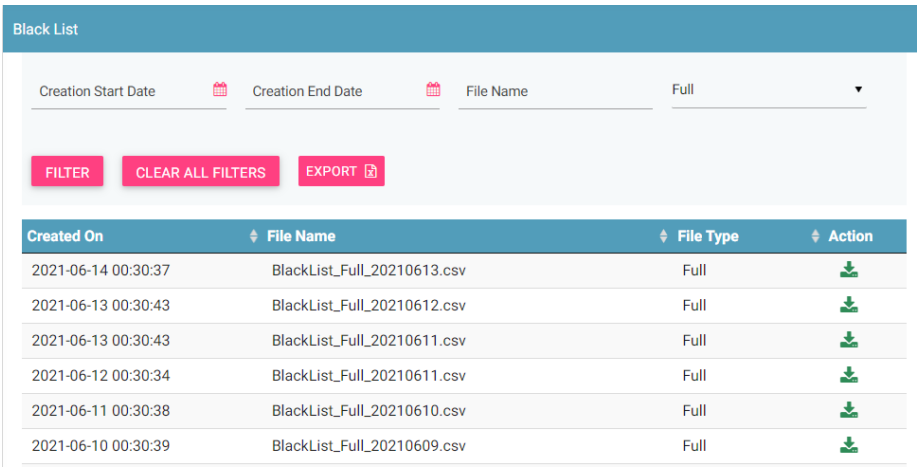


Figure 44: Filtered Blacklists

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 is refreshed.

2.16 Sorting Blacklists

By default, all records displayed are sorted based on modified date. User can sort the records as per his convenience 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.

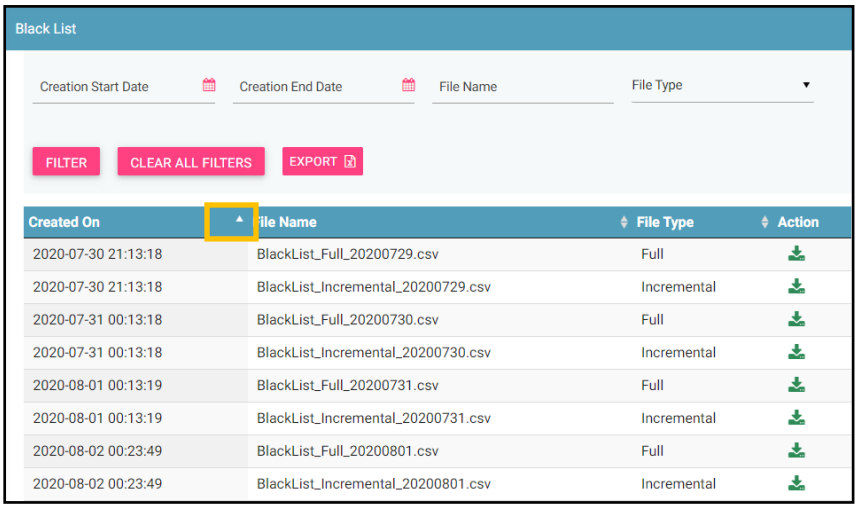


Figure 45: Sort Blacklists

Copyright @ 2020 DMC All Rights Reserved

2.17 Export Blacklist

The blacklist files can be downloaded in a **.csv** file. This is done using an export utility.

To export blacklist files:

1. Click **Export** (seen on the top right corner of the **Black List** page).

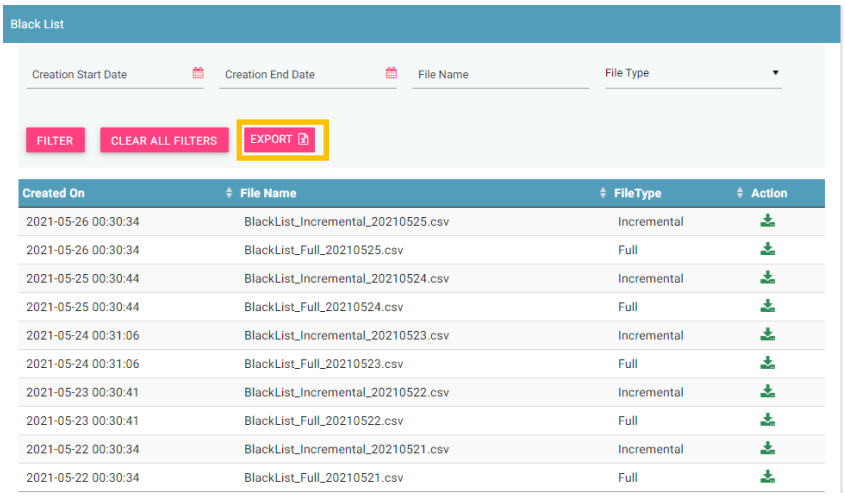


Figure 46: Black List

The following page appears.

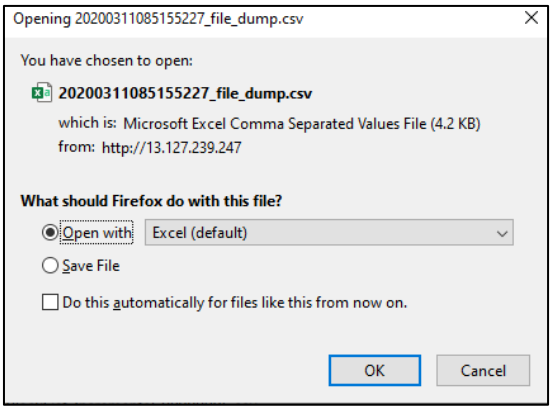


Figure 47: Open or Save Exported Blacklist File

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

Copyright @ 2020 DMC All Rights Reserved

	A	B	C
1	Created On	File Name	File Type
2	14-06-2021 00:30	BlackList_Incremental_20210613.csv	Incremental
3	14-06-2021 00:30	BlackList_Full_20210613.csv	Full
4	13-06-2021 00:30	BlackList_Incremental_20210612.csv	Incremental
5	13-06-2021 00:30	BlackList_Incremental_20210611.csv	Incremental
6	13-06-2021 00:30	BlackList_Full_20210612.csv	Full
7	13-06-2021 00:30	BlackList_Full_20210611.csv	Full
8	12-06-2021 00:30	BlackList_Incremental_20210611.csv	Incremental
9	12-06-2021 00:30	BlackList_Full_20210611.csv	Full
10	11-06-2021 00:30	BlackList_Incremental_20210610.csv	Incremental

Figure 48: Exported Blacklists

Instead of exporting all the blacklist files, operators can export filtered blacklist files. First, filter the blacklist data based on specific filters (refer to *Filter Blacklists*) and then export the filtered blacklist files using the export utility.

2.18 Grievance Management

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

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

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

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

To raise a grievance

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

Copyright @ 2020 DMC All Rights Reserved

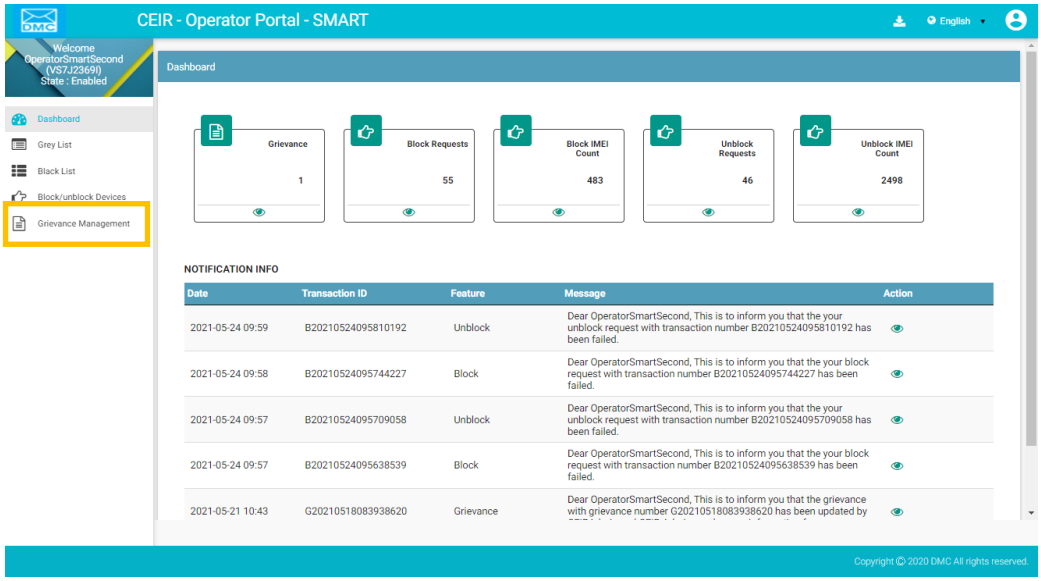


Figure 49: Home Page

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

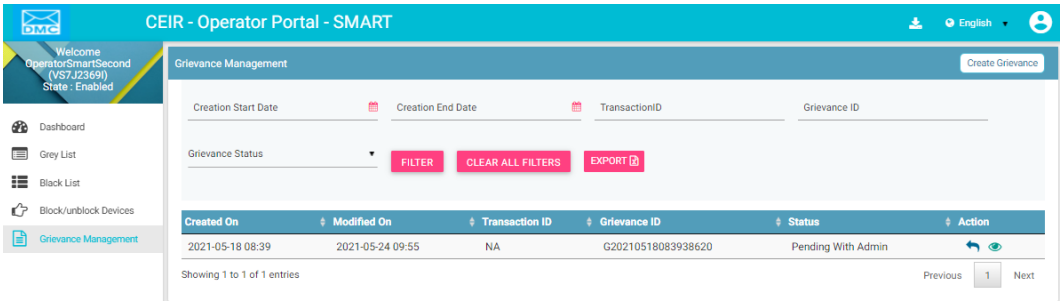


Figure 50: Grievance Management

The **Report Grievance** page appears.

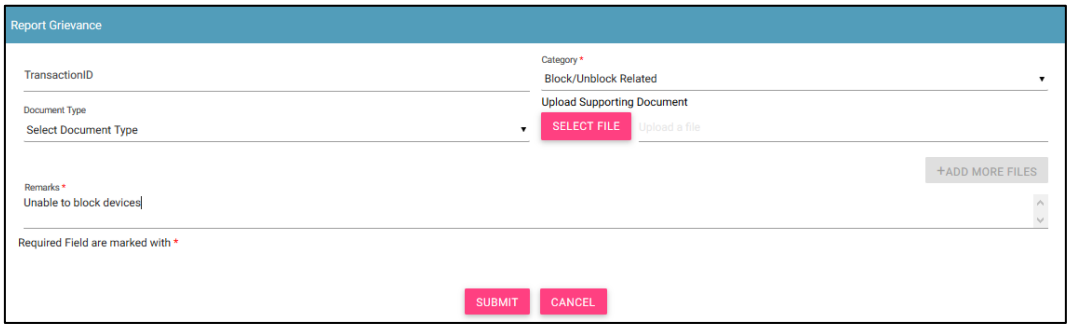


Figure 51: Report Grievance

5. Enter the following information:

a. **Transaction ID**: Enter the transaction ID of the block/unblock request if the grievance is related to blocking/unblocking or the ID of the grey ID list if related to the grey list or the ID of the blacklist if related to blacklist.

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

- Block/Unblock Related
- Greylist Related
- Blacklist Related
- Other

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

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

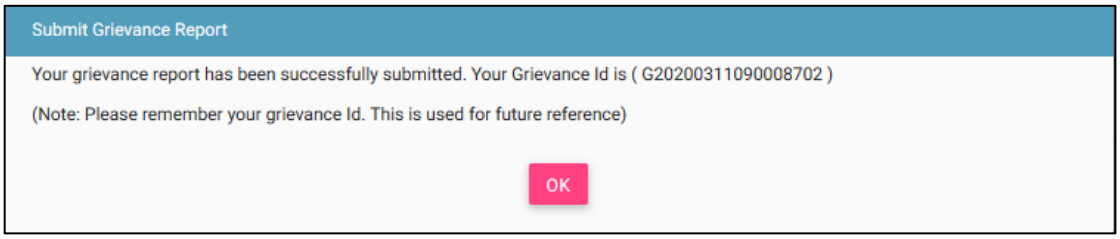
e. To upload more documents, click **+Add More Files.**

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.

6. Click **SUBMIT**.

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



The new grievance appears on the top of the page.

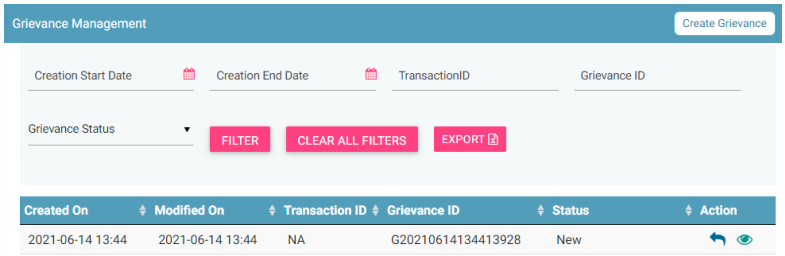


Figure 52: Grievance Management

Copyright @ 2020 DMC All Rights Reserved

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

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

Copyright @ 2020 DMC All Rights Reserved

2.19 Filter Grievances

The operator can view selective grievances depending on specific filter values. For example, the operator 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:

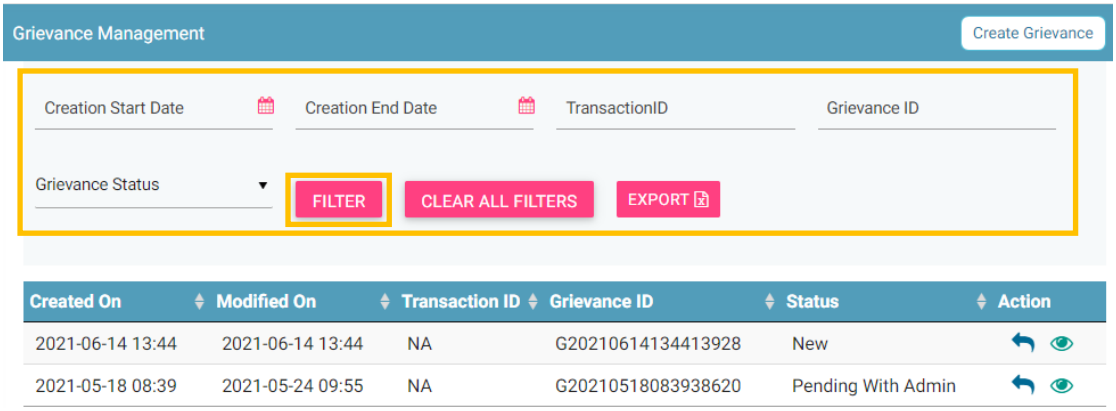


Figure 53: Filter Grievances

3. 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
4. Click **Filter**.

The filtered grievances are shown on the page.

Copyright @ 2020 DMC All Rights Reserved

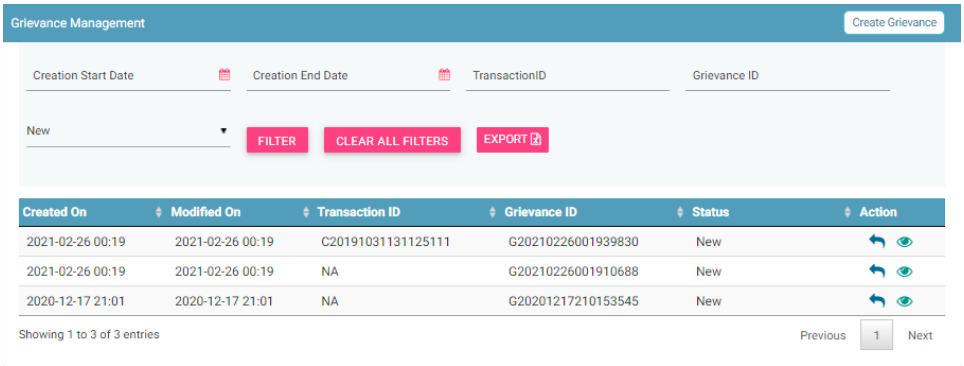


Figure 54: Filtered Grievances

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 is refreshed.

2.20 Sorting Grievances

By default, all records displayed are sorted based on modified date. User can sort the records as per his convenience 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.

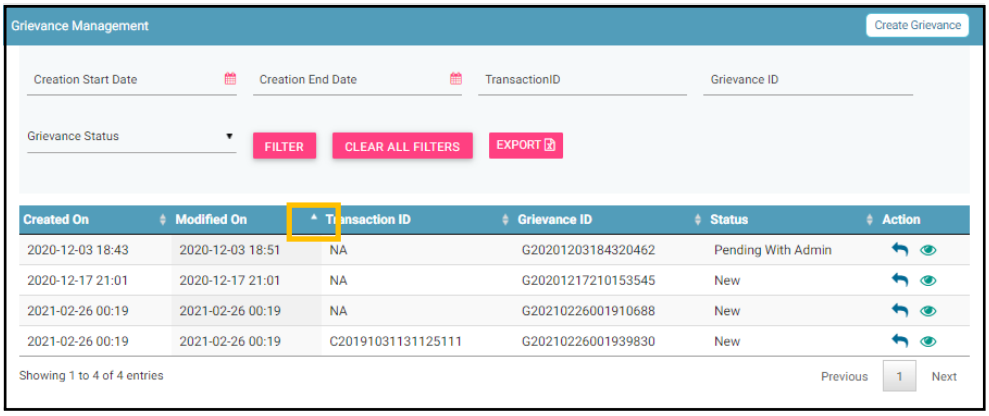


Figure 55: Sort Grievances

2.21 Export Grievances

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

To export the grievances:

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

Copyright @ 2020 DMC All Rights Reserved

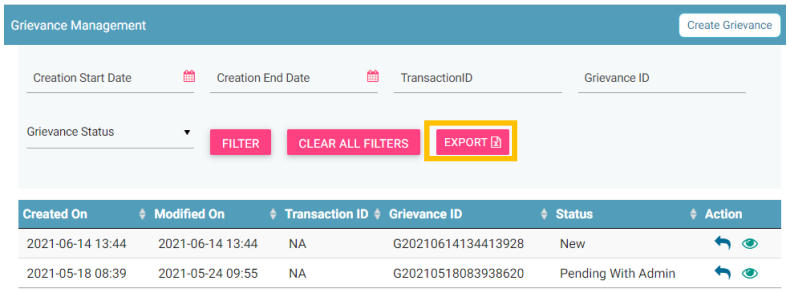


Figure 56: Grievance Management

The following page appears.

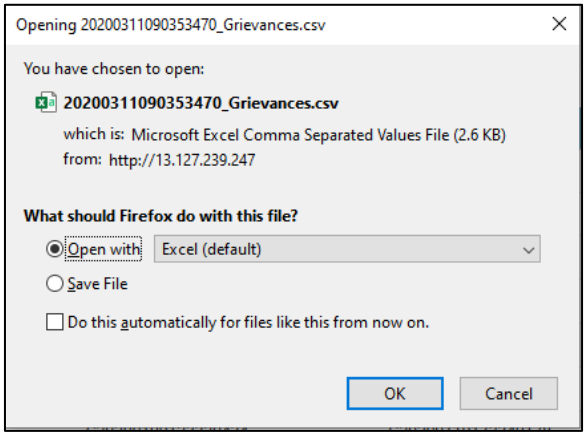


Figure 57: Open or Save Exported Grievance File

4. 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 58: Exported Grievances

Instead of exporting all the grievances, operators 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