ve

**Operator User Manual v 2.1**

* **Central Equipment Identity Register Portal**

Document Change History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Change Type | Description | Date |
| Draft |  | Submitted for internal review | February 2020 |
| Version 2.1 |  | Multiple System Admin, Configurable Notifications, Filter and sorting, Field Validations, History of the request, Address management | June 2021 |

Contents

[1 Overview 1](#_Toc75769956)

[1.1 Scope 1](#_Toc75769957)

[1.2 Acronyms & Abbreviations 1](#_Toc75769958)

[1.3 Conventions 1](#_Toc75769959)

[2 Operations 3](#_Toc75769960)

[2.1 Application Overview 3](#_Toc75769961)

[2.2 Logging into the Application 3](#_Toc75769962)

[2.3 Application User Interface 11](#_Toc75769963)

[2.4 Dashboard 14](#_Toc75769964)

[2.5 Block/Unblock Devices 18](#_Toc75769965)

[2.5.1 Single Device Blocking/Unblocking 18](#_Toc75769966)

[2.5.2 Bulk Device Blocking/Unblocking 23](#_Toc75769967)

[2.6 Edit Block/Unblock Device Requests 26](#_Toc75769968)

[2.7 Filter Block/Unblock Device Requests 27](#_Toc75769969)

[2.8 Sorting Block/Unblock requests 29](#_Toc75769970)

[2.9 Export Block/Unblock Device Requests 29](#_Toc75769971)

[2.10 Greylist 30](#_Toc75769972)

[2.11 Filter Greylist 33](#_Toc75769973)

[2.12 Sorting Greylists 35](#_Toc75769974)

[2.13 Export Greylist 35](#_Toc75769975)

[2.14 Blacklist 36](#_Toc75769976)

[2.15 Filter Blacklist 39](#_Toc75769977)

[2.16 Sorting Blacklists 41](#_Toc75769978)

[2.17 Export Blacklist 41](#_Toc75769979)

[2.18 Grievance Management 43](#_Toc75769980)

[2.19 Filter Grievances 46](#_Toc75769981)

[2.20 Sorting Grievances 48](#_Toc75769982)

[2.21 Export Grievances 48](#_Toc75769983)

Figures

[Figure 1: DMC Home Page 3](#_Toc75811729)

[Figure 2: Operator Registration 4](#_Toc75811730)

[Figure 3: Verify OTP 6](#_Toc75811731)

[Figure 4: Enter OTP 7](#_Toc75811732)

[Figure 5: Login 8](#_Toc75811733)

[Figure 6: Home Page 9](#_Toc75811734)

[Figure 7: Forgot Password 9](#_Toc75811735)

[Figure 8: Set New Password 10](#_Toc75811736)

[Figure 9: Home Page 11](#_Toc75811737)

[Figure 10: Edit Information 12](#_Toc75811738)

[Figure 11: Password confirmation 12](#_Toc75811739)

[Figure 12: Verify OTP notification 13](#_Toc75811740)

[Figure 13: Verify OTP 13](#_Toc75811741)

[Figure 14: Change Password 13](#_Toc75811742)

[Figure 15: Manage Account 14](#_Toc75811743)

[Figure 16: Home Page 15](#_Toc75811744)

[Figure 17: Block/Unblock Devices 15](#_Toc75811745)

[Figure 18: Block/Unblock Devices 16](#_Toc75811746)

[Figure 19: Grievance Management 17](#_Toc75811747)

[Figure 20: Home Page 17](#_Toc75811748)

[Figure 21: Home Page 18](#_Toc75811749)

[Figure 22: Block/Unblock Devices 19](#_Toc75811750)

[Figure 23: Report Block 19](#_Toc75811751)

[Figure 24: Report Block 23](#_Toc75811752)

[Figure 25: Block/Unblock Devices 24](#_Toc75811753)

[Figure 26: Report Block 24](#_Toc75811754)

[Figure 27: Block/Unblock Devices 26](#_Toc75811755)

[Figure 28: Edit Block Device (Single Device) 27](#_Toc75811756)

[Figure 29: Edit Block Device (Bulk Device) 27](#_Toc75811757)

[Figure 30: Block/unblock Devices 28](#_Toc75811758)

[Figure 31: Filtered Device Block/Unblock Requests 29](#_Toc75811759)

[Figure 32: Sort Block/Unblock Requests 29](#_Toc75811760)

[Figure 33: Block/Unblock Devices 30](#_Toc75811761)

[Figure 34: Open or Save Exported Block/Unblock Devices File 30](#_Toc75811762)

[Figure 35: Exported Block/Unblock Devices 30](#_Toc75811763)

[Figure 36: Home Page 31](#_Toc75811764)

[Figure 37: Grey List 31](#_Toc75811765)

[Figure 38: Grey List 34](#_Toc75811766)

[Figure 39: Filtered Greylists 34](#_Toc75811767)

[Figure 40: Sort Greylists 35](#_Toc75811768)

[Figure 41: Grey List 36](#_Toc75811769)

[Figure 42: Open or Save Exported Greylists 36](#_Toc75811770)

[Figure 43: Exported Greylists 36](#_Toc75811771)

[Figure 44: Home Page 37](#_Toc75811772)

[Figure 45: Black List 37](#_Toc75811773)

[Figure 46: Black List 40](#_Toc75811774)

[Figure 47: Filtered Blacklists 40](#_Toc75811775)

[Figure 48: Sort Blacklists 41](#_Toc75811776)

[Figure 49: Black List 42](#_Toc75811777)

[Figure 50: Open or Save Exported Blacklist File 42](#_Toc75811778)

[Figure 51: Exported Blacklists 42](#_Toc75811779)

[Figure 52: Home Page 43](#_Toc75811780)

[Figure 53: Grievance Management 44](#_Toc75811781)

[Figure 54: Report Grievance 44](#_Toc75811782)

[Figure 55: Grievance Management 45](#_Toc75811783)

[Figure 56: Filter Grievances 47](#_Toc75811784)

[Figure 57: Filtered Grievances 47](#_Toc75811785)

[Figure 58: Sort Grievances 48](#_Toc75811786)

[Figure 59: Grievance Management 48](#_Toc75811787)

[Figure 60: Open or Save Exported Grievance File 49](#_Toc75811788)

[Figure 61: Exported Grievances 49](#_Toc75811789)

# Overview

## 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.

## 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 |

## Conventions

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

# Operations

## Application Overview

The CEIR (Central Equipment Identity Register) 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

## 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.

A screenshot of a cell phone

Description automatically generated

Figure 1: DMC Home Page

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

A screenshot of a cell phone

Description automatically generated

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

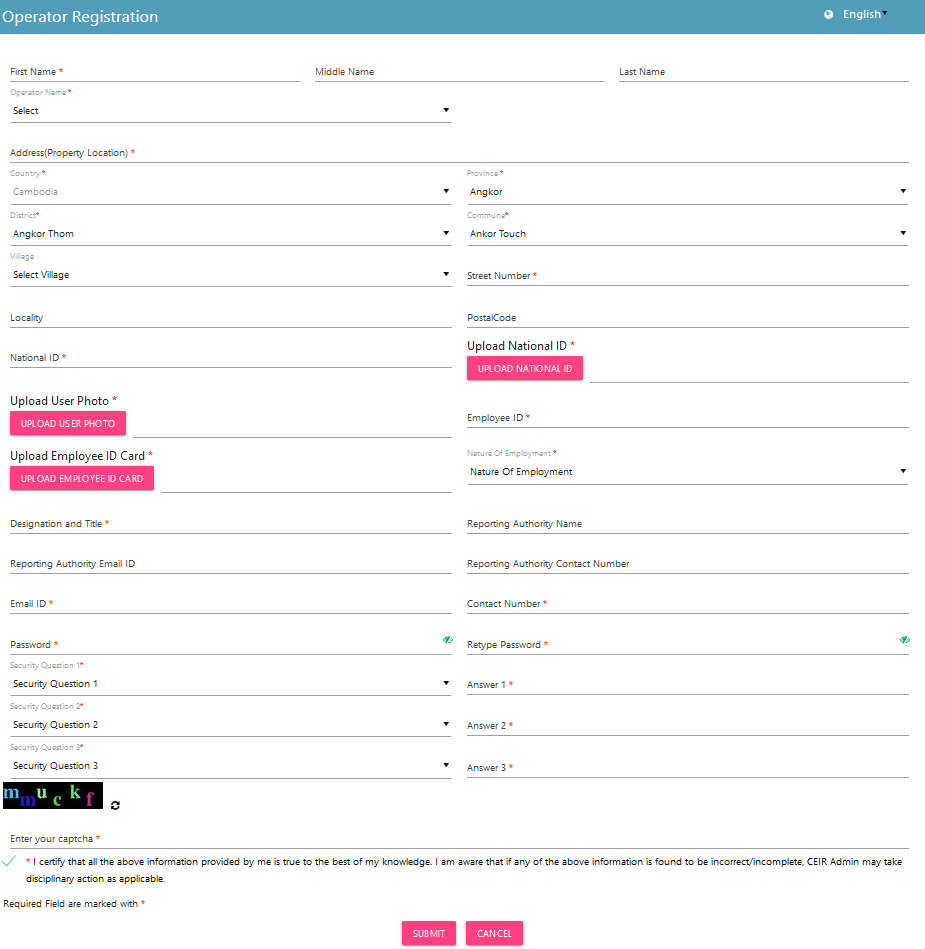


Figure 2: Operator Registration

1. **\*First Name**: Enter the first name.
2. **Middle Name**: Enter the middle name (if any).
3. **Last Name**: Enter the last name.
4. **\*Type**: Select the operator type:
   * Metfone
   * Smart
   * Seatel
   * Cellcard
5. **Address**: Enter the operator’s address:
   * **\***Street Number
   * Village
   * Locality
   * **\***District
   * **\***Commune
   * **\***Province
   * **\***Country
6. **\*National ID:** Enter the national ID of operator personnel.
7. **\*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.
8. **\*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.
9. **\*Employee ID**: Enter the employee ID of the operator.
10. **\*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.
11. **\*Nature of Employment**: Select the type of employment of the operator personnel:
    * Permanent
    * Temporary
    * Contract
12. **\*Designation and Title**: Enter the designation of the operator’s personnel.
13. **Reporting Authority Name**: Enter the name of the officer to whom the operator’s personnel reports to.
14. **Reporting Authority Email ID**: Enter the mail ID of the officer to whom the operator’s personnel reports to.
15. **Reporting Authority Contact Number**: Enter the contact number of the officer to whom the operator personnel reports to.
16. **Email ID**: Enter the mail ID of operator’s personnel. This mail ID would be used for communication with the operator.
17. **\*Contact Number**: Enter the mobile number of operator’s personnel. Operators receive notifications at this mobile number.
18. **\*Password**: Enter a login password. This is the password that would be used to log into the CEIR Operator Portal application.
19. **\*Confirm Password**: Re-enter the password for confirmation.
20. **\***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.
21. **\***Enter the captcha shown on the page. This is required to prove to the system that the operator is not a robot.
22. **\***Select the declaration check box.
23. Click **SUBMIT**.

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

A screenshot of a cell phone

Description automatically generated

Figure 3: Verify OTP

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

A screenshot of a cell phone

Description automatically generated

Figure 4: Enter OTP

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

A screenshot of a social media post

Description automatically generated

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

A screenshot of a cell phone

Description automatically generated

Figure 5: Login

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

A screenshot of a cell phone

Description automatically generated

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

Username is the registration ID that is sent on mail to the 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*.

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

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

On entering correct information, the application Home page appears.

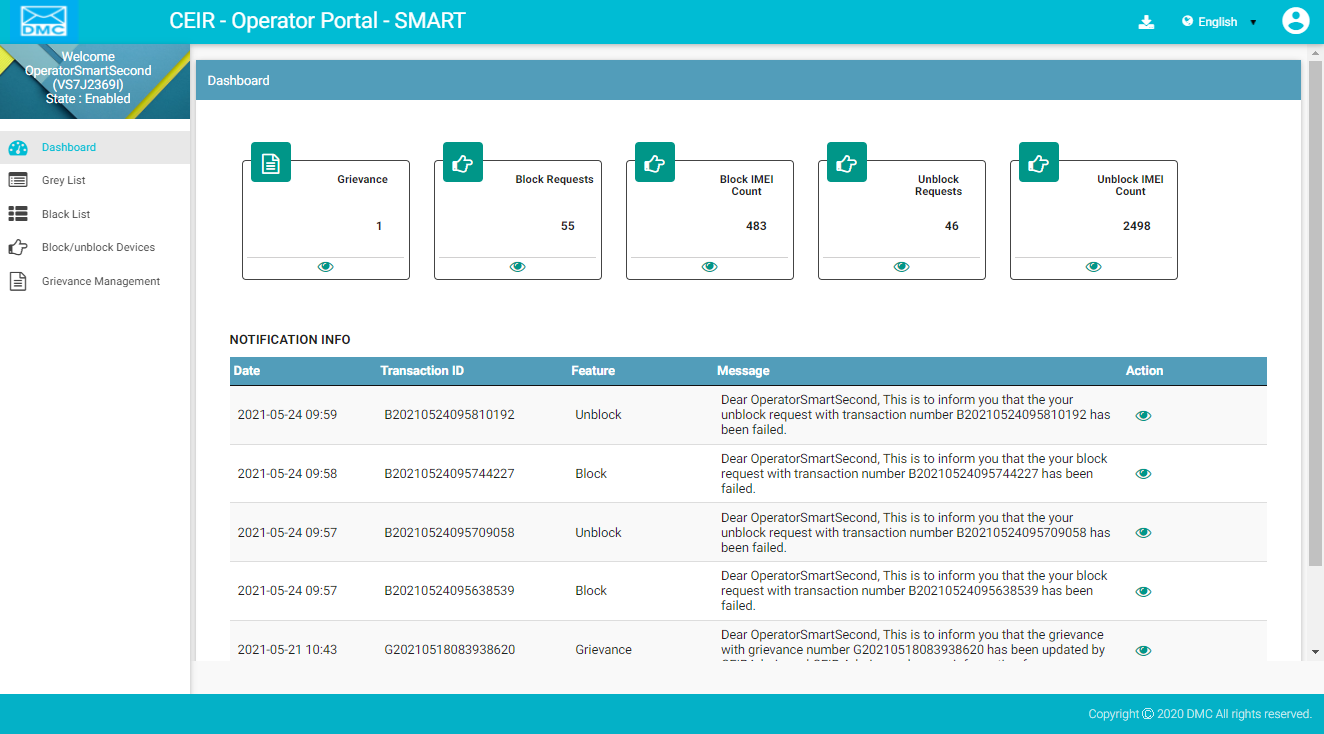


Figure 6: Home Page

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

A screenshot of a cell phone

Description automatically generated

Figure 7: Forgot Password

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

The **Set New Password** page appears.

A screenshot of a cell phone

Description automatically generated

Figure 8: Set New Password

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

## Application User Interface

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

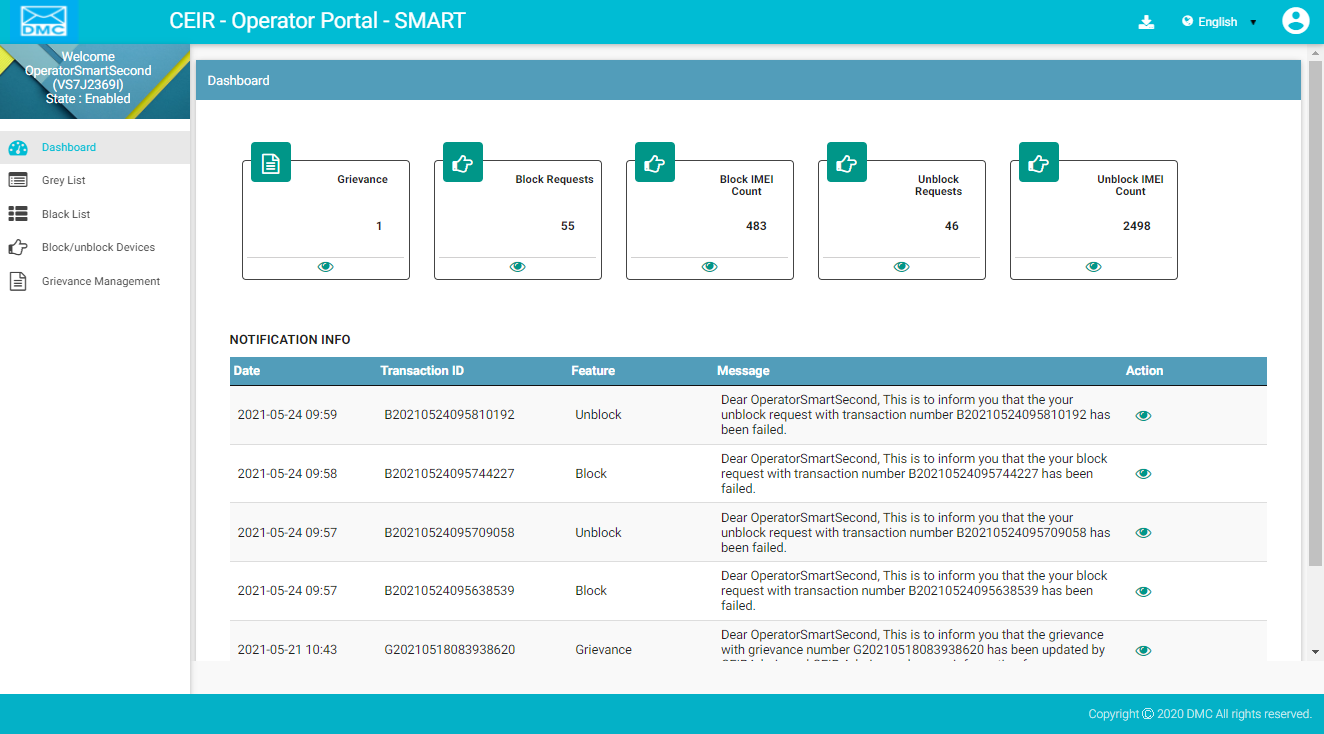


Figure 9: Home Page

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.

A close up of a logo

Description automatically generated

* A close up of a logo

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

A screenshot of a cell phone

Description automatically generated

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

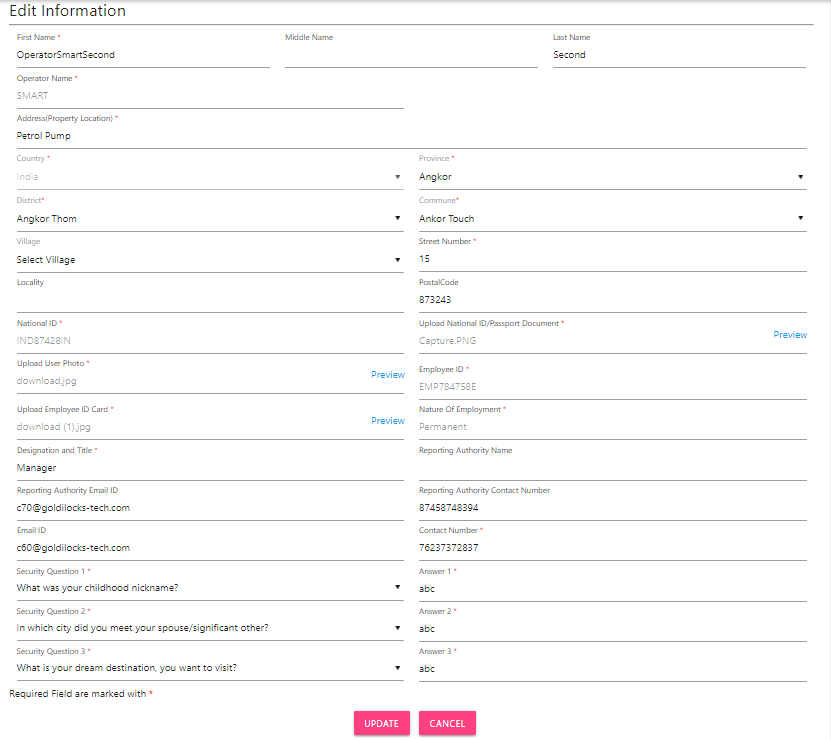


Figure 10: Edit Information

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

User is prompted to enter the password for confirmation of edit profile.

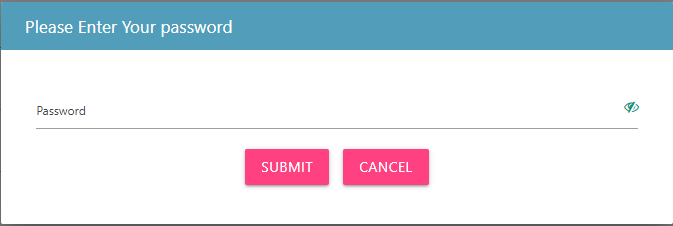


Figure 11: Password confirmation

OTP is sent to the user in case contact number or email id is changed.

A screenshot of a cell phone

Description automatically generated

Figure 12: Verify OTP notification

A screenshot of a cell phone

Description automatically generated

Figure 13: Verify OTP

Enter the two OTPs and click **Done**.

If the two OTPs match, the following message appears. If the OTPs do not match, click **Resend OTP**. The two OTPs are resent, one to the contact number and the other to the mail account.

After the OTPs are verified successfully, user profile is updated.

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

A screenshot of a cell phone

Description automatically generated

Figure 14: 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**): 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.

A screenshot of a cell phone

Description automatically generated

Figure 15: Manage Account

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

## Dashboard

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

* Block/Unblock Requests
* Block/Unblock Device Count
* Grievances

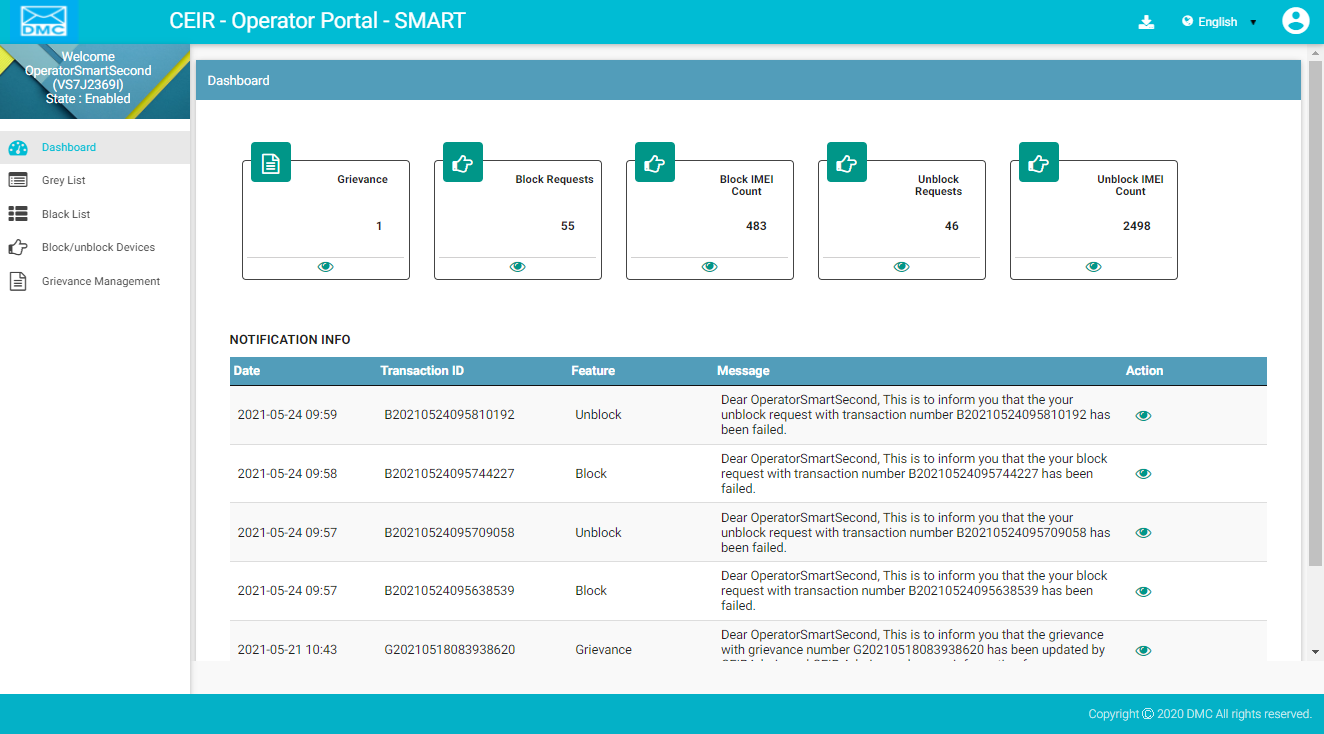
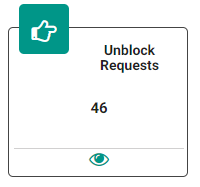
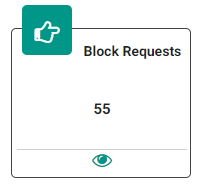


Figure 16: Home Page

**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.

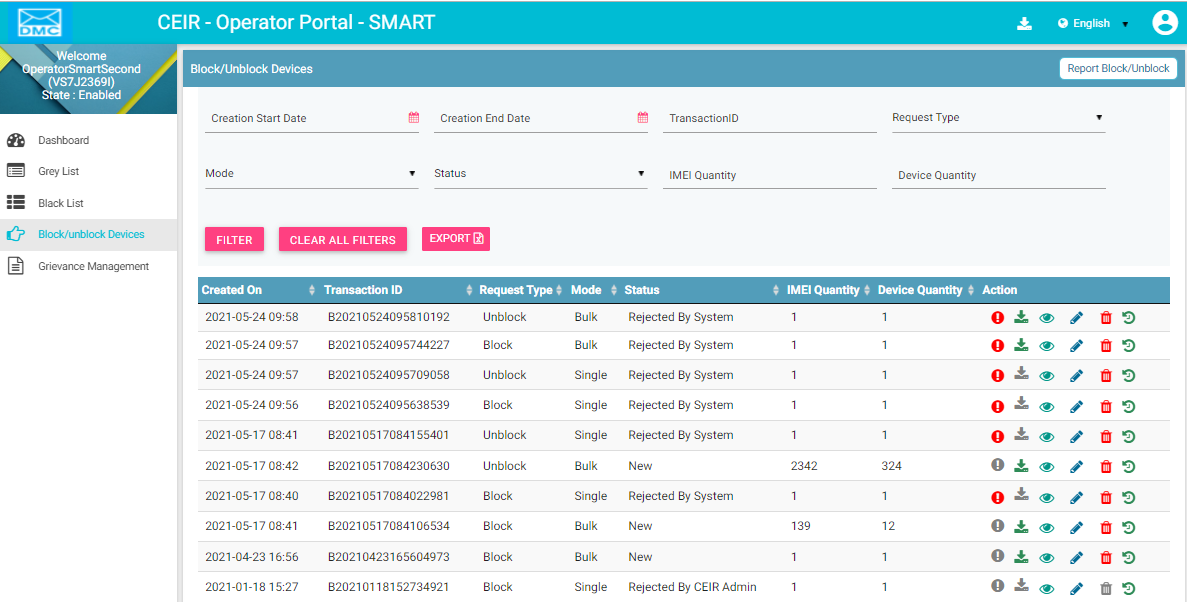
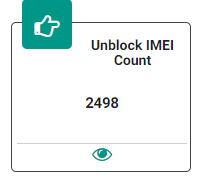
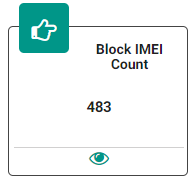


Figure 17: Block/Unblock Devices

**Block/Unblock Device Count**

The box displays the total number of devices (IMEIs) 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.

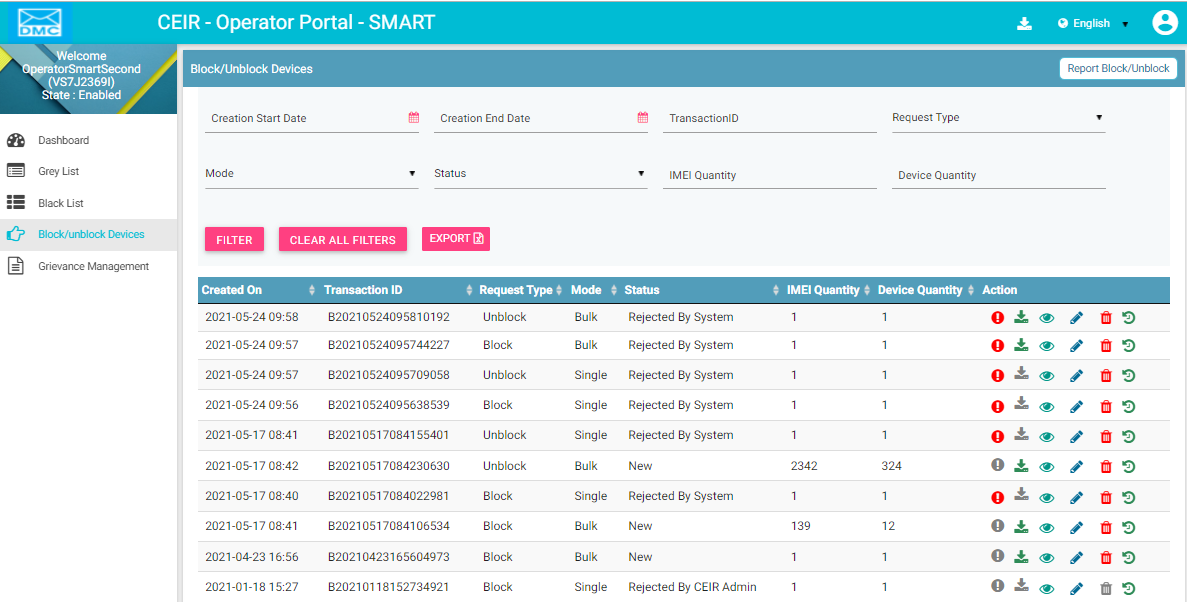


Figure 18: Block/Unblock Devices

**Grievance**

This box displays the total number of grievances raised.

A screenshot of a cell phone

Description automatically generated

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

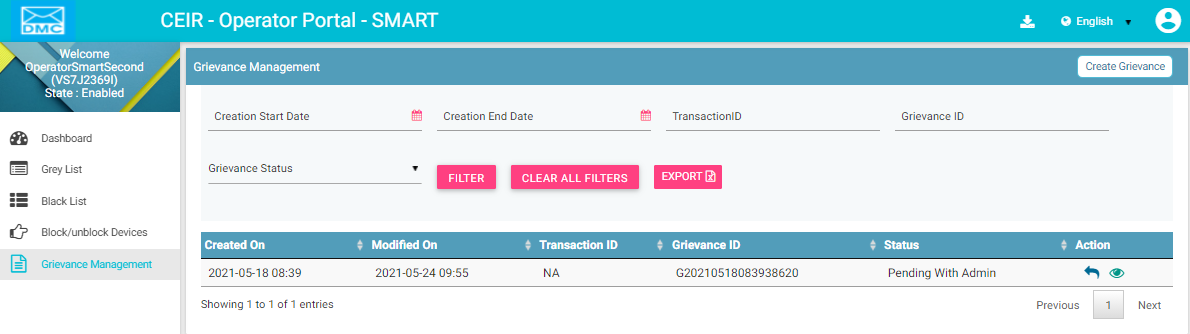


Figure 19: Grievance Management

**Notification Information**

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

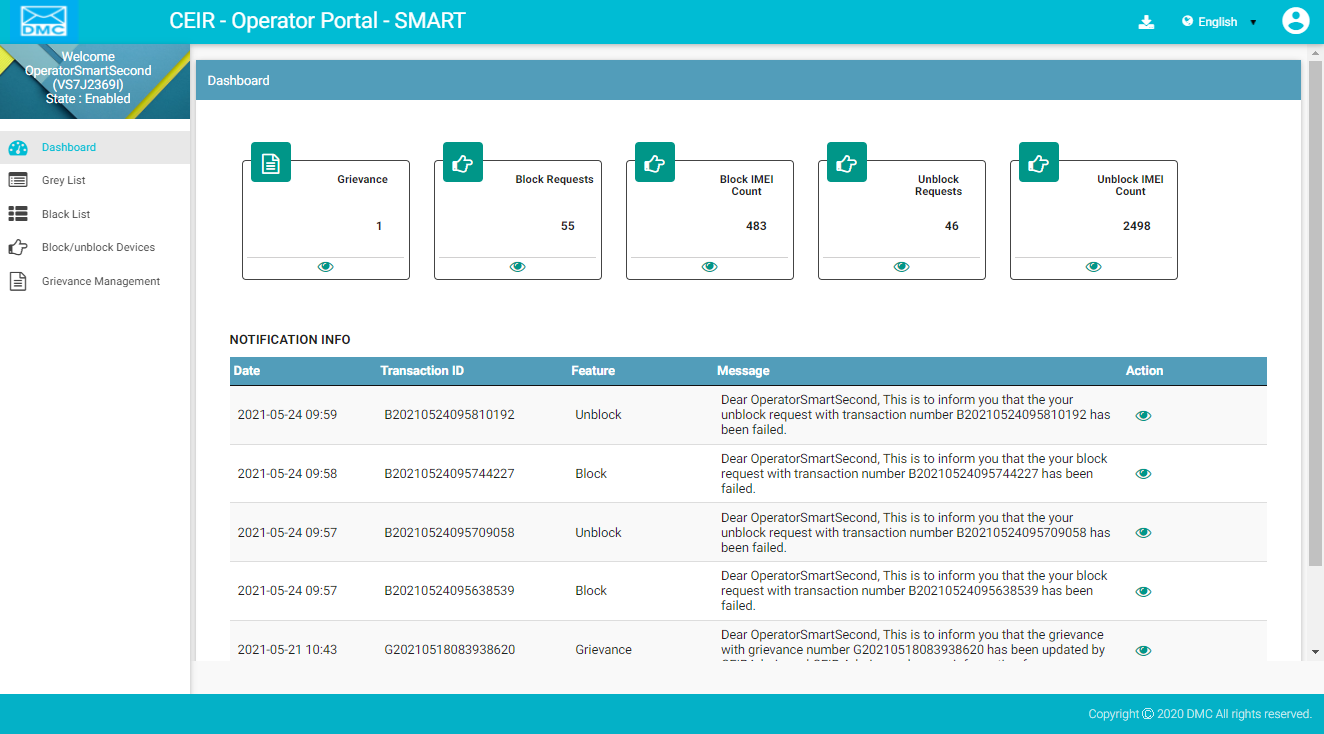


Figure 20: Home Page

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
* **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 .

## 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.

### Single Device Blocking/Unblocking

To block or unblock a single device:

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

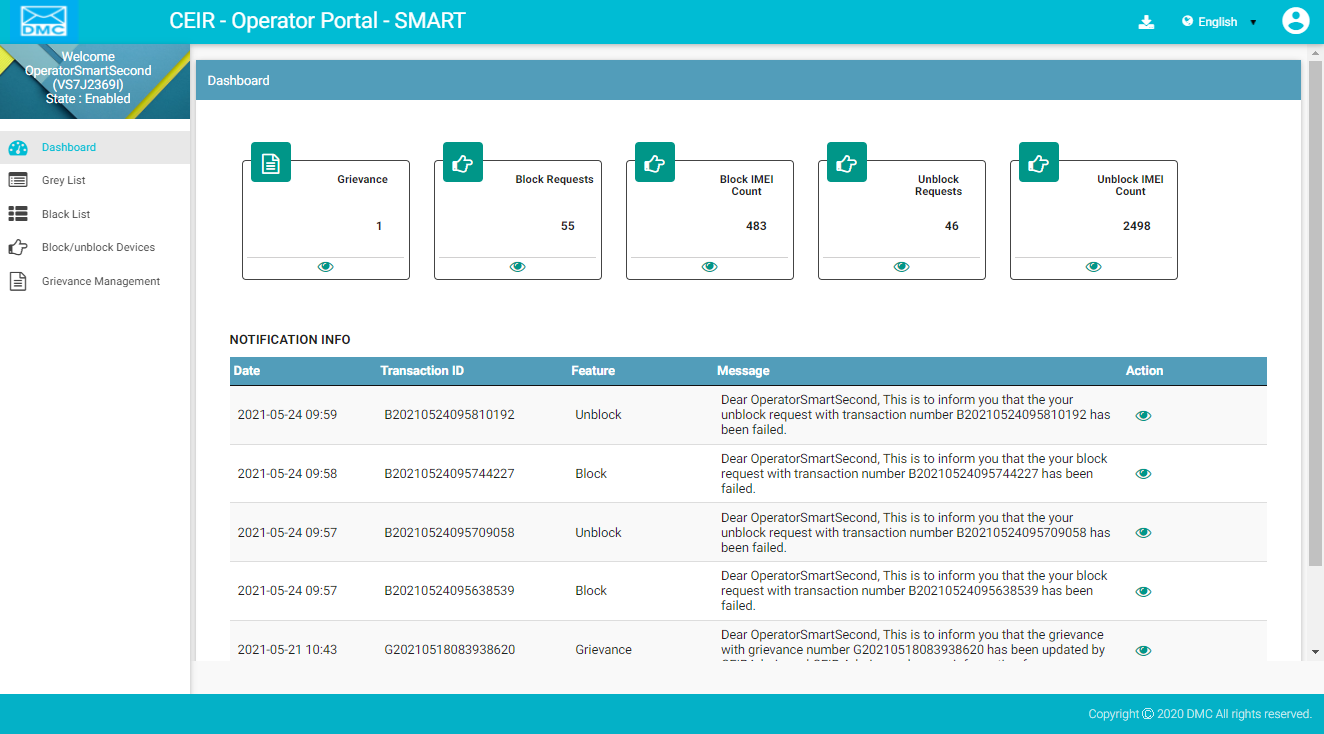


Figure 21: Home Page

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

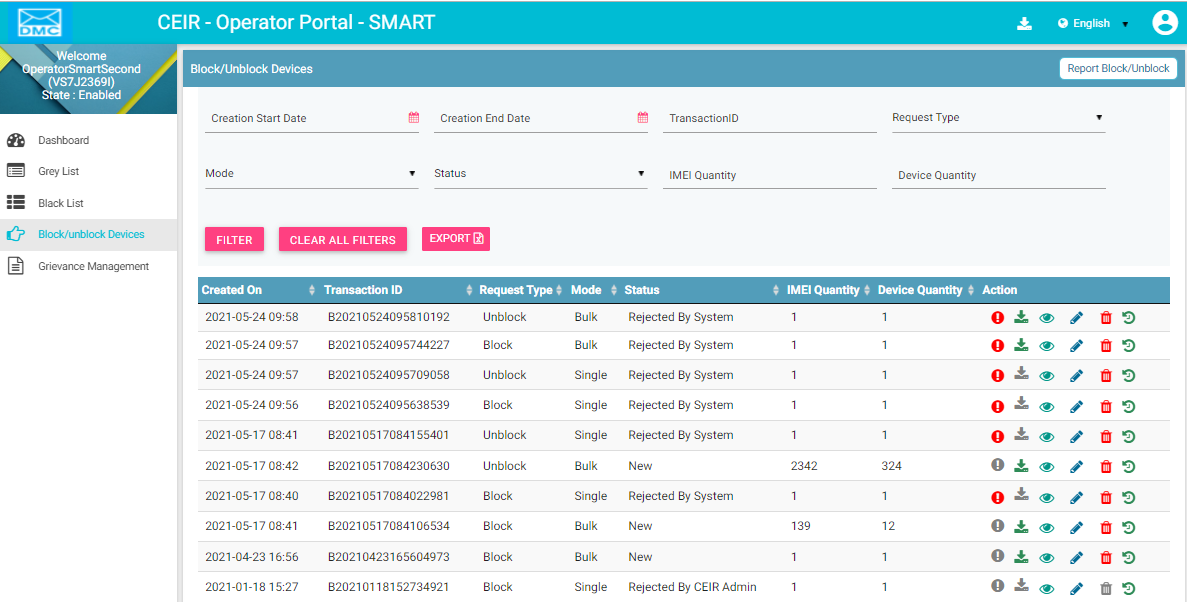


Figure 22: Block/Unblock Devices

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



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

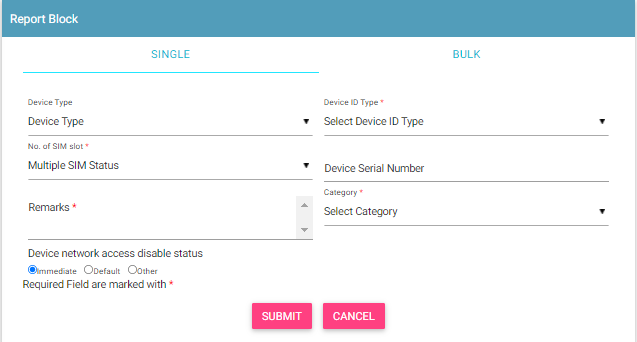


Figure 23: Report Block

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

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

1. 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 A picture containing clock, door, drawing

    Description automatically generated.
* **IMEI**: Enter the value of the IMEIs of the device to be blocked.

1. 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.

A screenshot of a social media post

Description automatically generated

For each request, the dashboard displays the following information:

| **Column** | **Description** |
| --- | --- |
| Date | Date of registering the request to 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.   + 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. |
| IMEI 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. |
| Device Quantity | Total number of devices 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 A circuit board    Description automatically generated: 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. * View : This is used to view the request. Click on it view the request details. * Edit A close up of a logo    Description automatically generated: This is used to modify the request. This is allowed 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. |

### 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.

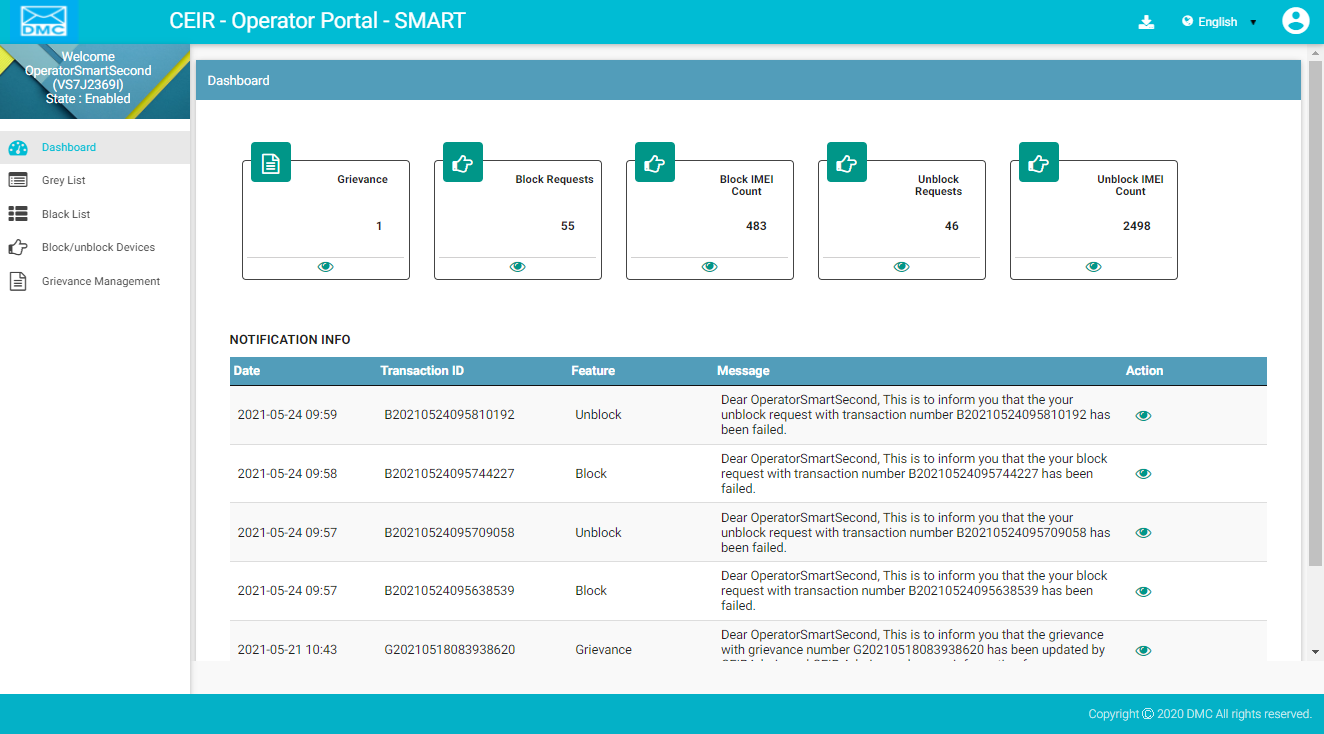


Figure 24: Report Block

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

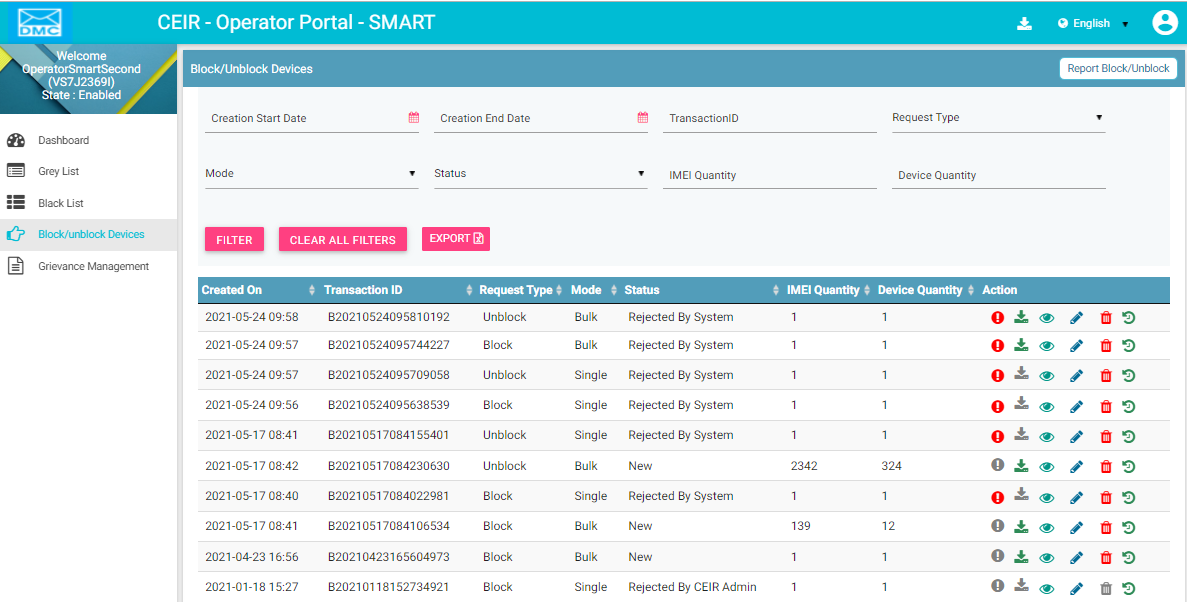


Figure 25: Block/Unblock Devices

1. Click **Report Block/Unblock**.



1. Select **Block** or **Unblock**.
2. On selecting **Block**, the **Report Block** page appears. Select **Bulk**.

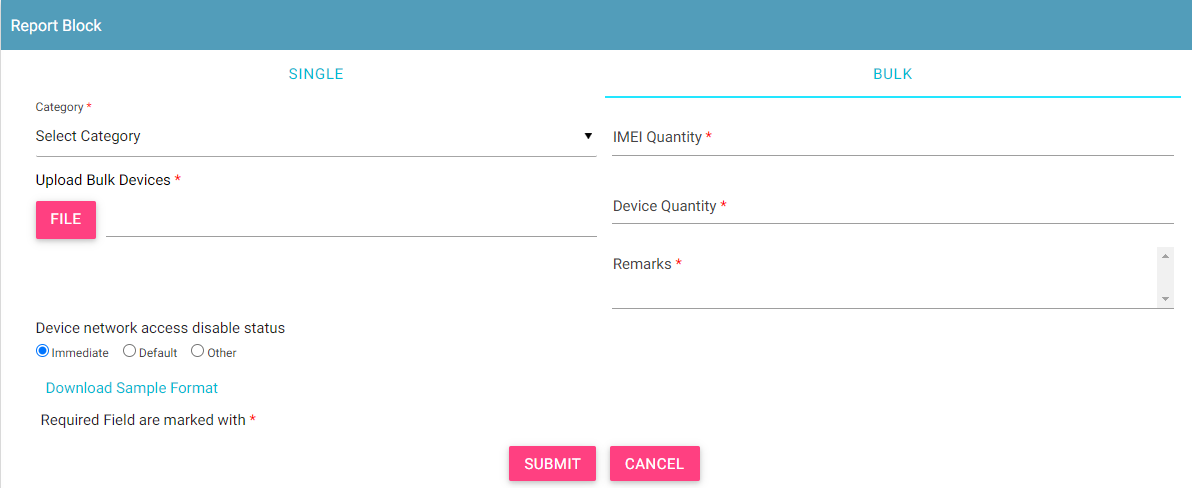
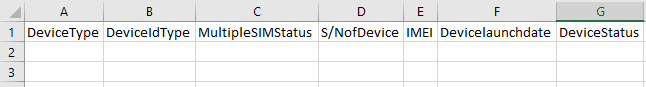


Figure 26: Report Block

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.



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.
  + **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)



* 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.

## 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 (**A close up of a logo

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

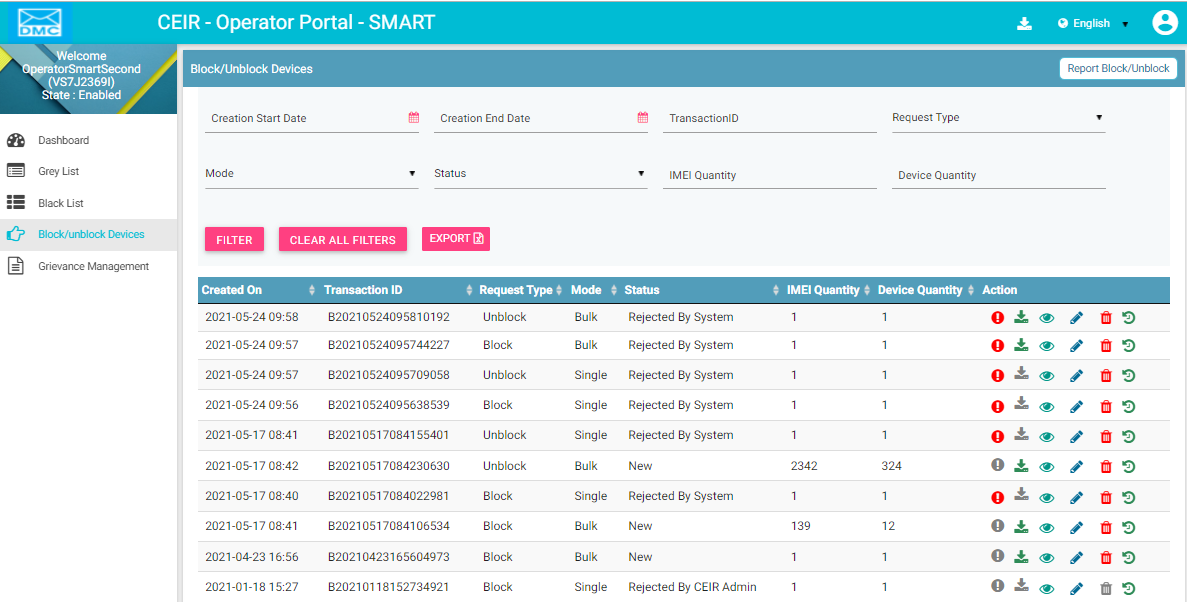


Figure 27: Block/Unblock Devices

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

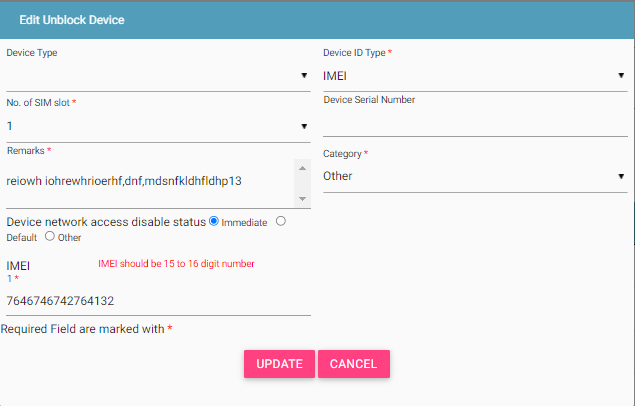


Figure 28: Edit Block Device (Single Device)

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

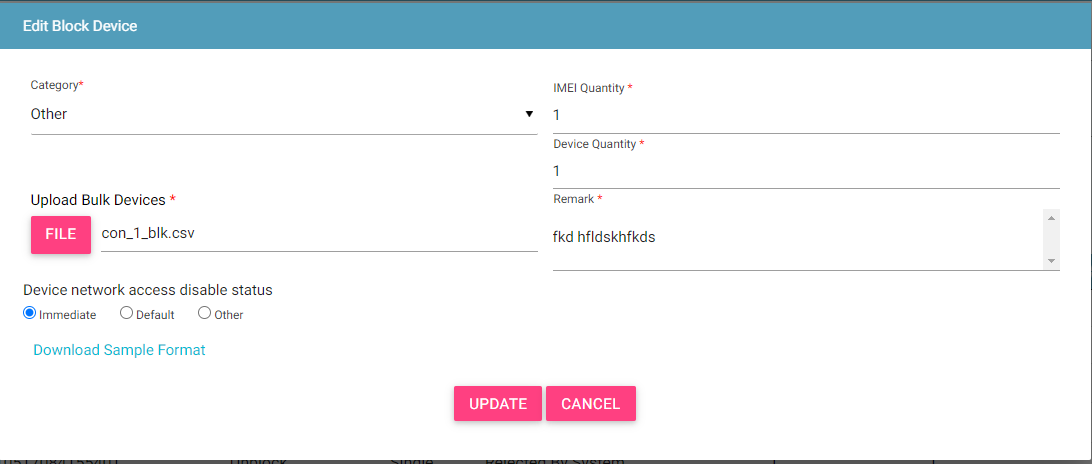


Figure 29: Edit Block Device (Bulk Device)

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

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

## Filter 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:

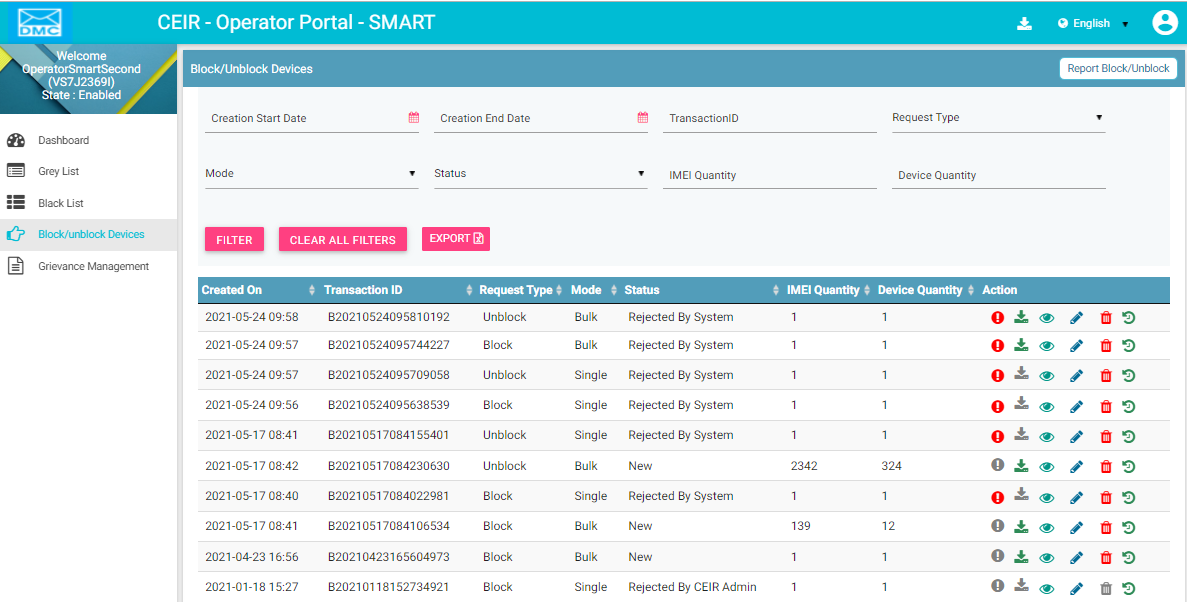


Figure 30: Block/unblock Devices

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.
* **Status**: This refers to the status of the request:
  + New
  + Processing
  + Rejected by System
  + Rejected CEIR Admin
  + Approved CEIR Admin
  + Withdrawn CEIR Admin
  + Withdrawn by User
* **IMEI Quantity**: Enter the number of IMEIs in the request.
* **Device Quantity**: Enter the number of devices in the request.

1. Click **FILTER**.

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

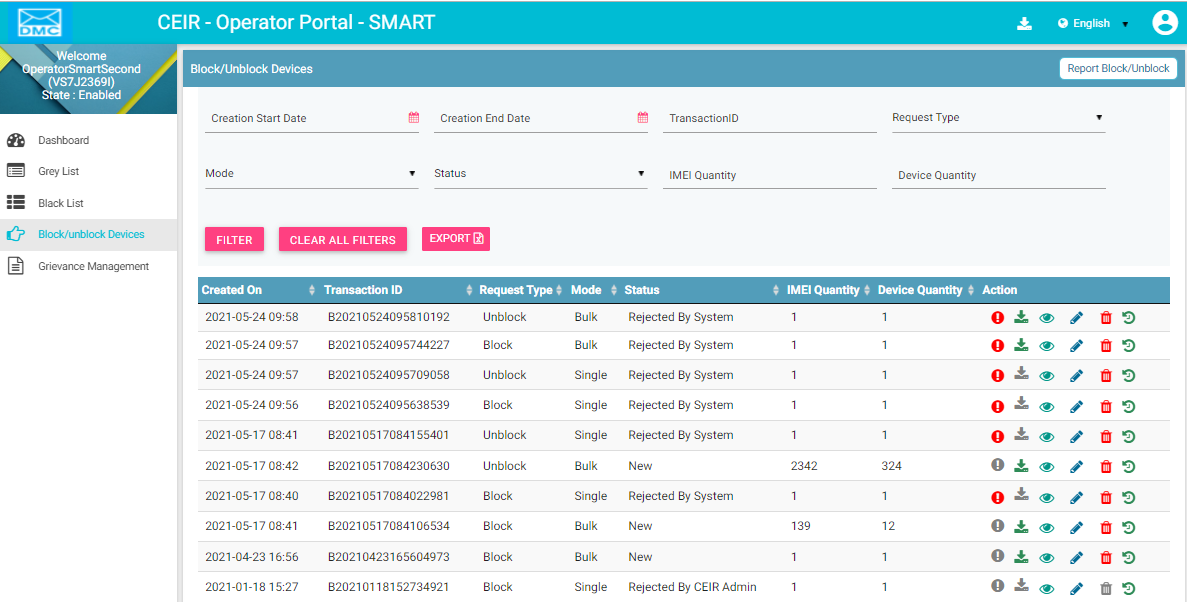


Figure 31: Filtered Device Block/Unblock Requests

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

## 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.

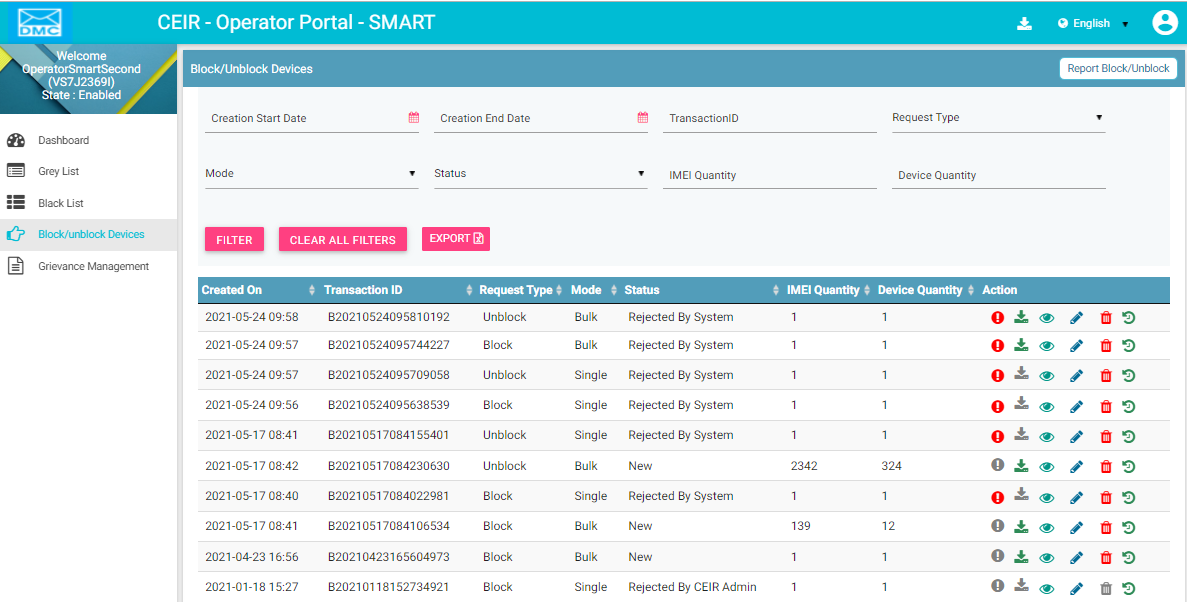


Figure 32: Sort Block/Unblock Requests

## 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**.

A screenshot of a cell phone

Description automatically generated

Figure 33: Block/Unblock Devices

The following page appears.

A screenshot of a cell phone

Description automatically generated

Figure 34: Open or Save Exported Block/Unblock Devices File

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

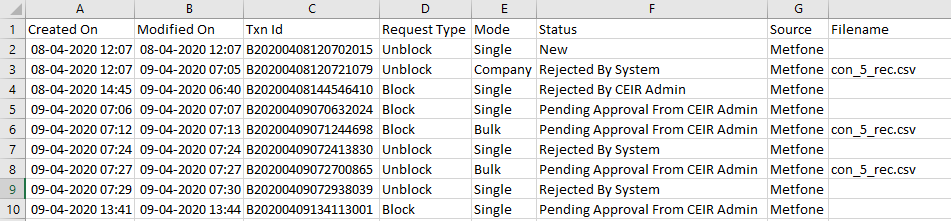


Figure 35: Exported Block/Unblock Devices

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.

## 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.

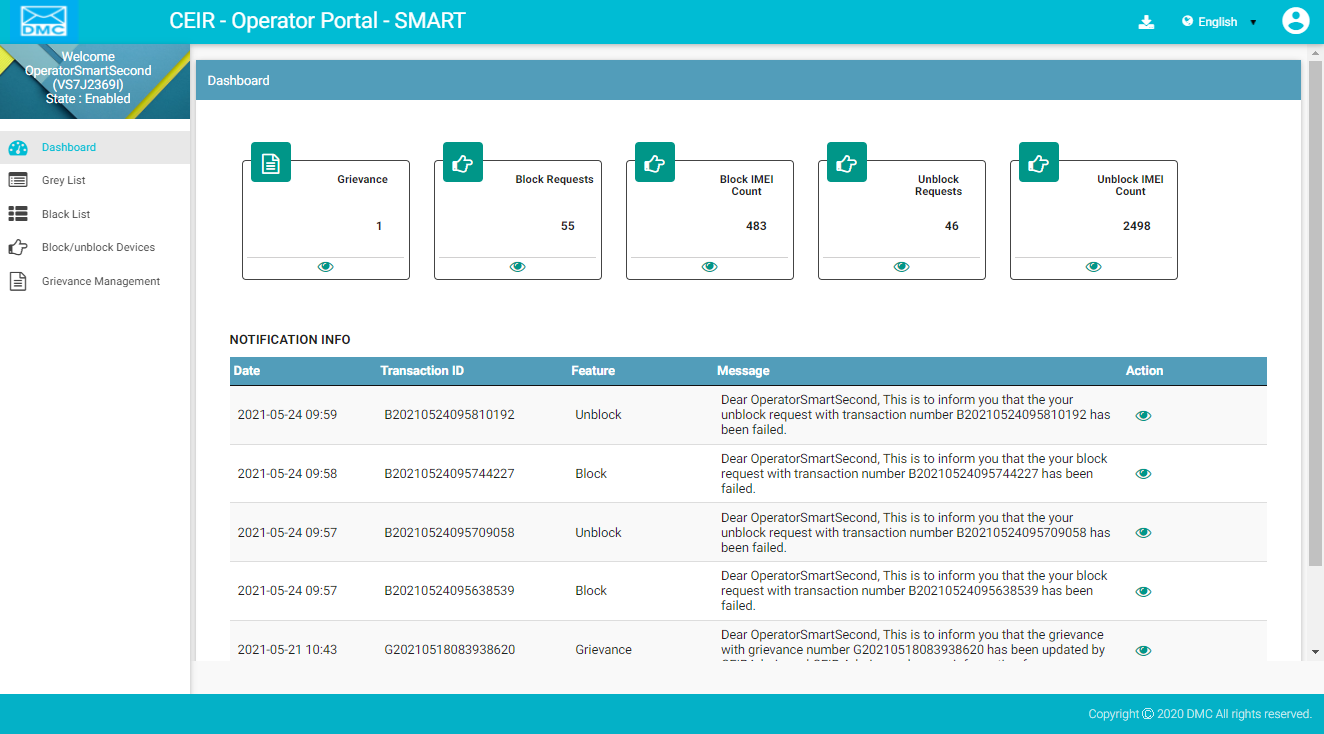


Figure 36: Home Page

The **Grey List** page appears.

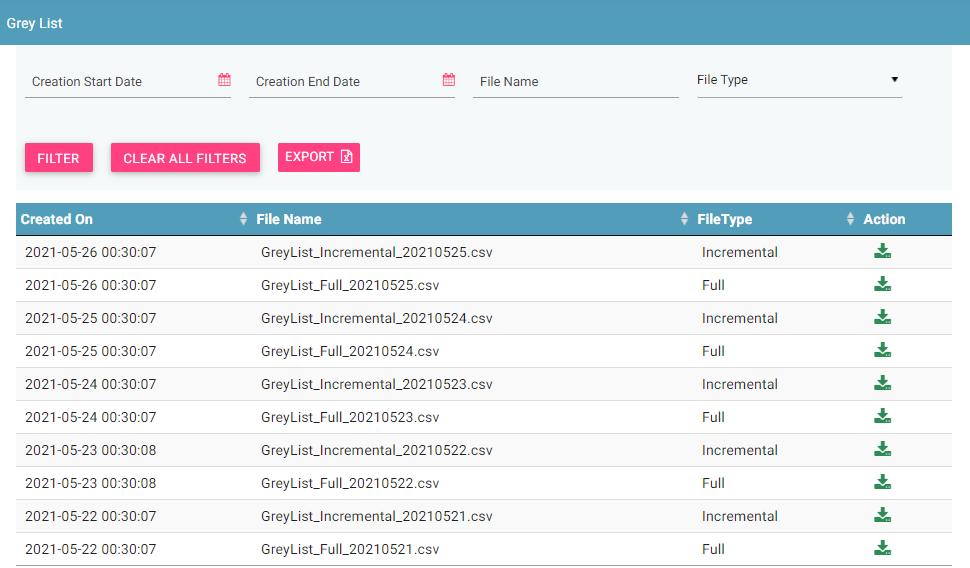


Figure 37: Grey List

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

| **Column** | **Description** |
| --- | --- |
| Created On | Date on which the file is created. |
| File Name | Name of the file.  The file naming convention is:  **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 A circuit board  Description automatically generated: This is used to take a dump of the file to view it. |

A sample incremental file is shown.

A screenshot of a cell phone

Description automatically generated

A sample full file is shown.

A screenshot of a cell phone

Description automatically generated

## 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:

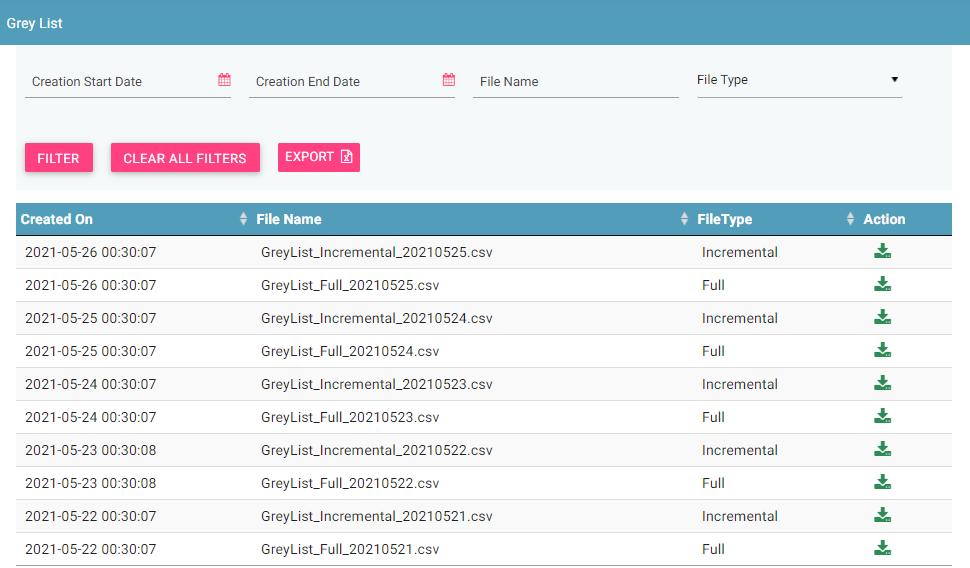


Figure 38: Grey List

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

1. Click **FILTER**.

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

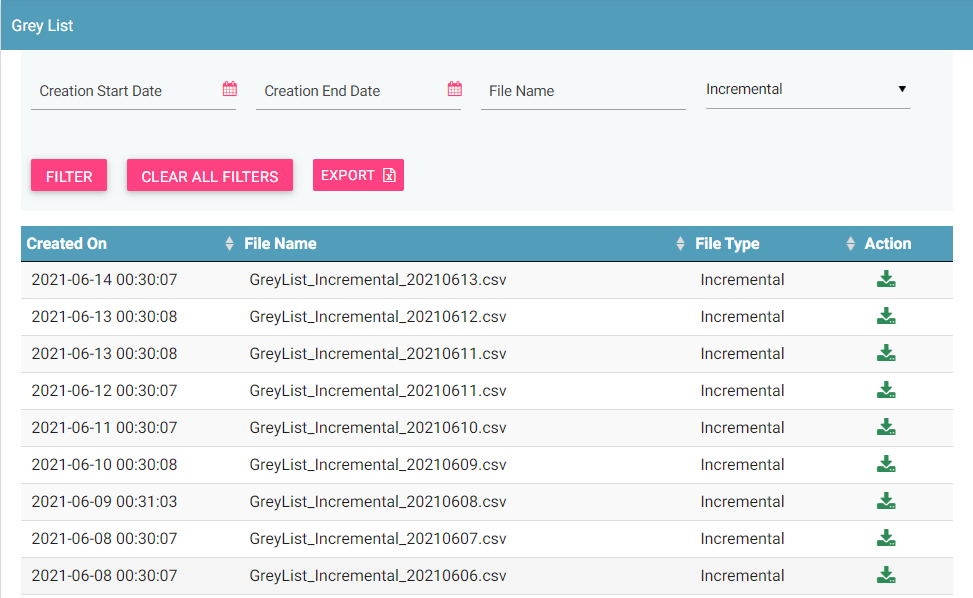


Figure 39: Filtered Greylists

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.

## 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.

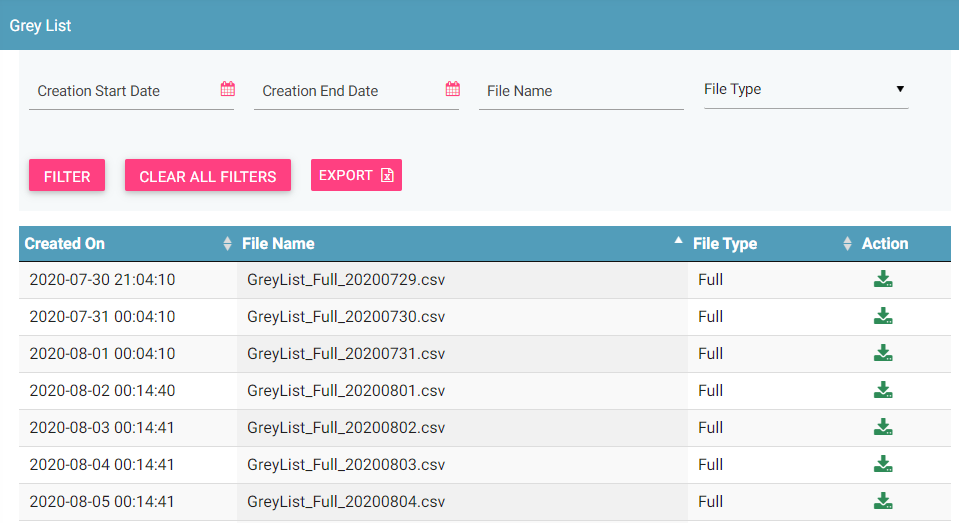


Figure 40: Sort Greylists

## 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).

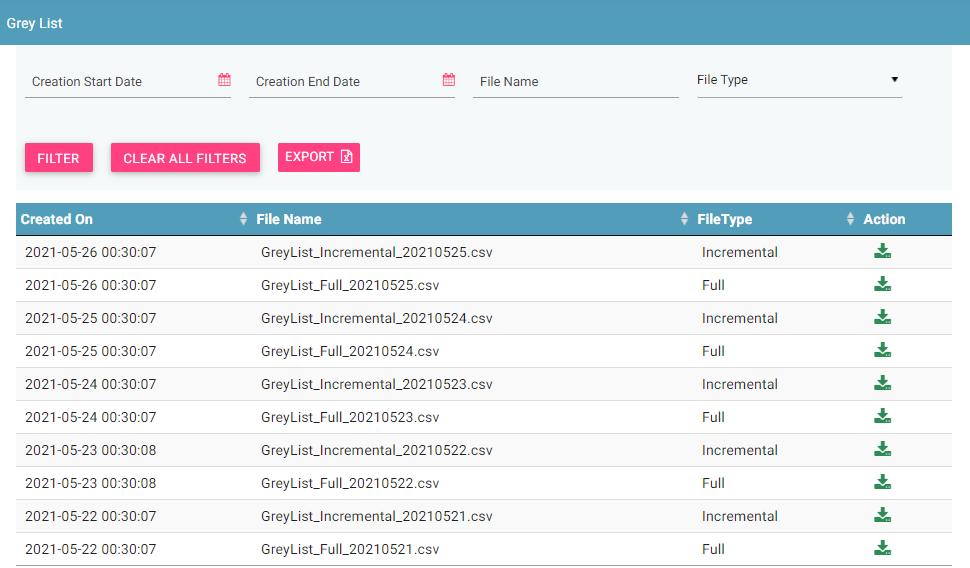


Figure 41: Grey List

The following page appears.

A screenshot of a cell phone

Description automatically generated

Figure 42: Open or Save Exported Greylists

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

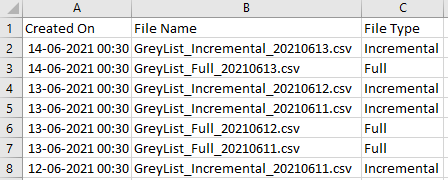


Figure 43: Exported Greylists

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.

## 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.

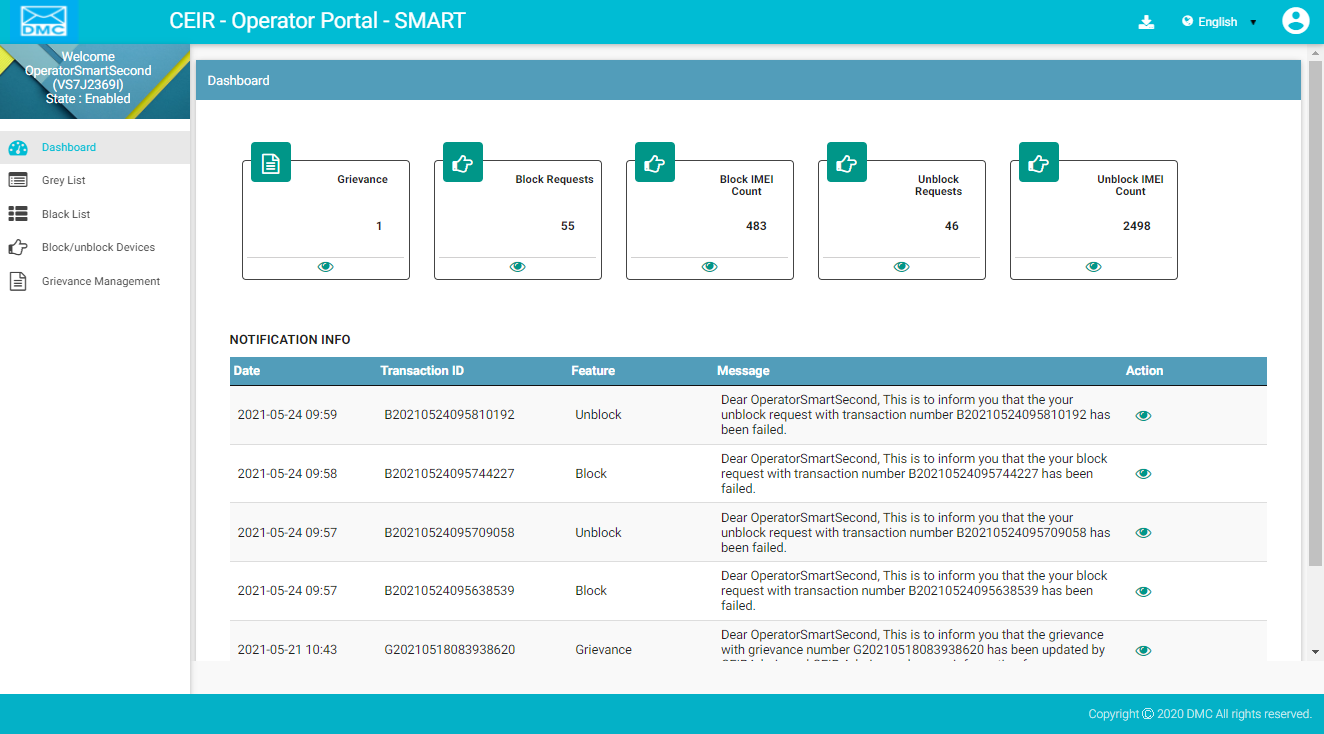


Figure 44: Home Page

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

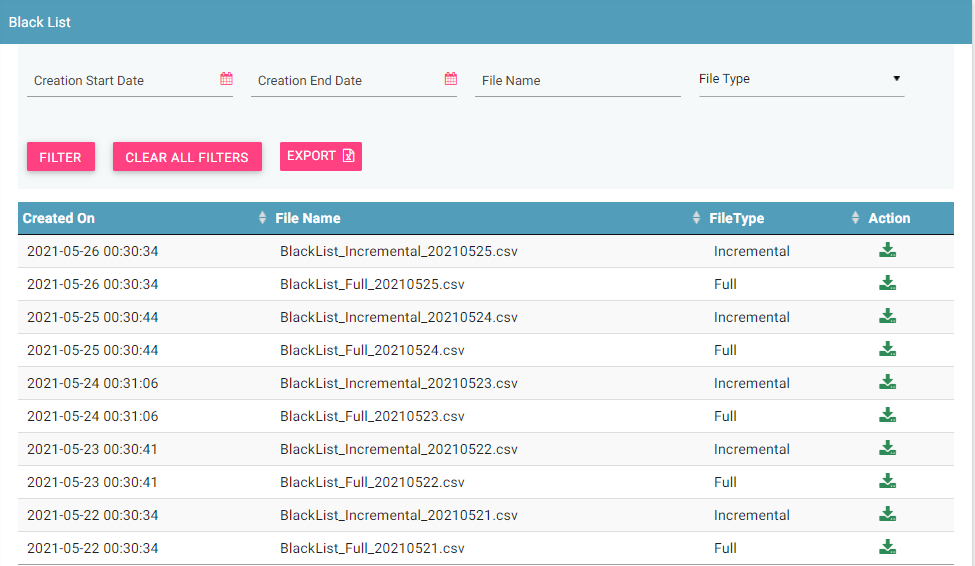


Figure 45: Black List

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

| **Column** | **Description** |
| --- | --- |
| Created 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**:   + Full: A full file shows all the device IDs in the blacklist as on date (yyyymmdd).   + 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.  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 A circuit board  Description automatically generated: This is used to take a dump of the file to view it. |

A sample partial blacklist file is shown.

A screenshot of a computer

Description automatically generated

A sample full blacklist file is shown.

A screenshot of a cell phone

Description automatically generated

## 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:

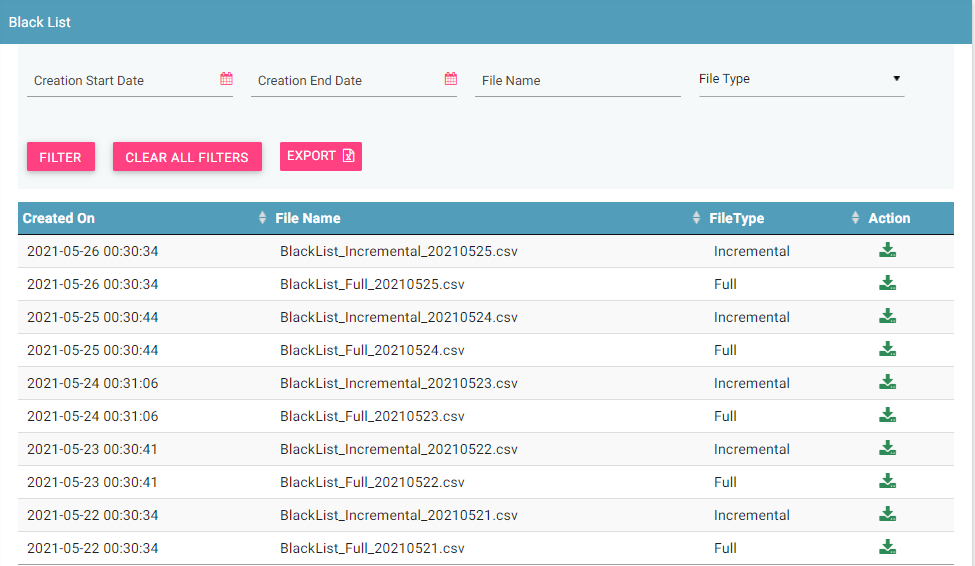


Figure 46: Black List

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

* **Start Date** and **End Date**: Period of generated blacklist files.
* **FileName:** This refers to the filename.
* **File Type**: The type can be:
  + Full
  + Incremental

1. Click **Filter**.

The filtered files are shown on the page.

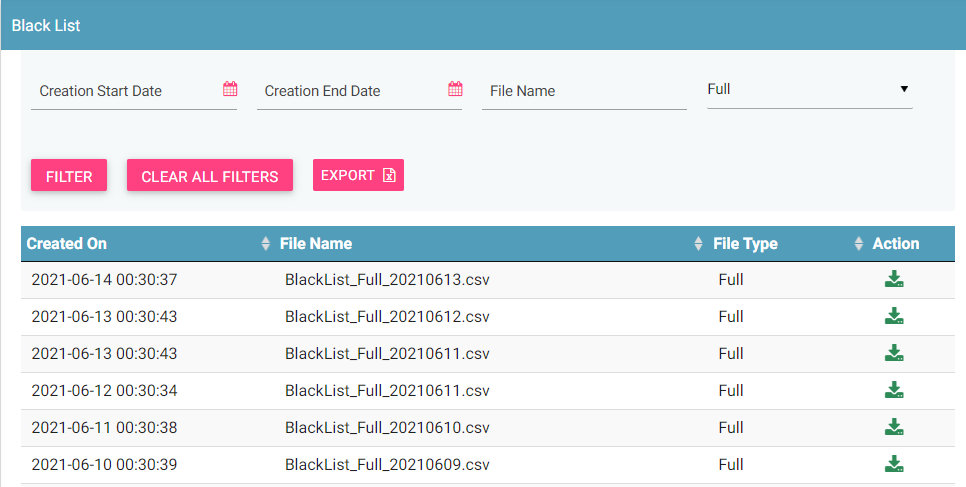


Figure 47: Filtered Blacklists

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.

## 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.

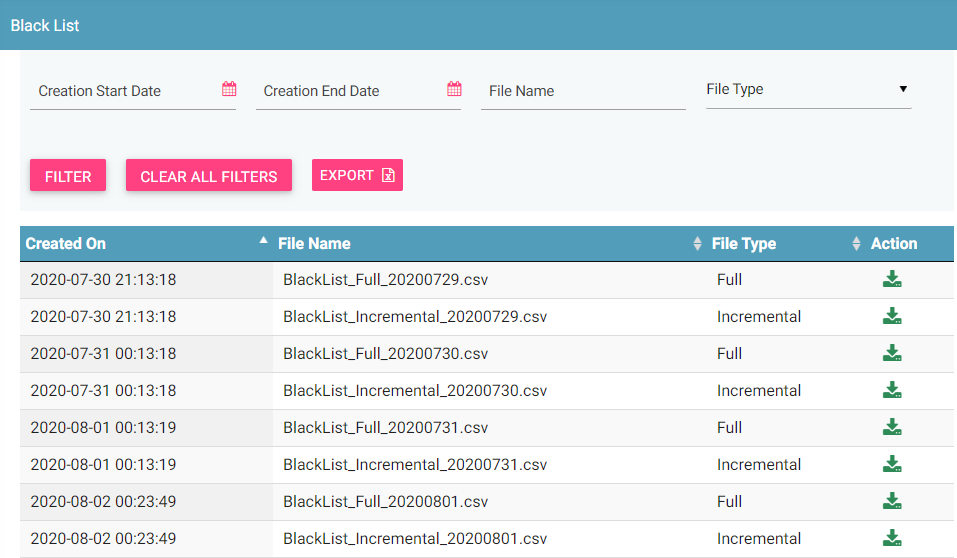


Figure 48: Sort Blacklists

## 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).

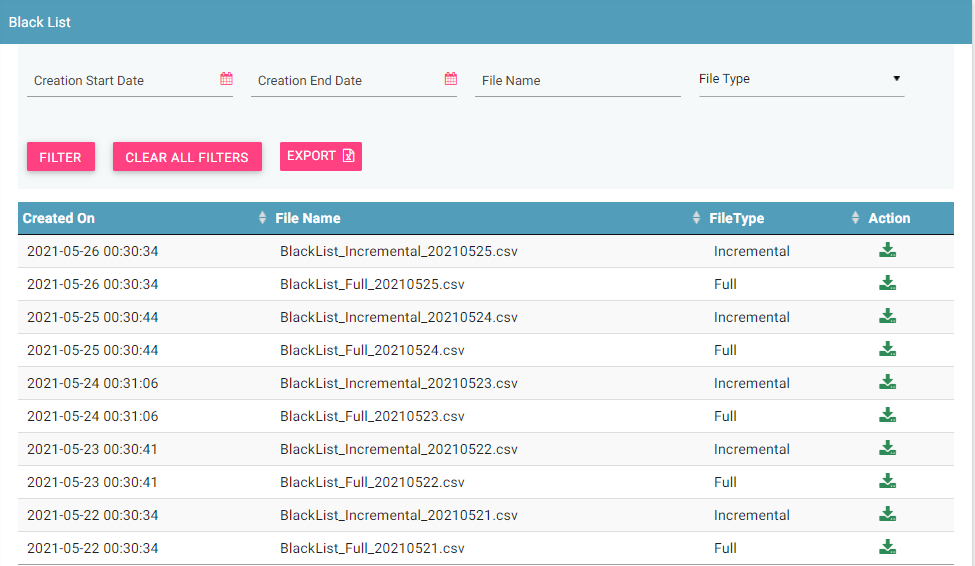


Figure 49: Black List

The following page appears.

A screenshot of a cell phone

Description automatically generated

Figure 50: Open or Save Exported Blacklist File

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

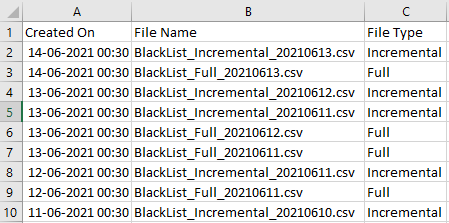


Figure 51: Exported Blacklists

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.

## 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

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

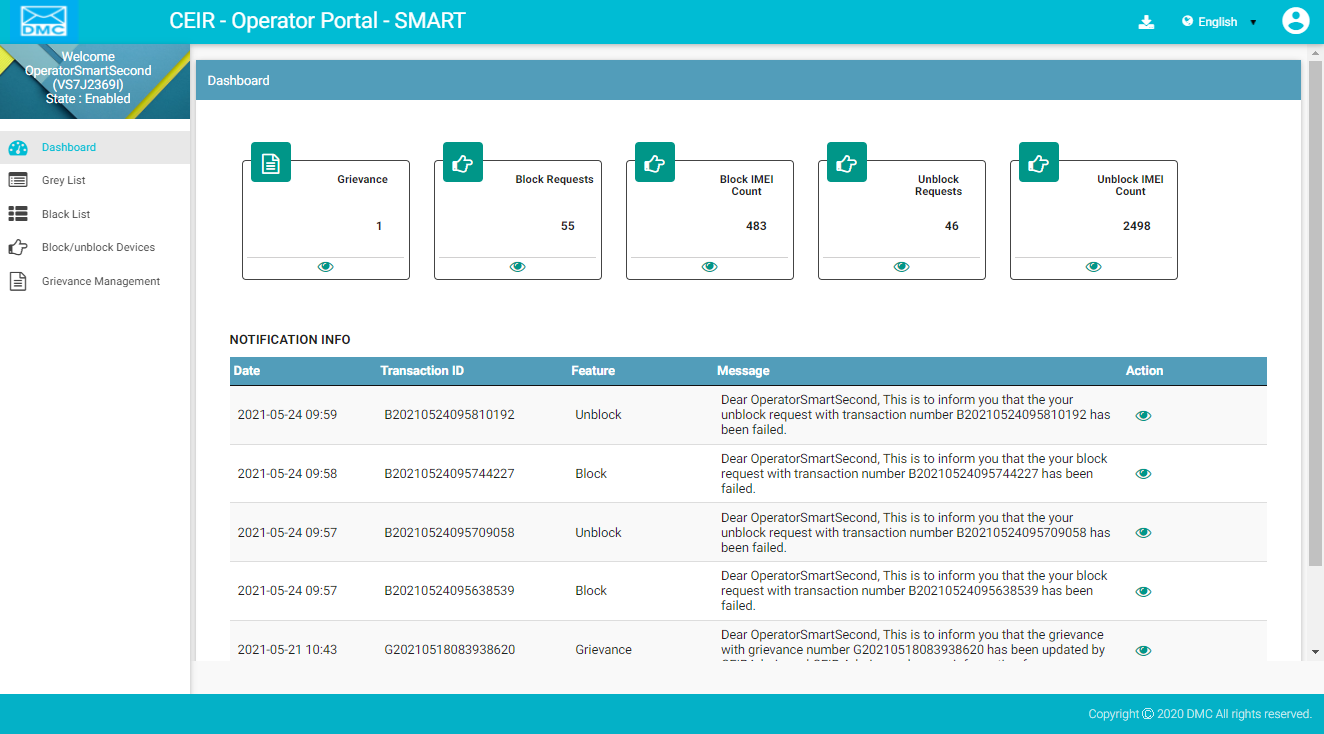


Figure 52: Home Page

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

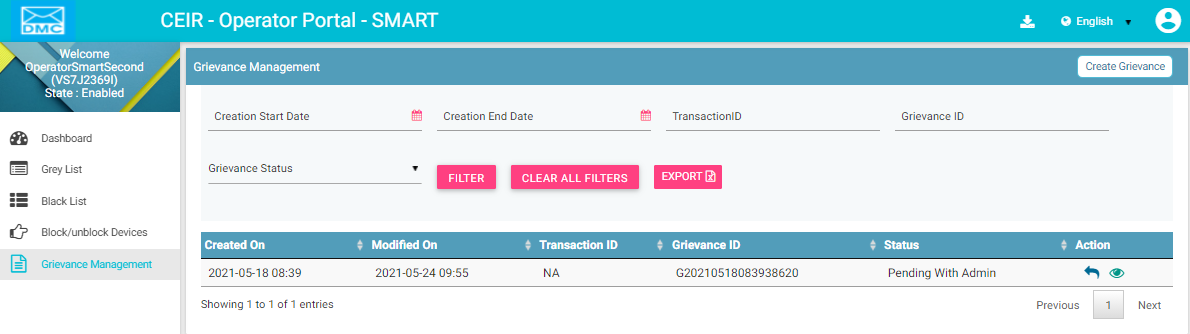


Figure 53: Grievance Management

The **Report Grievance** page appears.

A screenshot of a cell phone

Description automatically generated

Figure 54: Report Grievance

1. Enter the following information:
   1. **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.
   2. **\*Category**: Select the category of the grievance. The options are:

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

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

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

1. Click **SUBMIT**.

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

A screenshot of a social media post

Description automatically generated

The new grievance appears on the top of the page.

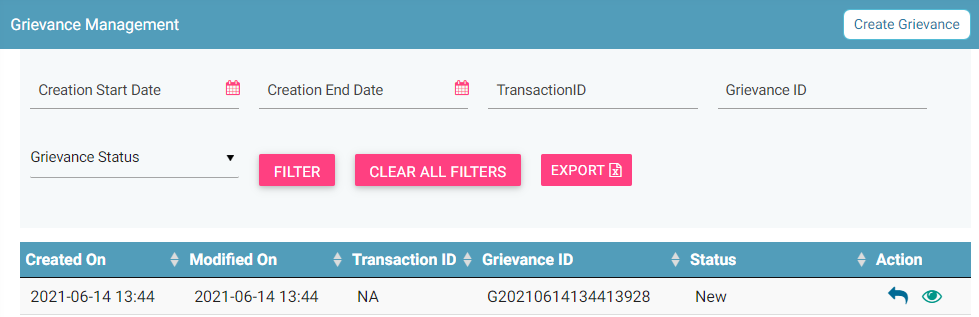


Figure 55: Grievance Management

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

| **Column** | **Description** |
| --- | --- |
| Created On | Date of raising a grievance. |
| Modified On | The date when the grievance was modified. |
| Transaction ID | The transaction ID of request for which a grievance was raised. |
| Grievance ID | This is the ID that is automatically assigned to the grievance. |
| Grievance Status | The uploaded grievance goes through different status modes.   * New: When a grievance is raised. * Pending with CEIR 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 A close up of a logo    Description automatically generated: This is used to view the grievance response history. The operator can see all the responses exchanged for any grievance. |

## 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:

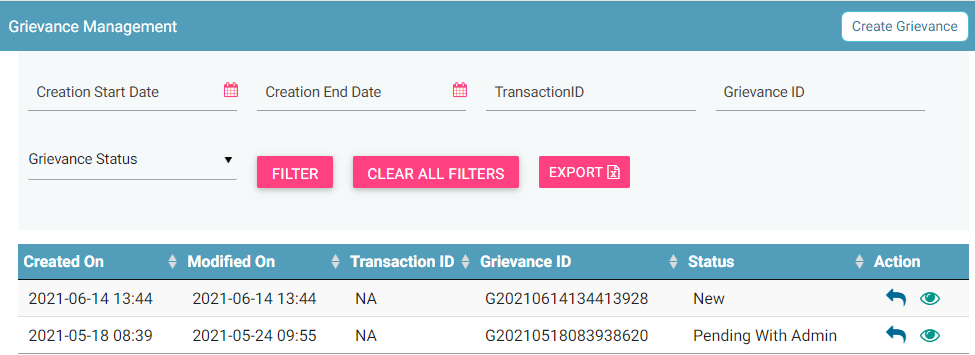


Figure 56: Filter Grievances

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

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

1. Click **Filter**.

The filtered grievances are shown on the page.

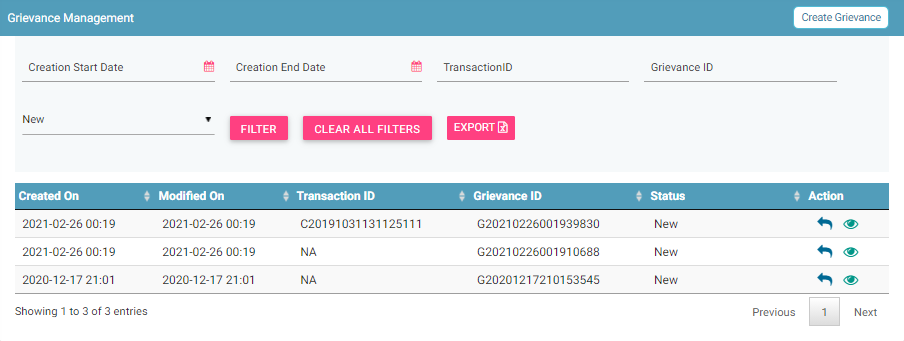


Figure 57: Filtered Grievances

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.

## 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.

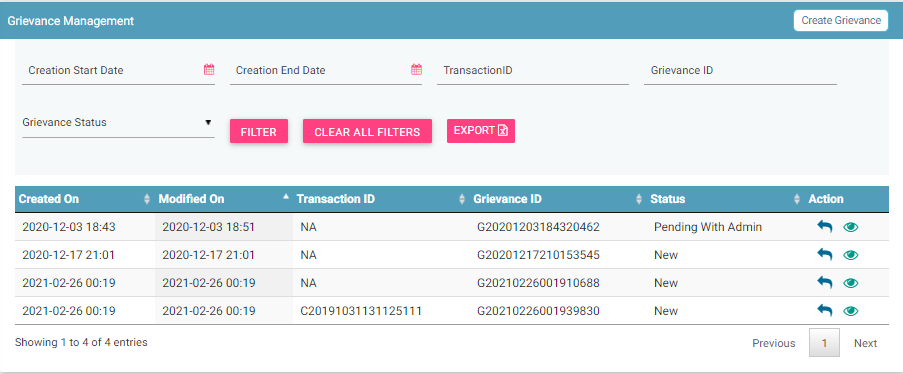


Figure 58: Sort Grievances

## Export Grievances

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

To export the grievances:

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

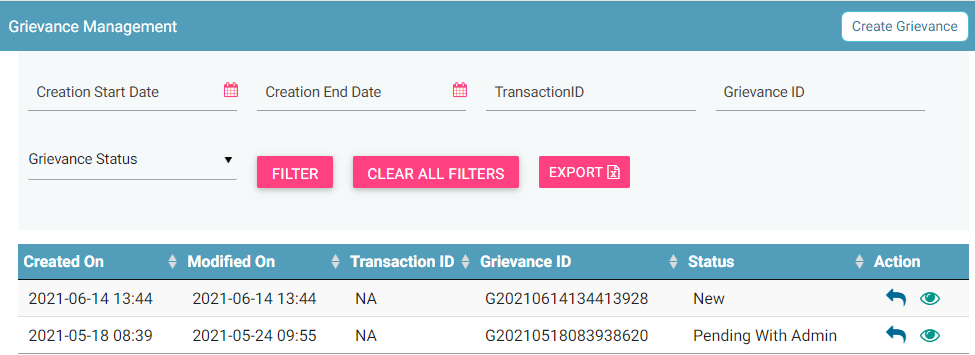


Figure 59: Grievance Management

The following page appears.

A screenshot of a cell phone

Description automatically generated

Figure 60: Open or Save Exported Grievance File

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

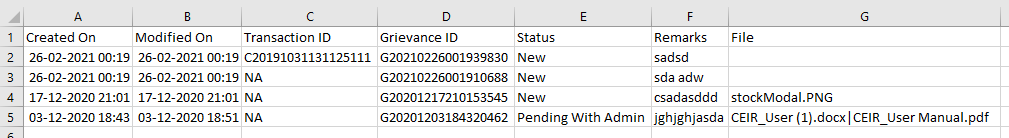


Figure 61: Exported Grievances

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.