ve

* **Central Equipment Identity Register Portal**

**Operations User Manual v 2.1**

Document Change History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Change Type | Description | Date |
| Draft |  | Submitted for internal review | February 2020 |
| Version 2.0 |  | Multiple System Admin, Configurable Notifications, Filter and sorting, Field Validations, History of the request, Address management | June 2021 |

Contents

[1 Overview 1](#_Toc75767747)

[1.1 Scope 1](#_Toc75767748)

[1.2 Acronyms & Abbreviations 1](#_Toc75767749)

[1.3 Conventions 1](#_Toc75767750)

[2 Operations User - Operations 2](#_Toc75767751)

[2.1 Application Overview 2](#_Toc75767752)

[2.2 Logging into the Application 2](#_Toc75767753)

[2.3 Application User Interface 4](#_Toc75767754)

[2.4 Block/Unblock Devices 5](#_Toc75767755)

[2.4.1 Single Device Blocking/Unblocking 6](#_Toc75767756)

[2.4.2 Bulk Device Blocking/Unblocking 10](#_Toc75767757)

[2.5 Edit Block/Unblock Device Requests 12](#_Toc75767758)

[2.6 Filter Block/Unblock Device Requests 14](#_Toc75767759)

[2.7 Export Block/Unblock Device Requests 15](#_Toc75767760)

[2.8 Alert Management 17](#_Toc75767761)

[2.9 Edit Alerts 17](#_Toc75767762)

[2.10 Filter Alerts 18](#_Toc75767763)

[2.11 Running Alert Management 19](#_Toc75767764)

[2.12 Filter Running Alerts 20](#_Toc75767765)

[2.13 IP log management 20](#_Toc75767766)

[2.14 Filter Ip logs 21](#_Toc75767767)

[2.15 SLA Management 22](#_Toc75767768)

[2.16 Filter SLA Management 23](#_Toc75767769)

[2.17 DB Tables 24](#_Toc75767770)

Figures

[Figure 1: Login 3](#_Toc75767771)

[Figure 2: Home Page 4](#_Toc75767772)

[Figure 3: Edit Information 5](#_Toc75767773)

[Figure 4: Change Password 5](#_Toc75767774)

[Figure 5: Block/Unblock Devices 6](#_Toc75767775)

[Figure 6: Report Block 7](#_Toc75767776)

[Figure 7: Report Block 10](#_Toc75767777)

[Figure 8: Report Block 11](#_Toc75767778)

[Figure 9: Block/Unblock Devices 13](#_Toc75767779)

[Figure 10: Edit Block Device (Single Device) 13](#_Toc75767780)

[Figure 11: Edit Block Device (Bulk Device) 14](#_Toc75767781)

[Figure 12: Block/unblock Devices 14](#_Toc75767782)

[Figure 13: Filtered Device Block/Unblock Requests 15](#_Toc75767783)

[Figure 14: Block/Unblock Devices 16](#_Toc75767784)

[Figure 15: Open or Save Exported Block/Unblock Devices File 16](#_Toc75767785)

[Figure 16: Exported Block/Unblock Devices 16](#_Toc75767786)

[Figure 17: Alert Management– View All 17](#_Toc75767787)

[Figure 18: Alert Management - Edit 18](#_Toc75767788)

[Figure 19: Alert Management– Filter Option 18](#_Toc75767789)

[Figure 20: Running Alert Management – View All 19](#_Toc75767790)

[Figure 21: Running Alert Management – Filter Option 20](#_Toc75767791)

[Figure 22: IP log Management – View All 21](#_Toc75767792)

[Figure 23: Ip log management – Filter Option 21](#_Toc75767793)

[Figure 24: SLA management 22](#_Toc75767794)

[Figure 25: Filter SLA management – Filter Option 23](#_Toc75767795)

[Figure 26: DB Tables 24](#_Toc75767796)

[Figure 27: DB Tables – view specific table 24](#_Toc75767797)

# Overview

## Scope

The objective of this manual is to help operations user use the CEIR (Central Equipment Identity Register) application to clear consignments, raise confiscated stock requests, collect tax for register devices and report grievances.

## Acronyms & Abbreviations

| **Acronym** | **Full Form** |
| --- | --- |
| CEIR | Central Equipment Identity Register |
| IMEI | International Mobile Equipment Identity |
| PDA | Personal Digital Assistant |
| TAC | Type Allocation Code |
| TRC | Telecommunication 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 User - Operations

## Application Overview

The CEIR (Central Equipment Identity Register) Operation User Portal is used in various work-flow in the CEIR application.

Operations user perform the following tasks:

* Block/unblock devices
* Alert Management
* Running alert management
* IP log management
* SLA management

## Logging into the Application

To register:

As part of configuration, the System Admin would provide the login details to the Operation user. It is advised to change the password once System Admin creates the account.

To login:

1. Open the browser and enter the CEIR Operations Portal URL in the address bar. The login screen appears.

A screenshot of a cell phone

Description automatically generated

Figure 1: 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 System Admin after successful registration in the system.

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 you are prompted to re-enter the login details.

On entering correct information, the application Search page appears.

If the Operation user forgets the assigned password, then the same need to request from the System admin. The **Forgot Password** link work for external user who register themselves from the DMC portal

## Application User Interface

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

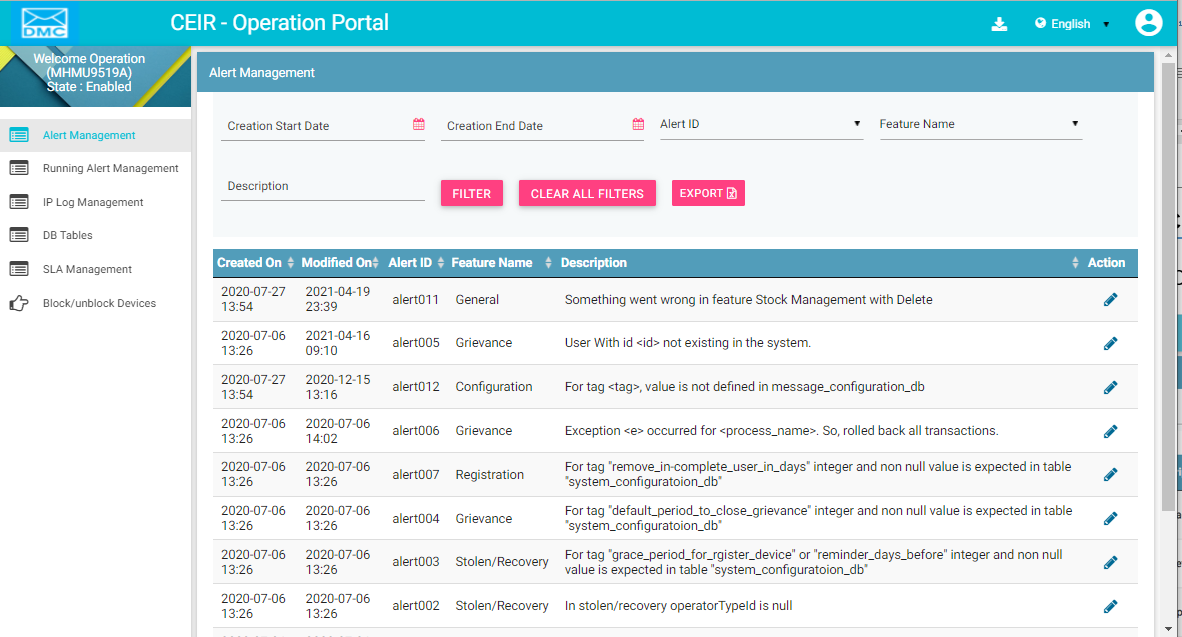


Figure 2: Home Page

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

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

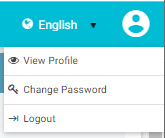
* **Download**: Click to download this user manual.
* **English**: Select **English** or **Khmer**. All the field and column labels appear in the selected language. User inputs are, however, in English.

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:



* (**View Profile**): Click on it to view the registered information. The **View Profile** page opens.

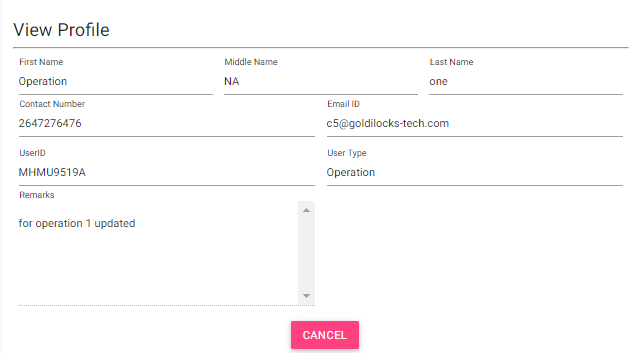


Figure 3: Edit Information

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

A screenshot of a cell phone

Description automatically generated

Figure 4: 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**.

## Block/Unblock Devices

CEIR Operation user can block devices (IMEI) on special requests. The operation users can block or unblock a single device at a time or multiple devices at a time.

Whenever a device is blocked, the IMEI of the device is kept in a greylist. This is done for a given duration after which the device IMEI 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.

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

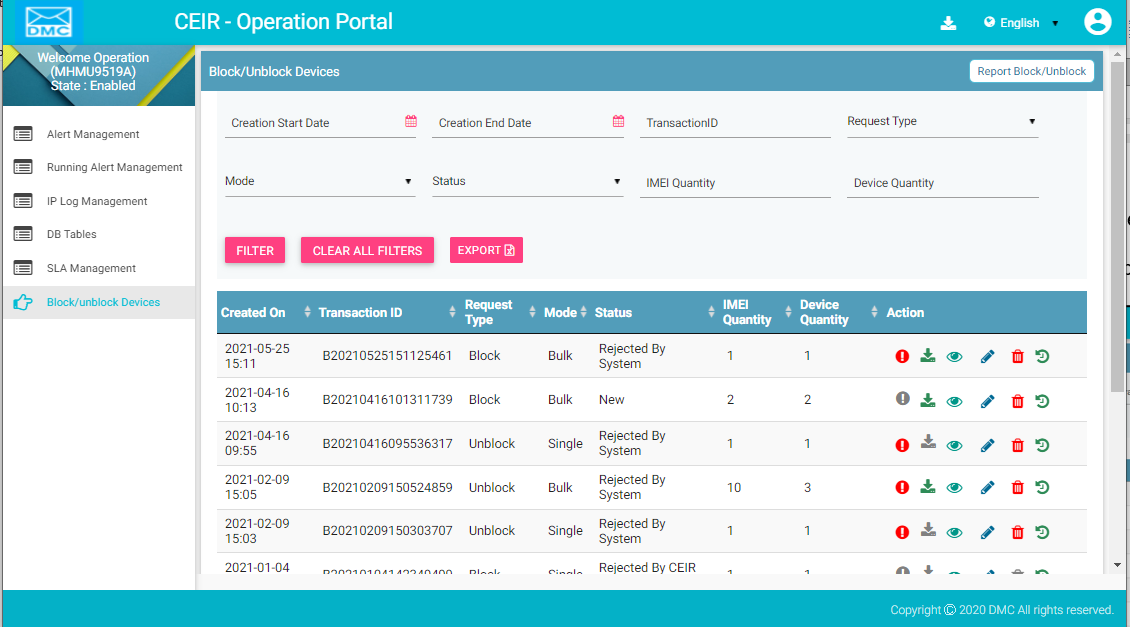


Figure 5: Block/Unblock Devices

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.

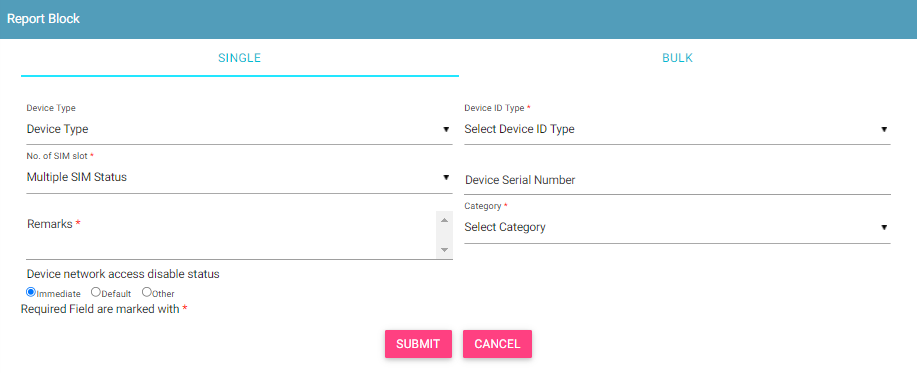


Figure 6: Report Block

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
* **\*Multiple SIM Status**: Number of SIMs 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. |
| 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 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, operations user can block or unblock multiple devices at a time. This saves time and speeds up the processing.

To block or unblock multiple devices, operations user is 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.

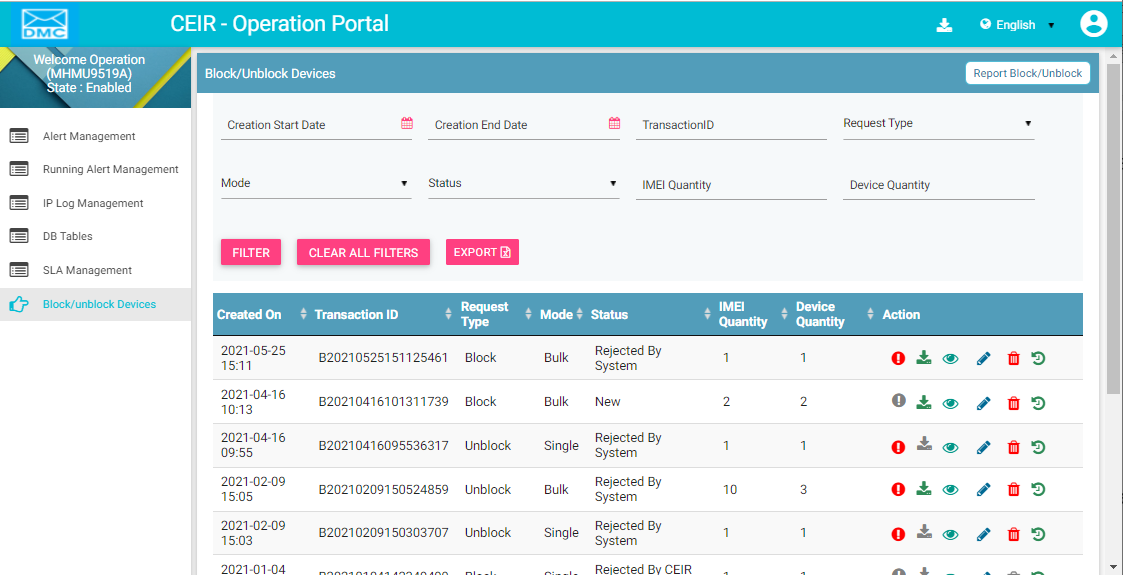


Figure 7: Report Block

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

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



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

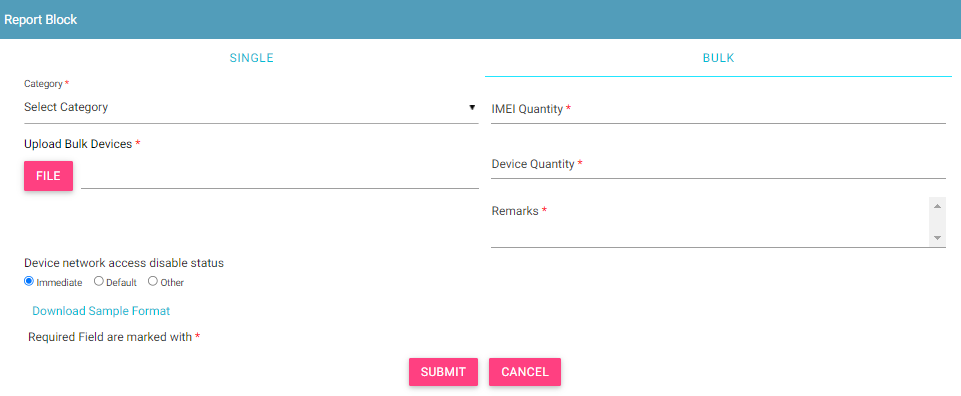
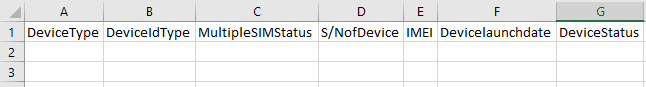


Figure 8: Report Block

1. 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.

1. **\* IMEI Quantity**: The number of IMEIs to be blocked or unblocked.
2. **\* Device Quantity**: The number of devices.
3. 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.



1. 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**: Number of SIMs 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)



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

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

The request appears on top of the dashboard.

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

## Edit Block/Unblock Device Requests

Operations user 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.

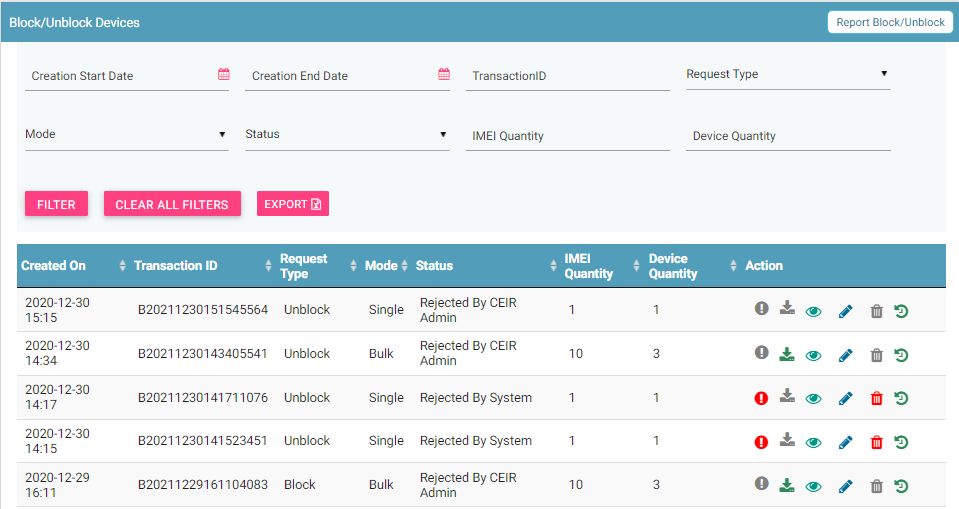


Figure 9: Block/Unblock Devices

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

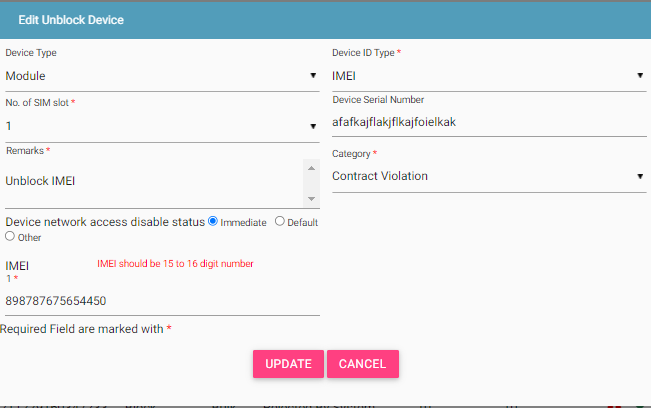


Figure 10: Edit Block Device (Single Device)

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

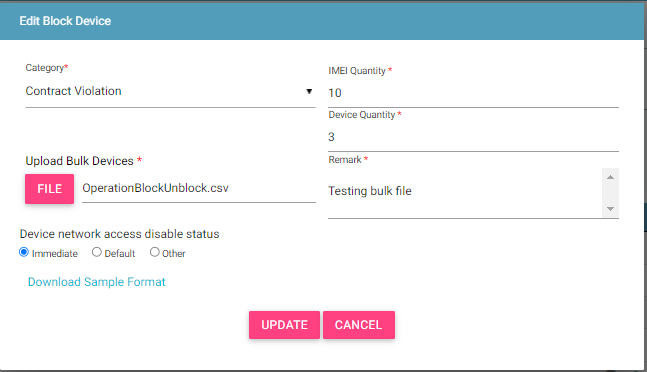


Figure 11: Edit Block Device (Bulk Device)

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

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

To filter block/unblock device requests:

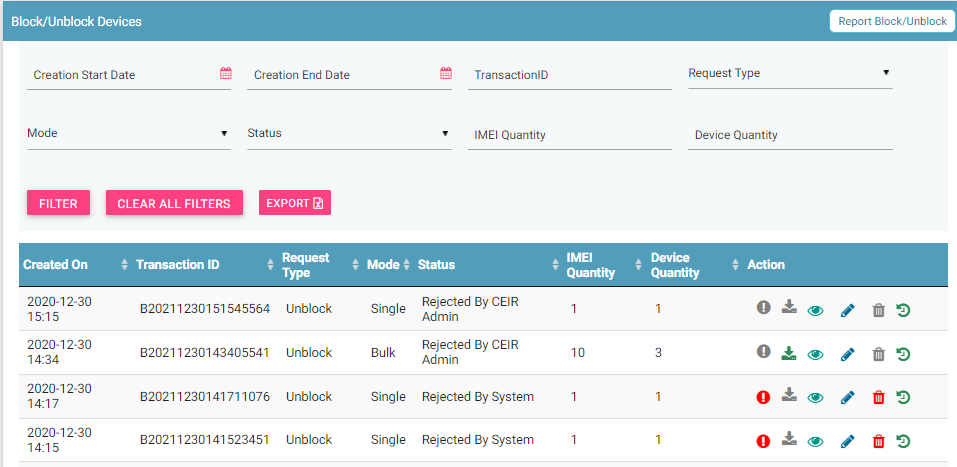


Figure 12: Block/unblock Devices

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. Operations user 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
* **IMEI Quantity:** This refers to the IMEI quantity of the request
* **Device Quantity:** This refers to the device quantity of the request.

1. Click **FILTER**.

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

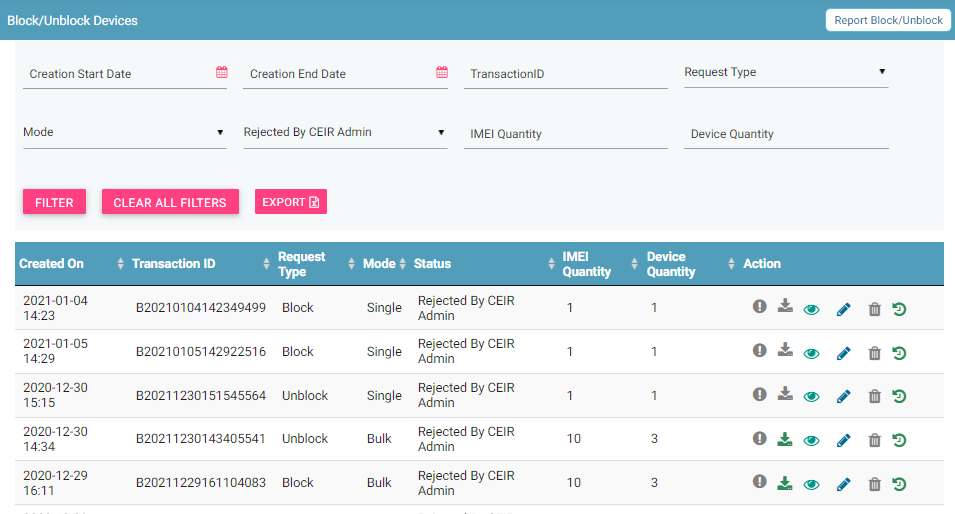


Figure 13: Filtered Device Block/Unblock Requests

## Export Block/Unblock Device Requests

Operations user 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**.

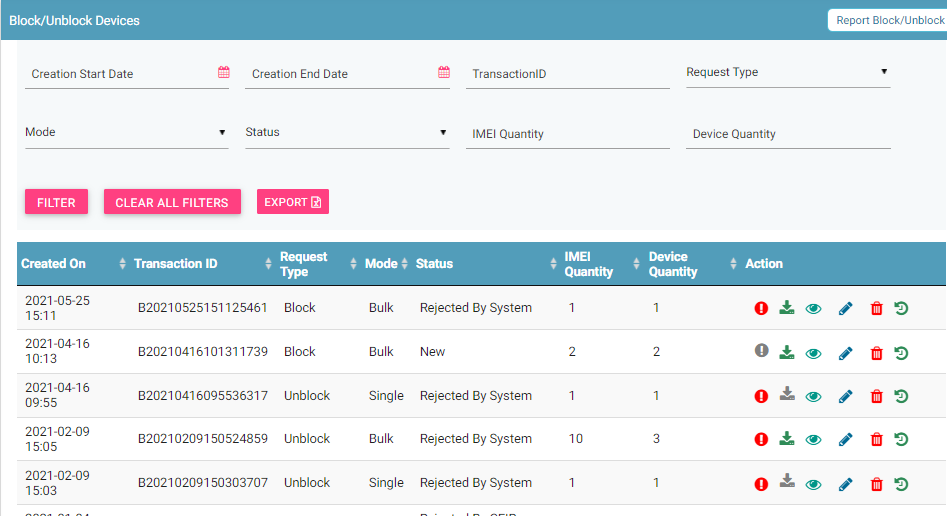


Figure 14: Block/Unblock Devices

The following page appears.

A screenshot of a cell phone

Description automatically generated

Figure 15: Open or Save Exported Block/Unblock Devices File

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

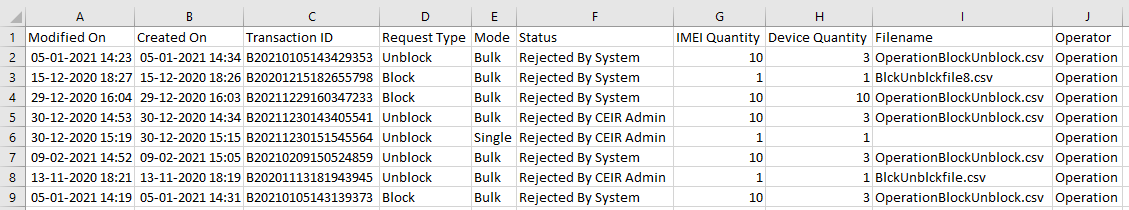


Figure 16: Exported Block/Unblock Devices

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.

## Alert Management

System Admins can configure the alert management information using this feature.

To configure Alerts:

1. Select **Alert management** in the left panel.

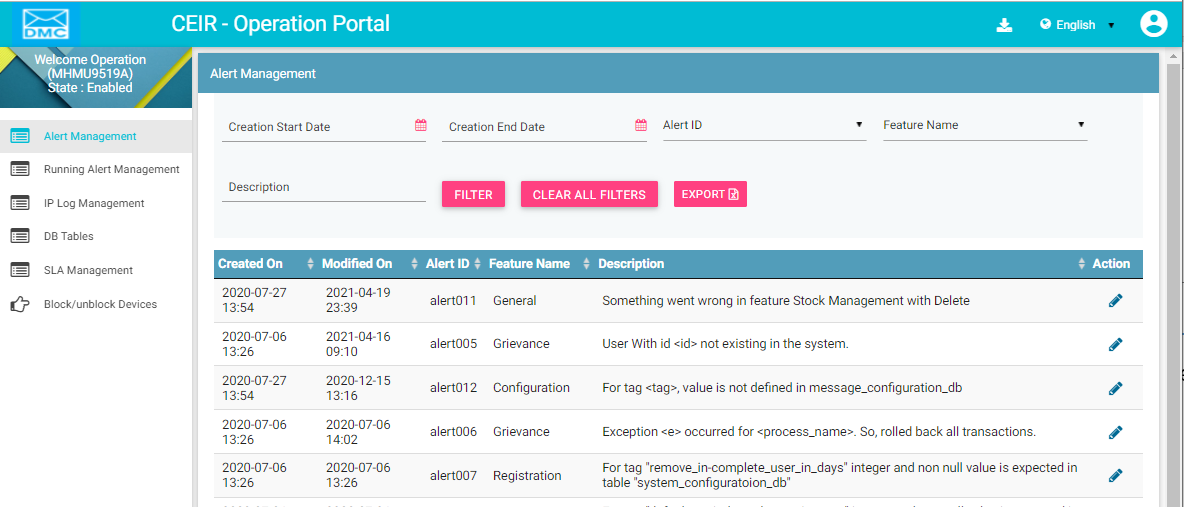


Figure 17: Alert Management– View All

The following columns are seen in the Alert Management Page

| **Column** | **Description** |
| --- | --- |
| Created On | This is the date of creation of alert. |
| Modified On | Date when alert was last modified. |
| Alert ID | Alert ID |
| Feature Name | Feature name of the alert |
| Description | Description of the alert |
| Action | This displays different actions that can be performed on the alerts.   * Edit A close up of a logo    Description automatically generated: This is used to modify the alert details. |

## Edit Alerts

System Admins can modify the alerts.

To edit alerts:

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

   Description automatically generated)** against the alert entry to be modified.
2. The **Edit Alert** page appears.

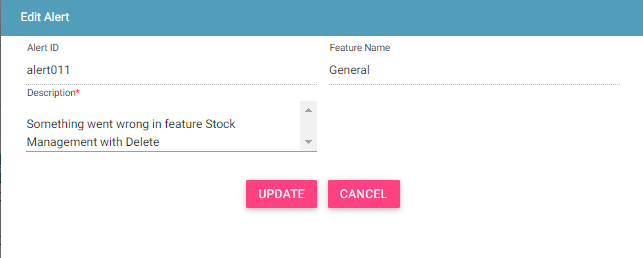


Figure 18: Alert Management - Edit

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

## Filter Alerts

System Admins can view selective information by defining specific values in the listed fields. For example, System Admins can view the alerts based on feature name.

To view specific parameter:

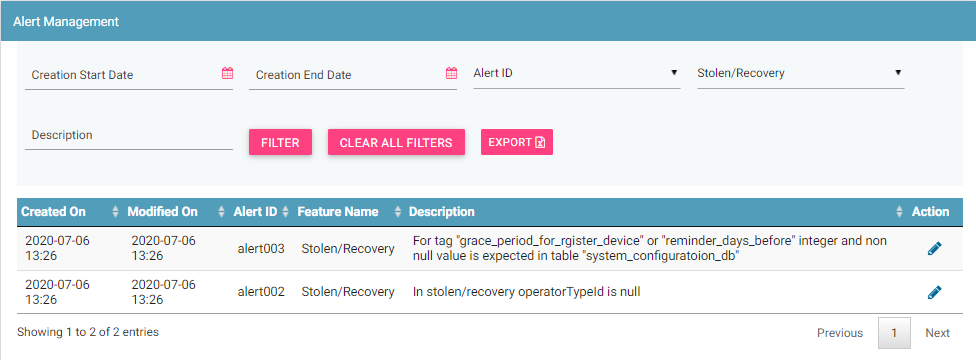


Figure 19: Alert Management– Filter Option

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

* **Date**: Select the dates
* **Alert ID**: Alert Id which is to be filtered
* **Feature Name**: Select Feature name
* **Description**: Select description

1. Click **FILTER**.

The alerts that matches the specified values is shown in the dashboard.

## Running Alert Management

System Admins can view the list of alerts raised in the system, when any unexpected event occurs.

To view running alert management:

1. Select **Running Alert** in the left panel.

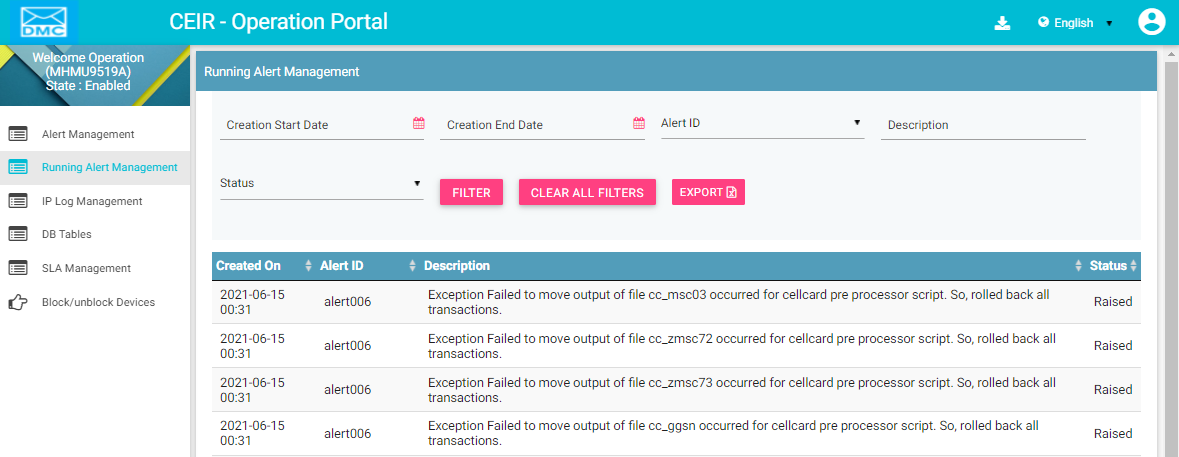


Figure 20: Running Alert Management – View All

The following columns are seen in the Running alert management Page

| **Column** | **Description** |
| --- | --- |
| Created On | This is the date of installation of system. |
| Modified On | Date when message is last modified. |
| Alert ID | ID of the alert |
| Description | Description of the alert |
| Status | Status of the alert |

## Filter Running Alerts

System Admins can view selective information by defining specific values in the listed fields. For example, System Admins can view specific alerts

To view specific running alerts:

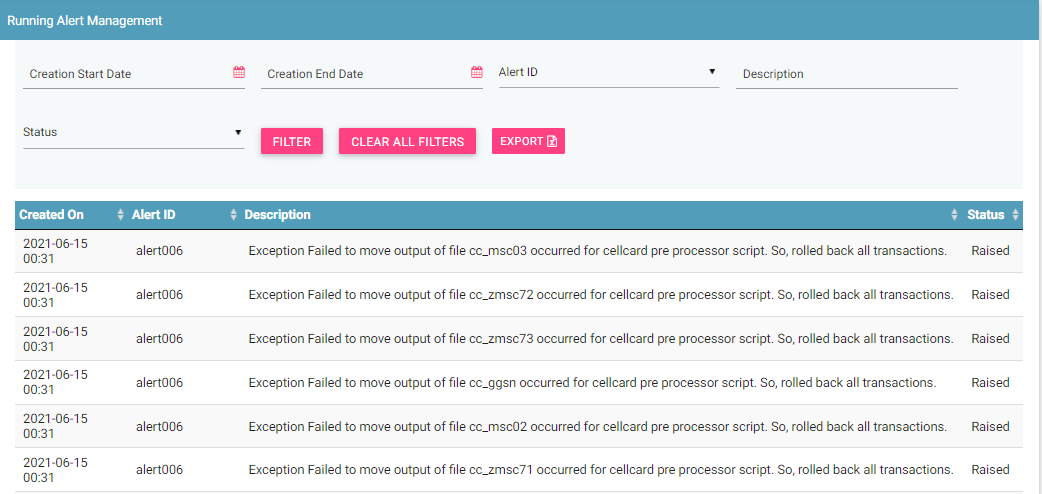


Figure 21: Running Alert Management – Filter Option

1. Enter the required value in one or more of the listed fields:
   1. **Date**: Select the dates
   2. **Alert ID**: Alert Id which is to be filtered
   3. **Feature Name**: Select Feature name
   4. **Description**: Select description
2. Click **FILTER**.

The parameter that matches the specified values is shown in the dashboard.

## IP log management

System Admins can view the IP logging information using this feature.

To view IP log related parameters:

1. Select **IP log Management** in the left panel.

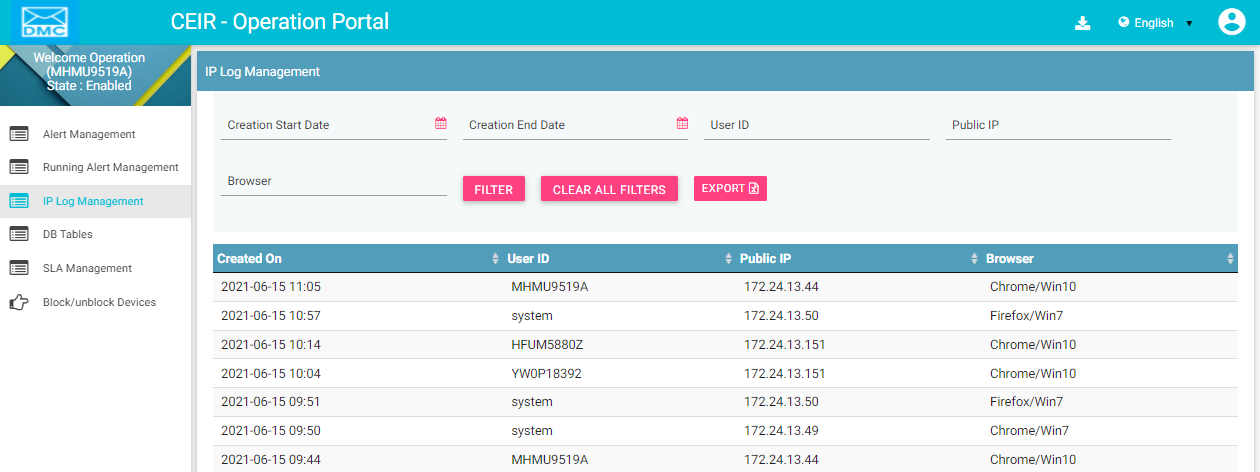


Figure 22: IP log Management – View All

The following columns are seen in the IP log management Page

| **Column** | **Description** |
| --- | --- |
| Created On | This is the date of installation of system. |
| User ID | User ID |
| Public IP | IP of the user machine |
| Browser | Browser which was used to access the application |

## Filter Ip logs

System Admins can view selective information by defining specific values in the listed fields. For example, System Admins can view the Ip logs.

To view specific parameter:

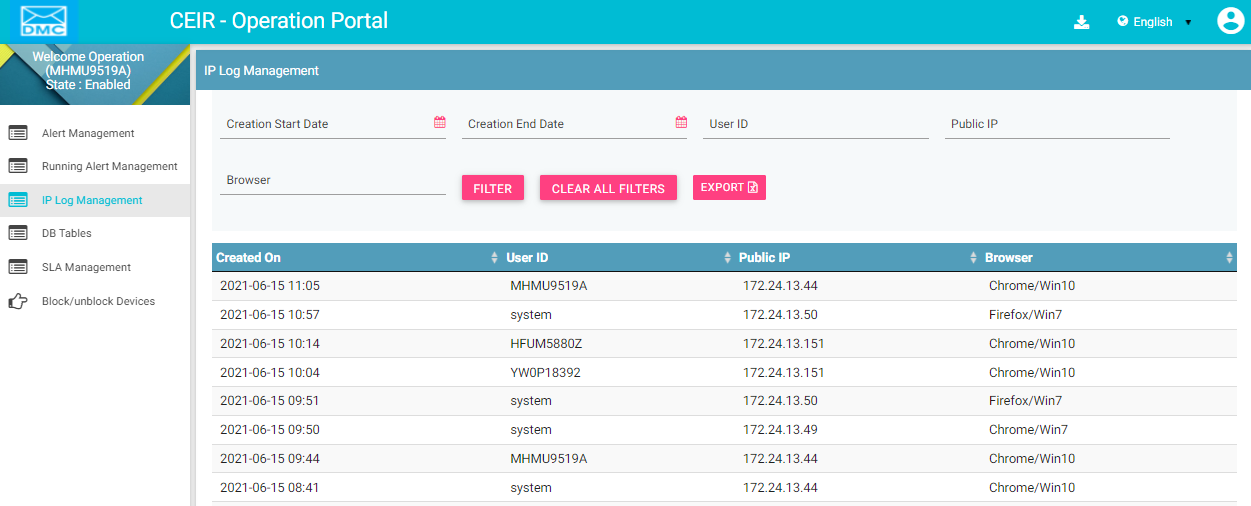


Figure 23: Ip log management – Filter Option

1. Enter the required value in one or more of the listed fields:
   1. **Date**: Select the dates
   2. **User ID**: User ID
   3. **Public IP** : Select public IP
   4. **Browser**: Select browser
2. Click **FILTER**.

The parameter that matches the specified values is shown in the dashboard.

## SLA Management

CEIR Admin has to perform certain activity within the defined timelines. In case the activity is not performed within the timelines, a SLA breach report is generated which denotes the activity where the SLA has not been met.

For example, if CEIR admin has to approve the consignment within 3 days and if CEIR admin is not able to approve the consignment within stipulated time, then on the 4th day, the SLA report will contain an entry for this consignment.

To view SLA Management Report

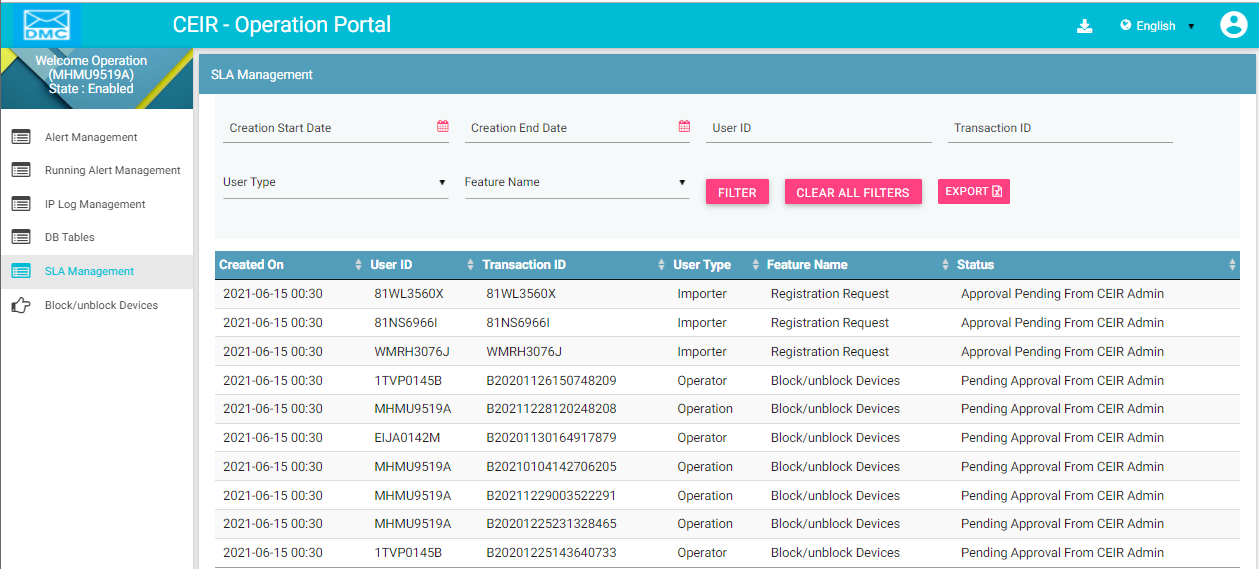


Figure 24: SLA management

For each request, the dashboard displays the following information:

| **Column** | **Description** |
| --- | --- |
| Created On | Date on which the request was created by user |
| User ID | User ID of the user who created the request |
| Transaction ID | Transaction ID of the request. |
| User Type | User Type of the user |
| Feature Name | Feature for which the request was initiated |
| Status | Status of the request |

## Filter SLA Management

System Admins can view selective information by defining specific values in the listed fields. For example, System Admins can view the SLA Management.

To view specific parameter:

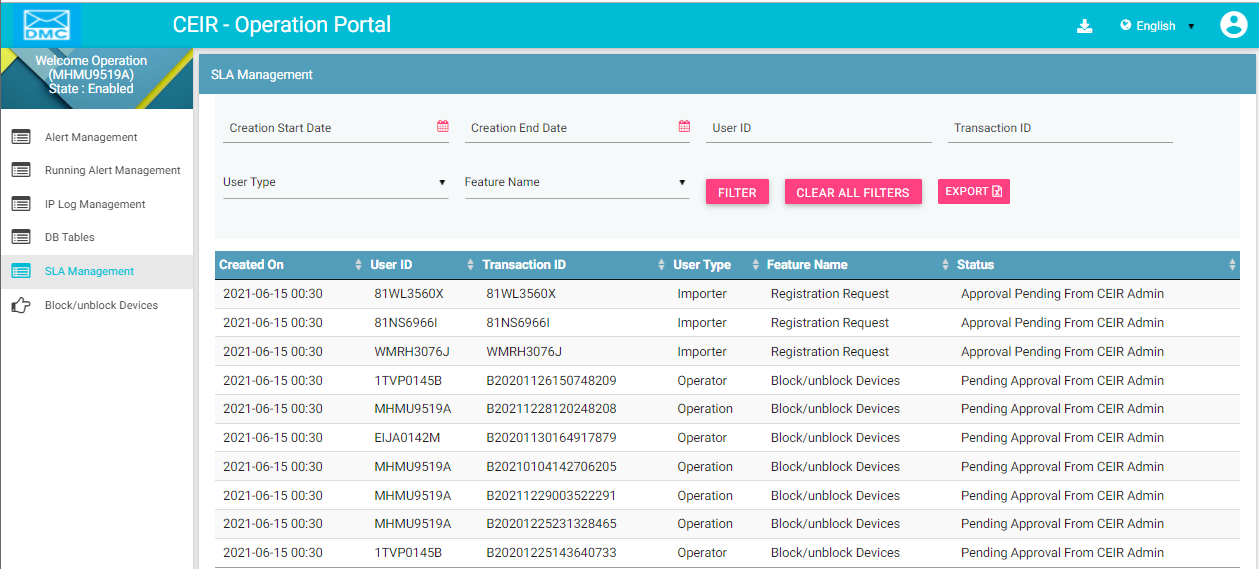


Figure 25: Filter SLA management – Filter Option

1. Enter the required value in one or more of the listed fields:
   1. **Date**: Select the dates
   2. **User ID**: Enter User ID
   3. **Transaction ID:** Enter Transaction ID
   4. **User Type**: Select User Type
   5. **Feature Type**: Select Feature Type.
2. Click **FILTER**.

The parameter that matches the specified values is shown in the dashboard.

## DB Tables

DB Tables feature is a troubleshooting tool to view and verify the parameter values in database tables. Also have the facility to export the tables.

System Admins can view the database tables using this feature.

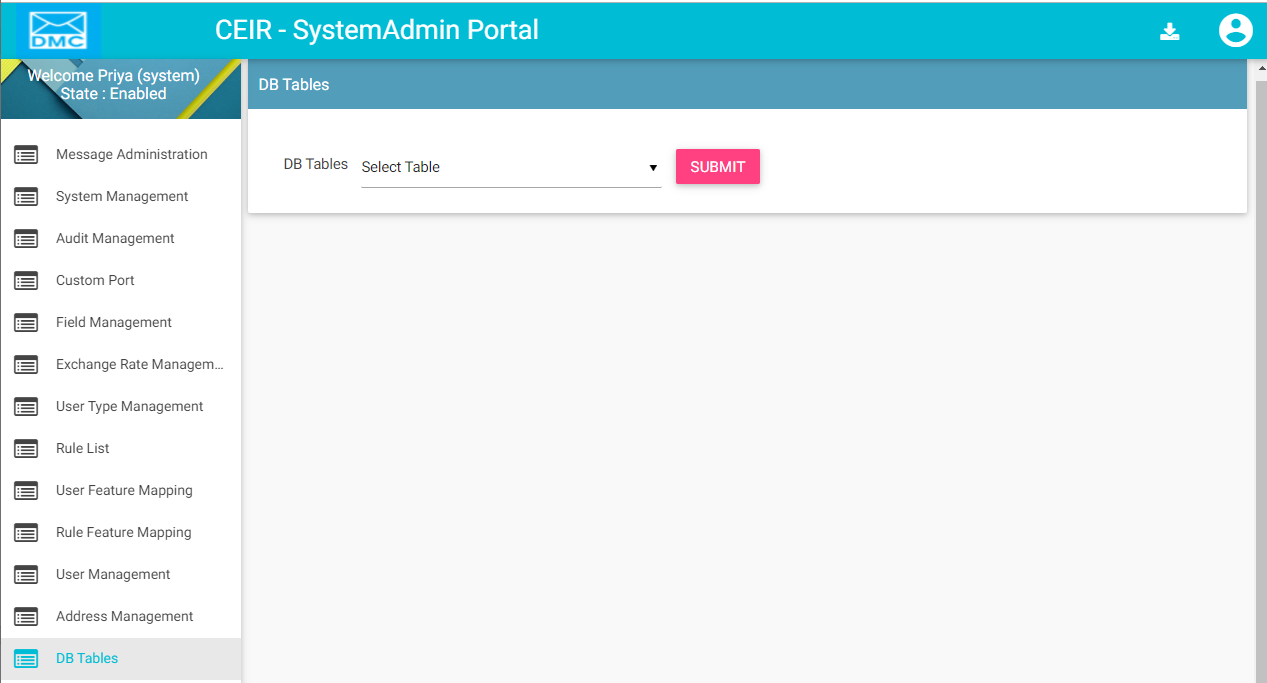


Figure 26: DB Tables

Data in tables can be sorted based on dates.

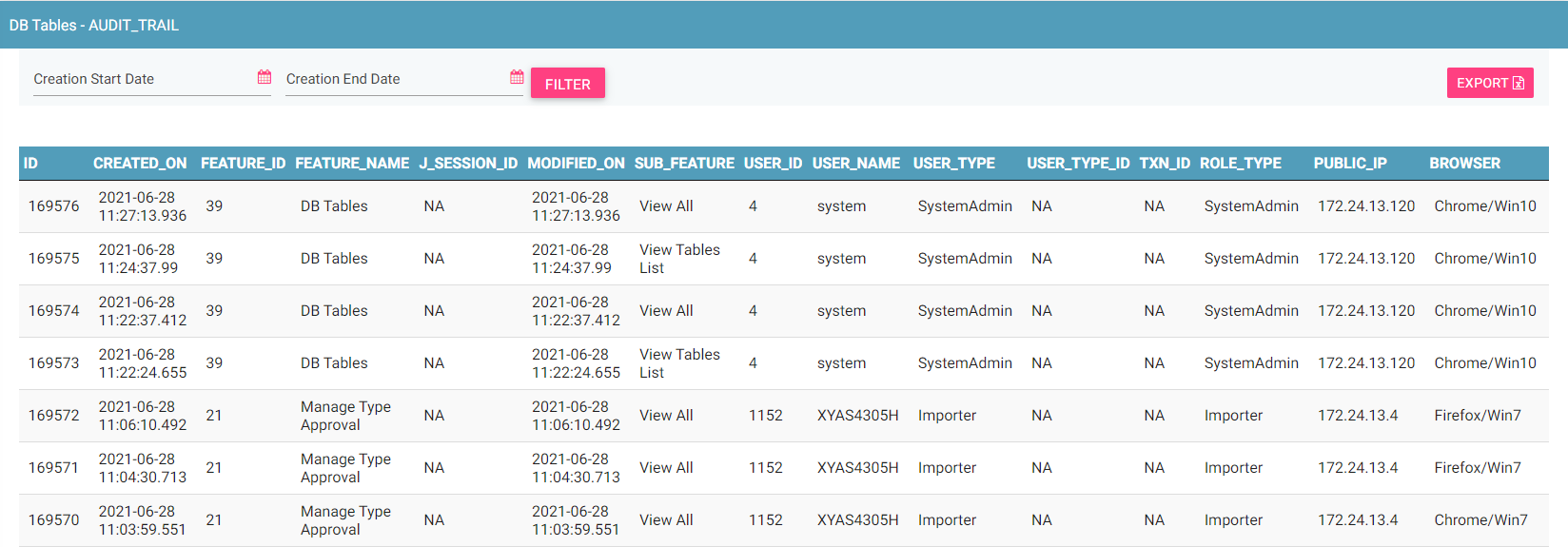


Figure 27: DB Tables – view specific table

The table data can be exported using the Export button on the top right.