CAN - COGNITIVE ASSISTANT FOR NETWORKS

User Manual For Desktop Application Version 5.5

AUGUST 17, 2021

AVANSEUS HOLDINGS PTE. LTD.

Disclaimer

THE SPECIFICATION AND INFORMATION REGARDING THIS USER MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION AND RECOMMENDATION IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USER MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY CONFIGURATIONS.

IN NO EVENT SHALL AVANSEUS OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL OR INCIDENTAL DAMAGES INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF USER OR INABILITY TO USE THIS MANUAL, EVEN IF AVANSEUS OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

NO PART OF THIS USER MANUAL SHOULD BE DUPLICATED OR CIRCULATED OR USED FOR PROFIT WITHOUT PRIOR WRITTEN APPROVAL FROM AVANSEUS TECHNOLOGIES PVT. LTD.

Preface

On the advent of CAN 5.5 release, we are pleased to share you the detailed user manual. This user manual provides you the detailed information on the various configuration aspects accessible for regular users, administrators and developers working on CAN 5.5. It may also be noted that some configurations may not be applicable to you depending on the type of integration you have chosen for.

This user manual is intended for ISP/Telecom Network NOC engineers or managers who manages the telecom network, their administrators and developers who possess technical knowledge and are familiar with the concepts of telecom networks. They would understand how to configure the different features and extract the best results out of this application.

For warranty, service or support information, kindly reach us at:

Avanseus Technologies Pvt. Ltd. N1 Block, 11th Floor, Manyata Tech Park, Thanisandra, Bengaluru, Karnataka 560045. Email: can.care@avanseus.com

Revision History

Version	Date	Change Description	Prepared by	Updated By	Approved by
V 1.0	August, 2016	Draft release		Sheenginee	Chiranjib
V 2.0	November, 2016	Updates		Sheenginee	Chiranjib
V 3.0	January, 2017	Updates		Sheenginee	Chiranjib
V 4.0	July, 2019	Updates	Sandeep Singh	Naveen	Chiranjib
V 5.0	March, 2020	Updates	Sandeep Singh	Sandeep Singh	Chiranjib
V 5.5	Aug, 2021	Updates	Sandeep Singh	Sandeep Singh	Chiranjib

Table of Contents

1. DASHBOARD APPLICATION SCREEN

Login Page

Executives can log on to the CAN desktop application using the single sign-in screen.

1. In the **Username** box, write your user name.
2. In the **Password** box, write your password.
3. Click the **Login** button.

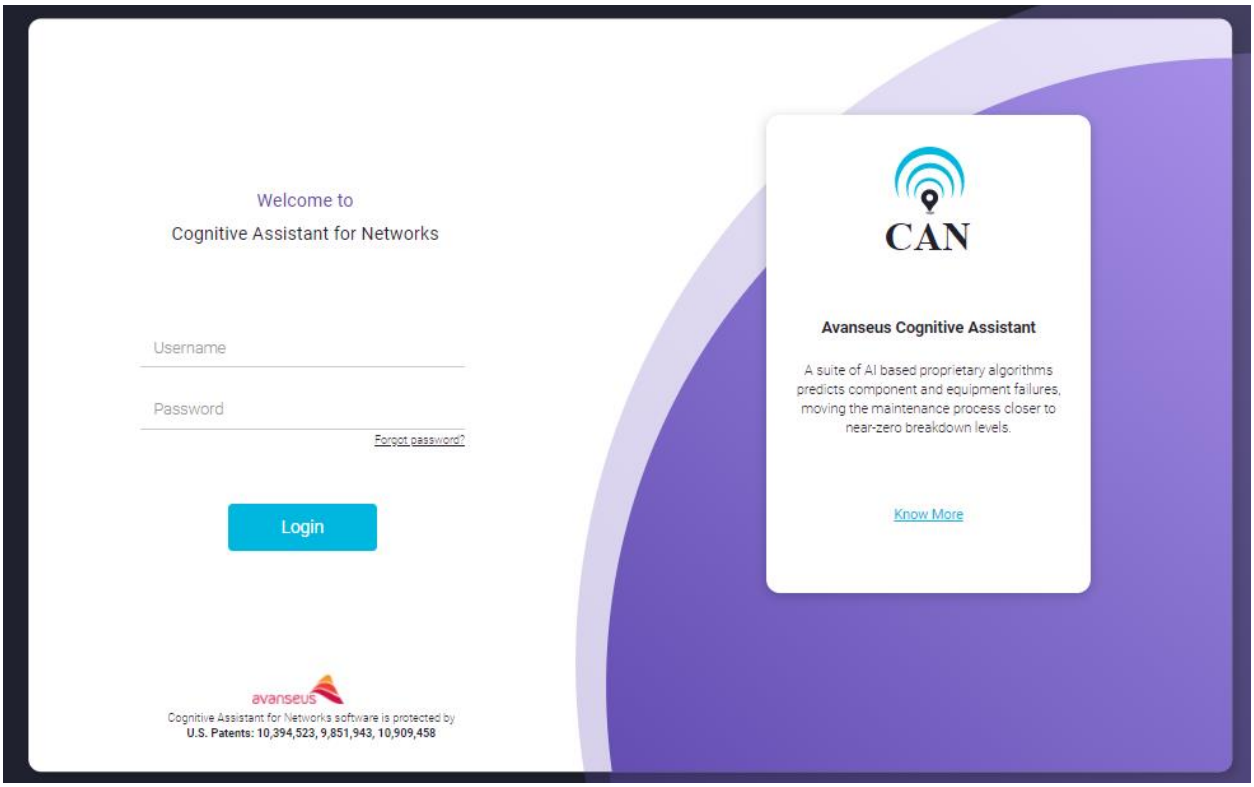


Figure 1.1 - Login Screen

4. You will receive an **OTP** on your registered email id.
5. Type your **OTP** in the One Time Password text box and click the **Submit OTP** button.

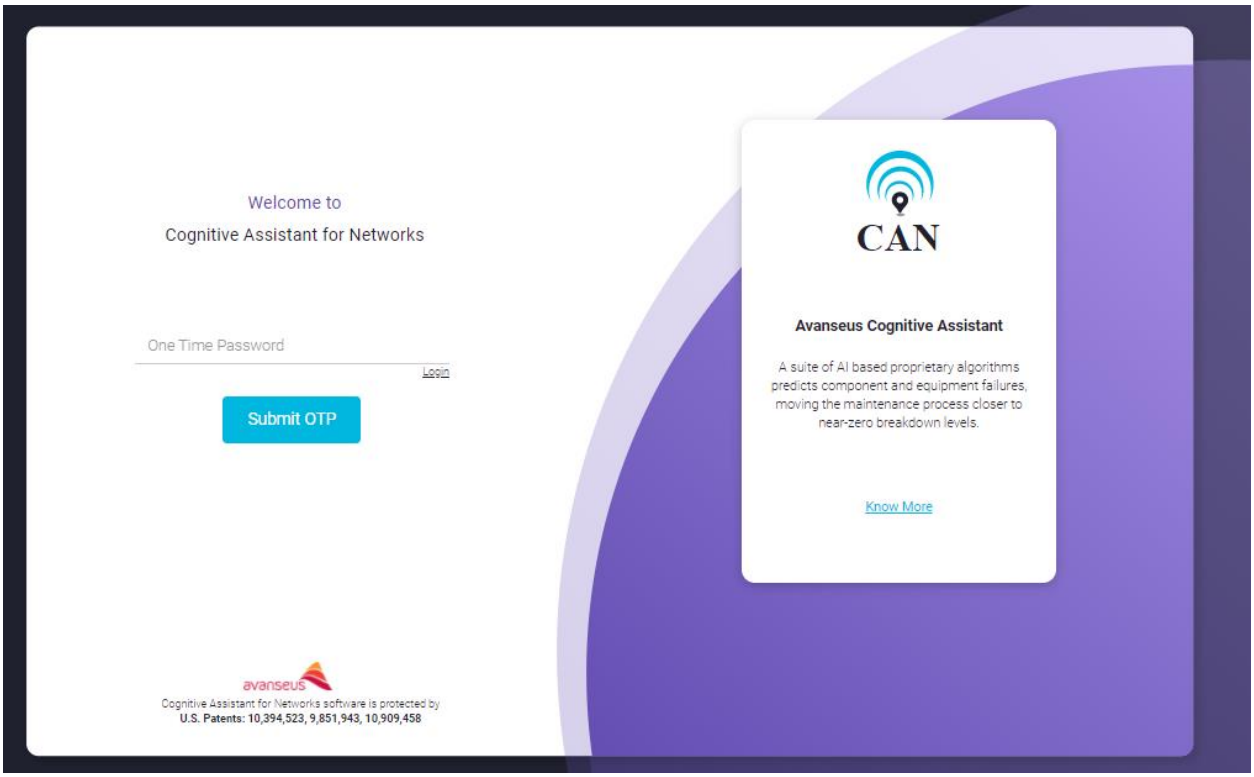


Figure 1.2 - Submit OTP Screen to Login

You can access the dashboard application.

To know more about CAN (Cognitive Assistant Network), click Know More.

Note: Currently CAN desktop application supports English (default), Russian, Spanish and Japanese.

Reset Your Password

To reset the Password, the steps are as follows:

1. Click **Forgot password** to reset the password.

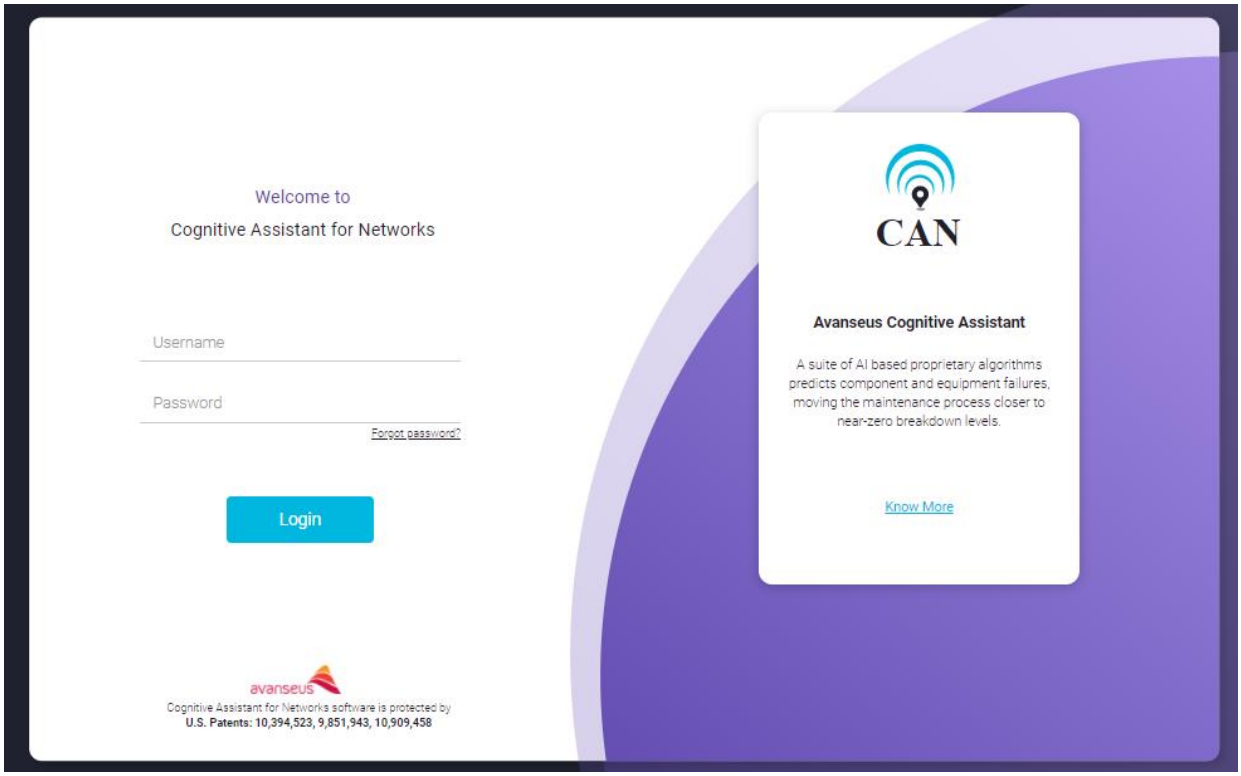


Figure 1.3 - Forgot Password Screen

2. Write Your Username and click the **Send OTP** button.

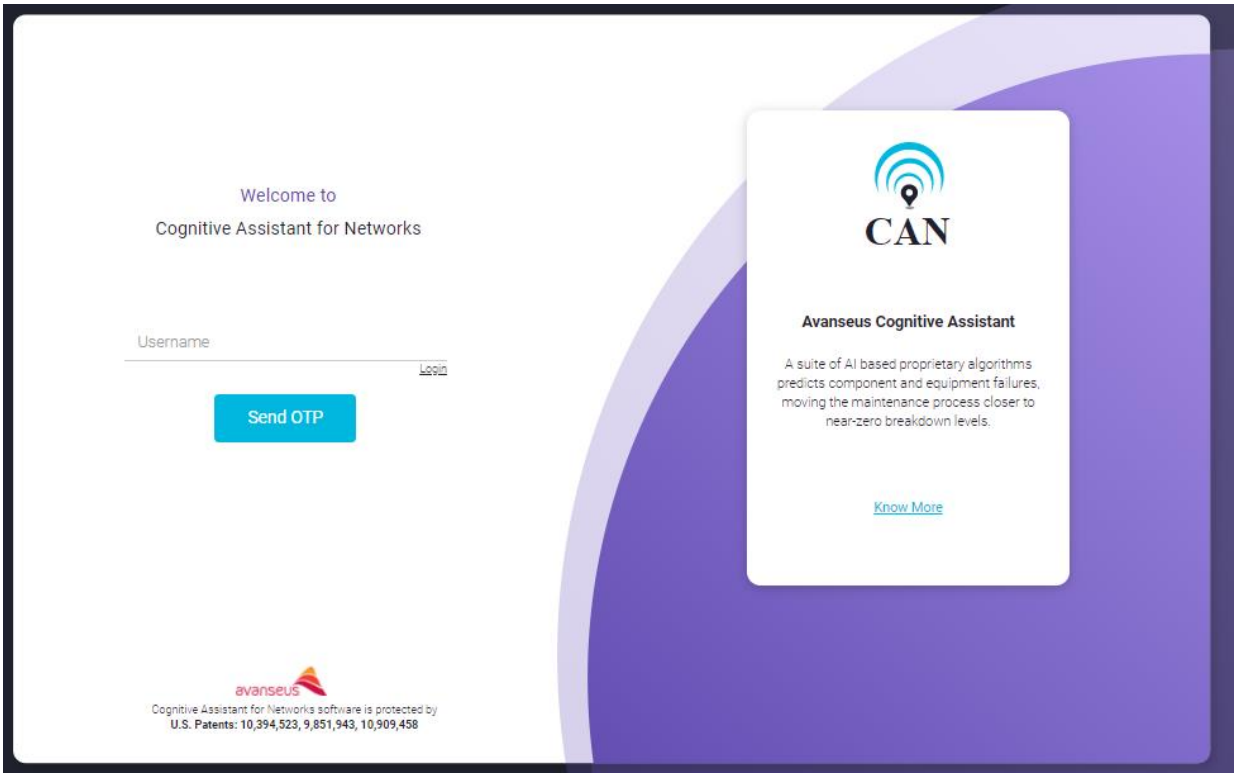


Figure 1.4 - Send OTP Screen

3. You will receive an **OTP** on your registered email id to reset your password.

4. Write the **One Time Password, New Password** and **Confirm New Password**.

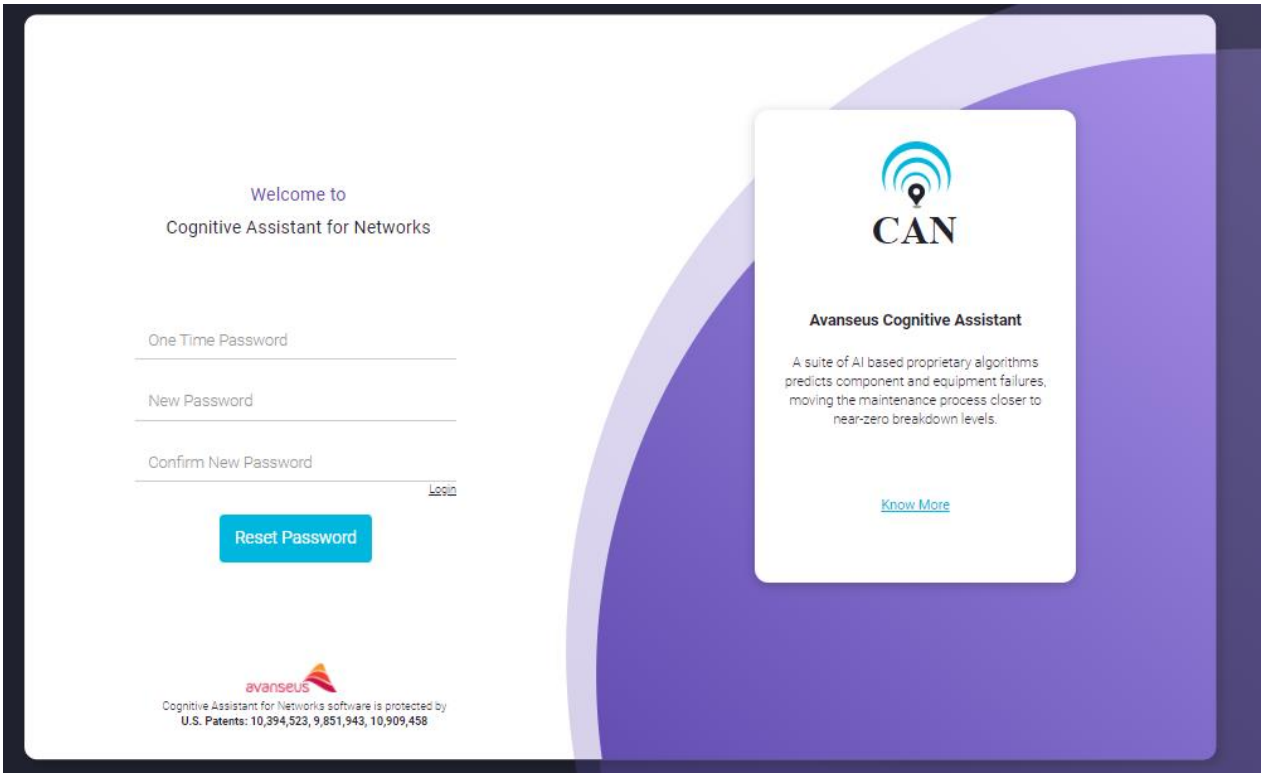


Figure 1.5 - Reset Password Screen

5. Click the **Reset Password** button to reset the Password.

User Profile

User Profile is available on the top right corner of the CAN Login Page. You can control settings for your account from your User Profile.

User Profile contains the below information:

- User Name - Your username is the account information. The username is displayed to indicate who is logged in.
- Role Category - User's role will be defined in the Role Category.
- Email Id - By default, this field will be filled with the email address you used to register for CAN.

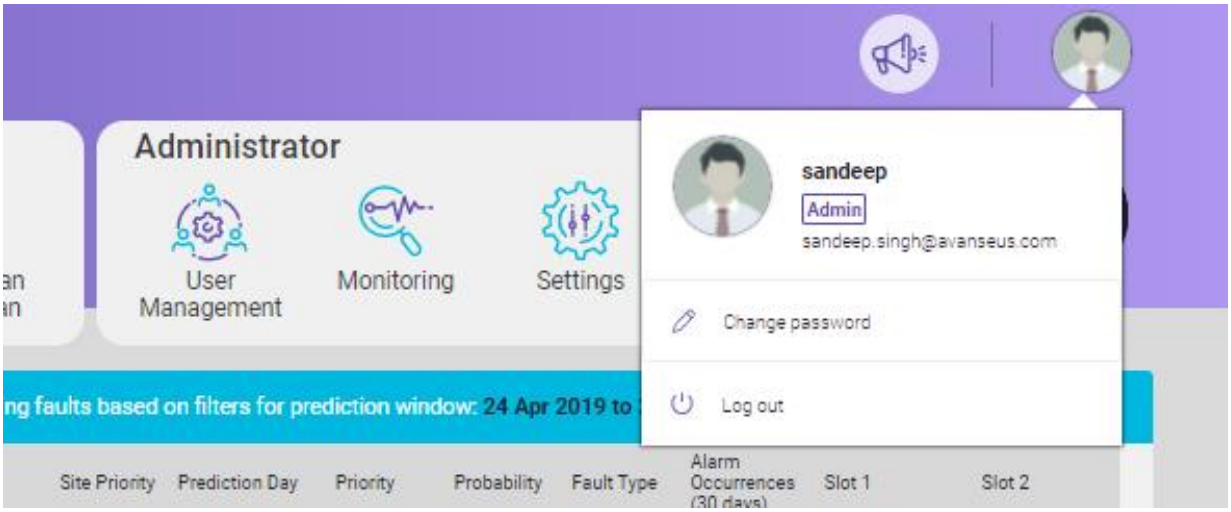


Figure 1.6 - User Profile

Update Your Password

1. Go to User Profile, select the edit icon .
2. Write your **Old Password**, **New Password** and **Confirm New Password** in the respective text box.
3. Click the **Apply** button to update the New Password.

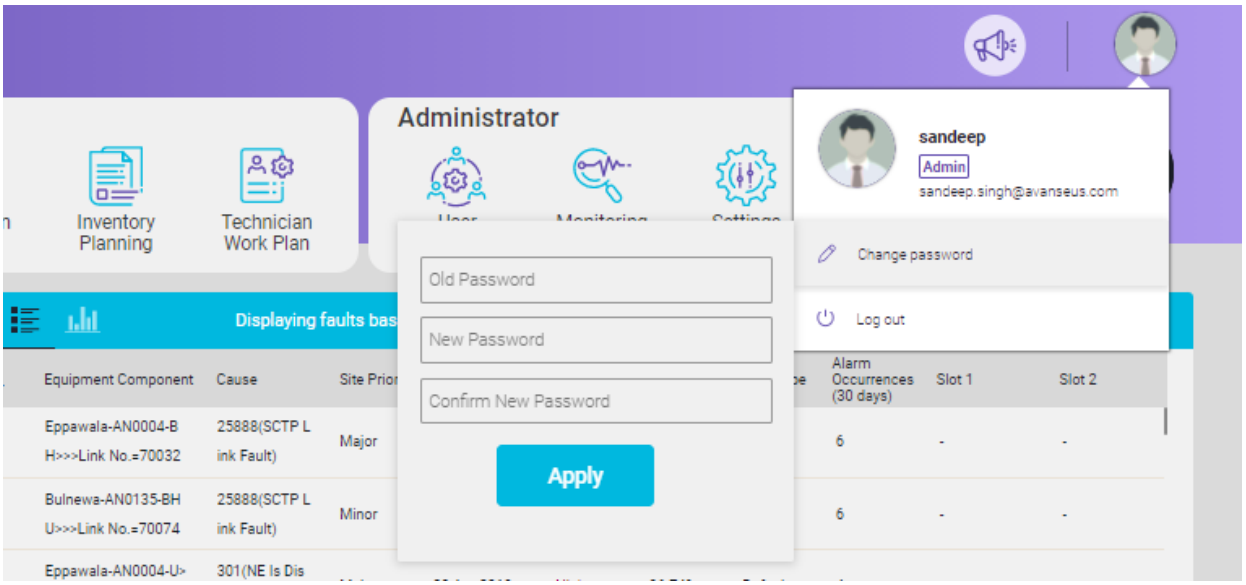


Figure 1.7 - Update Password Screen

Log Out

If you want to end your session, go to User Profile and click the **Log Out** button.

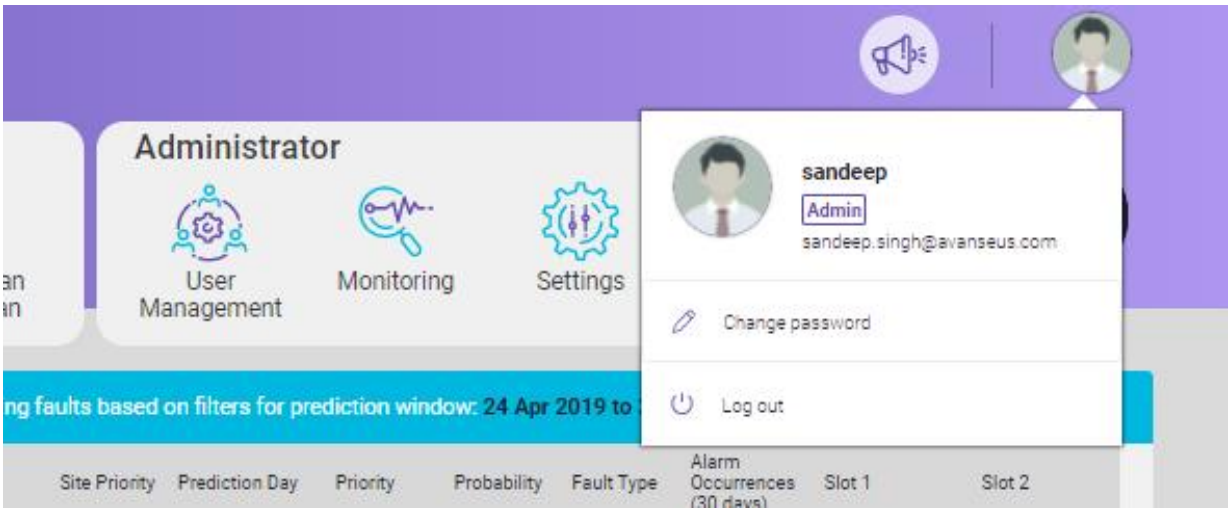


Figure 1.8 - Log Out Button

Page Intentionally Left Blank

2. EXECUTIVE DASHBOARD HOME

Executive dashboard home serves as a starting point for the application.

The executive dashboard has three different sections:

1. User
2. Administrator
3. Developer

The **User** section provides access to **Predictive Fault Analysis**, **Performance Prediction**, **Root Cause Prediction**, **Cross Domain Correlation**, **Integration Gateway**, **Inventory Planning**, **Technician Work Plan** and **Announcement**.

The **Administrator** section provides access to **User Management**, **Monitoring** and **Settings**.

The **Developer** section provides access to **Adaptation and VBI**.

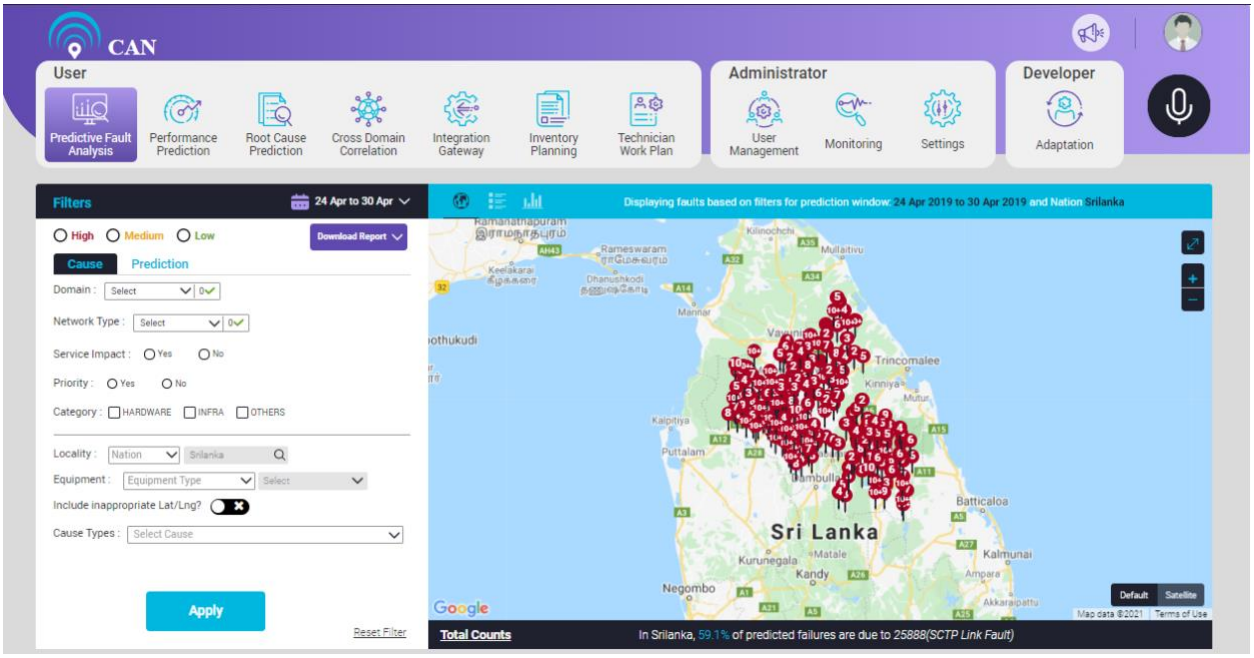


Figure 2.1 - Executive Dashboard Home

Page Intentionally Left Blank

3. PREDICTIVE FAULT ANALYSIS

Predictive Fault Analysis screen navigates to the fault predictions made by CAN for the available data. By default, Predictive Fault Analysis screen displays the predictions related to the latest prediction window in the tabular form.

Predictive Fault Analysis allows the executives to view the predicted faults Nation wise, Region wise, City wise and so on.

User can choose the Prediction Week from the Calendar to see the faults based on the filters for the selected Prediction Week.

By default, the screen displays the result for a latest prediction window for the selected week (Nation wise).

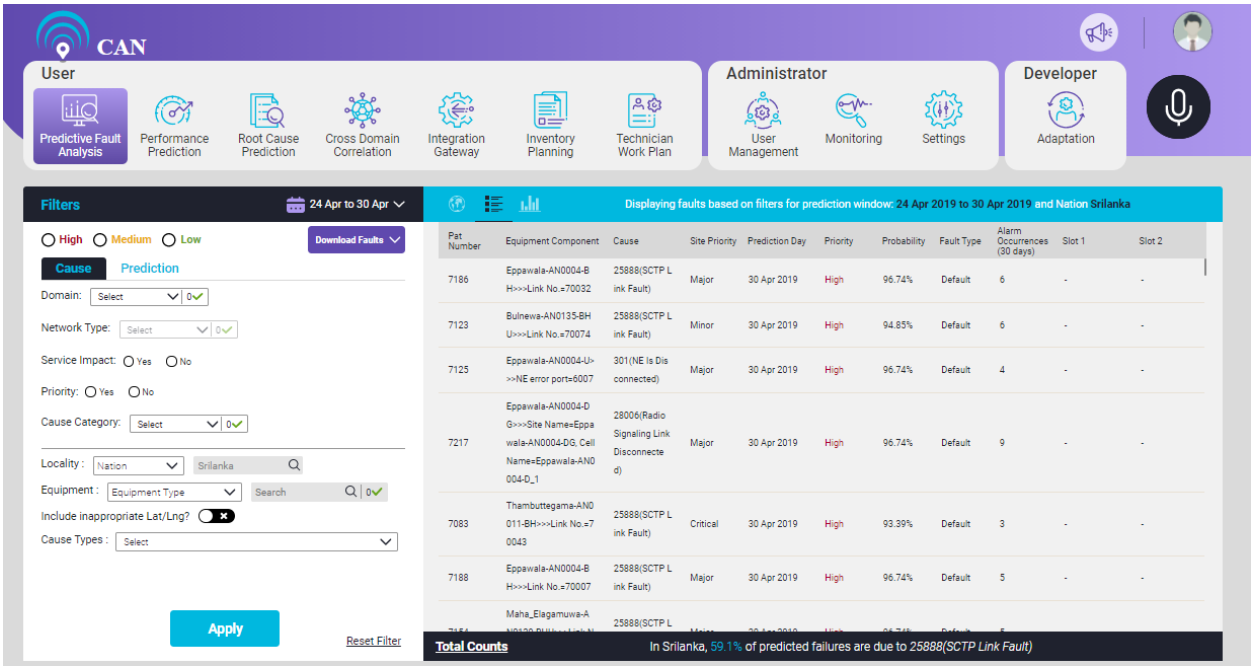


Figure 3.1 - Predictive Fault Analysis Screen

There are three priority check boxes:

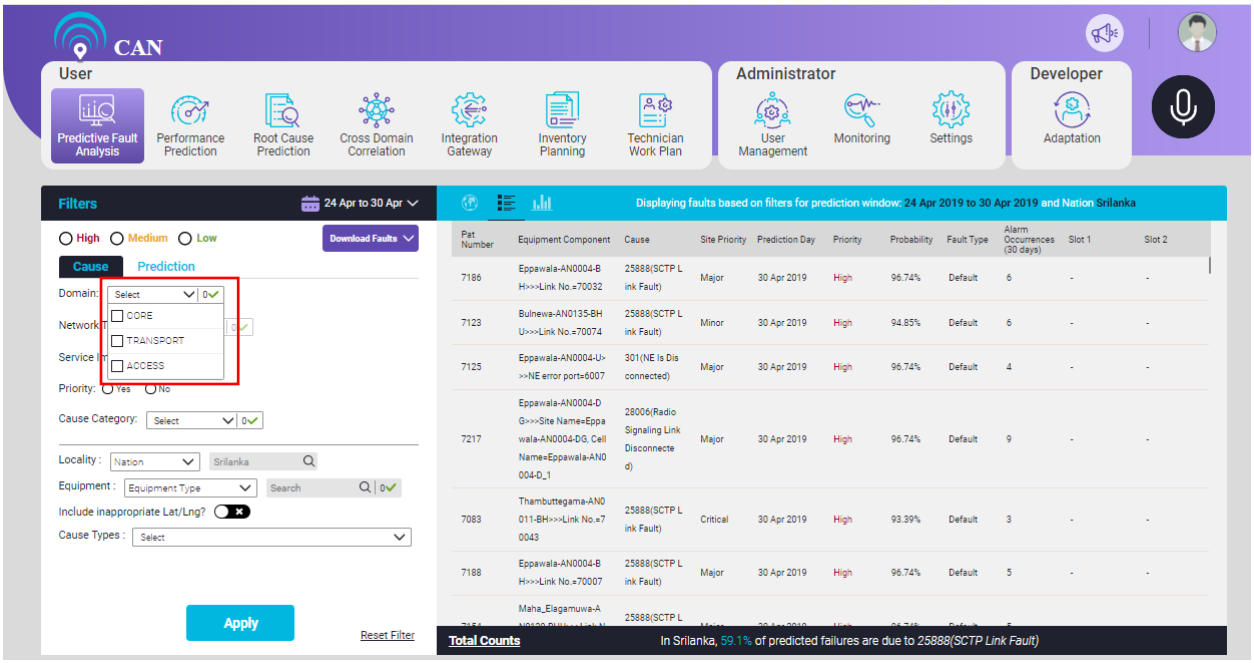
- High (written in red color)
- Medium (written in yellow color)
- Low (written in green color)

User can select any or all of the priorities check boxes at a time.

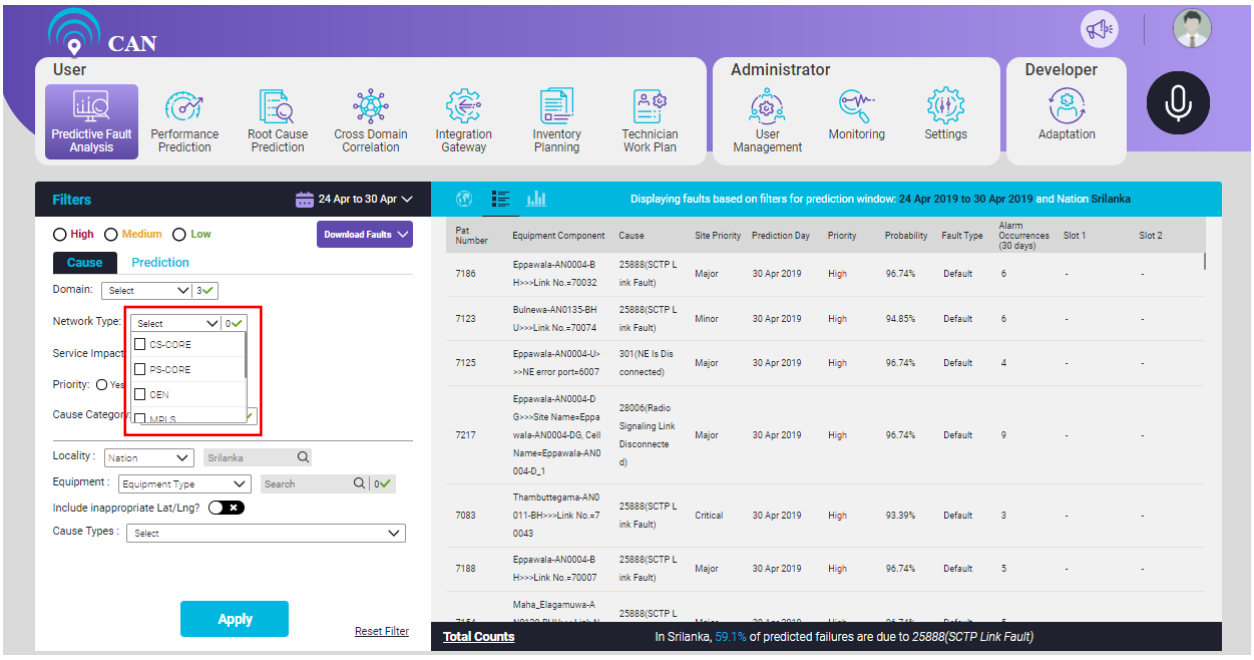
The filters have two tabs: **Cause** and **Prediction**.

By default, the **Cause** tab is selected. **Cause** tab is designed for advanced filtering the predictions based on various cause attributes that include:

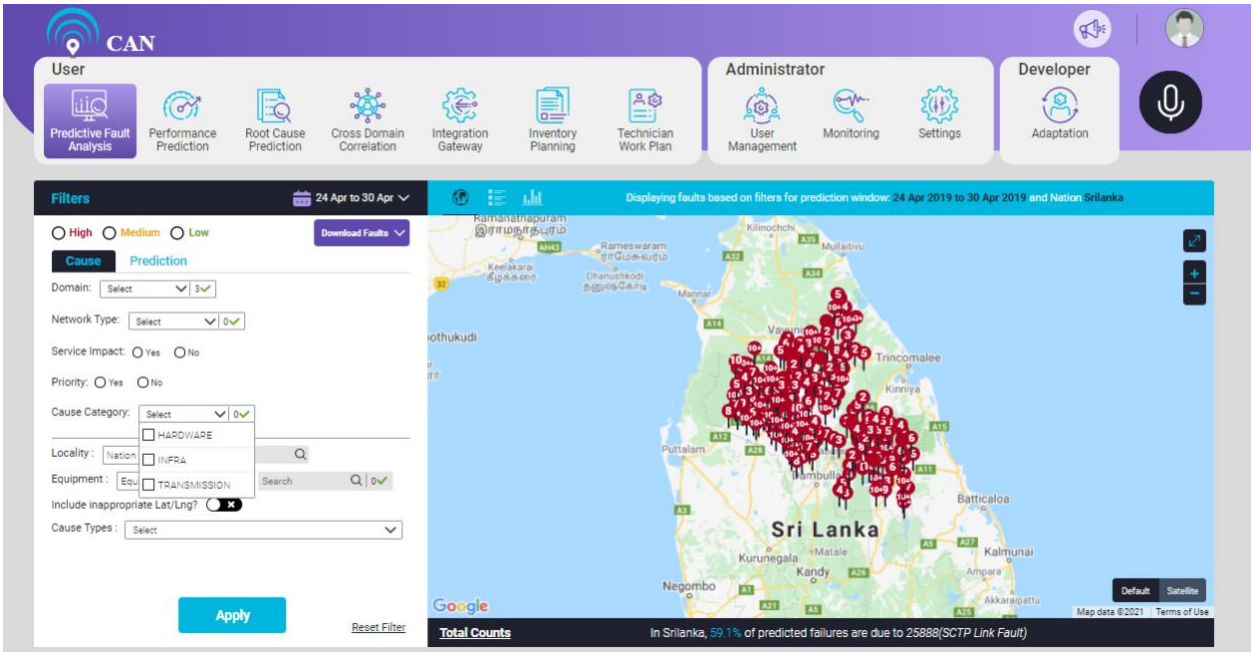
1. **Domain**: There can be multiple domains (Currently, the screen displays 3 domains i.e. **Core**, **Transport** and **Access**. Each **Domain** will have their dependent **Network Type**).



2. **Network Type**: There can be multiple **Network Type.** User can select the **Network Type** based on the selected **Domain**.



3. **Service Impact**: It has two radio buttons: Yes, and No.
4. **Priority**: It has two radio buttons: Yes, and No.
5. **Cause Category**: User can select the Cause Category from the drop down.



User can select the appropriate **Cause** attributes as per the requirement.

On the **Prediction** tab, user can select the required filters. **Prediction** tab has the following attributes:

1. **Prediction Date**: Prediction date displays the selected prediction dates in the selected window.
2. **Probability**: A slider button is available where user can select the probability threshold (usually >70) to display the data with higher probabilities of occurrence thereby enhancing the relevance.
3. **Ticket History**: A checkbox is available. User can select the check box to include the ticket history in predictions or exclude the data with previous ticket history.
4. **Category**: Category have two radio buttons: Prioritized and others. User can select the appropriate category.
5. **Technician**: There is a search text box. User can use the text box to search for the technician who had been assigned with the prediction from the list of filtered predictions.
6. **Predictive Tickets**: It has two radio buttons: Yes, and No. It shows those predictions where tickets are already booked or not.
7. **Alarm Occurrences**: It has two radio buttons: Repeating and Non repeating to show the repeating and non-repeating cases thereby improving the relevance of prediction.
8. **Site Priority**: It has three check boxes: Critical, Major and Minor to filter out respective priority sites
9. **Clustered Faults**: It has two radio buttons: Clustered and Non Clustered to filter out respective data.

In addition, there are more general filters that will enable filtering of data under consideration based on the attributes like locality, equipment type etc. These include:

1. **Locality**: There is a drop down to select the Nation, Region and City. Beside Locality we have search text box to select the Nation/Region/City from the list.

2. **Equipment**: There is a drop down to select Equipment Type, Office Code, Equipment, Equipment Component. User can select multiple values. Beside Locality we have search drop down to select the appropriate attribute as per the selected Equipment.
3. **Customer**: There is drop down to select the Customer (If there is only one customer this option will not be shown).
4. **Include inappropriate Lat/Lng**: A toggle button to include or exclude the inappropriate Lat/Lng.
5. **Cause Types**: There is a drop down to select the Cause Type. Cause type is available as applicable to selected filters where user can understand the KPI values based on the single selected cause type.

To see the Predicted Faults:

1. Select the appropriate filters as per the requirement.
2. Click the **Apply** button to see the results.

Predictive Fault Analysis has three representations:

- Map View
- Tabular View
- Graphical View

To select the Map view, click the map icon .

Map View

1. The markers on the map represents the predicted faults. The marker must be placed on the latitude and longitude where the equipment on which fault is predicted to occur is located.

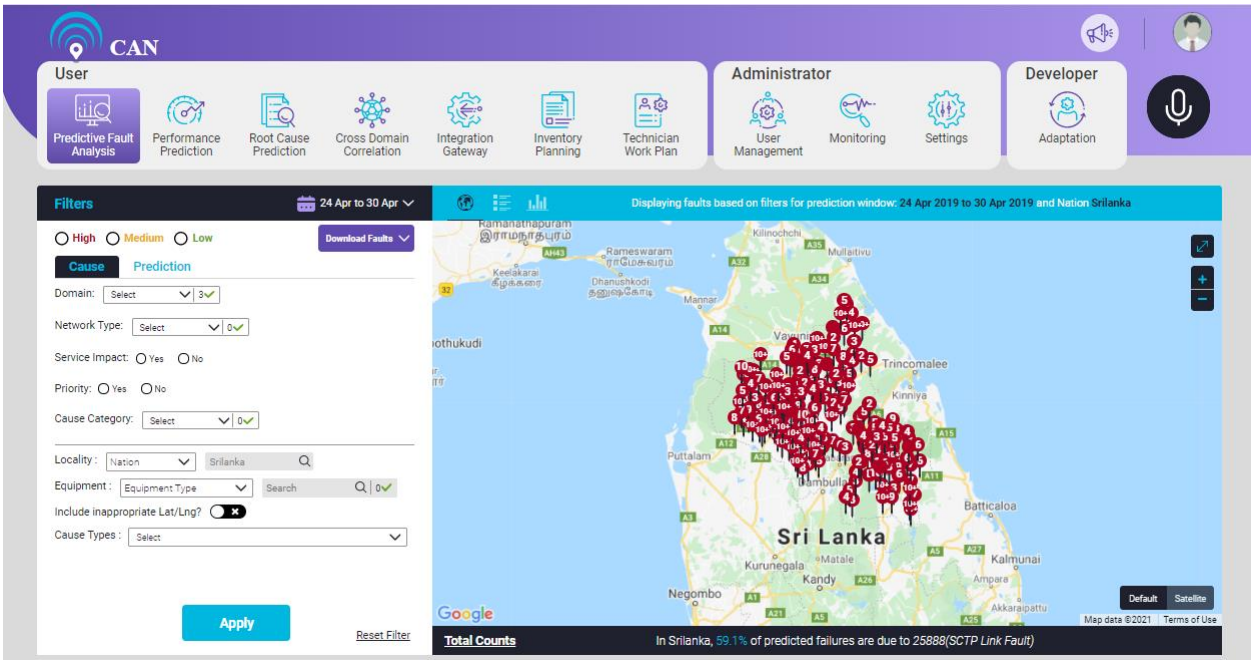


Figure 3.2 - Location Based Filtering

2. Predicted faults are classified based on their priority and are represented below:

Red - High priority predicted faults

Yellow - Medium priority predicted faults

Green - Low priority predicted faults

3. User can view the causes for the predicted faults and the percentage of its occurrence on the bottom section of the screen.

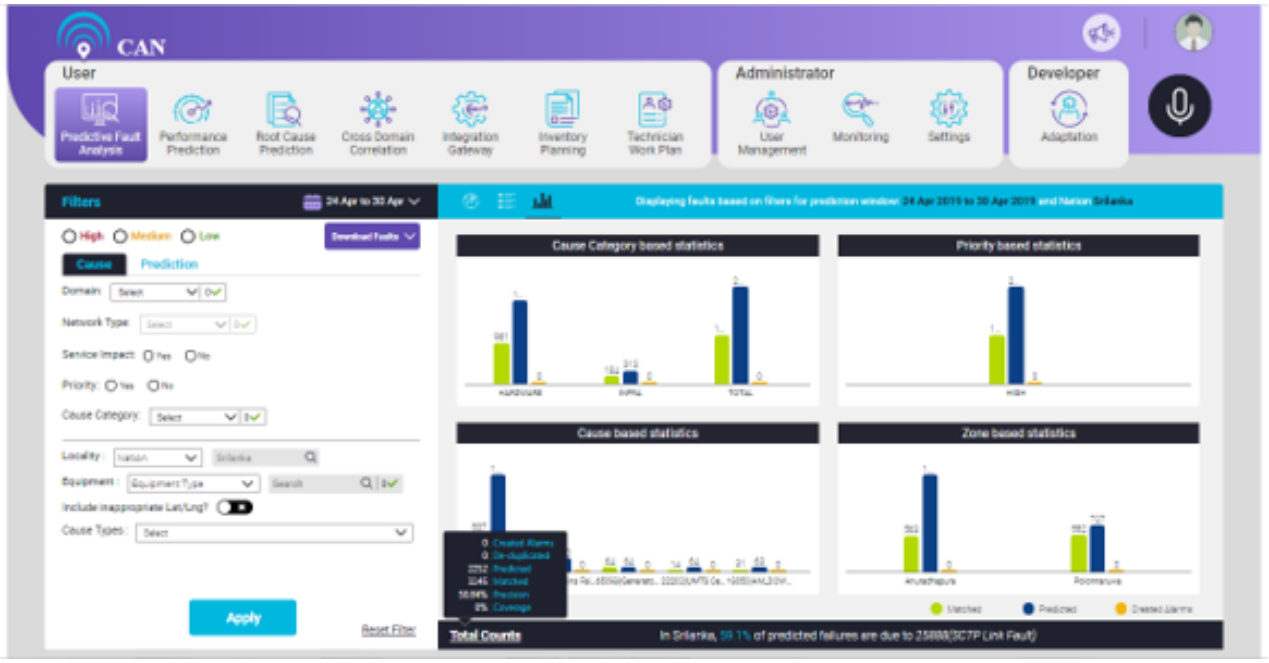


Figure 3.3 - Predicted Faults with Causes

4. If multiple predictions occur at the same latitude and longitude, (it will display minimum 1 prediction and up to 10 and anything higher than 10 will be marked as 10+). User can choose the equipment from the drop down menu. The screen will display the fault details of the selected equipment.

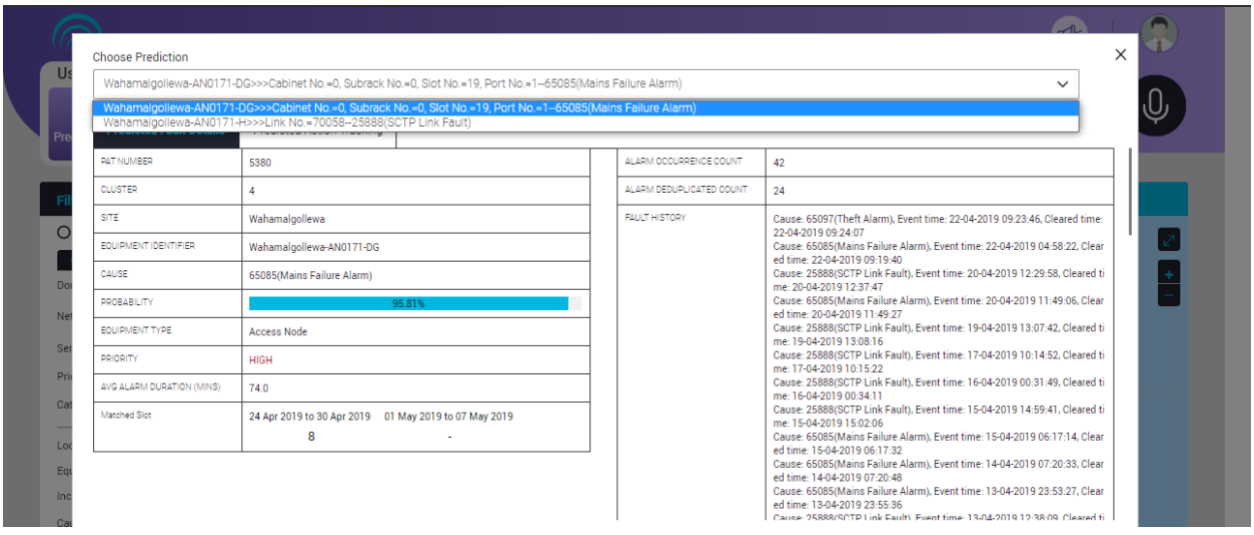


Figure 3.4 - Clustered Equipment

Tabular View

1. To view the tabular view, click the tabular icon .
2. The tabular icon has the following attributes:
   - Pat Number
   - Equipment Component
   - Cause
   - Site Priority
   - Prediction Day
   - Priority
   - Probability
   - Fault Type
   - Alarm Occurrences (30 days)
   - Slot 1 (7days) match
   - Slot 2 (7days) match

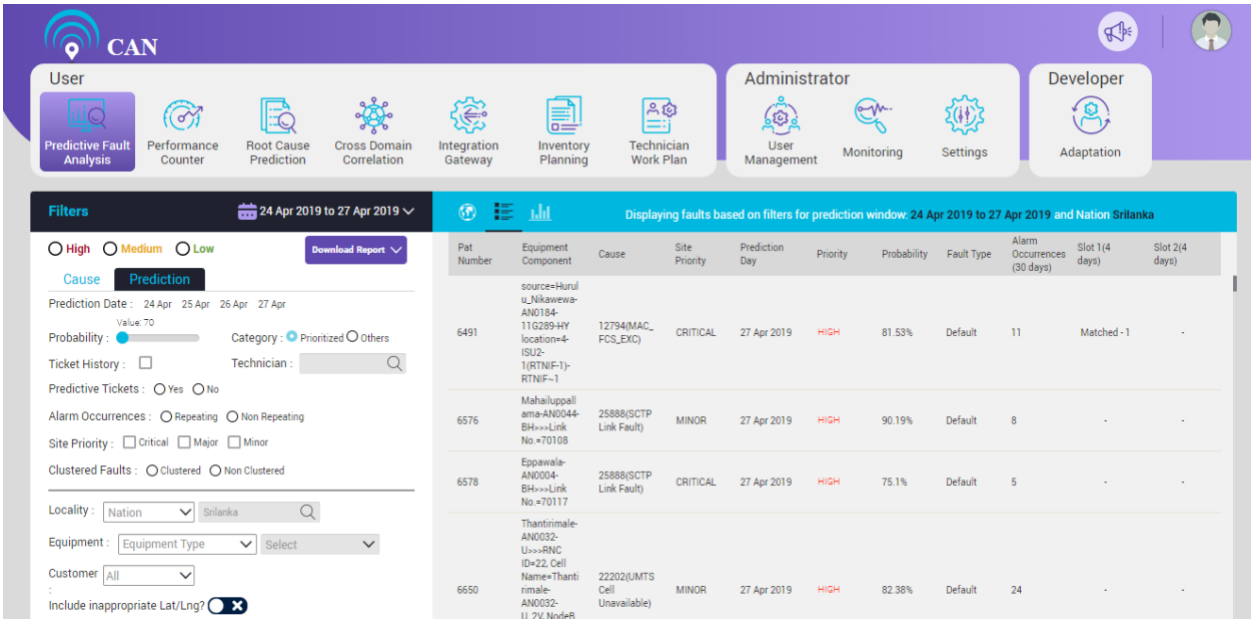


Figure 3.5 - Predictive Failure Analysis (Tabular View)

3. To view the **Predicted Fault Details**, click anywhere on the particular row.
4. Users can view the **Predicted Fault Details** and **Predicted Action Tracking** on the screen. The Predicted Fault Details tab includes the following fields:

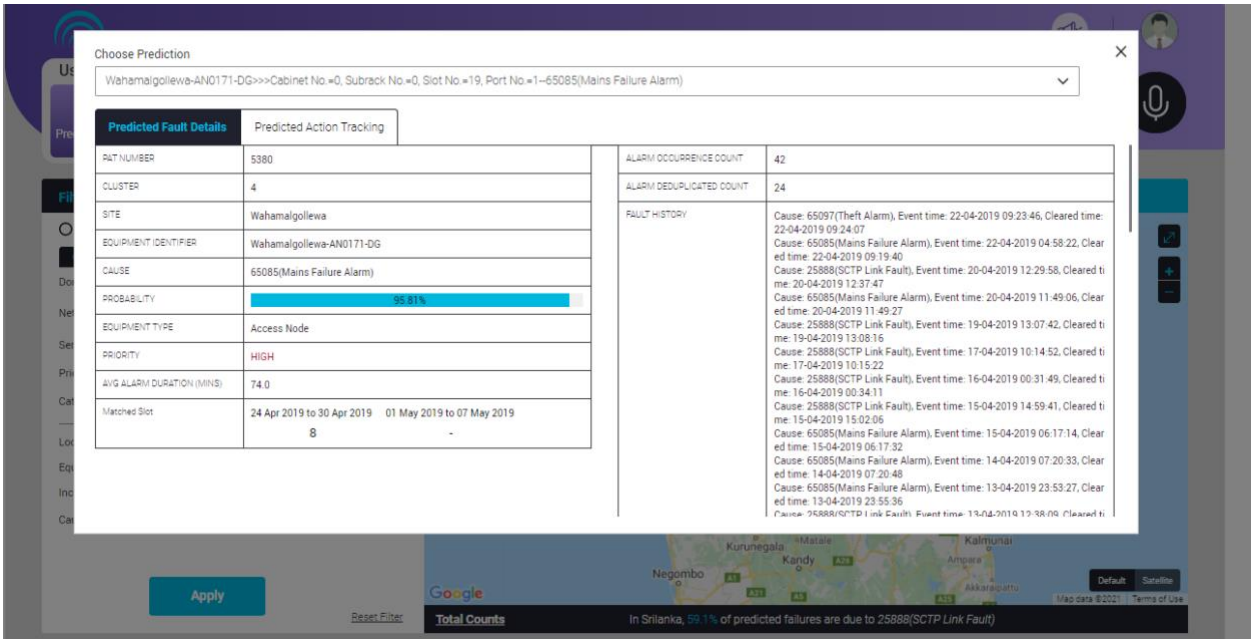


Figure 3.6 - Predicted Fault Details

The **Predicted Action Tracking** tab has the following information:

- The Recommended Technicians give the details of the technicians who are specialized to resolve the selected issue. The screen recommends the technician based on the availability and the rating of the technician.
- User can assign the technician for the ticket/prediction in case the screen displays no recommended technician.
- User/Technician can write their **Feedback** in the Feedback text box and click the **Update** button to save the feedback.

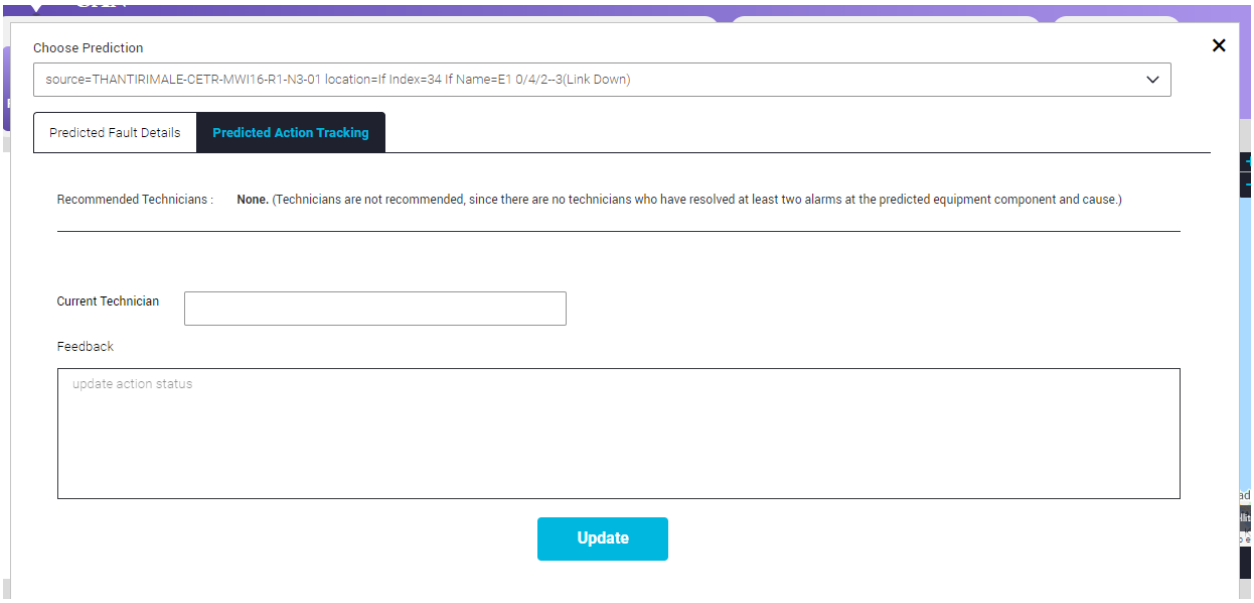


Figure 3.7 - Predicted Action Tracking

Graphical Representation (Chart view)

1. To view the graphical reprentation or chart view, click the graph icon . Chart view displays the statistics related to **Cause Category**, **Priority**, **Cause** and **Zone**.

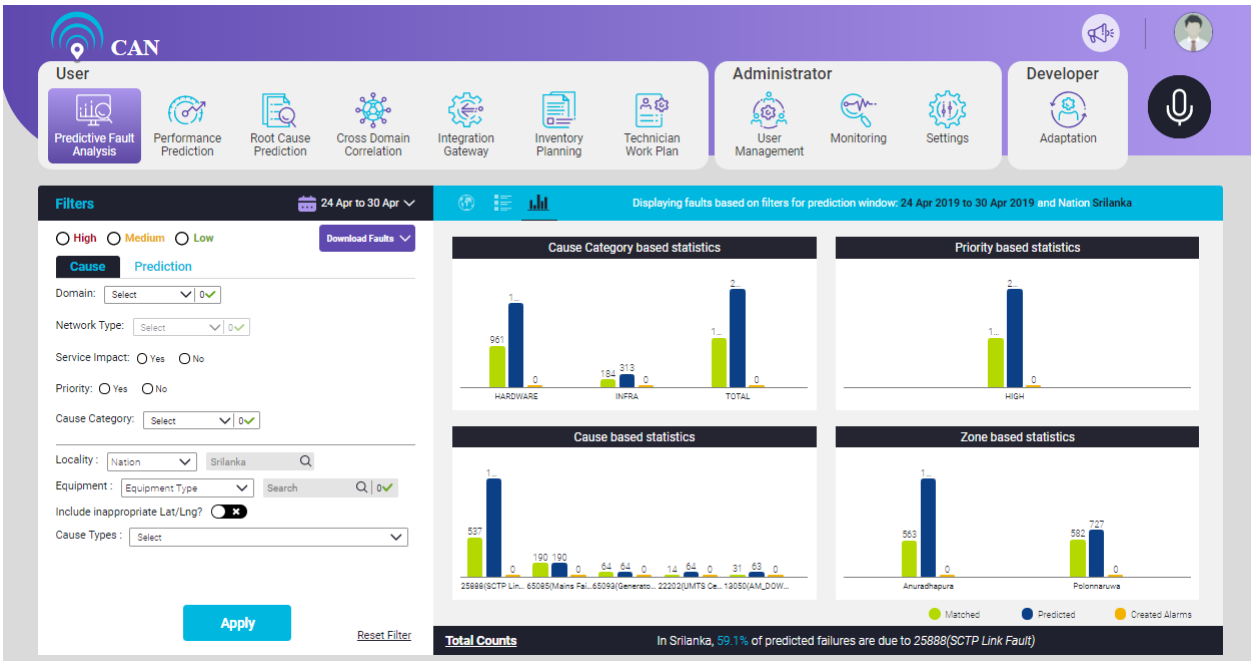


Figure 3.8 - Predictive Failure Analysis (Chart View)

Download Faults Report

User can download three types of fault report:

- Prediction Report
- Daily Report
- Filtered Report
- Alarm Matching Report
- Consolidated Report
- Filtered Report
- Ticket Matching Report
- Consolidated report

To download the **Prediction Fault Report**, select the option from the **Download Faults** drop down.

Prediction reports are of 2 types: **Daily Report** and **Filtered Report**

Matching reports are also of 2 types: **Consolidated Report** and **Filtered Report**.

Ticket Matching Report have only the **Consolidated Report**.

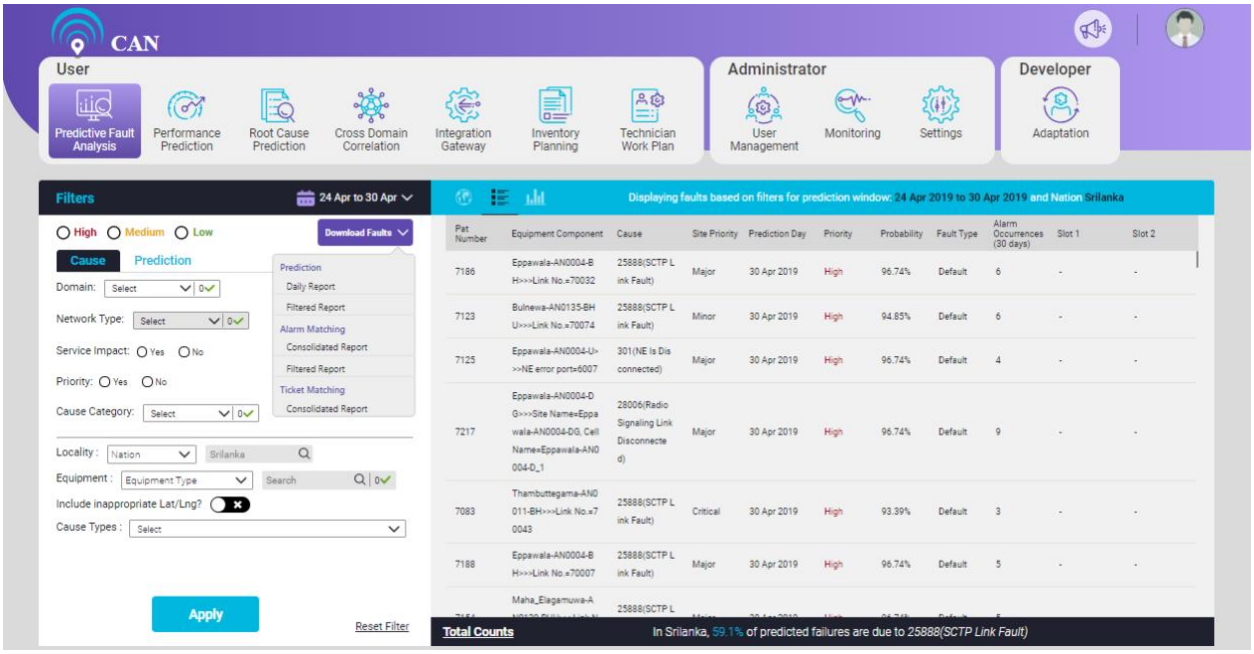


Figure 3.9 - Download Report

To view **Daily Report**, choose the time frame. Download the **Prediction Report** for the selected timeframe. Timeframe will begin from the start date of the selected prediction window to end date of the selected prediction window with an interval of 1 day. If the prediction report is not available for the given timeframe, the screen will display a popup message "**Report is not available for the search criteria**".

User can select filter(s) and view the Filtered **Predicted Report** based on the filters applied.

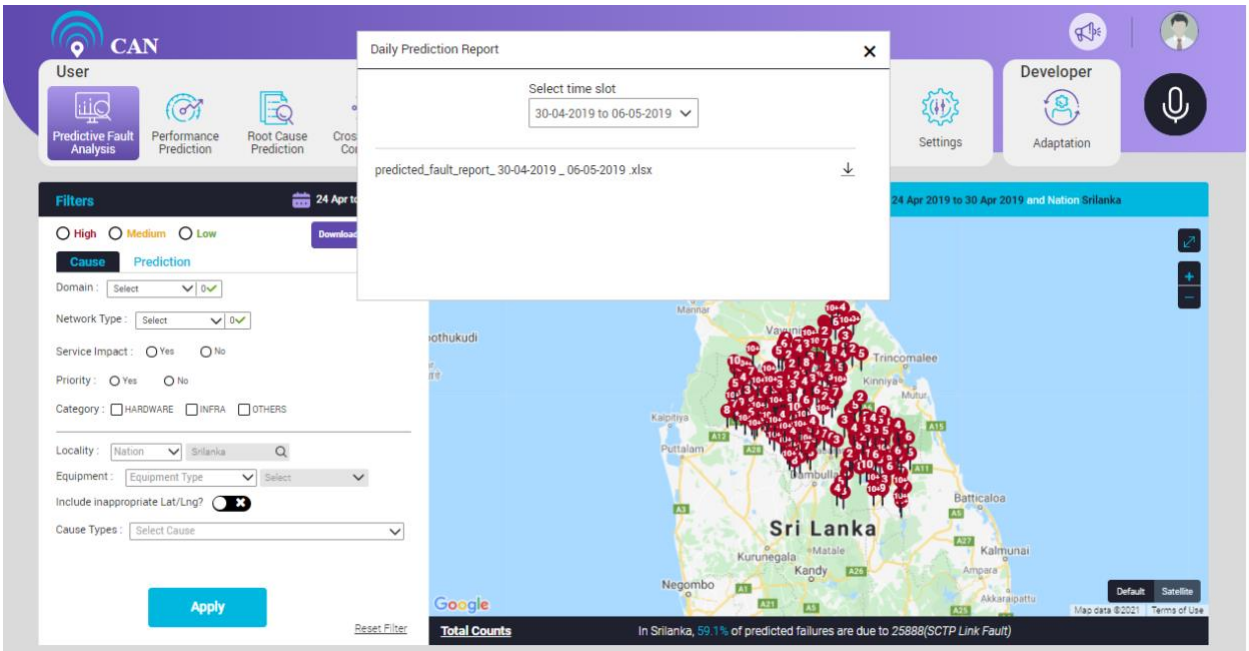


Figure 3.10 - Daily Report

User can download the **Matching Report** for the selected predicted week.

Consolidated Report: It will generate the matching report for the selected prediction window.

User can select filter(s) and view the Matching Filtered Report based on the filters applied.

See the below Figure for sample prediction report.

	PAT NUMBER	ZONE	CLUSTER	EQUIPMENT IDENTIFIER	CAUSE	SITE PRIORITY	EQUIPMEN
3	PAT032789	's-gravenhage	UnClustered	S12066	CELL LOGICAL CHANNEL AVAILABILITY SUPERVISION	1	2G
4	PAT032790	Amsterdam		RBSU11240	UtranCell_NbapReconfigurationFailure	2	UMTS
5	PAT032791			RBSU12539	UtranCell_ServiceUnavailable	2	UMTS
6	PAT032792	Appelscha		S04591	CELL LOGICAL CHANNEL AVAILABILITY SUPERVISION	2	2G
7	PAT032793	Appingedam		RBSU05314	UtranCell_ServiceUnavailable	2	UMTS
8	PAT032794	Arkel		S02499	CELL LOGICAL CHANNEL AVAILABILITY SUPERVISION	2	2G
9	PAT032795	Barendrecht		RBSU05429	UtranCell_NbapReconfigurationFailure	2	UMTS
10	PAT032796				UtranCell_ServiceUnavailable	2	UMTS
11	PAT032797	Bedum		RBSU07666	UtranCell_ServiceUnavailable	2	UMTS
12	PAT032798	Bergen op zoom		RBSU01496	UtranCell_ServiceUnavailable	2	UMTS
13	PAT032799			RBSU03852	AntennaBranch_AntennaProblemInBranchA	1	UMTS
14	PAT032800	Bleiswijk		RBSU02400	UtranCell_ServiceUnavailable	2	UMTS
15	PAT032801	Borger		RBSU12392	UtranCell_ServiceUnavailable	2	UMTS
16	PAT032802	Brakel		S04493	CELL LOGICAL CHANNEL AVAILABILITY SUPERVISION	2	2G
17	PAT032803	Capelle aan de ijssel		RBSU12518	UtranCell_ServiceUnavailable	2	UMTS
18	PAT032804	De steeg		RBSU05059	UtranCell_ServiceUnavailable	2	UMTS
19	PAT032805	Den haag		S12065	CELL LOGICAL CHANNEL AVAILABILITY SUPERVISION	1	2G
20	PAT032806	Domburg		RBSU11415	UtranCell_ServiceUnavailable	2	UMTS
21	PAT032807			RBSU12181	UtranCell_ServiceUnavailable	2	UMTS
22	PAT032808	Doornenburg		RBSU00561	UtranCell_ServiceUnavailable	2	UMTS
23	PAT032809	Eindhoven		RBSU03025	UtranCell_ServiceUnavailable	2	UMTS
24	PAT032810	Elspeet		S06236	CELL LOGICAL CHANNEL AVAILABILITY SUPERVISION	2	2G
25	PAT032811	Ermelo		RBSU02010	UtranCell_ServiceUnavailable	2	UMTS

Figure 3.11 - Downloaded Report

4. PERFORMANCE COUNTER

The Performance counter module enables CAN users to monitor the health status of every equipment along with its KPI behavior. In the event of threshold breach or health degradation corresponding devices are highlighted so that users can take appropriate action.

The Performance Counter has two tabs:

- Threshold Breach
- Alarm Superposition

Threshold Breach

Threshold breach screen shows the performance counter predictions.

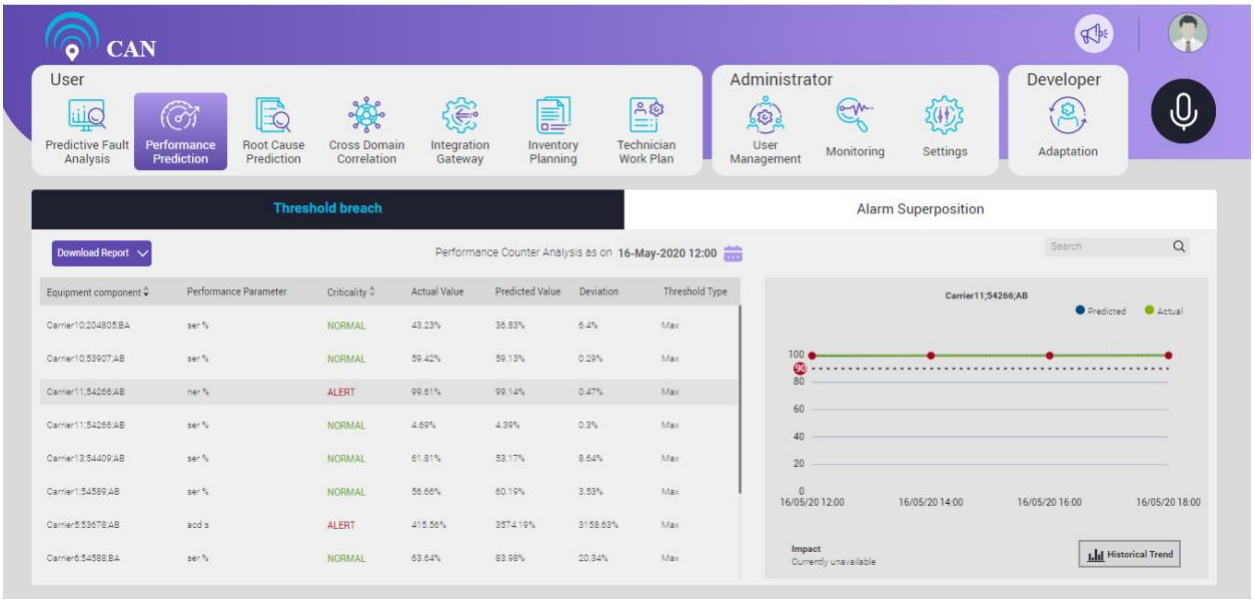


Figure 4.1 - Threshold Breach Screen

User can download the report from **Download Report** drop down menu.

User can select a particular date and time to see the performance counter predicted data for that selected date and time.

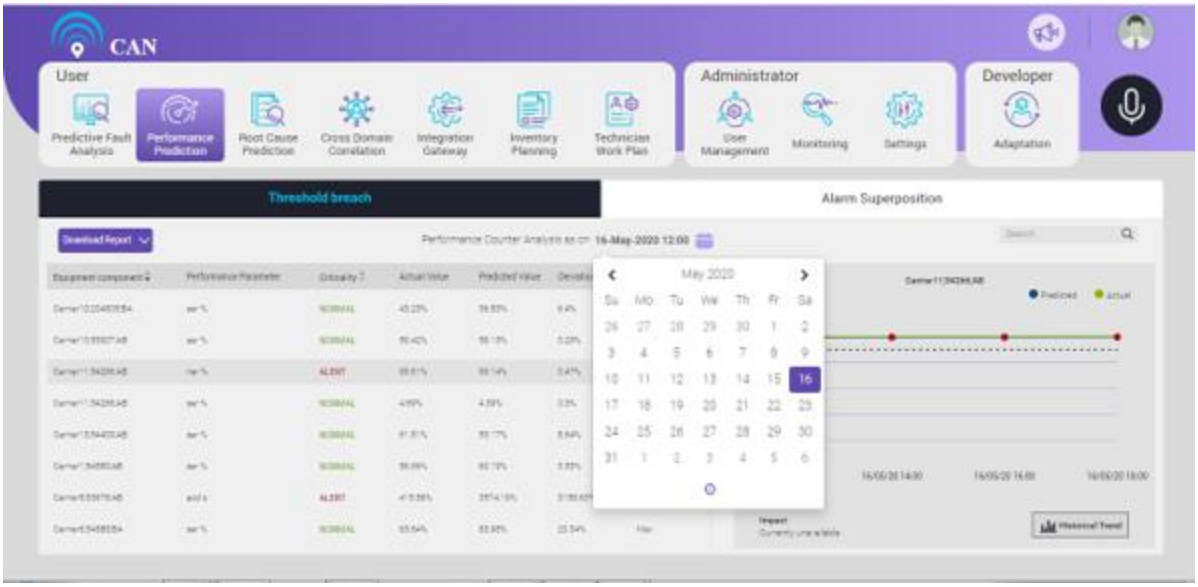


Figure 4.2 - Date Selection

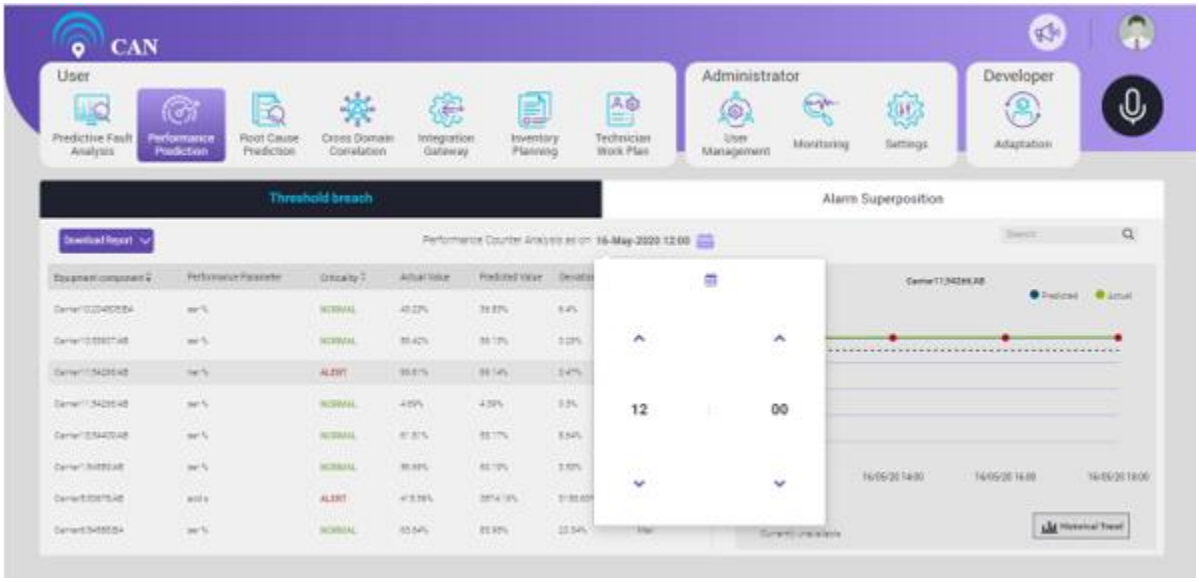


Figure 4.3 - Time Selection

Threshold Breach screen contains the following details:

- Equipment Component: It is also known as Device.
- Performance Parameter: Performance Parameter have 4 KPI (ser %, ner %, gmr_nb%, acd_s)
- Criticality: Criticality of the KPI will be categorized as either NORMAL or WARNING based on predicted value.
- Actual Value: The value which has been measured on the exact day is Actual Value.
- Predicted value: The value predicted by the CAN Prediction engine is Predicted Value.
- Deviation: The difference between the Actual value and Predicted value is known as Deviation.
- Threshold Type: Threshold type is the value above which the device can fail. There can be two values for threshold Type - Max or Min.

Equipment component and Criticality fields have the sorting option.

When predictions are done at real-time, users can only see predicted value as actual values are not known. Once after the duration of the prediction interval is crossed actual values will be available and shown in comparison with the predicted value.

The **Threshold Breach** screen has the search box. User can use the search box to search for the particular field such as Equipment component, Performance Parameter or Criticality etc. It is a generic search option.

For every PM counter prediction, there are data as well as graphical representation of the data. The graphical representation shows the actual value and predicted value.

The green colour line shows the actual value and the blue colour line shows the predicted value.

User can click the **Historical Trend** button to see the details of the graph.

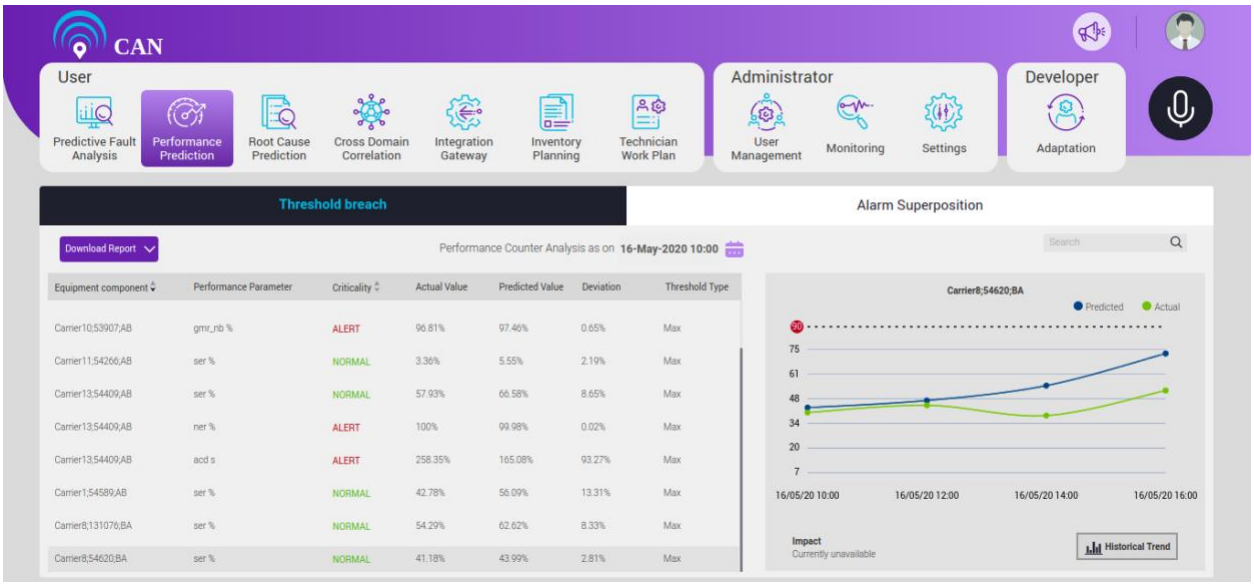


Figure 4.4 - Graphical Representation

If the user click the **Historical Trend** button for the particular graph, the **Performance Counter Historical Trend** screen pops up.

The Historical Trend is based on three fields:

- Equipment Component
- Performance Parameter
- Threshold Type

The scale shown in the figure is from 0 to 100 and the data is displayed at every 6 hours of interval.

Note: The scale of the graph and the time interval varies for different KPI or different Equipment Components.

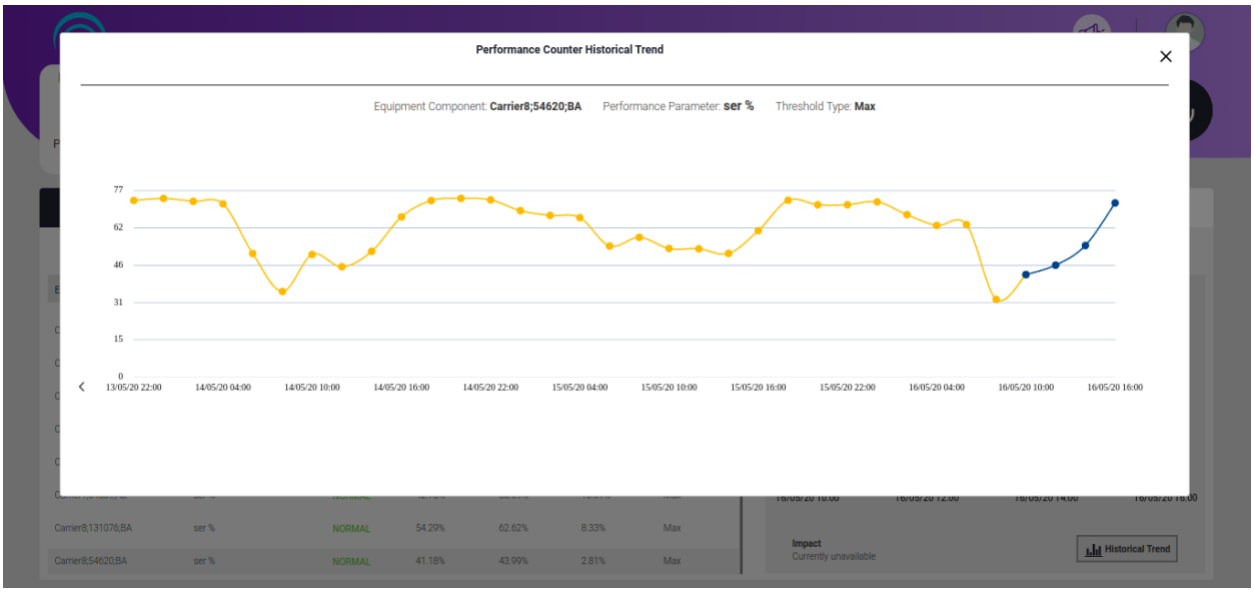


Figure 4.5 - Performance Counter Historical Trend

Alarm Superposition

Alarm Superposition screen shows the effects of the alarms on the performance counter and eventually produce the alarms. Alarm Superposition is used to figure out the health condition of the whole equipment.

User can download the report from **Download Report** drop down menu.

The screen has the search box. User can use the search box to search for particular component such as Equipment component or Criticality.

When the user clicks the **Equipment Component**, a graph appears on the right side of the screen which shows the prediction of the Equipment health.

The scale of the graph is fixed between 0 to 100.

Note: For the given image, the critical level of health index is set as 20. When the health index goes below 60 it's a warning zone and when it's goes below 20 it's a critical zone.

The critical level and warning zones varies for the different predictions.

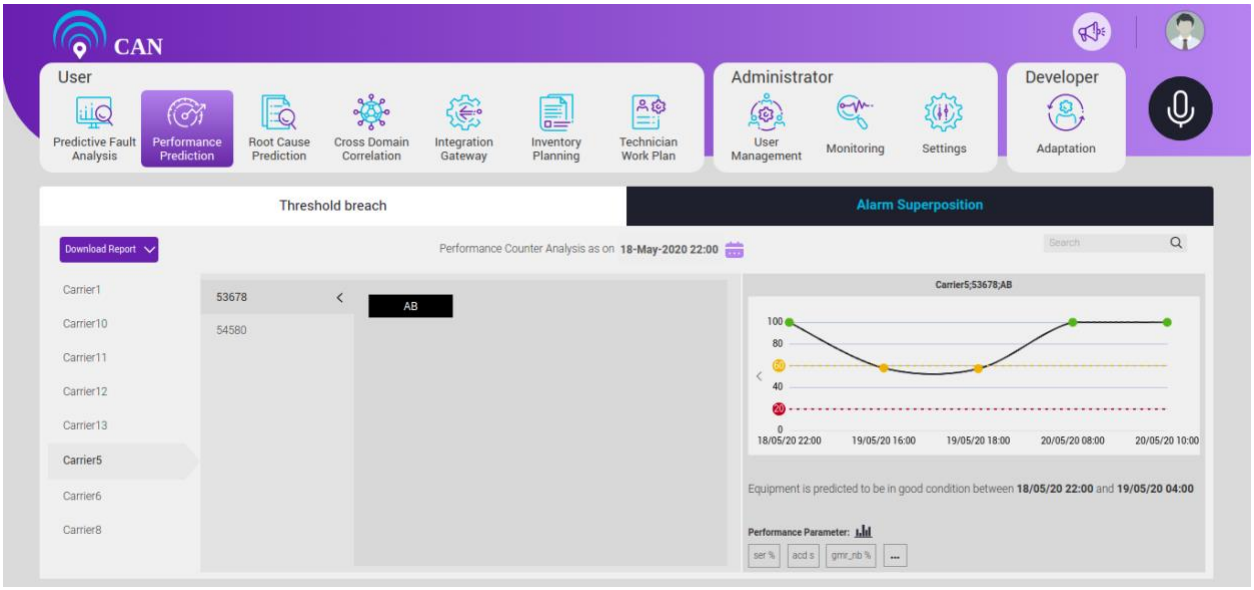


Figure 4.6 - Alarm Superposition Equipment Heath Prediction

If the user clicks on the **Performance Parameter KPI's**, Performance Counter Historical Trend screen pops up.

The Performance Counter Historical Trend has the following fields:

- Equipment Component
- Parameter Name
- Threshold Type

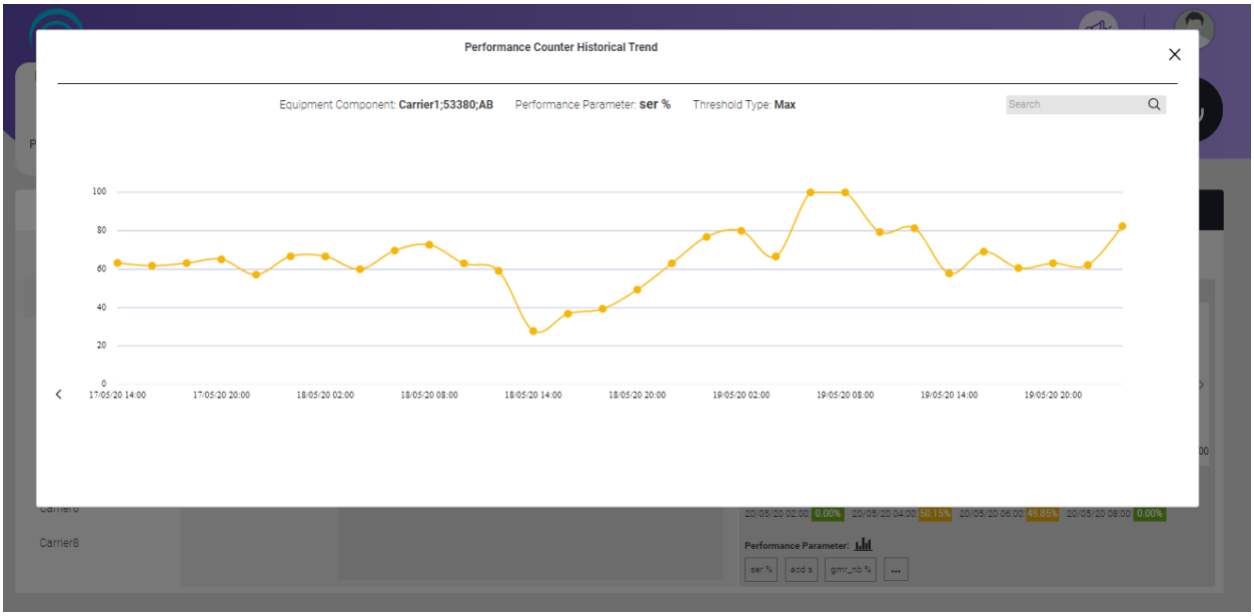


Figure 4.7 - Performance Counter Historical Trend

Page Intentionally Left Blank

5. ROOT CAUSE PREDICTION

Root Cause Prediction module pinpoints the causes of predicted faults.

The “Operationalisation flow” displays the following information:

- At the beginning, root causes for predicted faults are provided based on technical analysis i.e. based on knowledge of the equipment’s and alarms.
- As we proceed with more and more field actions, root causes are learnt based on the feedback received from the field.
- With time, technical causes are replaced by field learnt root causes that are more accurate.
- Within 6 months of field actions, we expect 80% of field learnt root causes.

This appears on the right side under each of the Root Cause Prediction tabs.

Root Cause Prediction module has two tabs:

1. Root Causes Based on Technical Analysis
2. Root Causes Based on Field Learning.

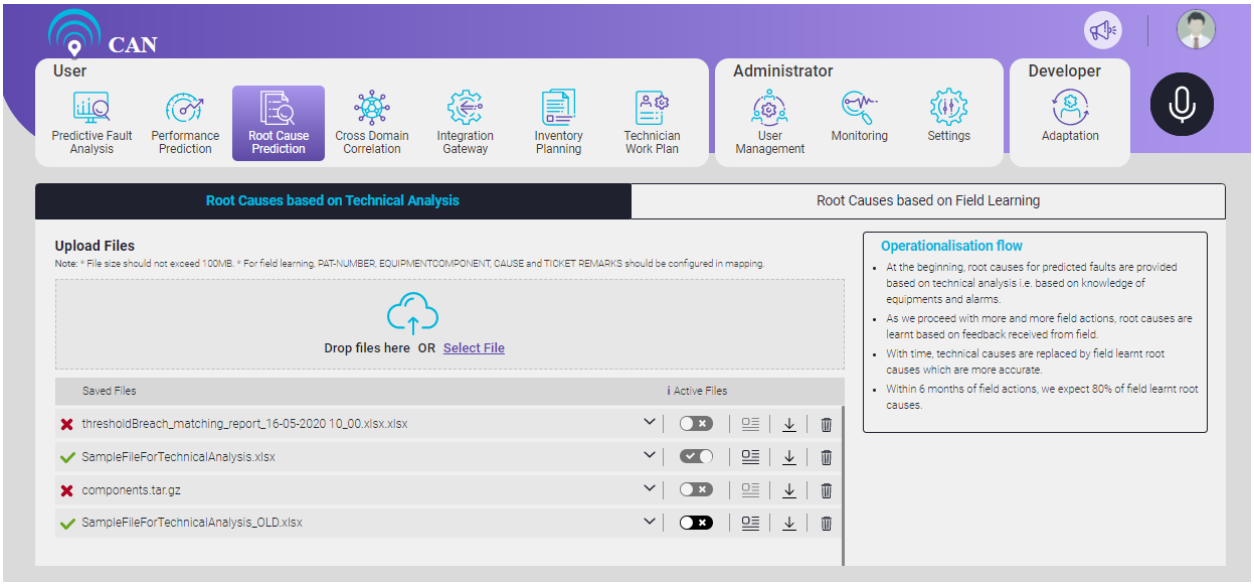


Figure 5.1 - Root Causes Based on Technical Analysis Tab

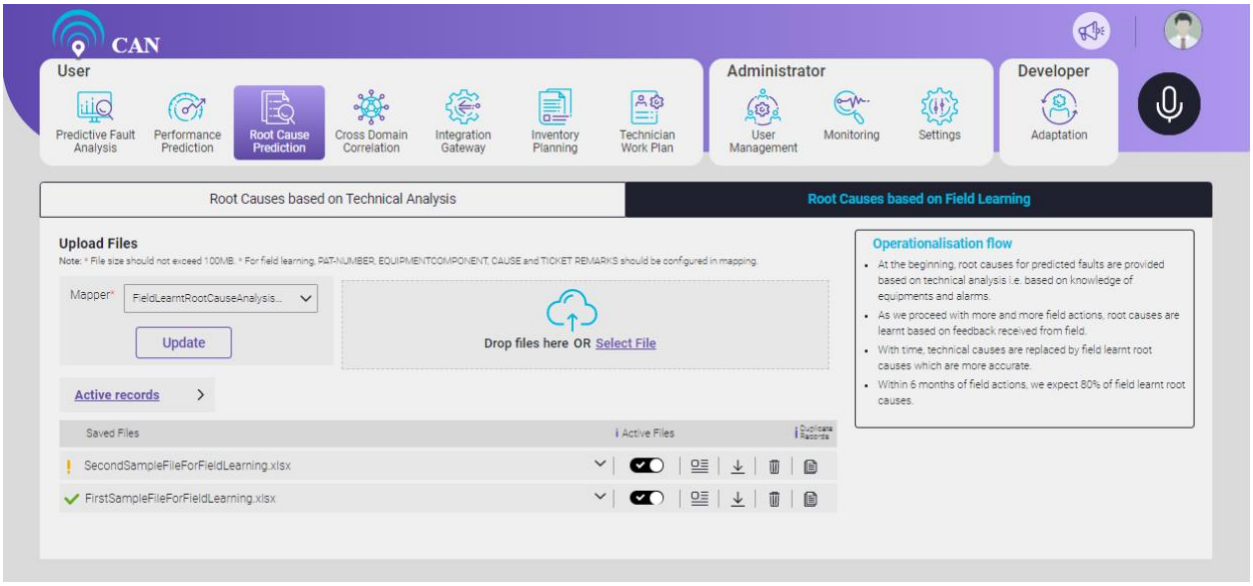


Figure 5.2 - Root Causes Based on Field Learning Tab

Root Causes Based on Technical Analysis

When the user clicks **Root Causes based on Technical Analysis** tab, the screen displays the following features:

- User gets an option to Upload the files. User can select the file to upload or use the drag and drop option to upload the file.

Note: User can upload any type of files. The maximum file size should not exceed 100 MB. * For field learning, PAT-NUMBER, EQUIPMENTCOMPONENT, CAUSE and TICKET REMARKS should be configured in mapping.

- User can analyse the technical root causes based on the active file information.
- By default, the latest uploaded file (if parsed successfully) is active.

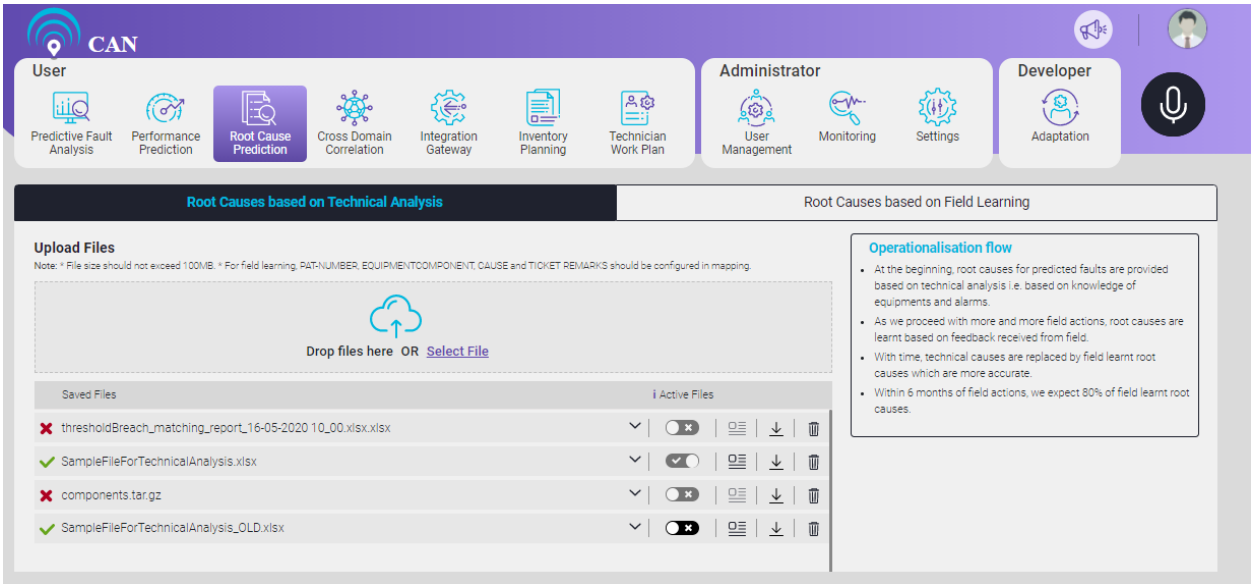


Figure 5.3 - Latest Upload File is Active

- If already one active file is present at the time of new file upload, the new file becomes active and the existing file becomes inactive.

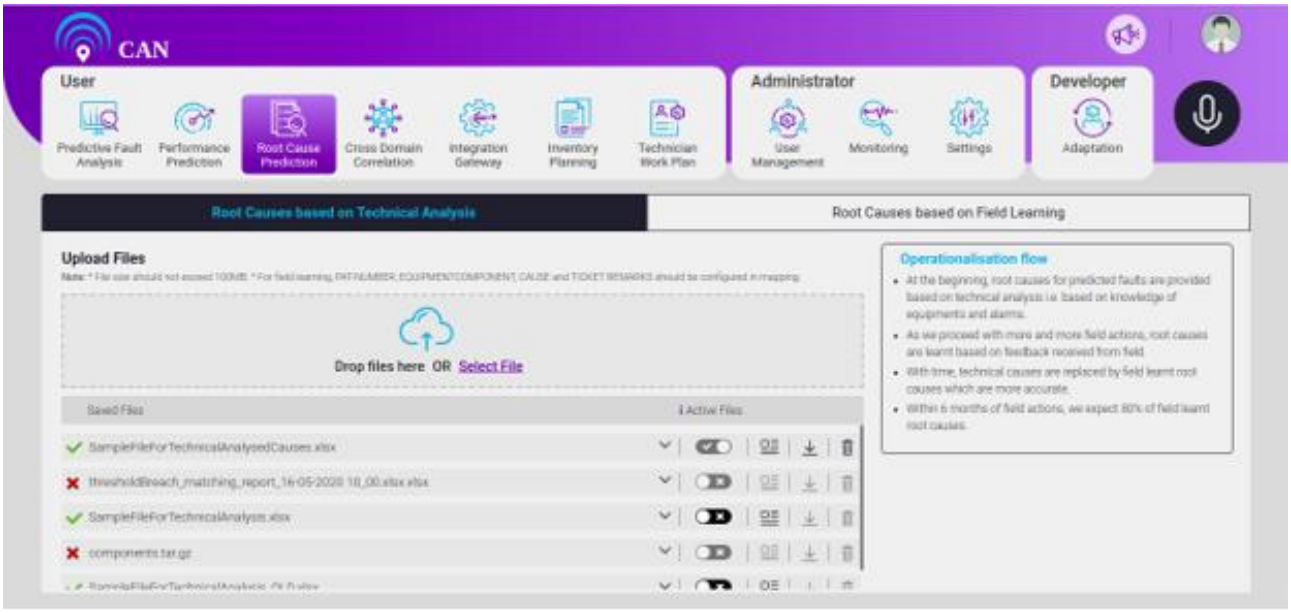


Figure 5.4 - Active against Multiple Files Scenario

- Click the **Detailed info** button to view the Detailed Information of the particular parsed file. The Detailed Information displays the following details on the screen:

    1. CAUSE
    2. FAULT HISTORY
    3. POSSIBLE REASON
    4. REMARKS

- Verify CAUSE name and FAULT HISTORY with pre-configured alarm causes and see if POSSIBLE REASON is available or not. If verified, the Remarks column shows green tick, otherwise the Remark column shows red cross with corresponding remarks.

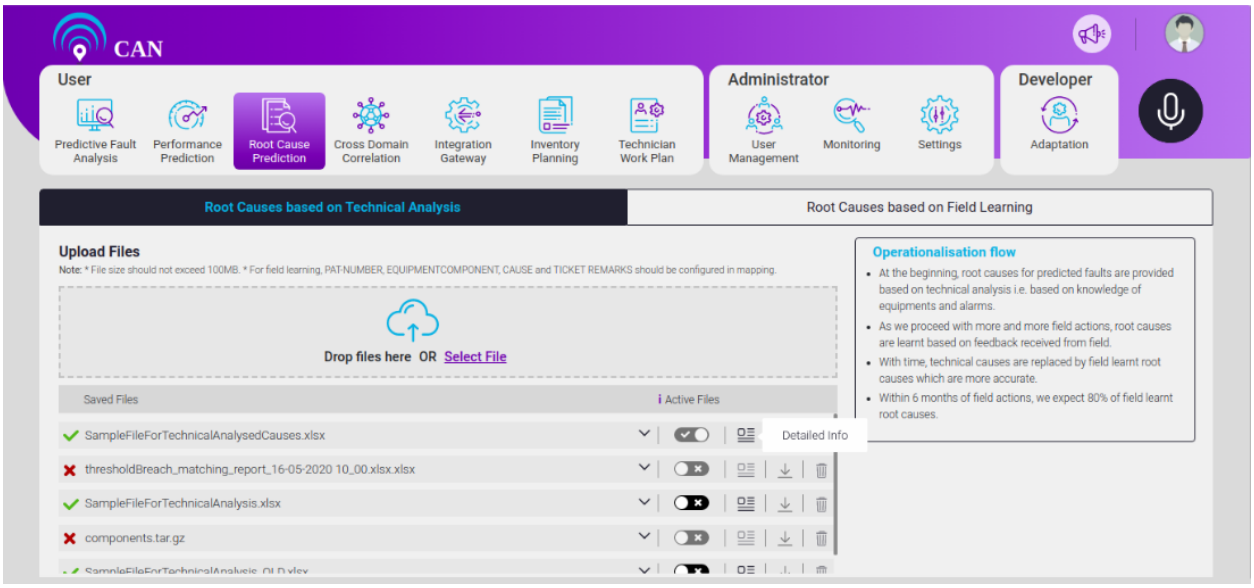


Figure 5.5 - Detailed Info Button

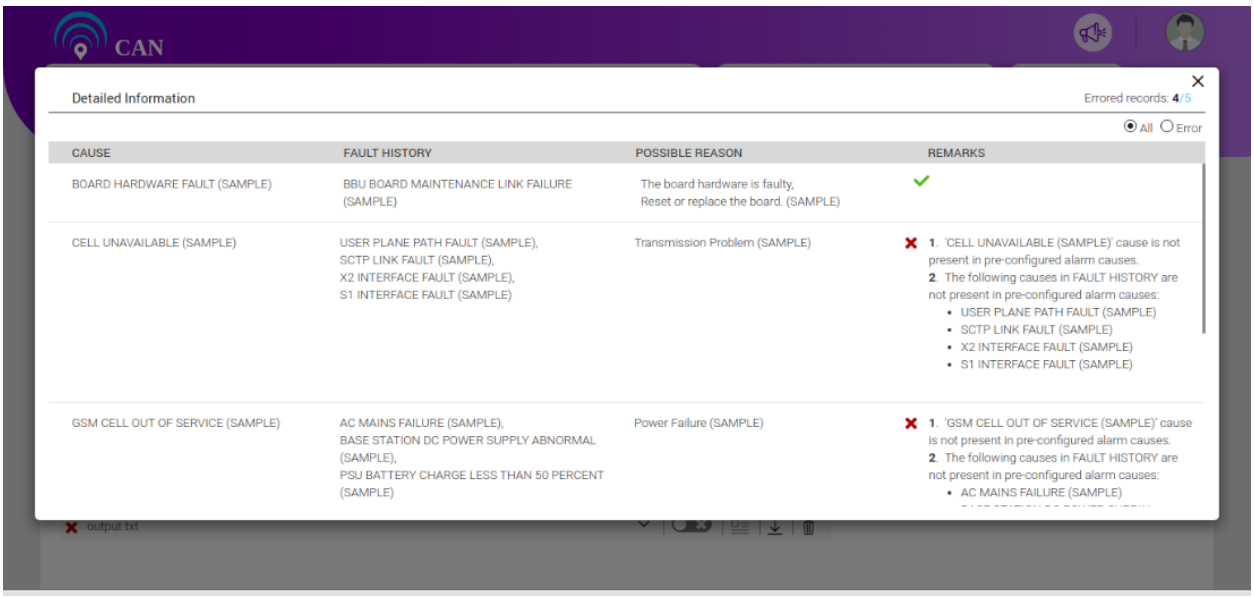


Figure 5.6 - File Details with Remarks

- On the **'Detailed Information**' pop-up, the screen displays the count of Errored records out of Total records. An errored record represents red cross with corresponding remarks in Remarks column. By default, the screen displays all the effective records. When user selects the 'Error' radio button ○ Error , user can see only the errored records on the screen.

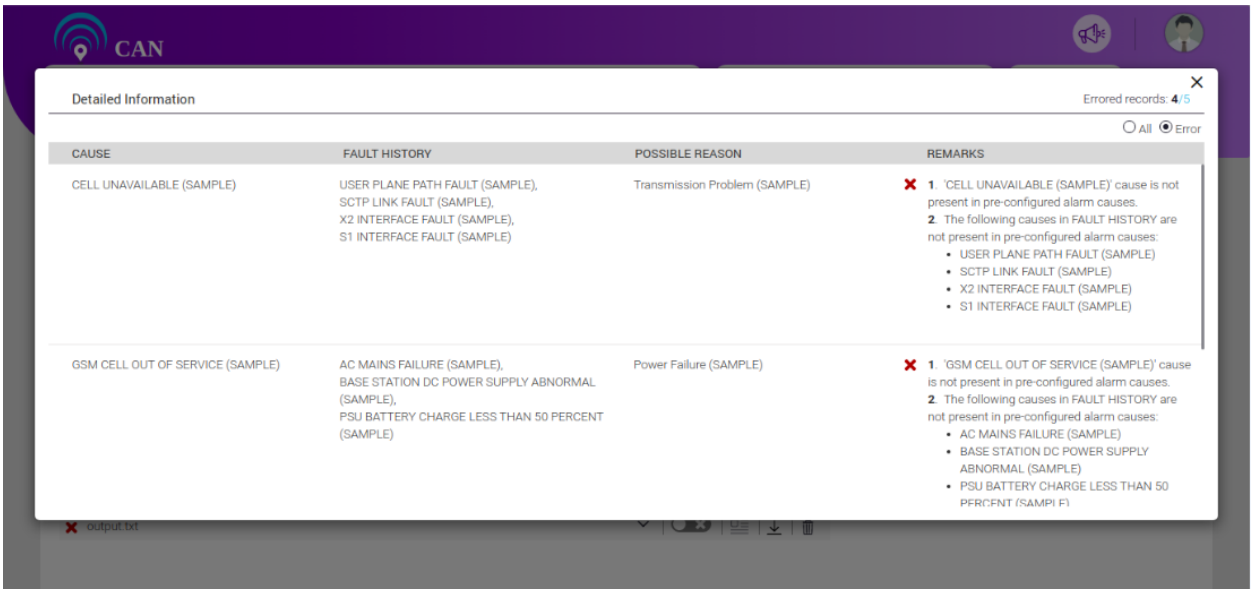


Figure 5.7 - Error Radio Button Selection and Errored Record Sample

- If the selected file is already active, toggle switch will be disabled.

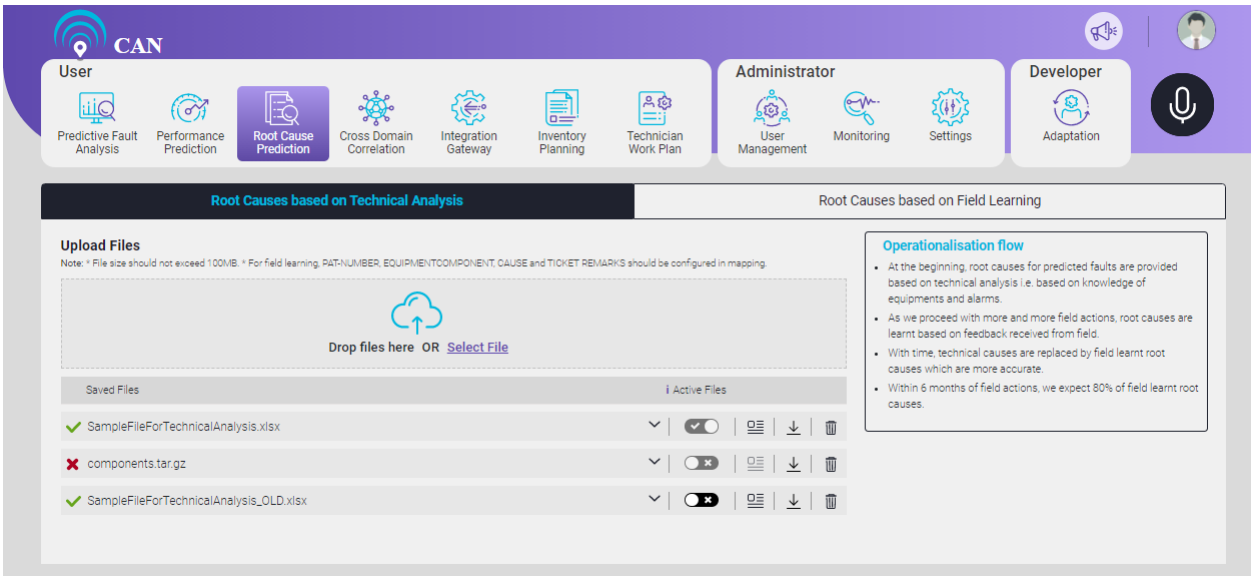


Figure 5.8 - Only File Active

- If the file is not active and contains discarded records, the pop-up displays the file contains the number of discarded records while we activate the file (The file can have one or multiple Discarded records). At a time, only one file can remain active.

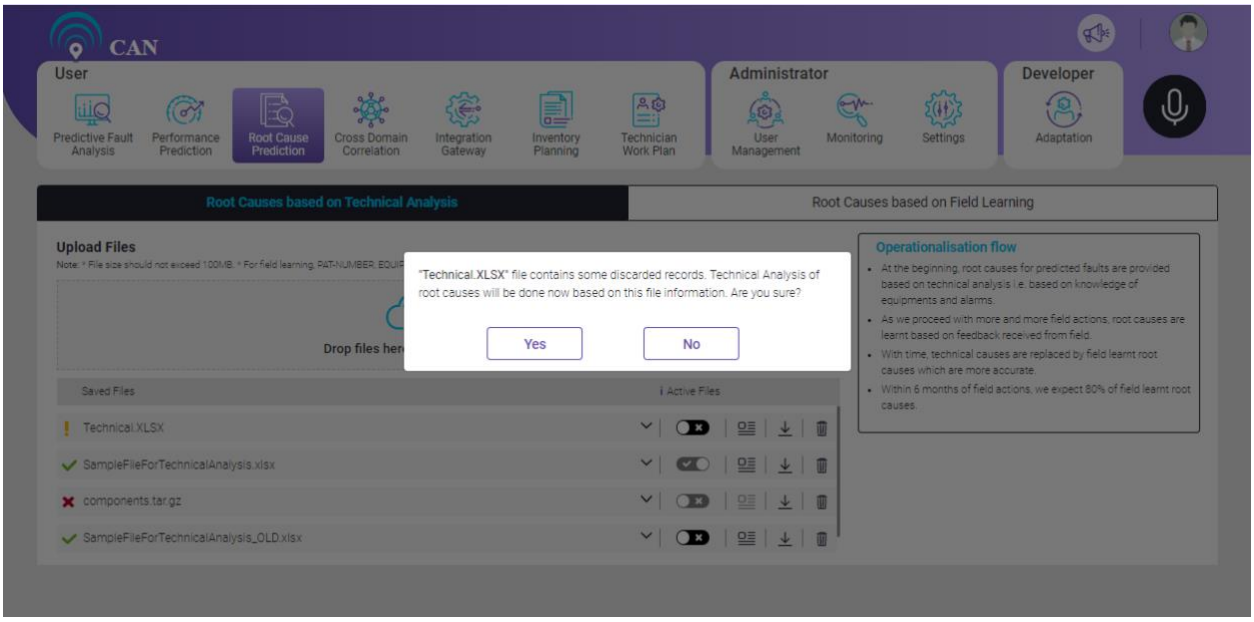


Figure 5.9 - Discarded Record Check

Root Causes Based on Field Learning

When user click the **Root Causes Based on Field Learning** tab, the screen displays the following features:

- User can upload any type of files based on the saved mapper configured in the parser screen. From the **Mapper** drop down menu, user can select the **Mapper** name and upload the file only after the mapper is saved.

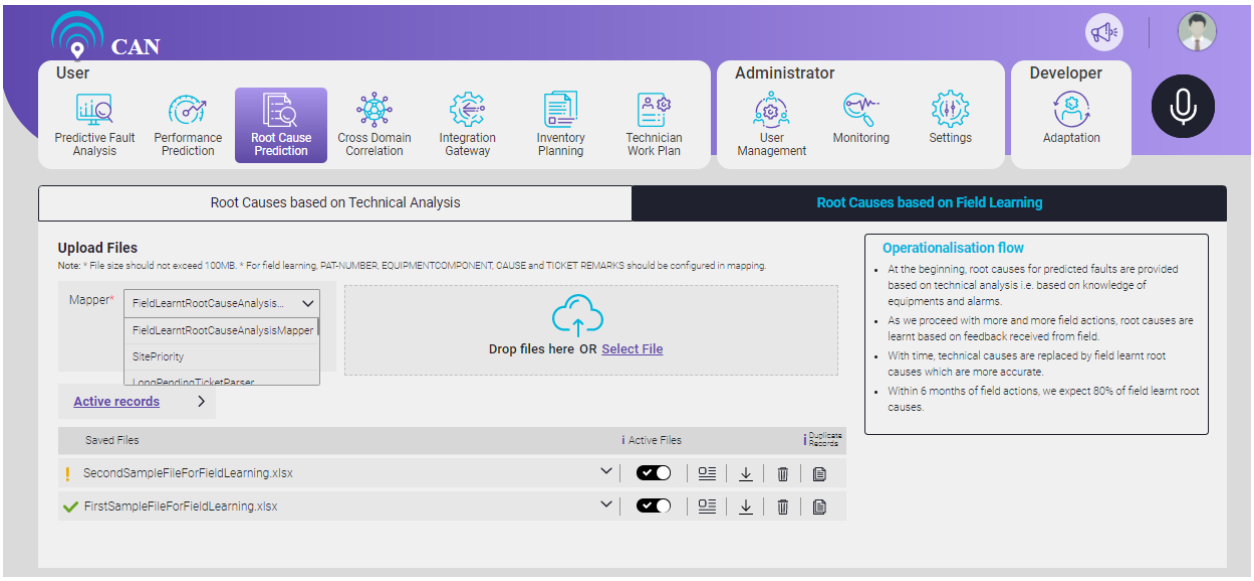


Figure 5.10 - Drop down Menu to Select Mapper Name

- If selected Mapper is not saved and user try to upload the file, an error message "**Before uploading file, please save the mapper**" appears on the screen.

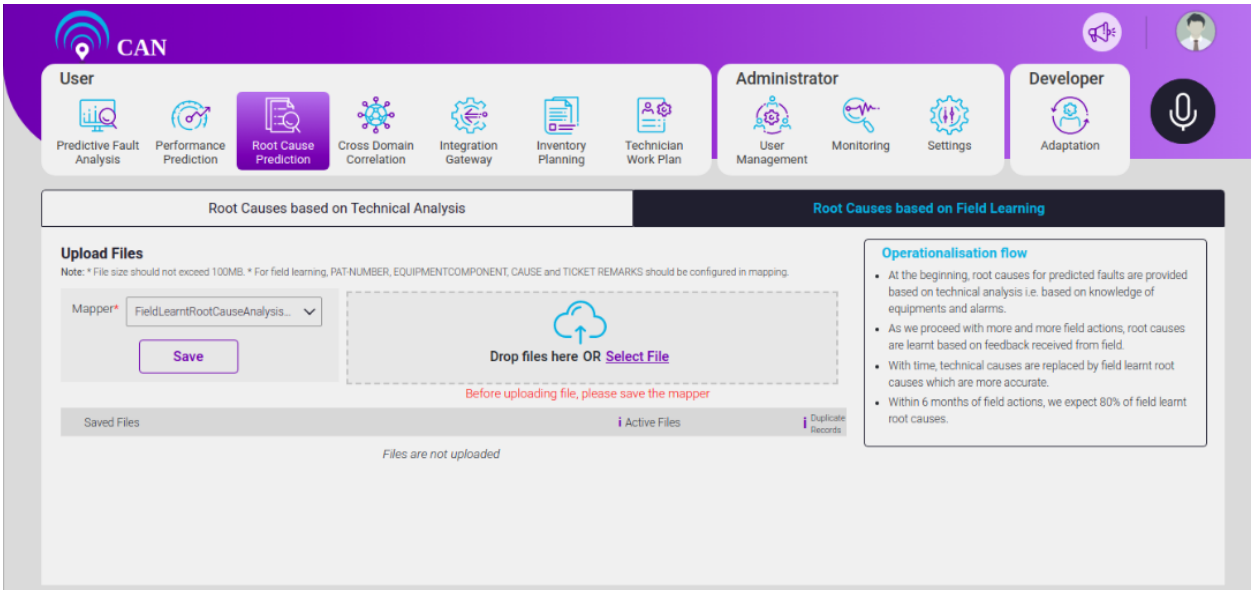


Figure 5.11 - Error Message when Parser is Not Saved

- By default, the latest uploaded file remains active. If already one active file is present at the time of new file upload, the new file becomes active and the existing file becomes inactive (same as Technical Analysis screen). For Field Learning, active file represents at least one record of that particular file is active. By default, all the records of the active file is active and based on the active records, the system analyses the field learnt root causes.

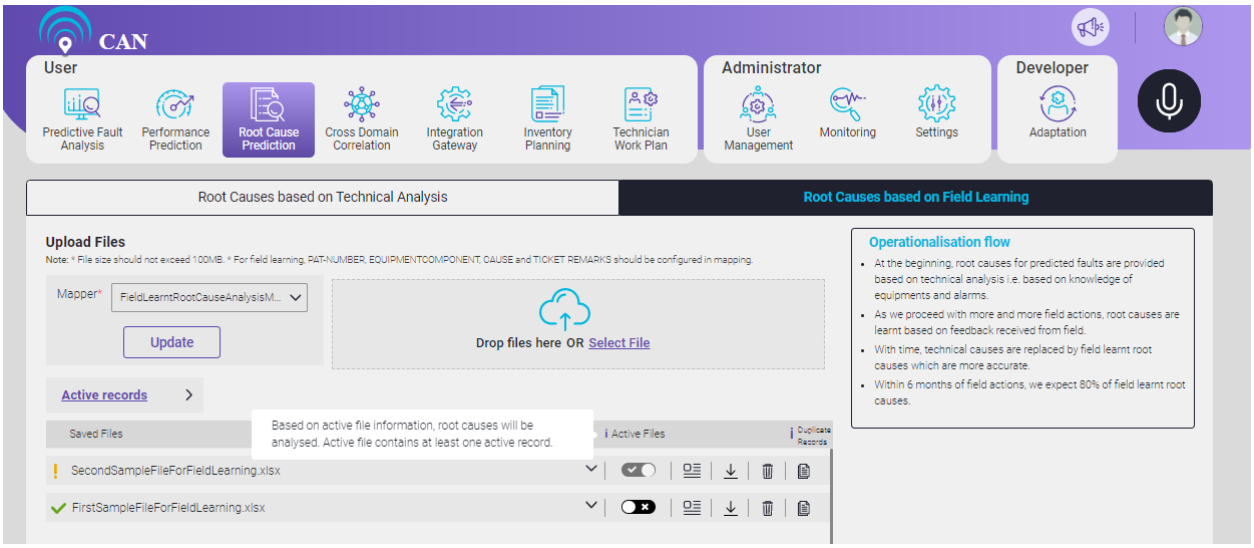


Figure 5.12 - Active file Contains at least One Active Record

- Click the **Details Info** tab to view the Detailed Information of the records from the parsed file.

The screen displays the following informations:

Mandatory Information

1. ACTIVE RECORD
2. PAT-NUMBER
3. EQUIPMENT_COMPONENT
4. CAUSE
5. TICKET REMARKS
6. REMARKS

Optional Information

7. OFFICECODE
8. PREDICTIVE TT RESPONSIBLE GROUP

NOTE: The screen displays the mandatory information. The screen might or might not display Optional information as per the user's requirement/mapping.

- Verify CAUSE name and EQUIPMENT_COMPONENT name with pre-configured alarm causes and equipment Components respectively. See the combination of PAT-NUMBER and EQUIPMENT_COMPONENT is available or not among the predictions. If verified, the Remarks column shows green tick, otherwise the Remark column shows red cross and corresponding remarks.

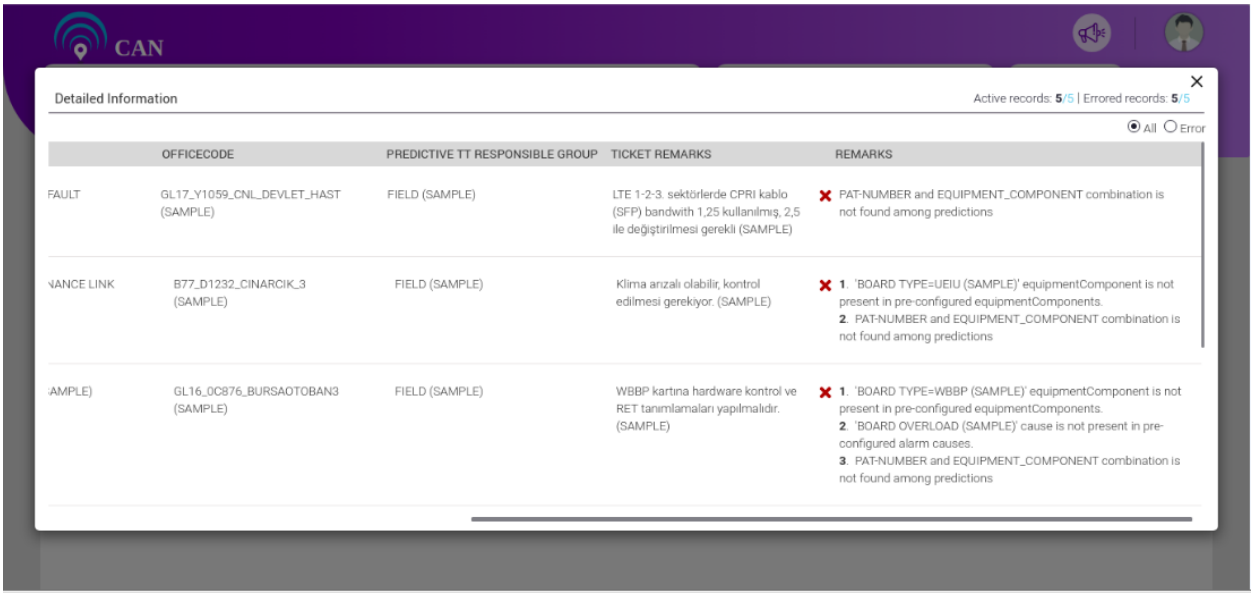


Figure 5.13 - Remarks for Field Learning

- On the **Detailed Information** pop-up, the screen displays the count of active records and errored records out of total record. An errored record represents the red cross with the corresponding remarks in the Remarks column. By default, the pop-up on the screen displays all the effective records.

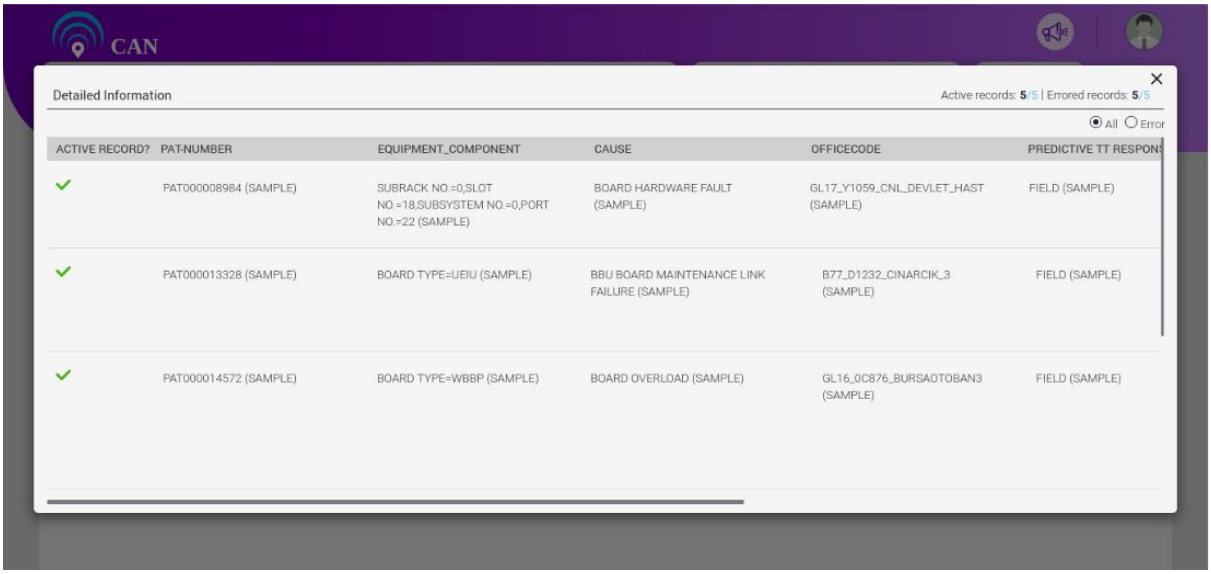


Figure 5.14 - Active Records Count, Total Records and Count out of Total Records

- To view only Error record, user can select the **'Error'** radio button. User can view the count of active records corresponding to that file. If the record is active, the ACTIVE RECORD column shows green tick, otherwise it shows red cross.

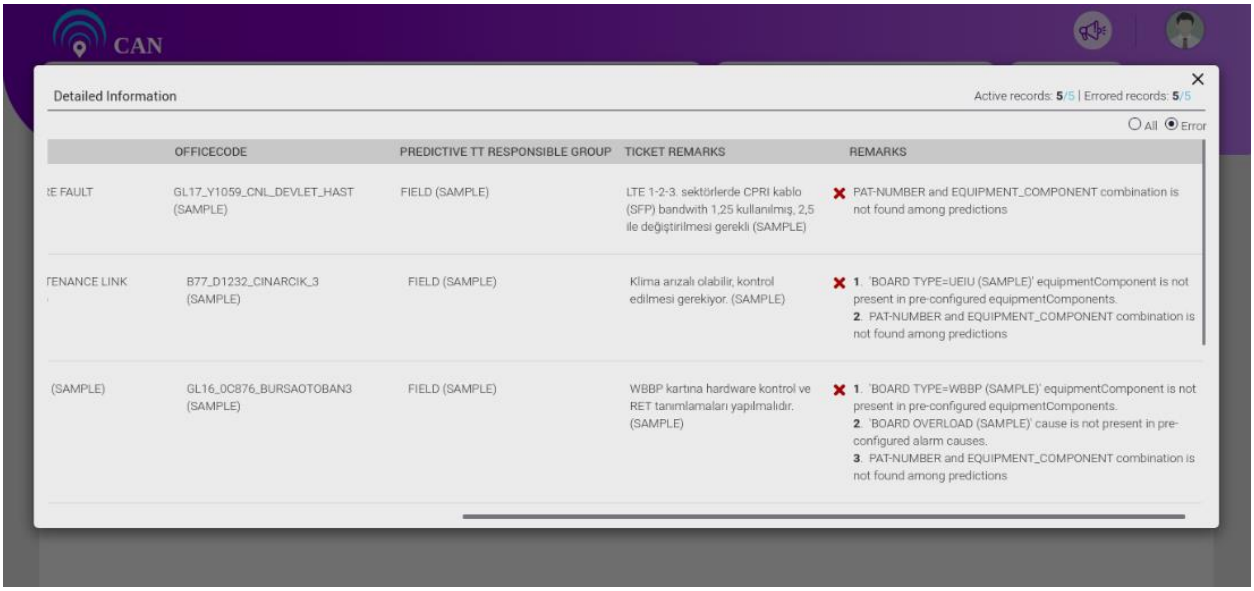


Figure 5.15 - Error Radio Button

- If a file contains duplicate records based on PAT-NUMBER, EQUIPMENT_COMPONENT and CAUSE combination, system would accept the first record and reject others.
- For each PAT-NUMBER, EQUIPMENT_COMPONENT and CAUSE combination, if multiple records are there across multiple files, then only the selected record remains active. By default all the records of the active file will be active.

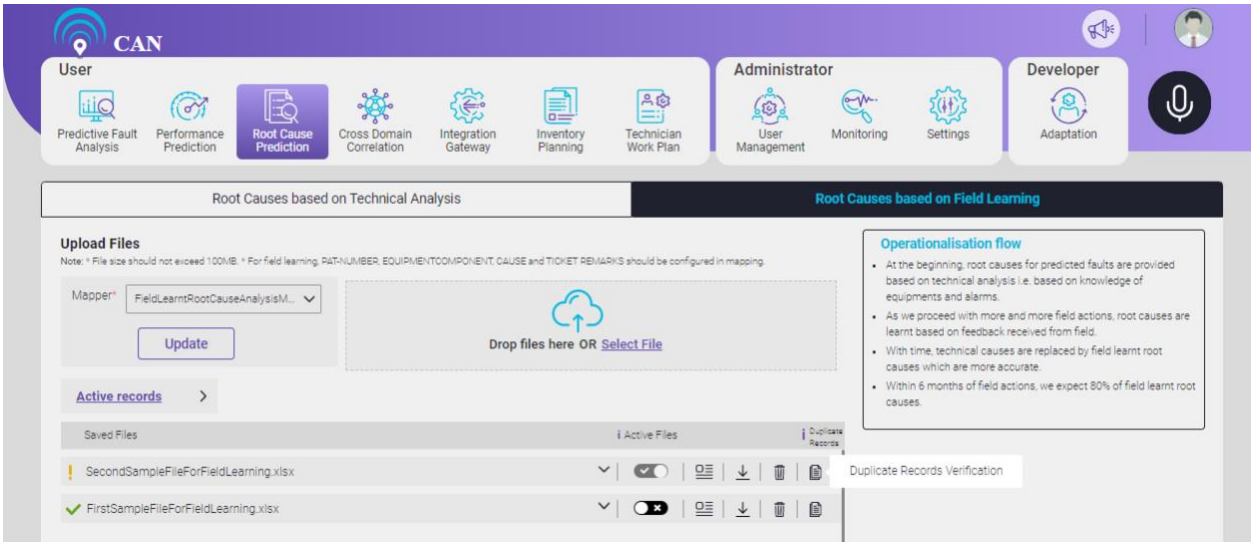


Figure 5.16 - Duplicate Record Verification Section

- To view the Duplicate Records Information, Click the "**Duplicate Records Verification**" checkbox. The Duplicate Records Information displays the following information:

    1. PAT-NUMBER
    2. EQUIPMENT_COMPONENT
    3. CAUSE

- The pop up on the screen displays the total No. of duplicate records.

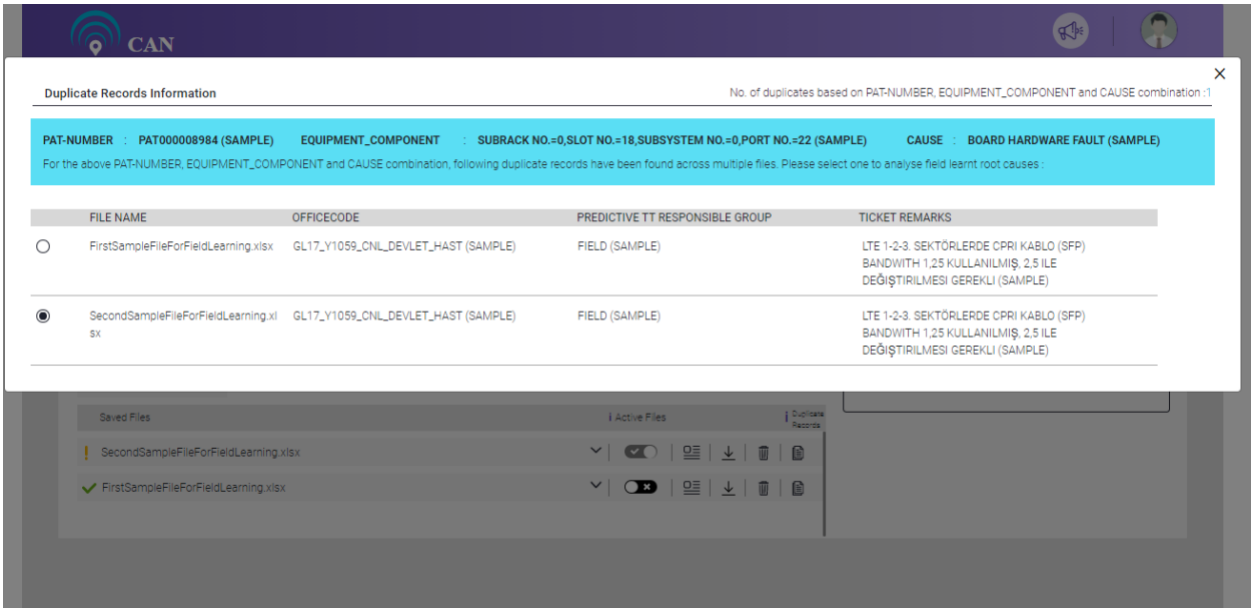


Figure 5.17 - No. of Duplicate Records Count and Duplicate Verification

- By default Active Records checkboxes are selected. If required user can select the other file information also. But at a time, user can select only one record among the duplicate records. Once user selects the record, that particular record becomes active.

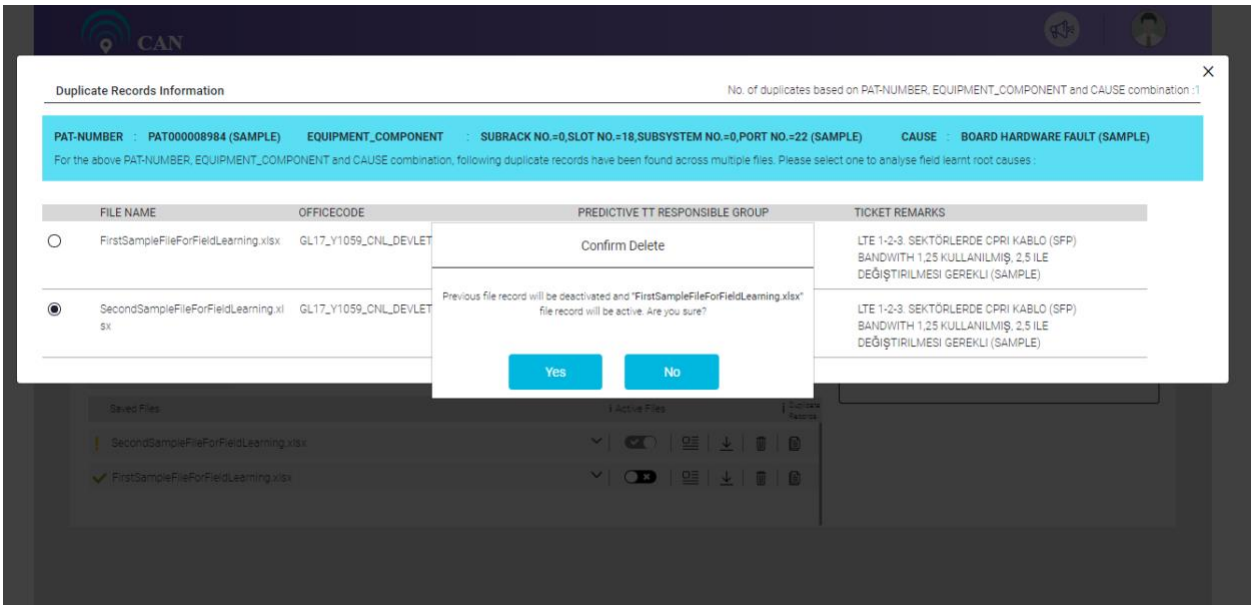


Figure 5.18 - Select the Other File Record

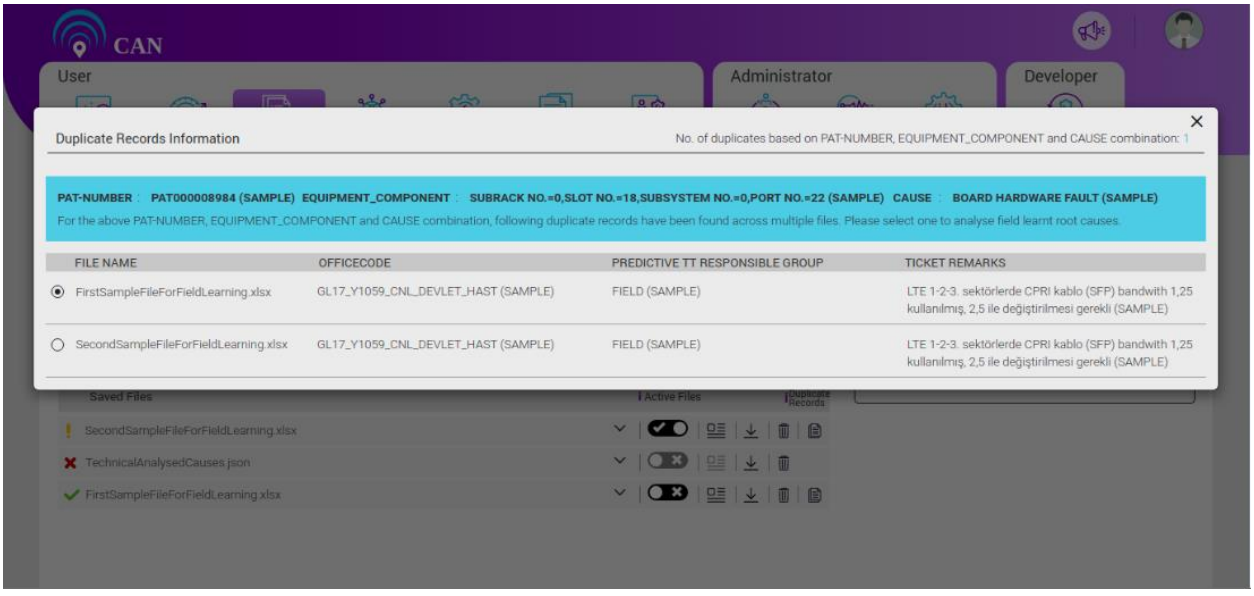


Figure 5.19 - Duplicate Record Verification

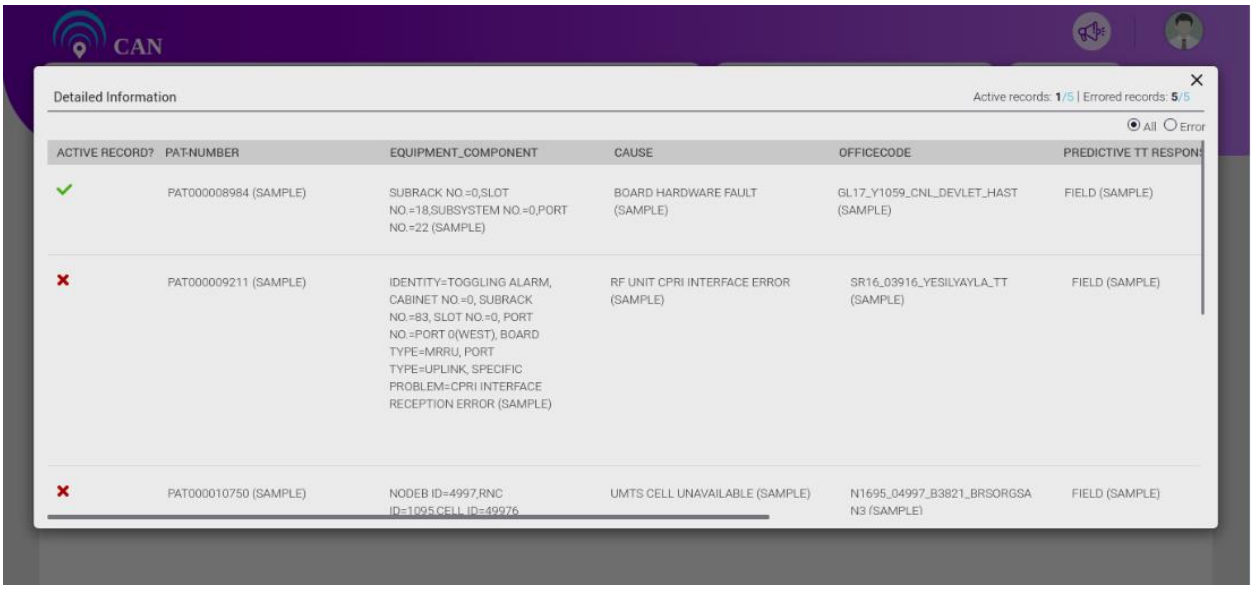


Figure 5.20 - One Active Record

- Click the Active File toggle switch to select a file. If the file is the only active file, the toggle swtich is disabled.

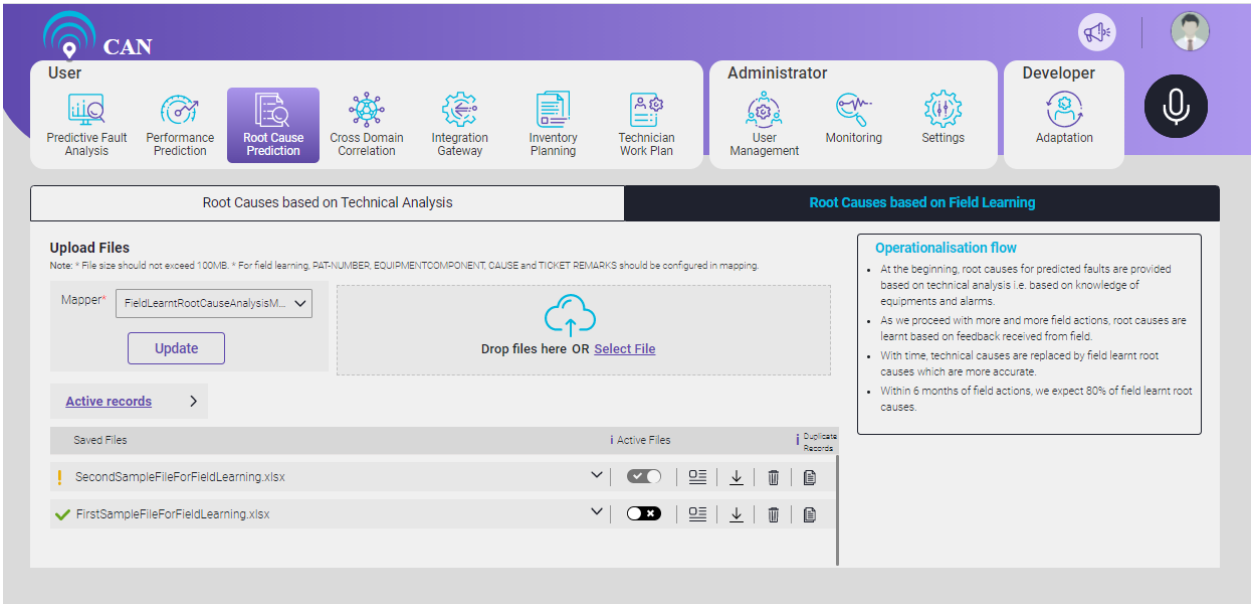


Figure 5.21 - Already Active File

- If duplicate records are not available across multiple files and user click to active the deactive file, a message **"Field Learning of root causes will be done now based on the "SampleFileForFieldLearntRCA-1.xlsx" information and all the records of this file will be active. Click Yes to deactive all the records of other files and make this file active"** appears on the screen.

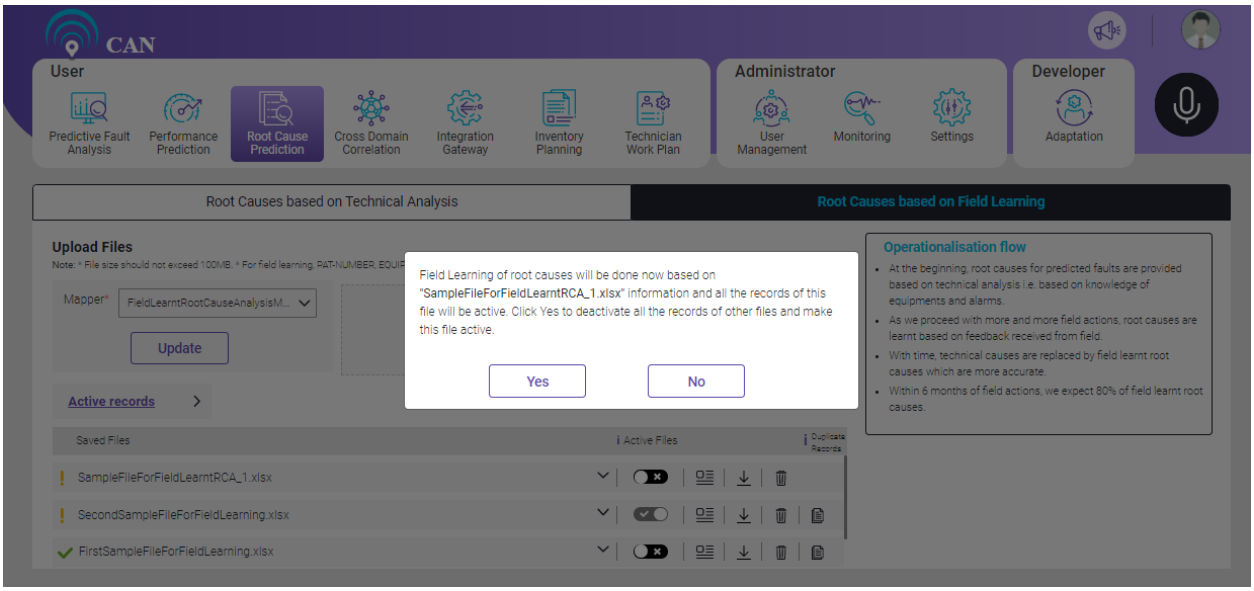


Figure 5.22 - No Duplicate Record in the File

- If multiple files have duplicate records and user tries to activate one file among multiple files, a message **"Field Learning of root causes will be done now based on "FirstSampleFileForFieldLearning.xlsx" file information. Since this file contains duplicate records, please verify those first and then proceed"** appears on the screen**.**

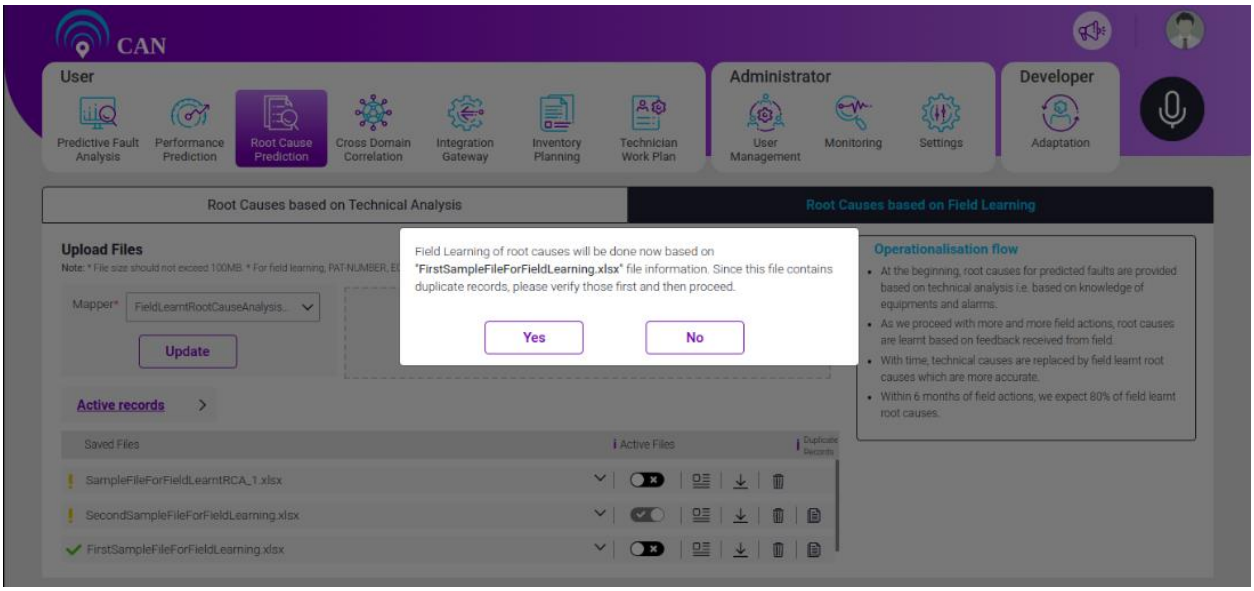


Figure 5.23 - File contains Duplicate Records

- If all the duplicates are not verified and user tries to activate the file, a message **"SecondSampleFileForFieldLearning.xlsx" file contains one discarded record. Field Learning information and all the records of this will be active. Please verify all the duplicates of this file. Click No to deactivate all the record; to continue with the same, click Yes** appears on the screen.

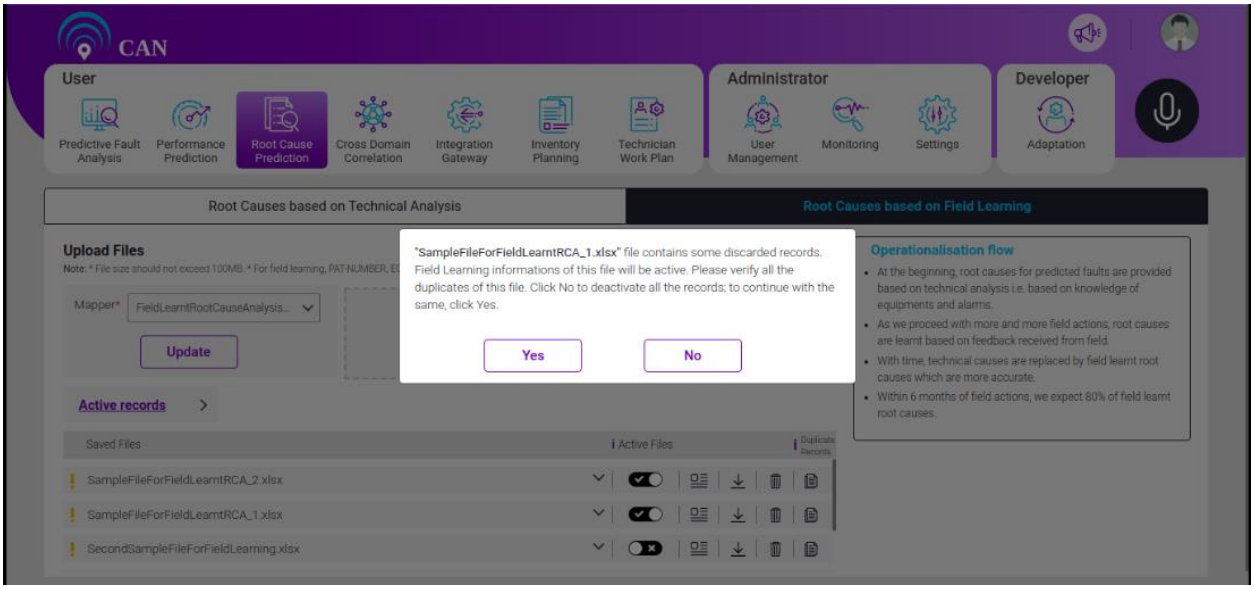


Figure 5.24 - All Duplicates are Not Verified

- After all the duplicate verification, click the **Active File** check box, if the file is already active, then click the **YES** button to activate all the records.
- Click the **No** button, to retain the previous active record(s).

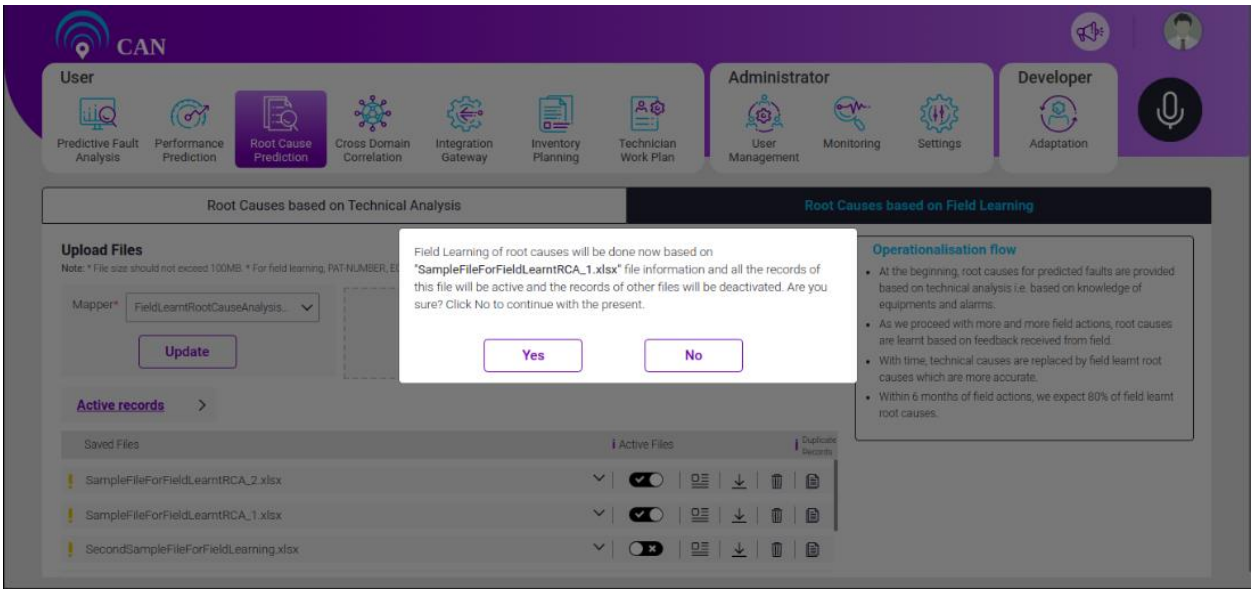


Figure 5.25 - All Duplicate Records are Verified but File contains Some Inactive Records

- At a time, multiple files can be active. Active file contains at least one active record if there are duplicates among them.

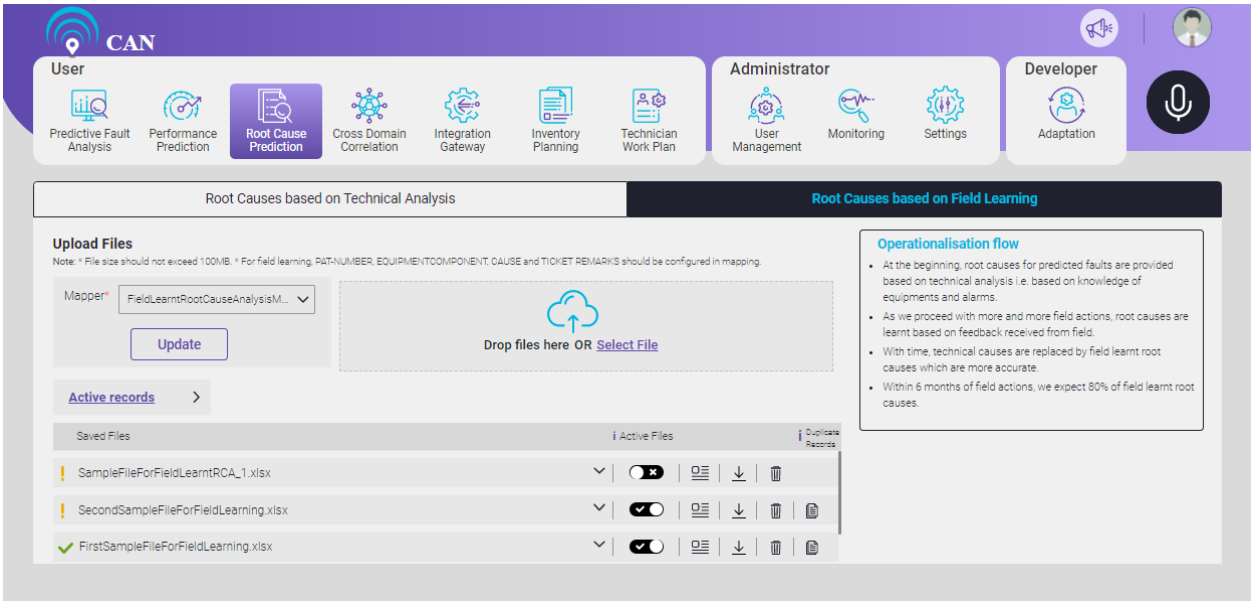


Figure 5.26 - Multiple Files Active at a Time

User can click the **Active records**.

User can see all the Active Records Information at one place.

No. of duplicates based on PAT-NUMBER, EQUIPMENT_COMPONENT and CAUSE combination.

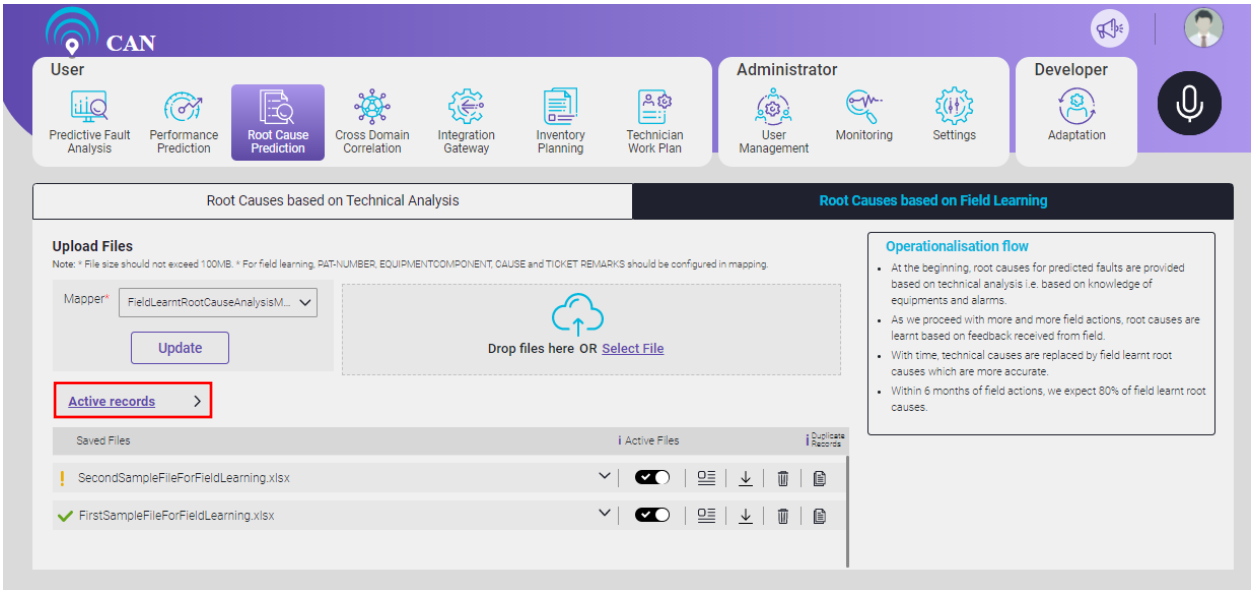


Figure 5.27 - Active records

The Active Records Information screen will display ALL the active records and Duplicate Records if applicable.

User can search the active records for a particular file with the search box 

.

By default, ALL radio button will be selected. The screen will display all the active records.

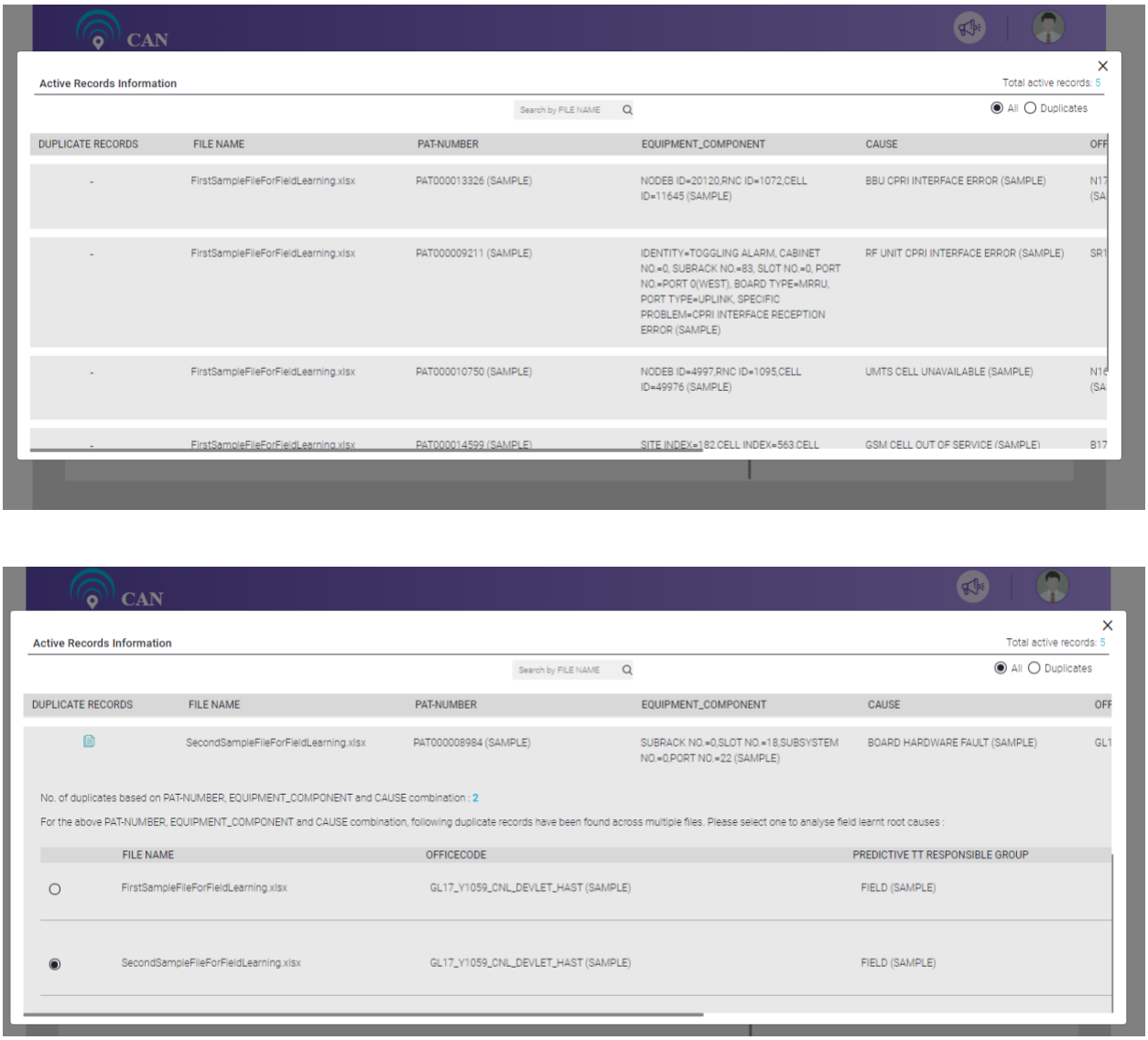


Figure 5.28 - Active Records Information

User can select the Duplicate radio button to see the Duplicate Records in the active records.

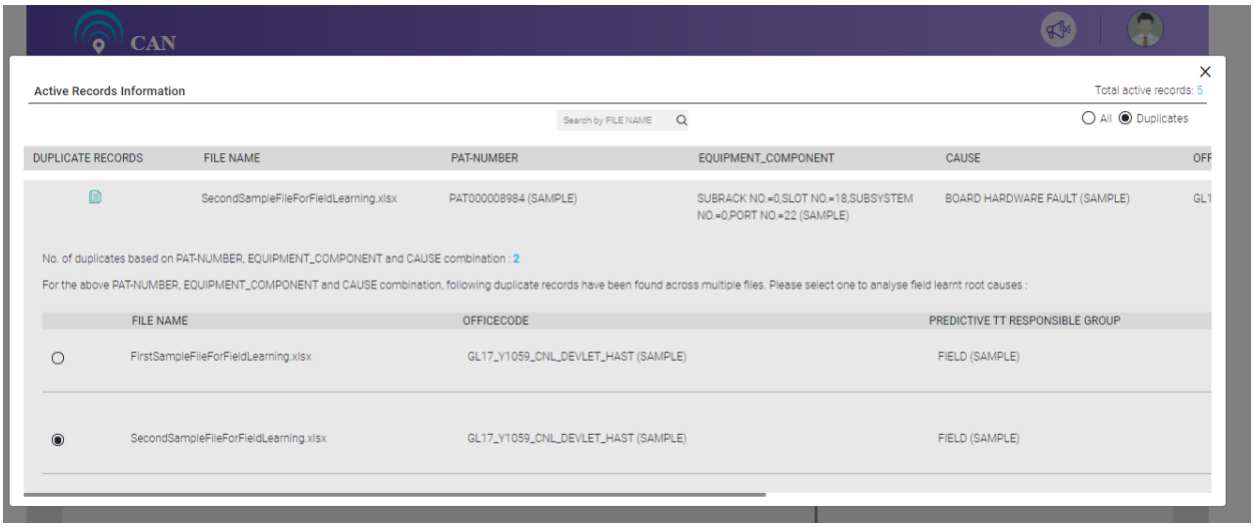


Figure 5.29 - Duplicate records

User can verify the duplicate records across multiple files.

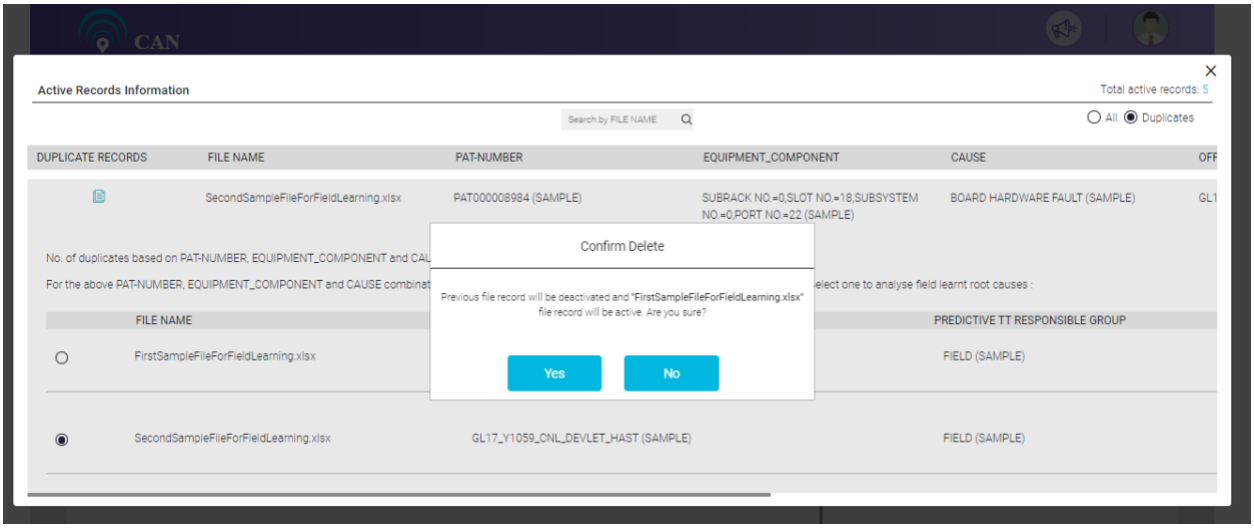


Figure 5.30 - Duplicate Records Verification

The following features are common for the above two tabs (Root Causes based on Technical Analysis and Root Causes based on Field Learning):

- For each file being uploaded, status icon is shown. ✖ icon denotes “All records rejection”, which means there is no parsed record.

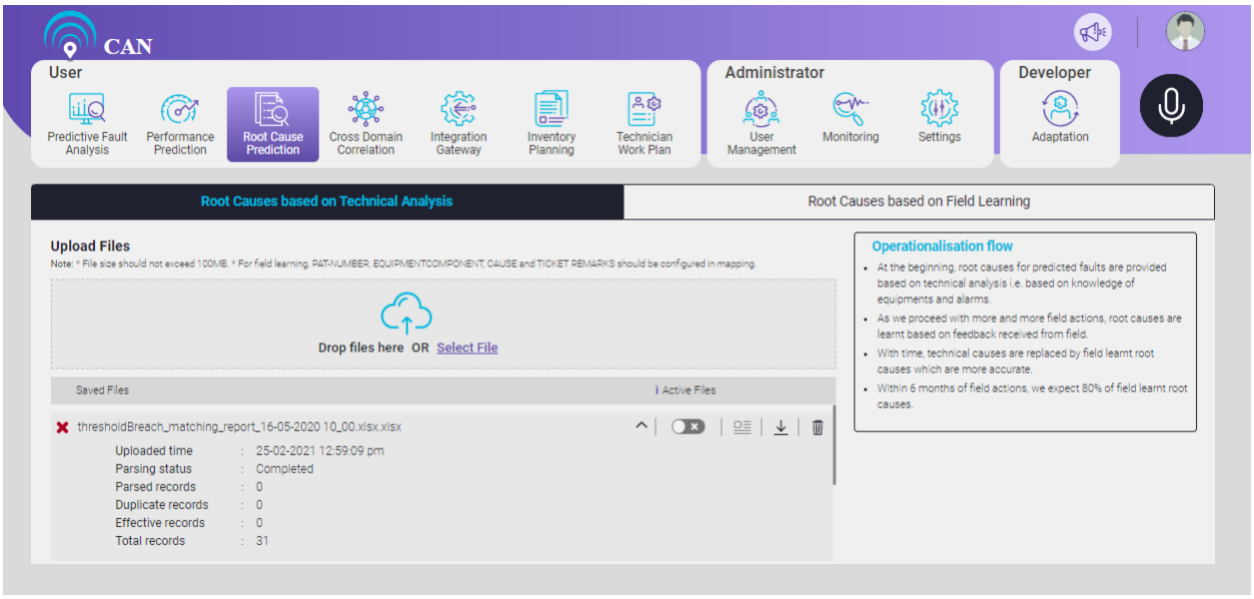


Figure 5.31 - All Records Rejection Details

- Alert icon denotes “Completed with partial error” that means effective records count is not equal to total records count for that particular file.

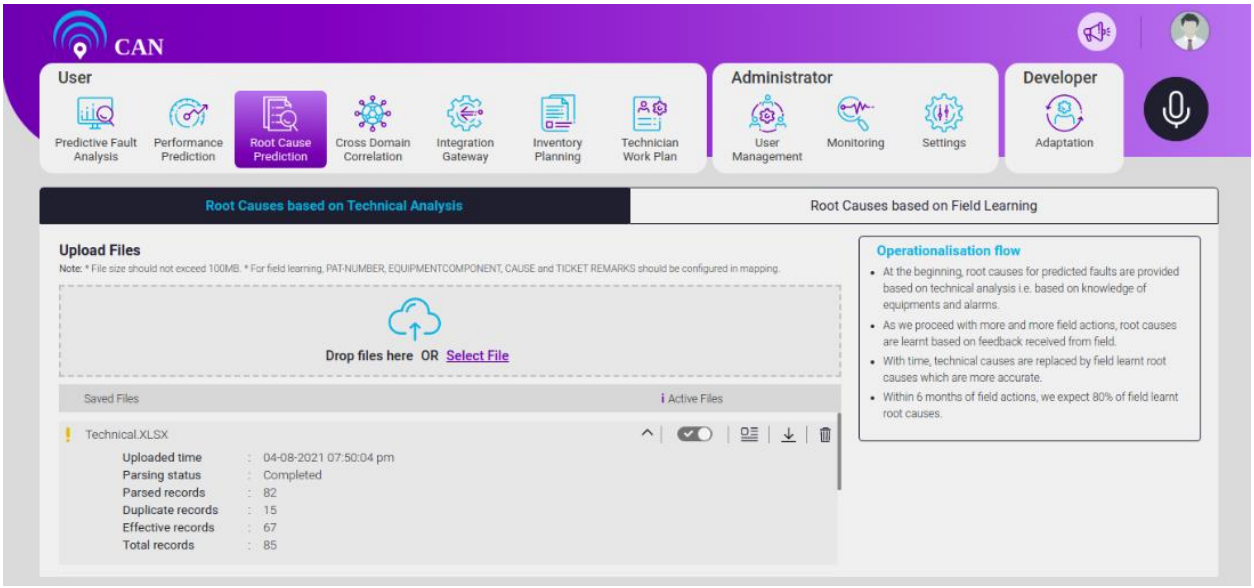


Figure 5.32 - Completed with Partial Error Details

- Green tick denotes 'Completed' that means all the records of the file have been parsed successfully and all of them are effective records.

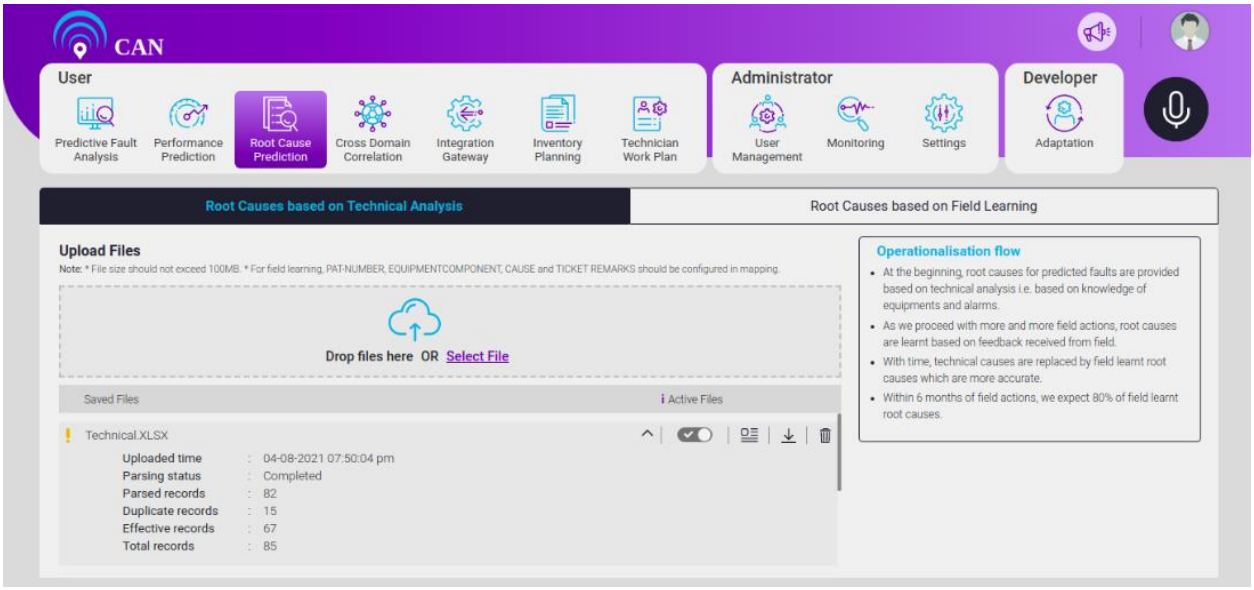


Figure 5.33 - Complete Information

Click the File name or drop down icon to view the the parsed details of each file. User can see the following details: **Uploaded time**, **Parsed status**, **Parsed records**, **Duplicate records, Effective records** and **Total records**.

- To download the required file, click the download icon .

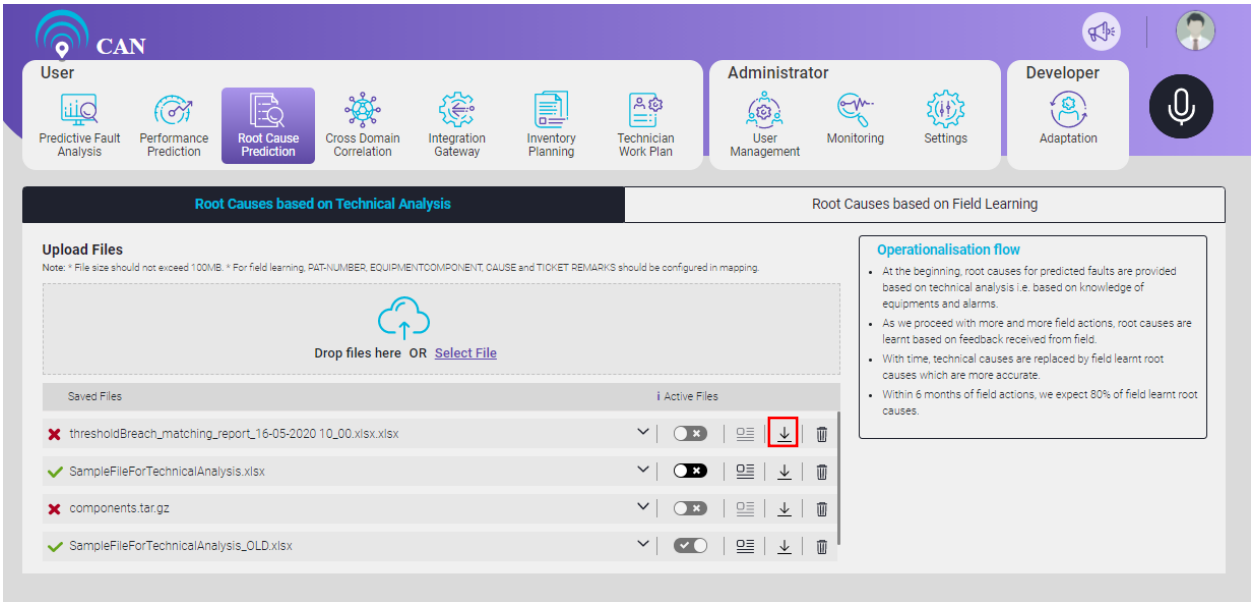


Figure 5.34 - Download Option

- To delete the file, click the delete icon .

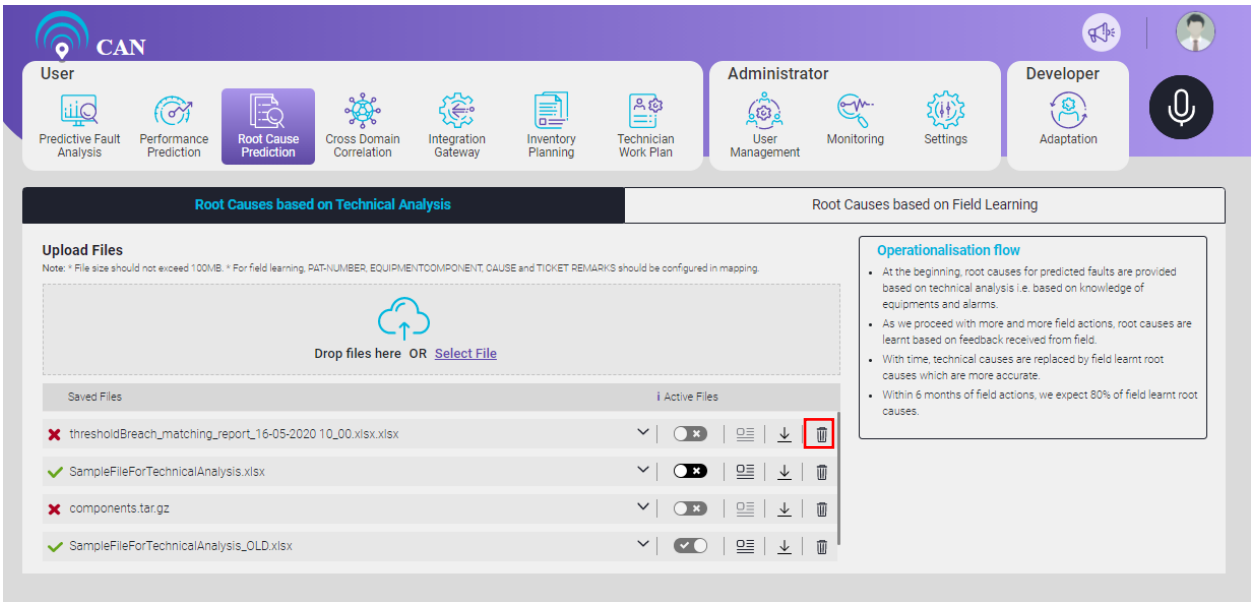


Figure 5.35 - Delete Option

NOTE: For technical analysis if user deletes the active file, the first file containing detailed information icon will automatically become active.

For field learning if user deletes the active file and if no other file is active, the first file containing detailed information icon will automatically become active.

6. CROSS DOMAIN CORRELATION

This screen displays the Cross Domain Correlation details. It depends on the Cluster data.

If there is no data, the screen displays "No cluster data found" along with the link to configure the cross domain parameters on the Advanced Configuration Page.

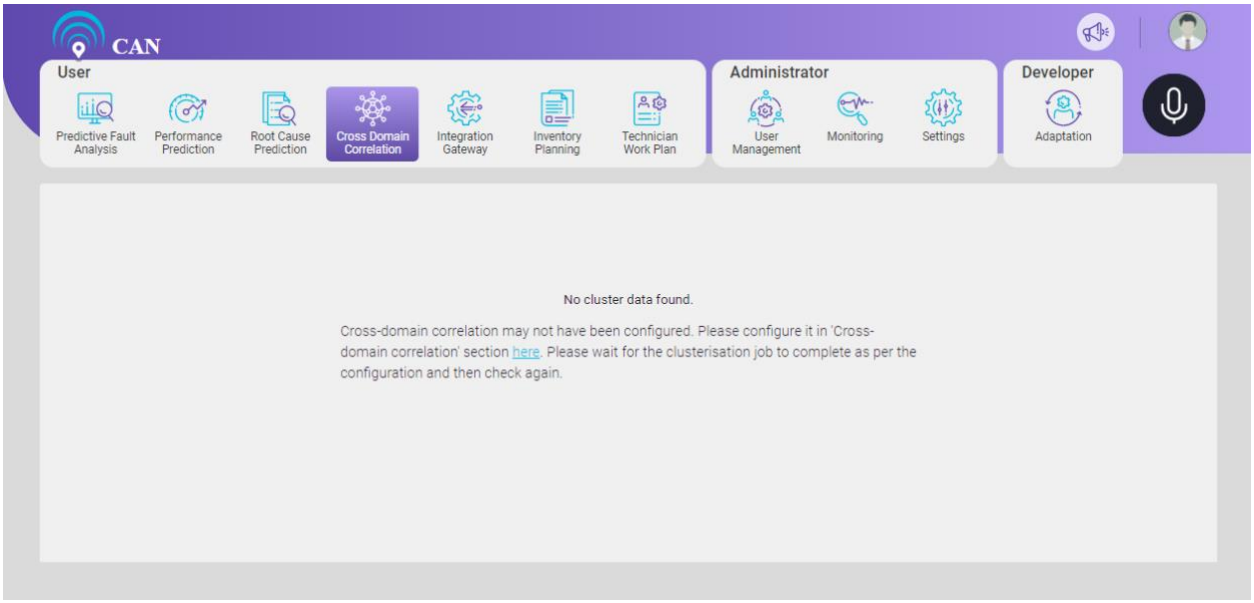


Figure 6.1 - Cross Domain Correlation Screen with No data

When adequate data is available, the page displays all the correlated faults according to their zone. If the number of zones is less than equal to five, then the screen displays all the zones. If zone details are not provided, by default, all clusters/correlated faults with their domain names are listed under a single zone.

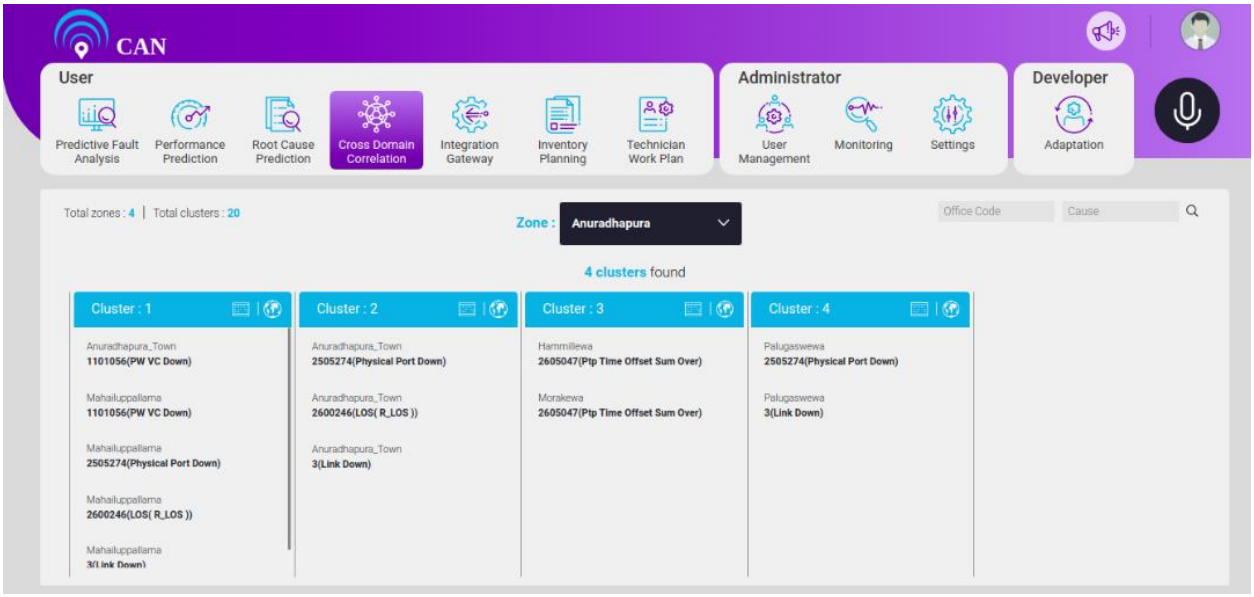


Figure 6.2 - Cross Domain Correlation

In case of more than five zones, the screen displays five zones. To navigate to the sixth and the subsequent zones, click › icon on the right side of the screen.

User can see total No. of zones and total No. of clusters (i.e. Cumulative sum of clusters of all the zones) at top left corner of the screen.

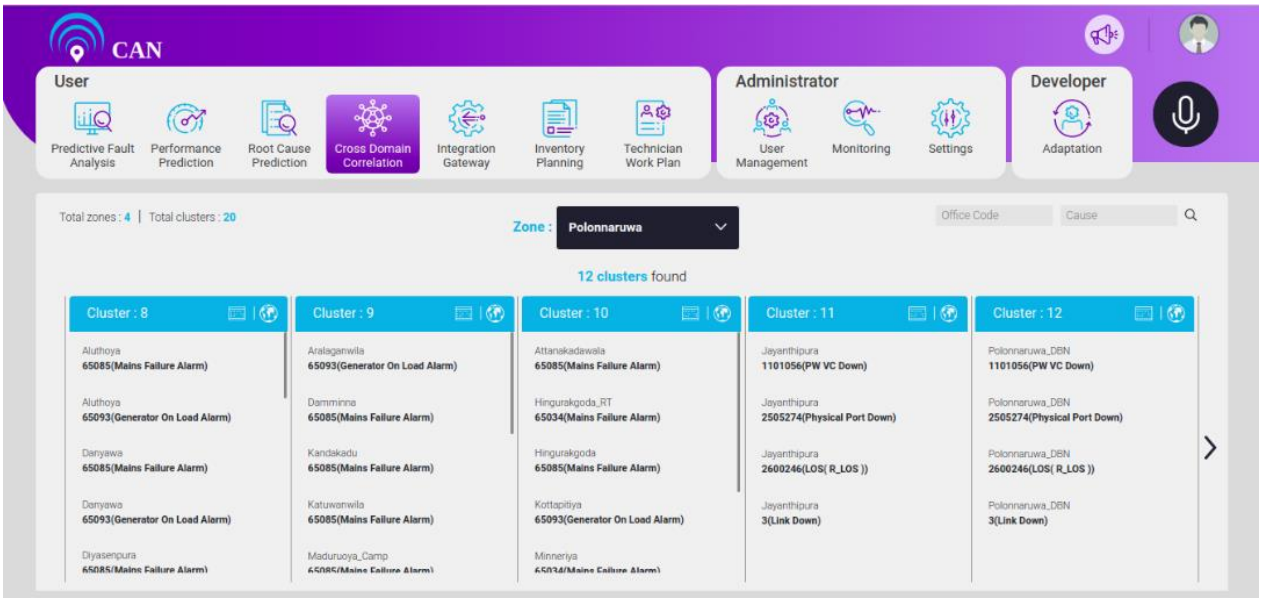


Figure 6.3 - No. of Zones and Clusters

User can select the **Zone** from the drop down to view the clusters under specific zone.

User can use the search text box to search the Office Code Office Code and Cause Cause separately as well as in combination.

User can write the **Office Code** in the Office Code text box with the help of auto-complete suggestions and click the search icon 🔍 to see the Office Code. The screen will display all the clusters with same Office Code.

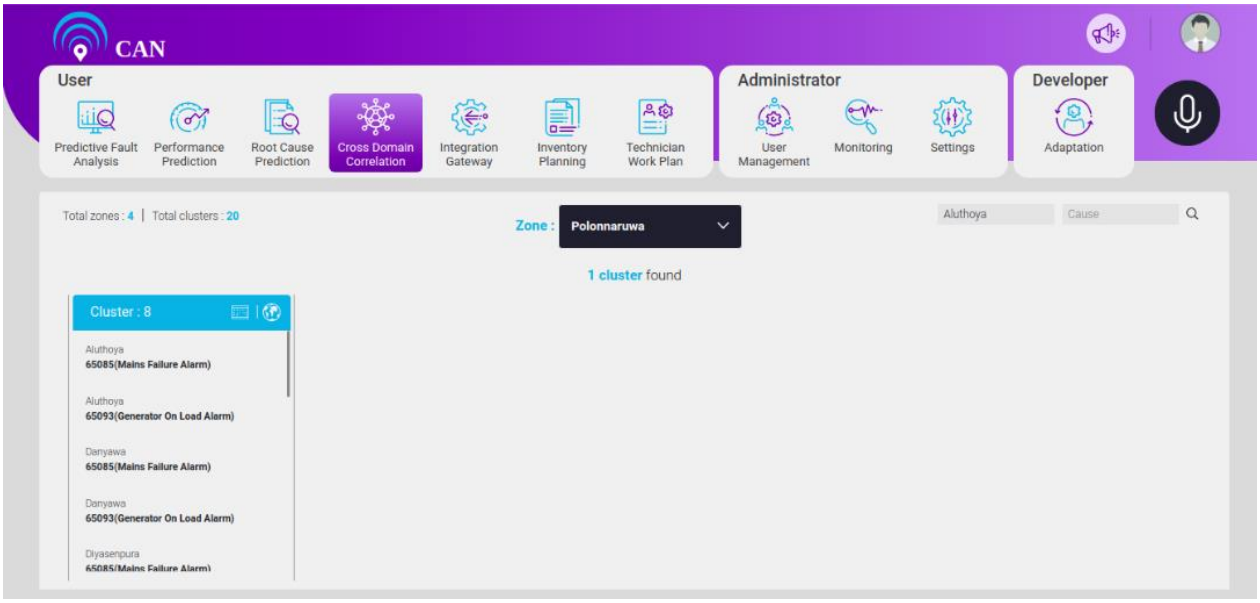


Figure 6.4 - Clusters with same Office Code

User can write the **Cause** in the Cause text box with the help of auto-complete suggestions and click search icon to see the Cause. The screen displays all the clusters with same Cause.

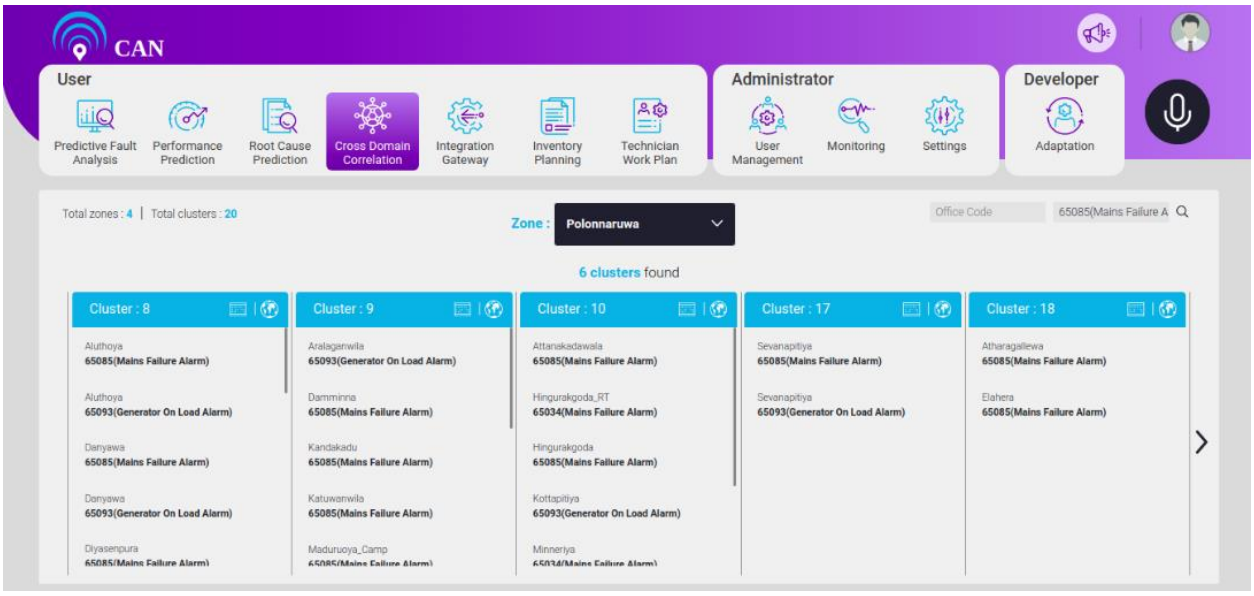


Figure 6.5 - Cluster details with Cause

User can write the Office Code and Cause and click the **search** icon to see the Office Code and its related Cause.

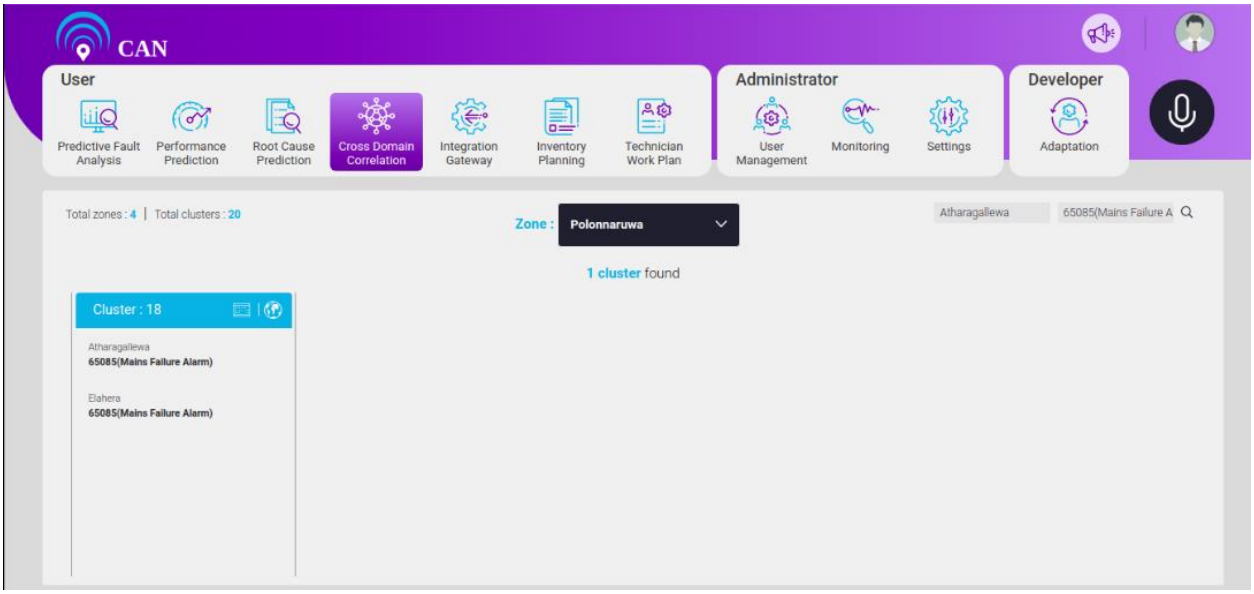


Figure 6.6 - Search Query (Cluster details with Office Code and Cause)

The screen displays the cluster details.

Each cluster has two views:

- Bit pattern view
- Map view

Bit pattern view:

This view displays all the combinations and the corresponding bit pattern for a unique Cluster Zone combination.

To scroll the pattern side wise, click the buttons. The slider decides the speed of the scroll (Fast or slow).

The screen displays the Start date, end date and correlation duration pattern. The duration of the pattern is set by default value of 60 minutes' slot. User cannot change the duration of the correlation pattern.

Note: This screen will display only the filtered cluster. If user hovers on the highlighted 1, date and time corresponding to that 1 will be displayed.

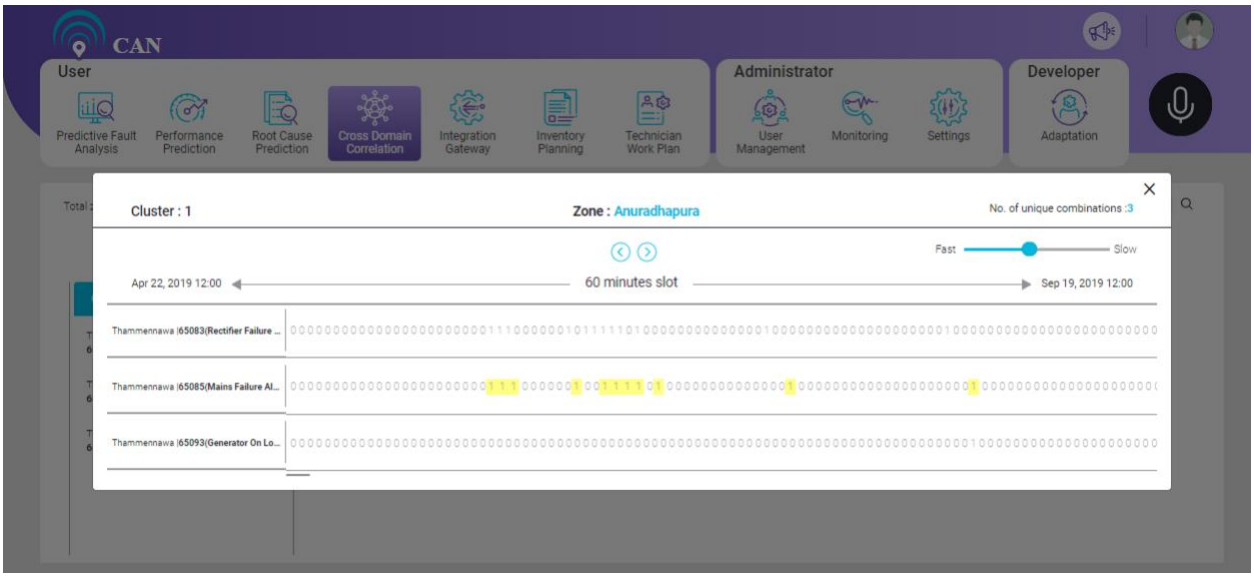


Figure 6.7 - Bit Pattern View

Map view:

This view displays the place where the office code and cause are present on a map. If place details are not present, the screen displays only map but not the pointer.

User can expand the view of the map to the full screen view with icon.

User can increase the size of the map to have a better view using icon and reduce the size of the map using icon.

User can also go to the street view in the map using pegman icon .

The four type of representations are there as per the four domains:

- Others
- Transmission Node
- Access Node
- IP Node

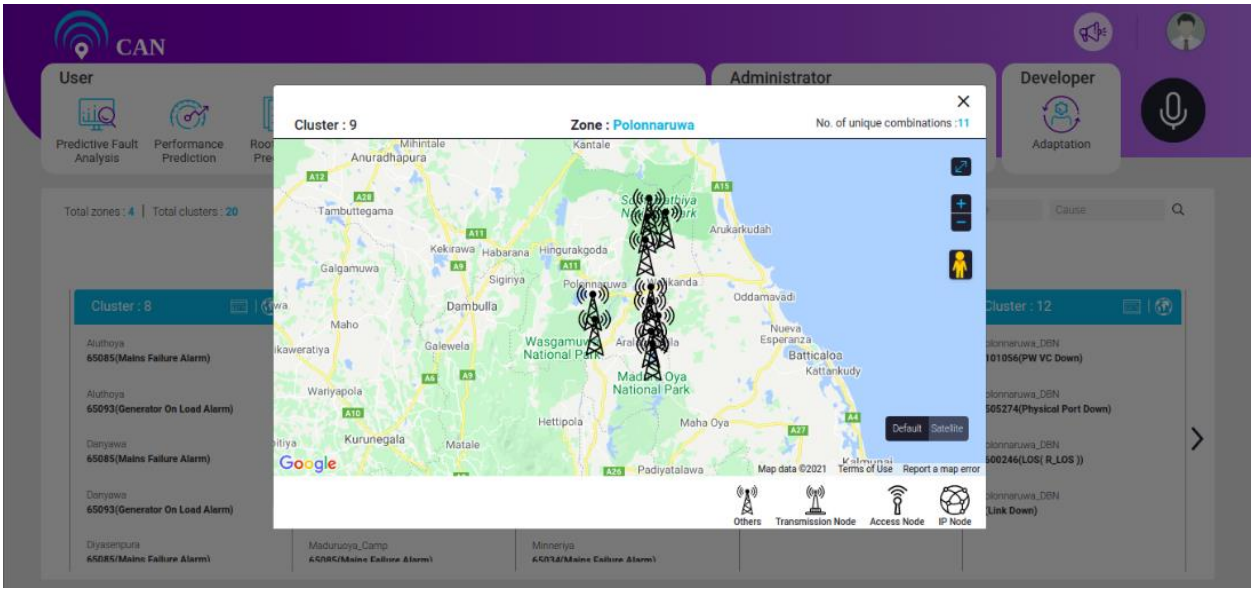


Figure 6.8 - Map View with Pointer

To see the details of the particular point, click the pointers.

When you will click the pointers a pop-up will appear on the screen.

The pop-up on the screen displays the place, Office Code, Cause and Equipment Component details.

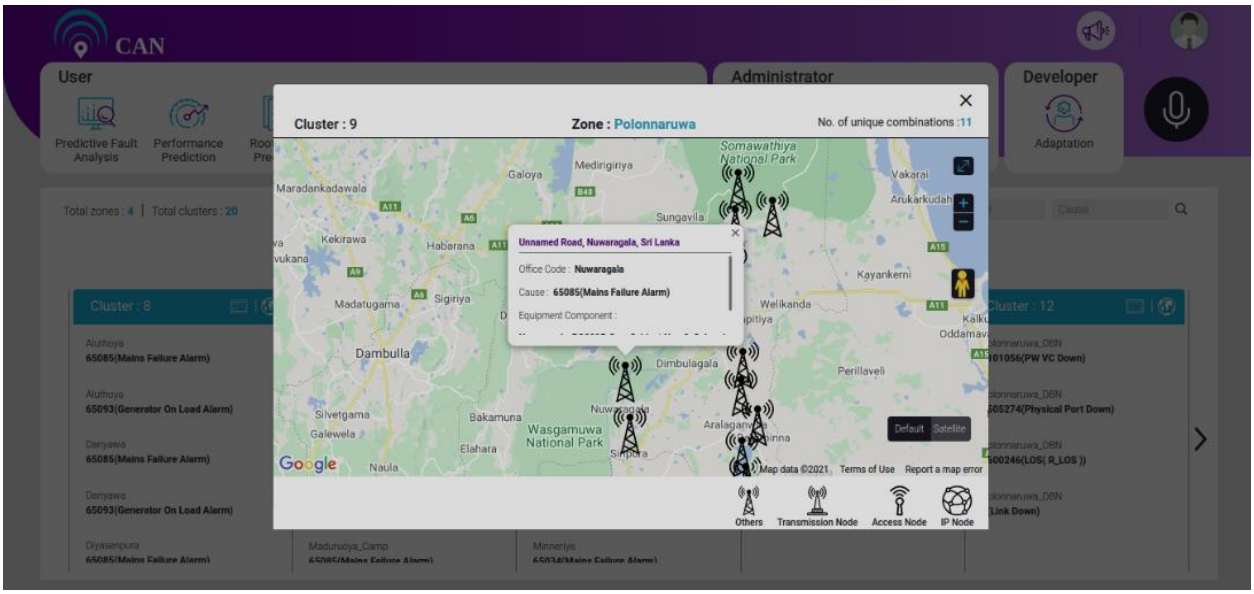


Figure 6.9 - Map View with Details

To close this pop-up, click the **Close** button ✕ available at the top right corner of the pop-up.

Note: Zone detail, Cluster Id and No. of combinations present for this particular cluster is shown above.

7. INTEGRATION GATEWAY

User can access the Integration Gateway screen from the dashboard home. Integration Gateway screen have four tabs:

- BMC Remedy
- ServiceNow
- Weather Integration
- Splunk

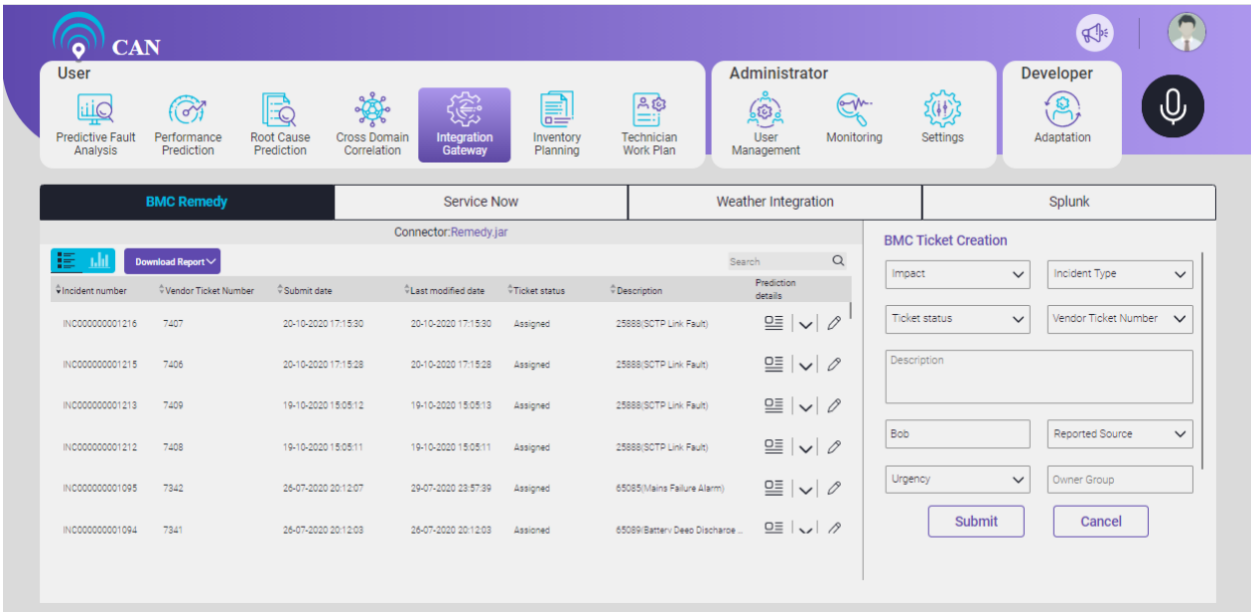


Figure 7.1 - BMC Remedy Screen

BMC Remedy

BMC remedy is a ticketing tool. It has many features. It provides a way to track your ticket Request (Configuration), Incident (Severity issues), Problem management (Code changes, tool fault), Change management (Some planned deployment) etc. Using BMC remedy, you can raise your concern and it provides a way to get it resolved within time by setting the priority. Every time when there is an update on your ticket, you will get notified through mail.

To Create New BMC Ticket

1. Click the **Vendor Ticket Number** on the drop down menu. When you click the drop down, a popup containing all the predictions will appear on the screen.
2. Select the required prediction for single ticket booking from the check box or select the multiple predictions for bulk ticket booking. You can use the search option to search for the particular ticket. Click the **Confirm** button to submit the ticket. Popup will close.

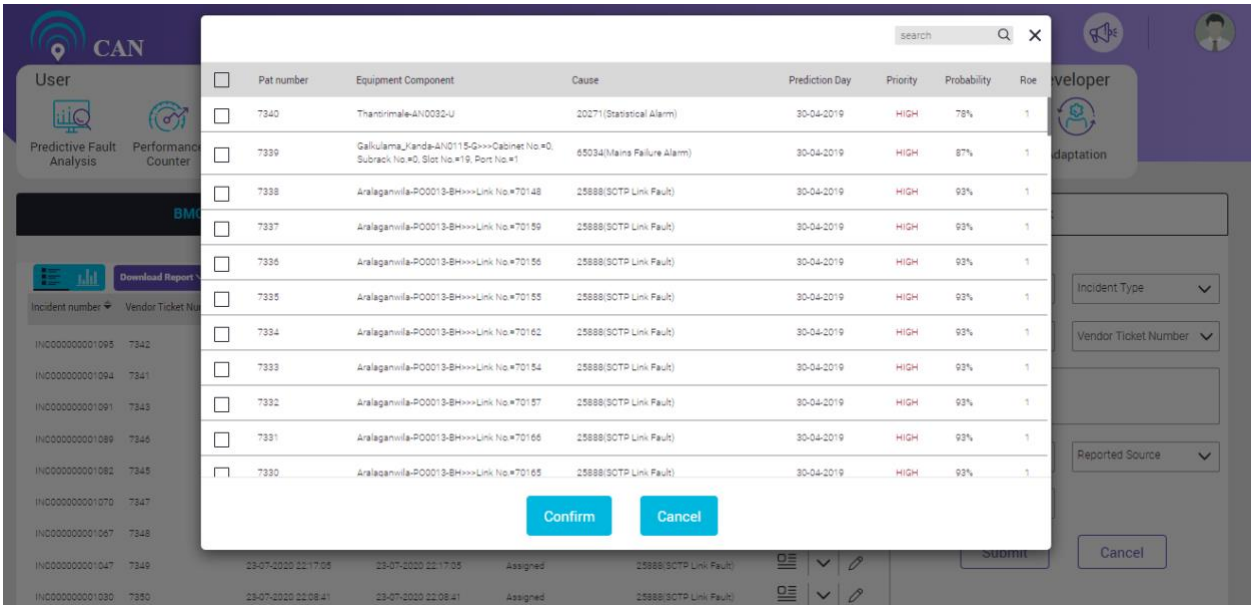


Figure 7.2 - BMC Single Ticket Creation

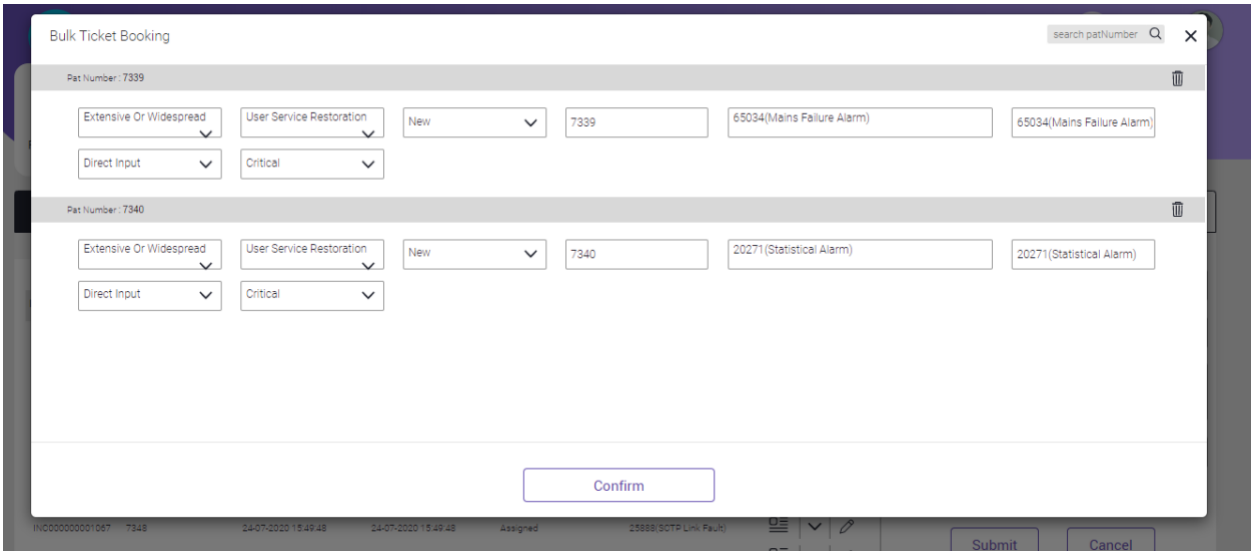


Figure 7.3 - BMC Bulk Ticket Booking

3. You will be directed to BMC ticket screen; the values will be auto populated in the BMC screen. Verify the values, if the values are not correct **edit** them and write the correct values.
4. After updating the values, click the **Confirm** button.
5. All the mandatory fields such as Impact, Incident Type, Ticket Status, Vendor Ticket Number, Description, Login ID and Reported Source will get auto filled.
6. Click the **Submit** button to create the New BMC ticket.

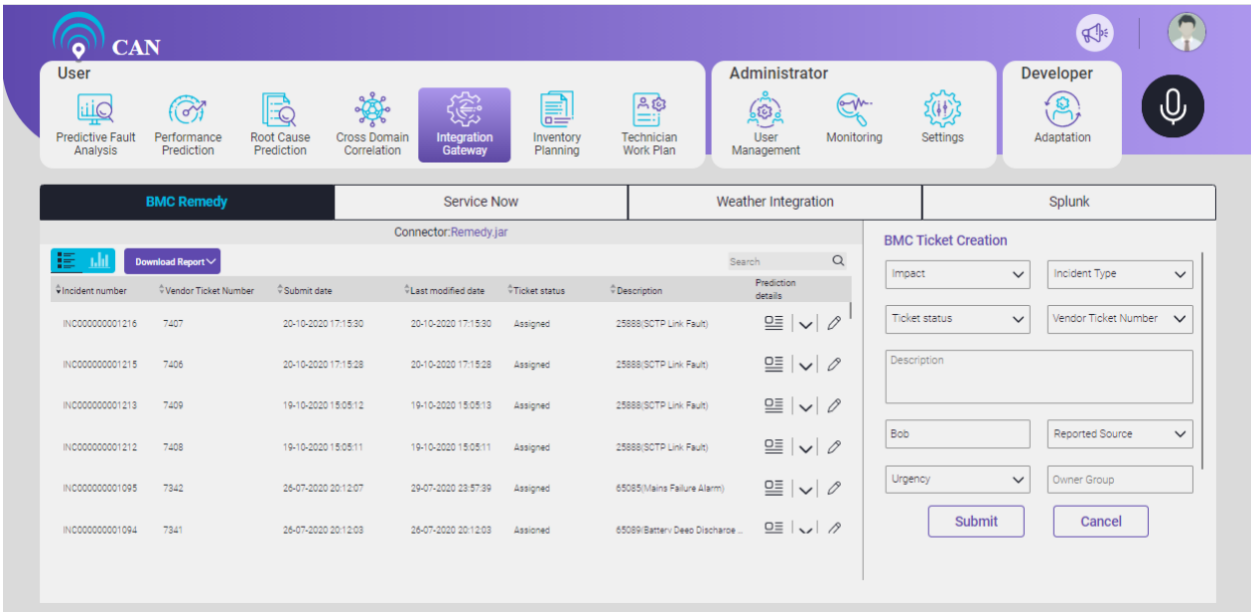


Figure 7.4 - BMC Ticket Creation Screen

To Update/Edit the Existing BMC Ticket

1. Click the edit icon and edit the respective field. User can make the changes manually or select from the existing drop down menus.

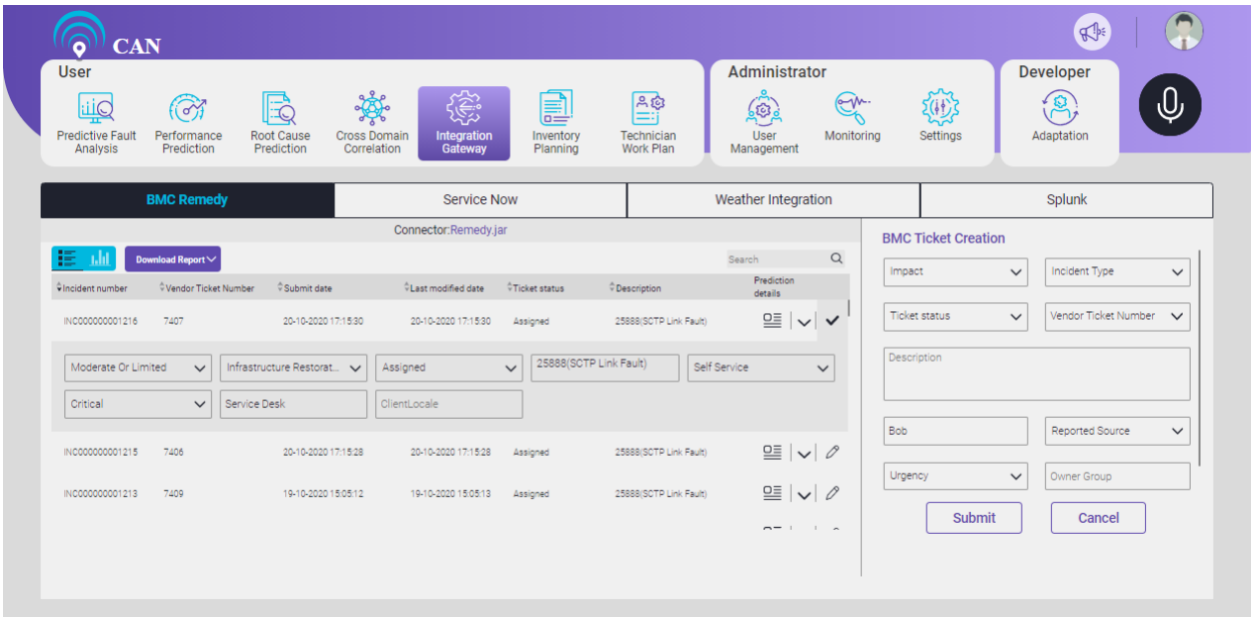


Figure 7.5 - BMC Ticket Update Screen

2. After edit or update, click the save icon to save the changes.
3. User can click the prediction details to see the predicted fault for the particular Incident number or Vendor Ticket Number.

4. User can click the view option to view the details of the existing tickets.
5. The screen also has the sorting and search option to sort and search the prediction tickets along with the detailed view.

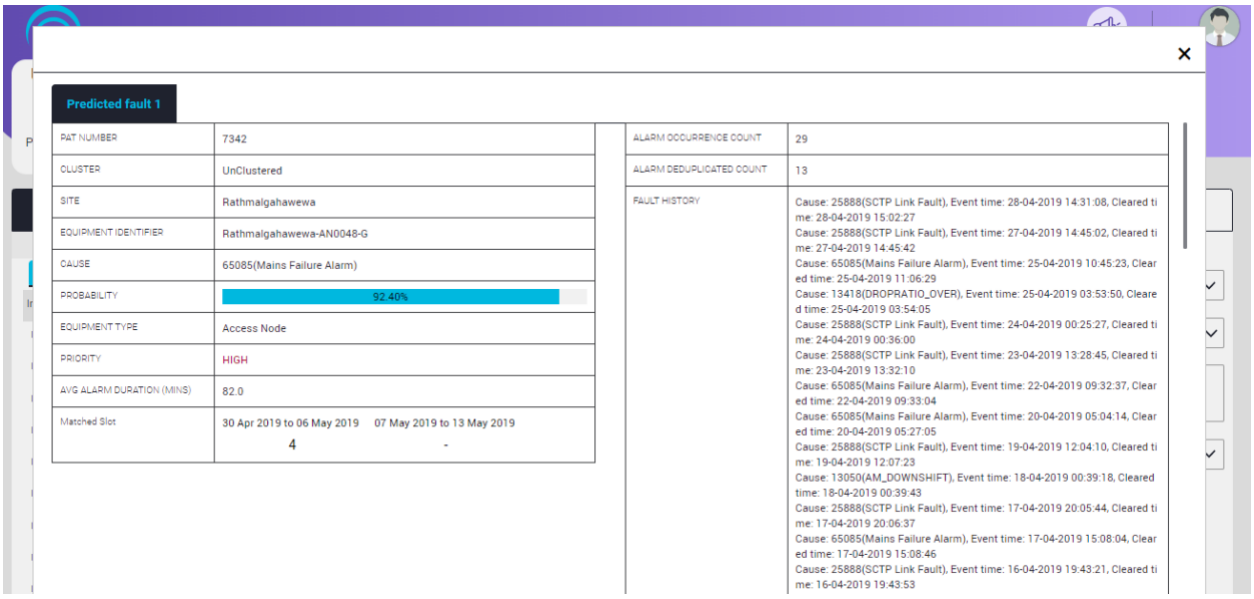


Figure 7.6 - BMC Remedy Prediction Fault Details

BMC Remedy screen shows the incidents or tickets in two views:

1. Tabular View

   By default the tabular icon is selected on the screen.

   The Tabular view shows the below attributes of the BMC Remedy:

   Incident number, Vendor Ticket Number, Submit Date, Last Modified Date, Ticket Status, Description, Prediction Details, Description, Request ID, Impact, Incident Type, Reported Source, Urgency.

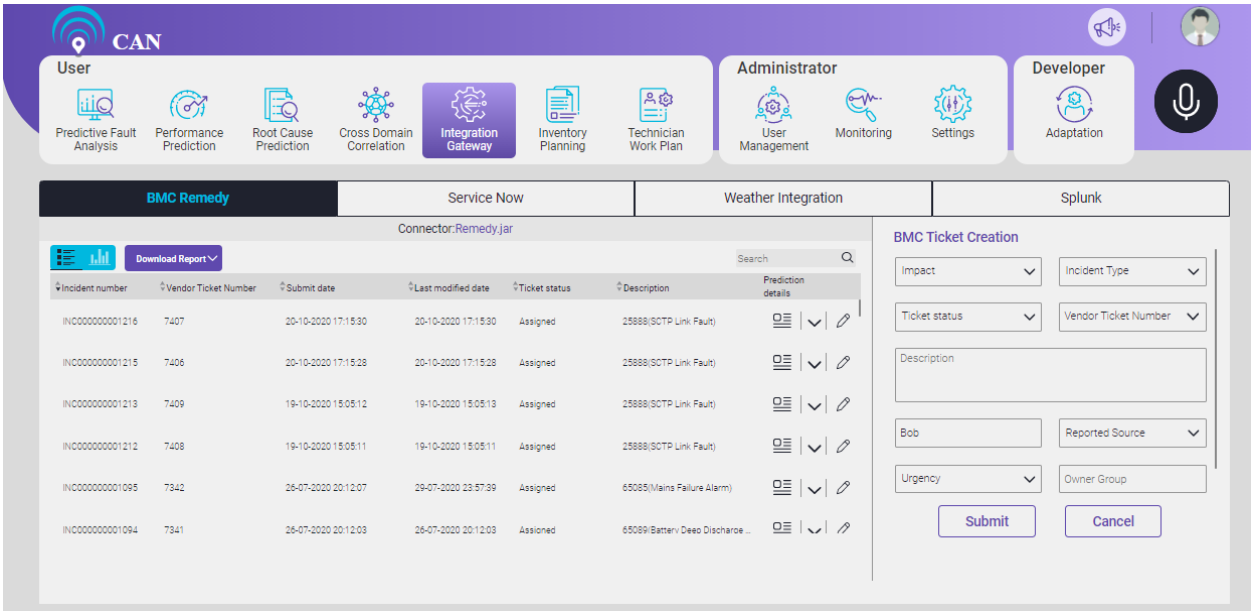


Figure 7.7 - BMC Remedy Tabular View

2. Graph View

Click the graph icon to view the graph view of the BMC remedy tickets.

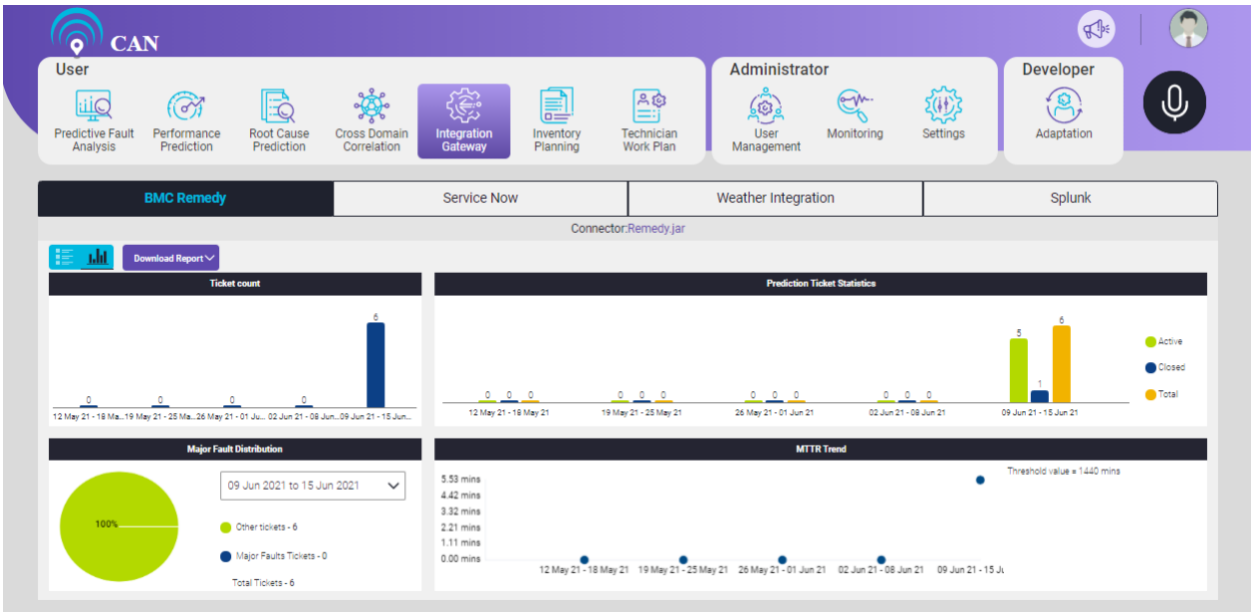


Figure 7.8 - BMC Remedy Graphical View

The graph view gives the detailed information of the Ticket Count, Prediction Ticket Statistics, Major Fault Distribution and MTTR Trend.

Ticket Count - The graph shows the total number of ticket created in the particular week.

Prediction Ticket Statistics - Clustered Statistics shows the details of the total number of tickets, active tickets and closed tickets for the particular weeks. Tickets quantities in this view have three colors to differentiate between them.

- Green color shows the Active tickets.
- Blue color shows the Closed tickets.
- Orange color shows the Total tickets.

Major Fault Distribution - Major Fault Distribution shows the details of Major Fault Tickets and other Tickets out of Total Tickets for the particular week.

Scatter Chart - Scatter chart helps the customer to know the time they take to close the tickets in the particular week. Threshold value – Mean threshold number of days' customer requires to close the tickets of a particular week.

Download Report

User can download the report of the Active tickets and Closed tickets for a particular week. To download the report, select the appropriate check box (Active tickets or Closed tickets) and select the particular week under Download Report drop down menu.

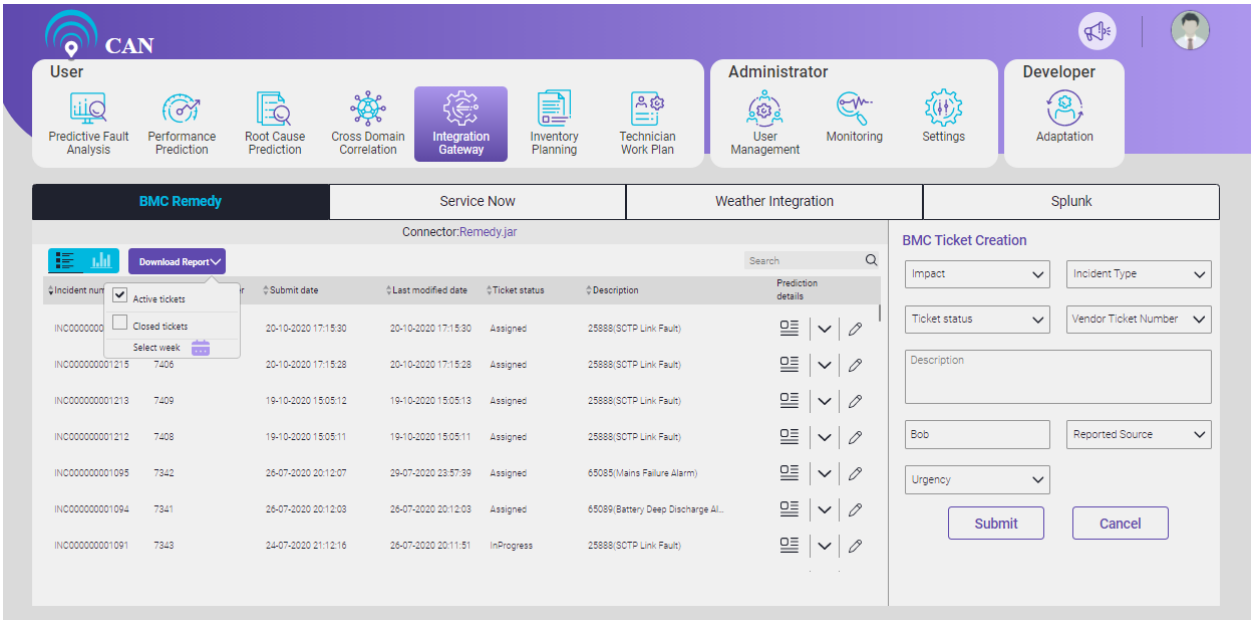


Figure 7.9 - BMC Remedy Download Reports

ServiceNow Integration

ServiceNow is an enterprise entity that provides solutions for IT asset management and other digitalization drives that happens in the IT ecosystem. One of the key product of ServiceNow includes the IT Service Management Tool that helps the telecom, IT customers to log in fault incidents, track and close them through the digital work flows.

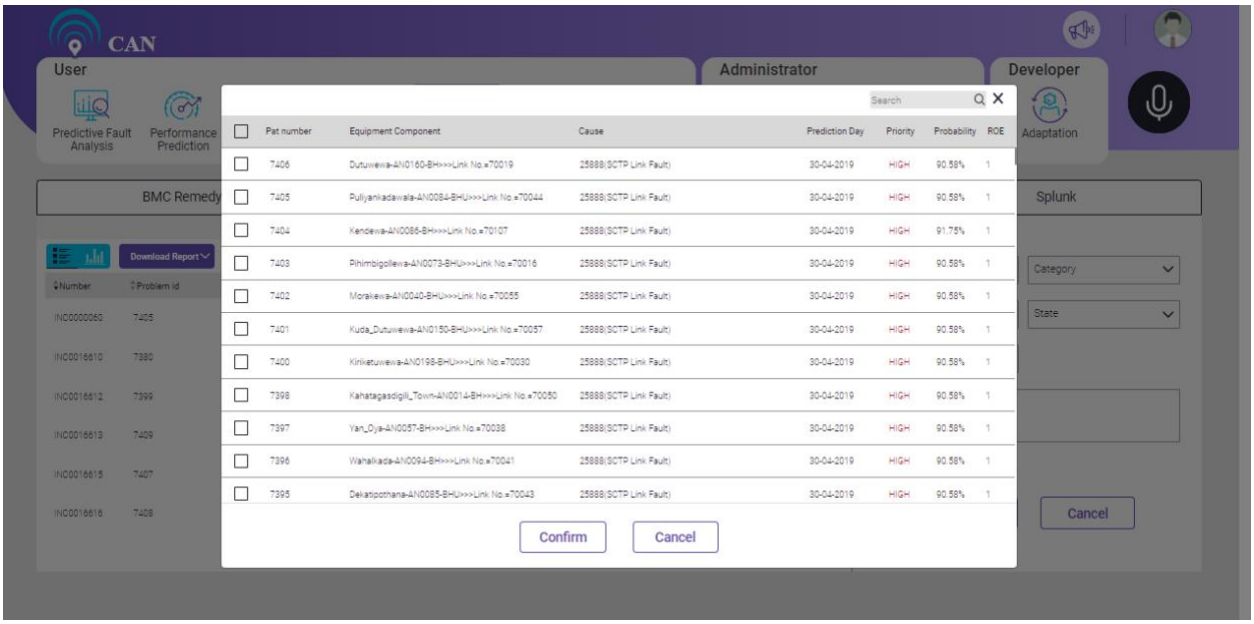
The main objective of the ServiceNow integration is to optimize the customer operations. It had been noted that there are multiple customers of CAN using ServiceNow ITSM tools and have raised the concern of integrating the software for seamlessness. This integration will bring in the seamlessness among the operation of both software mutually complimenting the cause of enhancing the customer operations and performance.

ServiceNow proactively monitors the health of your networks and services to prevent downtime. It detects:

- Network issues - Identify network issues and assess impacts across multiple network monitoring systems.
- Manages service health - Improve agent and customer experiences. Proactively notify customers of service events and empower agents with real-time service status using operational intelligence and machine learning.
- Identify the root cause - Use the power of AI to turn a tidal wave of events into a trickle of actionable alerts. Cut through the noise to rapidly identify and remediate the root cause of service issues.

To Create New ServiceNow Ticket

1. Click the Problem id Number on the drop down menu.
2. When you click the drop down, a popup containing all the predictions will display on the screen.



3. Select the required prediction (PAT Number) for single ticket booking from the check box or select the multiple predictions for bulk ticket booking.
4. For single ticket booking, select one **Pat number**, click the **Confirm** button to submit the ticket.

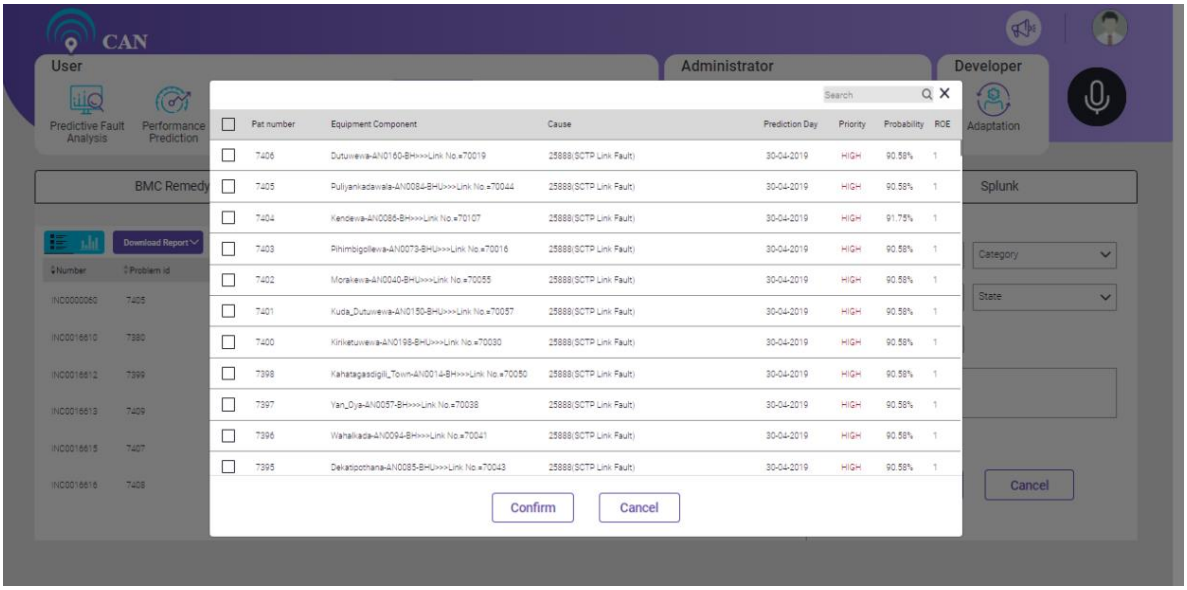


Figure 7.10 - ServiceNow Single Ticket Creation

5. For multiple tickets, select multiple tickets (Pat Numbers). You can use the search option to search for the particular tickets (Pat numbers).
6. Click the **Confirm** button. When you click the **Confirm** button, **Bulk Ticket Creation** screen will open; the values will be auto populated in the screen. Verify the values, if the values are not correct **edit** them and select the correct values from the drop down.

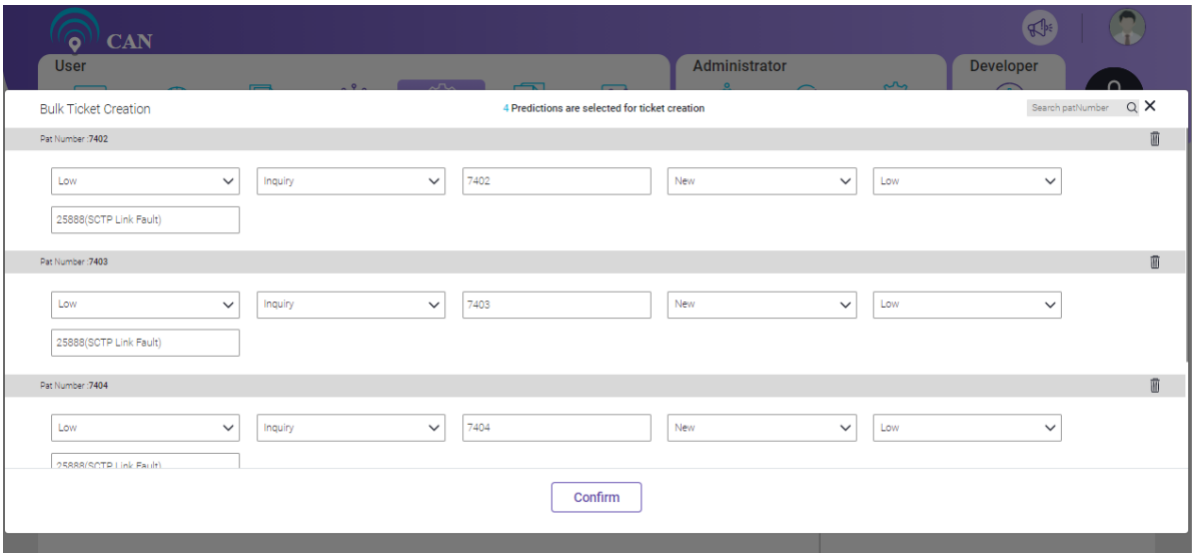


Figure 7.11 - ServiceNow Bulk Ticket Creation

7. After updating the values, click the **Confirm** button. The Pop up Screen will close.
8. You will be directed to ServiceNow ticket screen; the values will be auto populated in the ServiceNow screen. Verify the values, if the values are not correct **edit** them and write the correct values.
9. Click the **Submit** button to Create the New ServiceNow Ticket.

To Update/Edit the Existing ServiceNow Ticket

1. Click the edit icon and edit the respective field. User can make the changes manually or choose from the existing drop down menus.

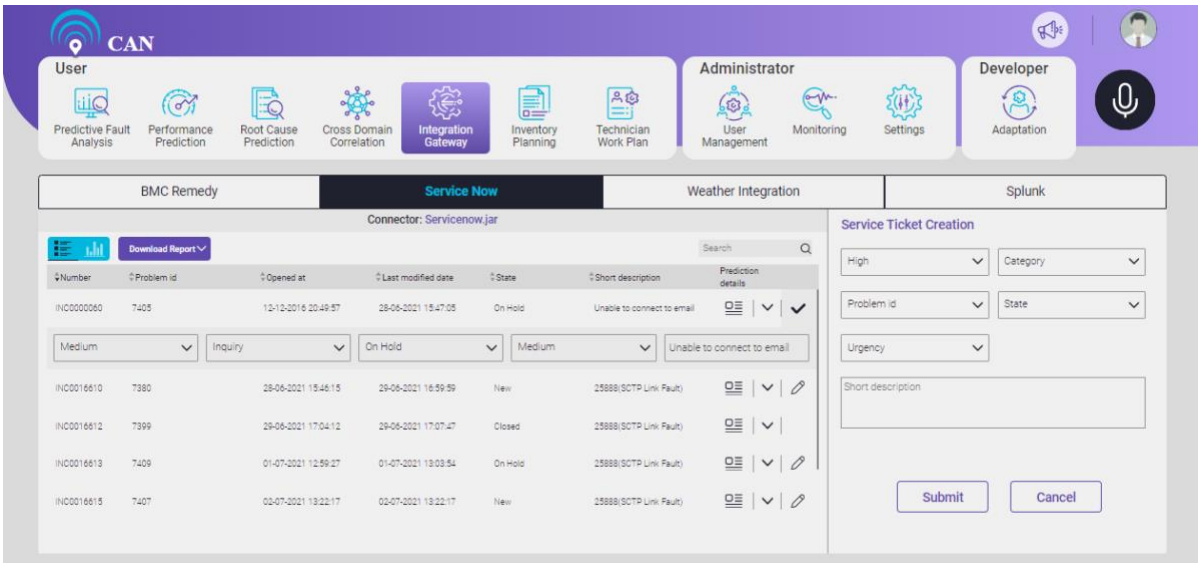


Figure 7.12 - ServiceNow Ticket Update Screen

2. After edit or update, click the save icon to save the changes.
3. User can click the prediction details to see the predicted fault for the particular Incident number or Problem id.
4. User can click the view option to view the details of the existing tickets.
5. The screen also has the sorting and search option to sort and search the prediction tickets along with the detailed view.

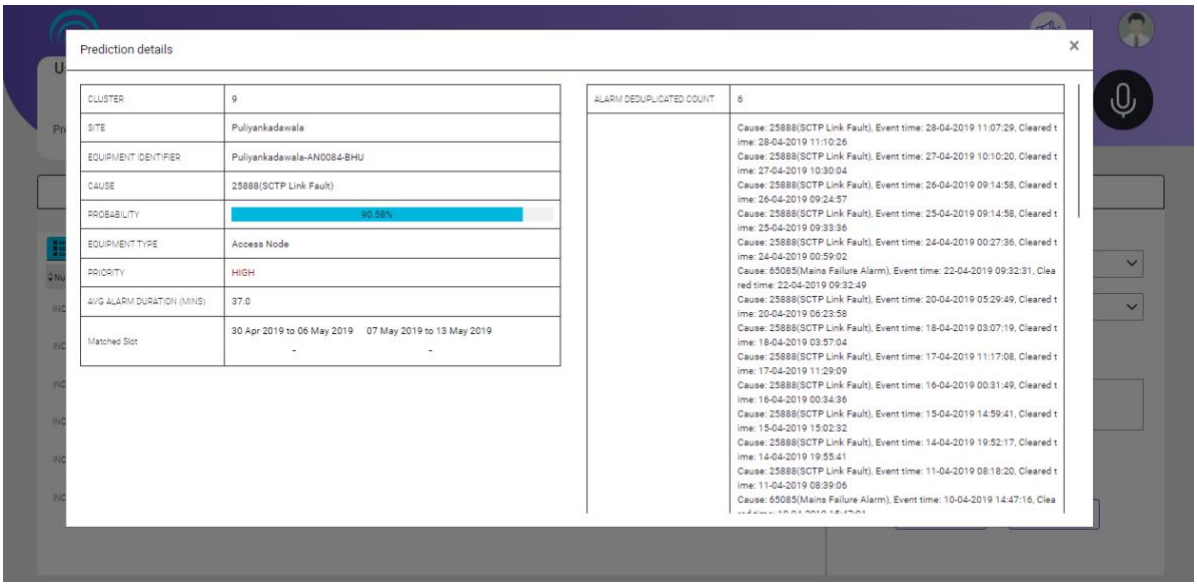


Figure 7.13 - ServiceNow Prediction Fault Details

ServiceNow screen shows the incidents or tickets in two views:

1. Tabular View

   By default the tabular icon is selected on the screen.

   The Tabular view shows the below attributes of the ServiceNow:

   Incident Number, Problem id, Opened at, Last modified date, State, Short description, Prediction Details.

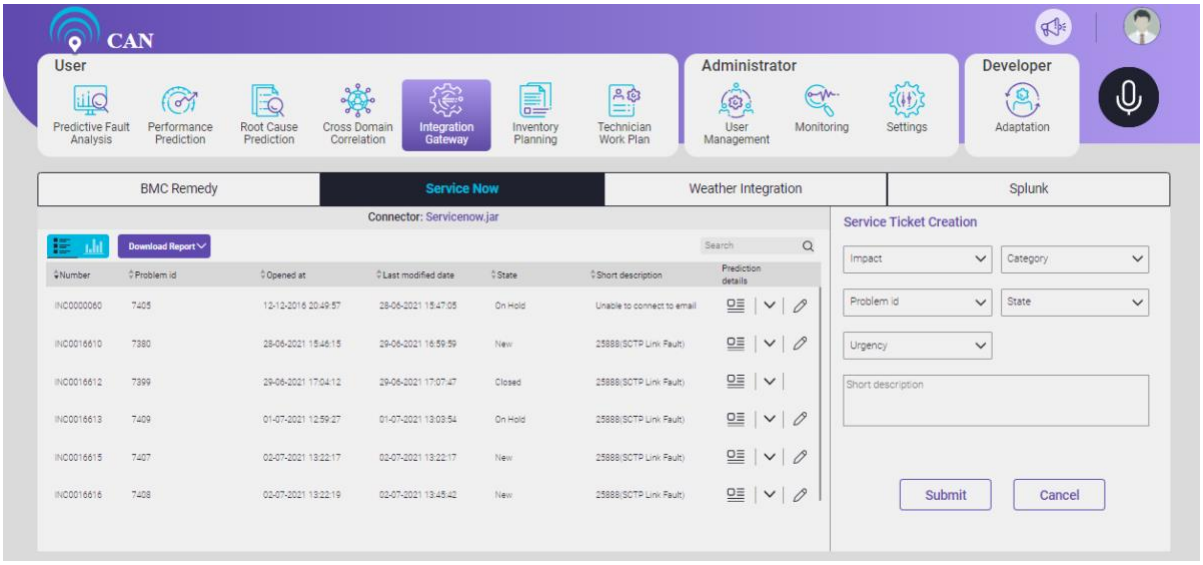


Figure 7.14 - ServiceNow Tabular View

2. Graph View

   Click the graph icon to view the graph view of the ServiceNow tickets.

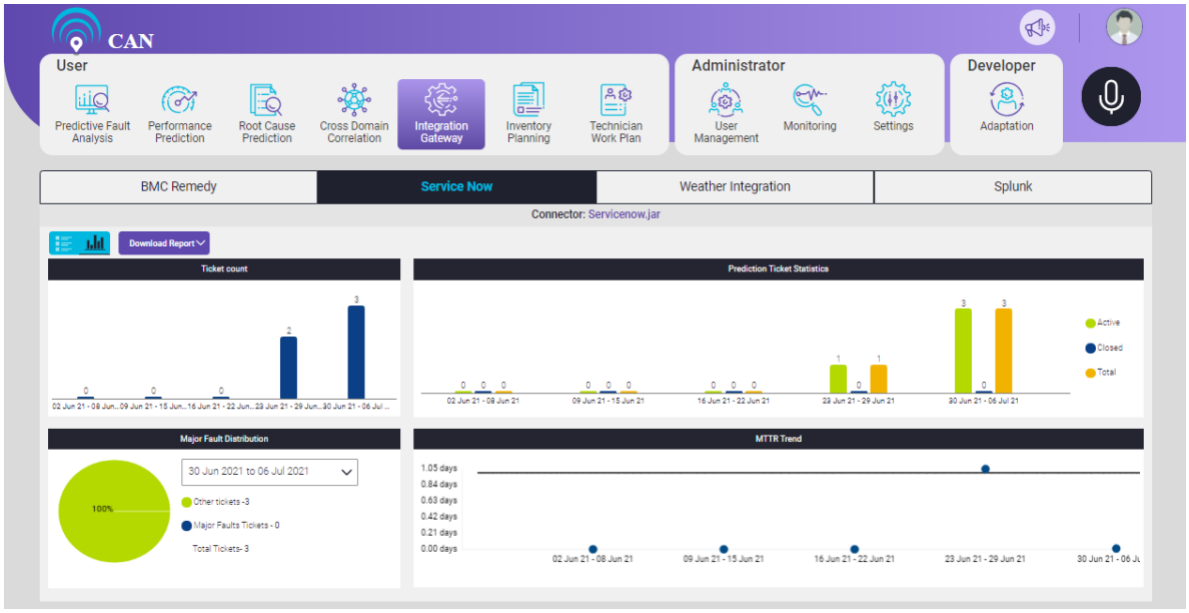


Figure 7.15 - ServiceNow Graphical View

The graph view gives the detailed information of the Ticket Count, Prediction Ticket Statistics, Major Fault Distribution and MTTR Trend.

Ticket Count - The graph shows the total number of ticket created in the particular week.

Prediction Ticket Statistics - Clustered Statistics shows the details of the total number of tickets, active tickets and closed tickets for the particular weeks. Tickets quantities in this view have three colors to differentiate between them.

- Green color shows the Active tickets.
- Blue color shows the Closed tickets.
- Orange color shows the Total tickets.

Major Fault Distribution - Major Fault Distribution shows the details of Major Fault Tickets and other Tickets out of Total Tickets for the particular week.

Scatter Chart - Scatter chart helps the customer to know the time they take to close the tickets in the particular week. Threshold value – Mean threshold number of days' customer requires to close the tickets of a particular week.

Download Report

User can download the report of the Active tickets and Closed tickets for a particular week. To download the report, select the appropriate check box (Active tickets or Closed tickets) and select the particular week under **Download Report** drop down menu.

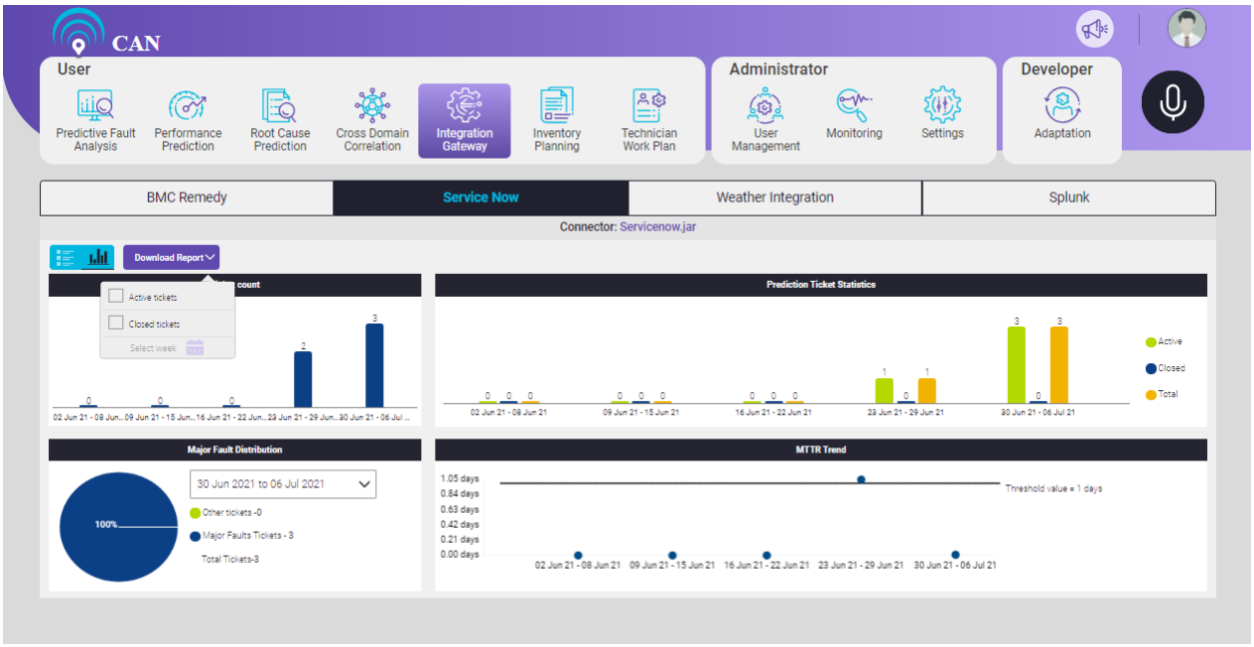


Figure 7.16 - ServiceNow Download Reports

Weather Integration

By default, the weather integration screen displays the weather forecast of a particular zone for next 5 days with the information of Forecast Start Time, Forecast End Time and Weather Alert.

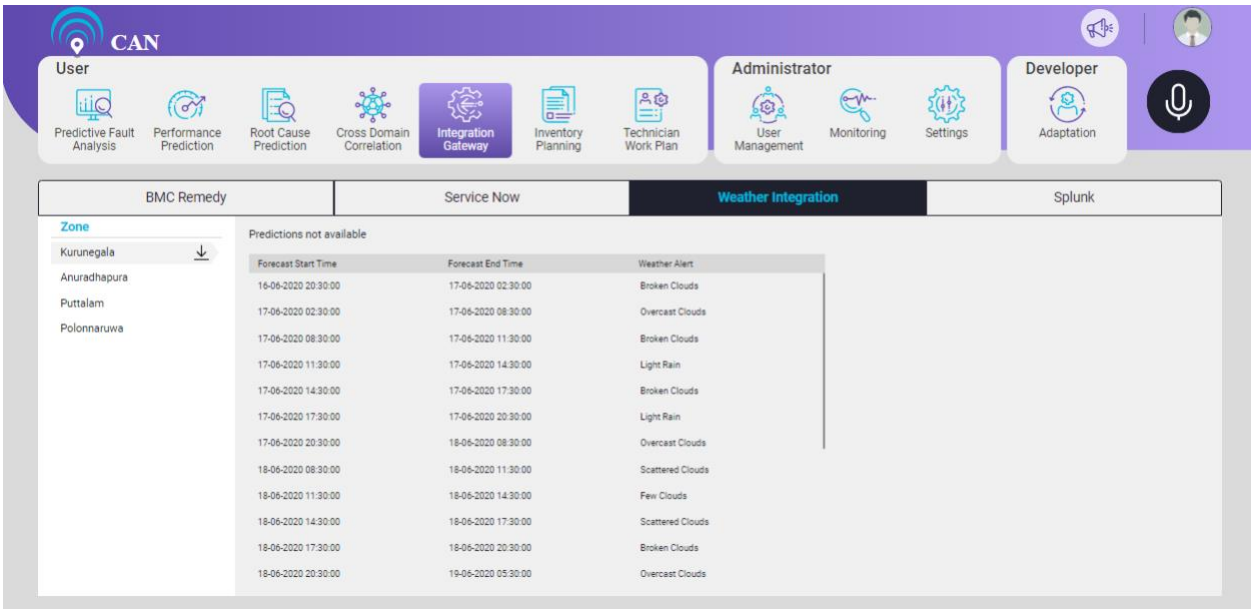


Figure 7.17 - Weather Forecast Information

The screen also displays the total prediction of the selected zone for latest 3 days. There are two views to show the prediction:

1. Tabular View
2. Map View

User can select the particular day to view the prediction for the particular day.

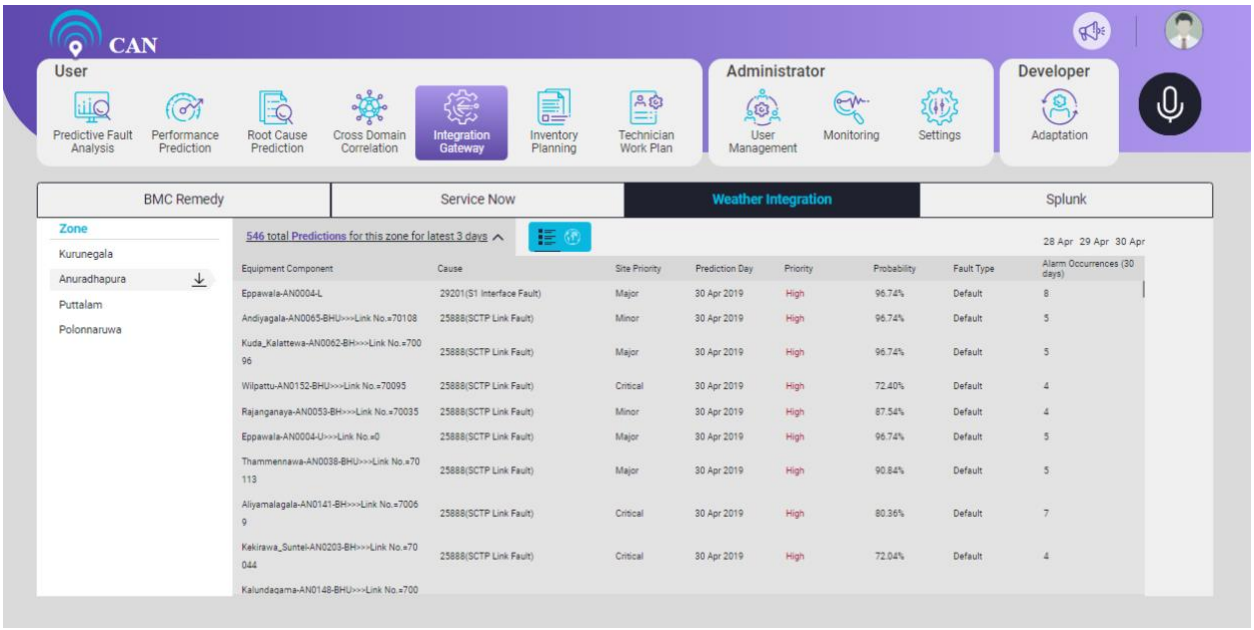


Figure 7.18 - Weather Prediction Tabular View

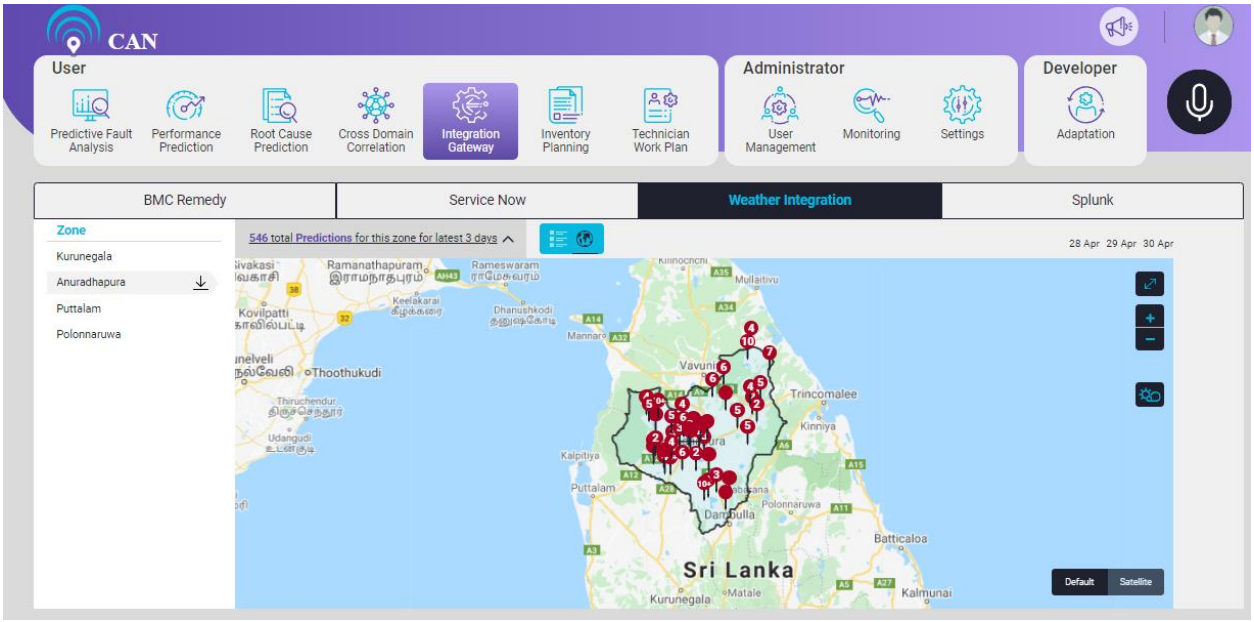
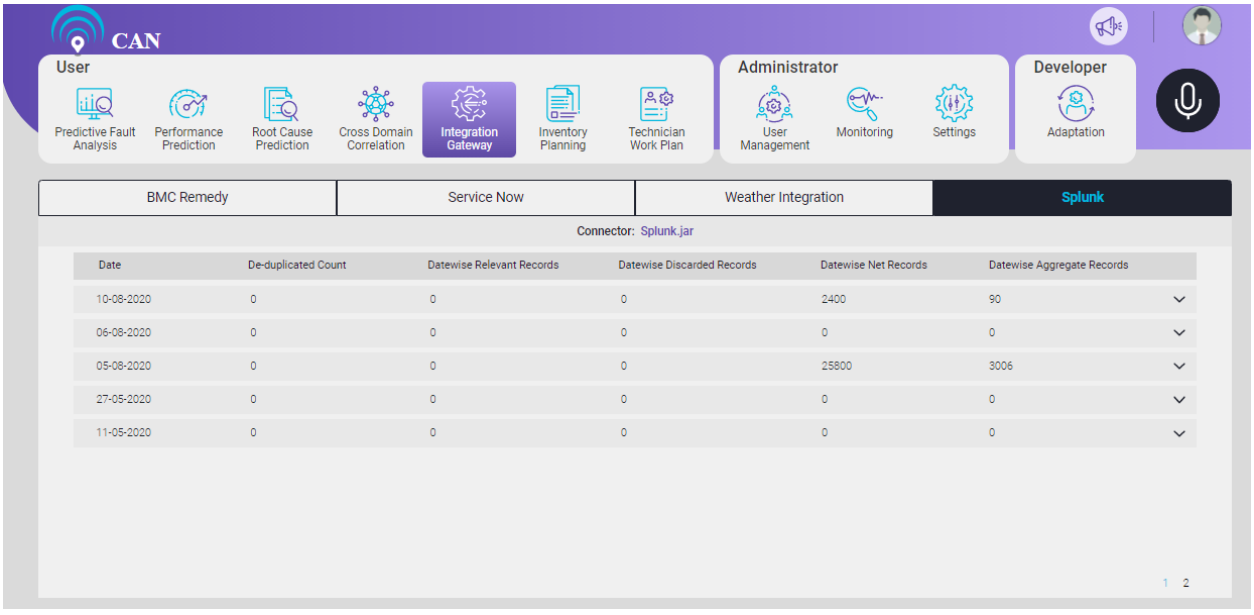


Figure 7.19 - Weather Prediction Map View

Splunk

By default, the Splunk screen shows the data.

This screen displays the Date, De-Duplicated Count, Datewise Relevant Records, Datewise Discarded Records, Datewise Net Records and Datewise Aggregated Records on a daily basis.



Date	De-duplicated Count	Datewise Relevant Records	Datewise Discarded Records	Datewise Net Records	Datewise Aggregate Records
10-08-2020	0	0	0	2400	90
06-08-2020	0	0	0	0	0
05-08-2020	0	0	0	25800	3006
27-05-2020	0	0	0	0	0
11-05-2020	0	0	0	0	0

Figure 7.20 - Splunk Logs Screen

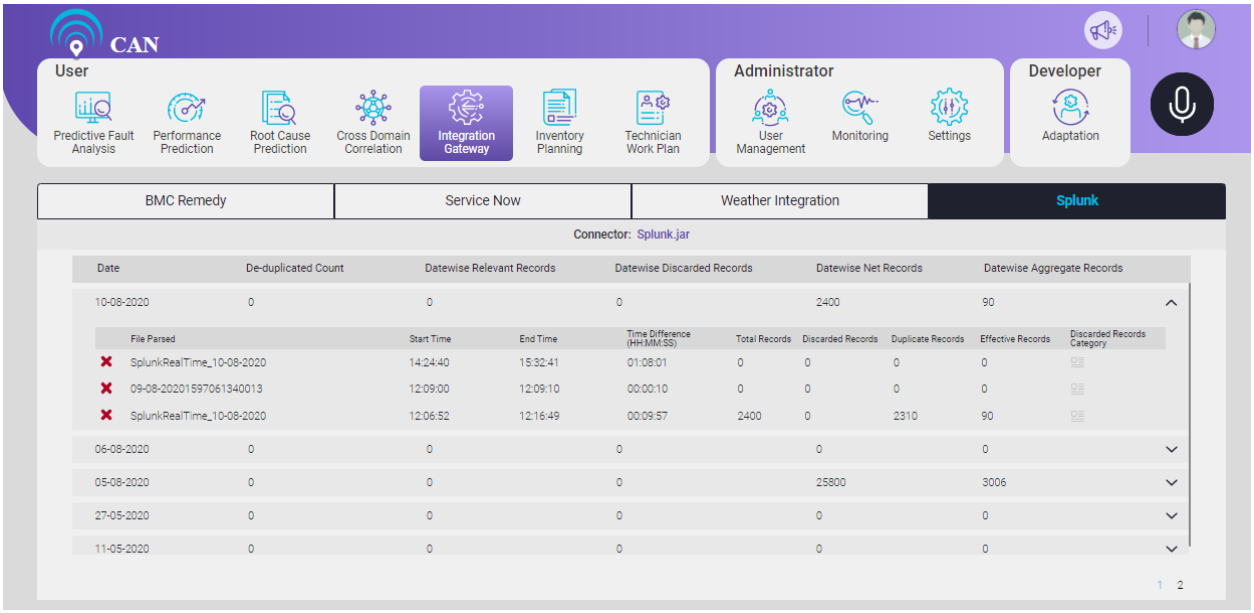


Figure 7.21 - Splunk Logs Screen

8. INVENTORY PLANNING

This screen shows the required items for the site engineers to resolve the predicted faults in the equipment. This enables early procurement of the required inventory, results in faster issue resolution even before the actual ticket registration in the trouble ticket management system.

Inventory Planning module has two tabs:

- Inventory Report
- Inventory Configuration

Inventory Report

This screen is used to map the inventory items with the Alarm attributes such as Equipment Component, Equipment Type, Cause, Prediction Day and Items.

User can select the prediction week from the **Available prediction slots** drop down menu. The screen displays the related faults with the inventory items for the selected week. User can also download the details of the predicted faults inventory for the selected week. Click the **download** icon to download.

The user can use the search text box to filter the items related to predicted faults.

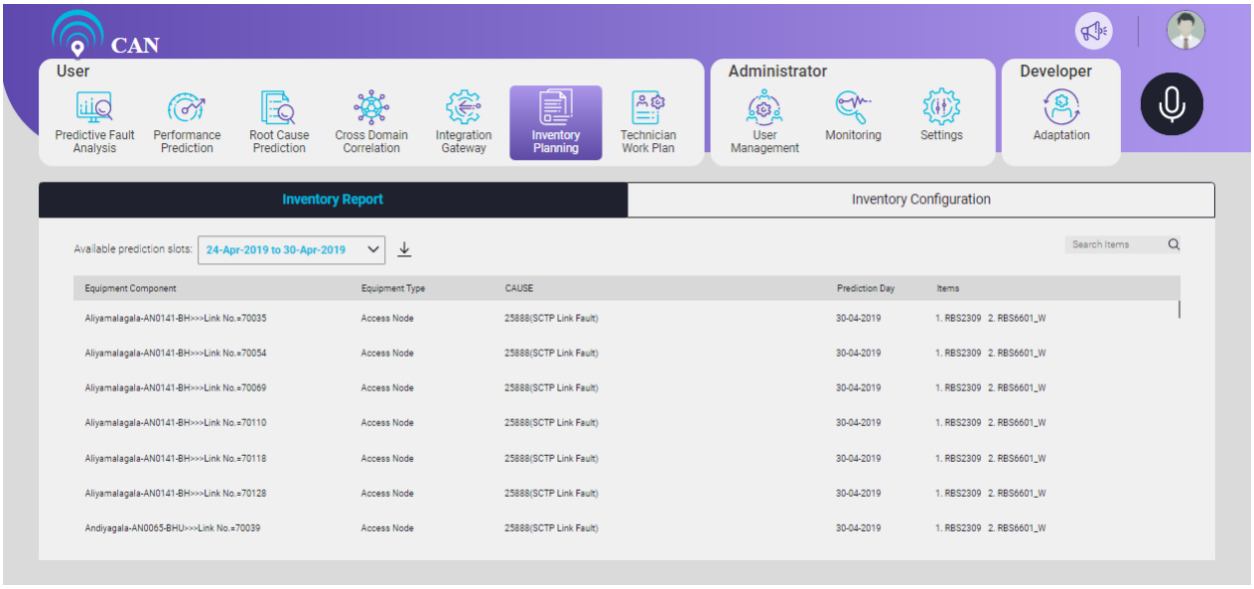


Figure 8.1 - Inventory Planning Home Page

Inventory Configuration

Click the **Inventory Configuration** tab to see the list of equipment items.

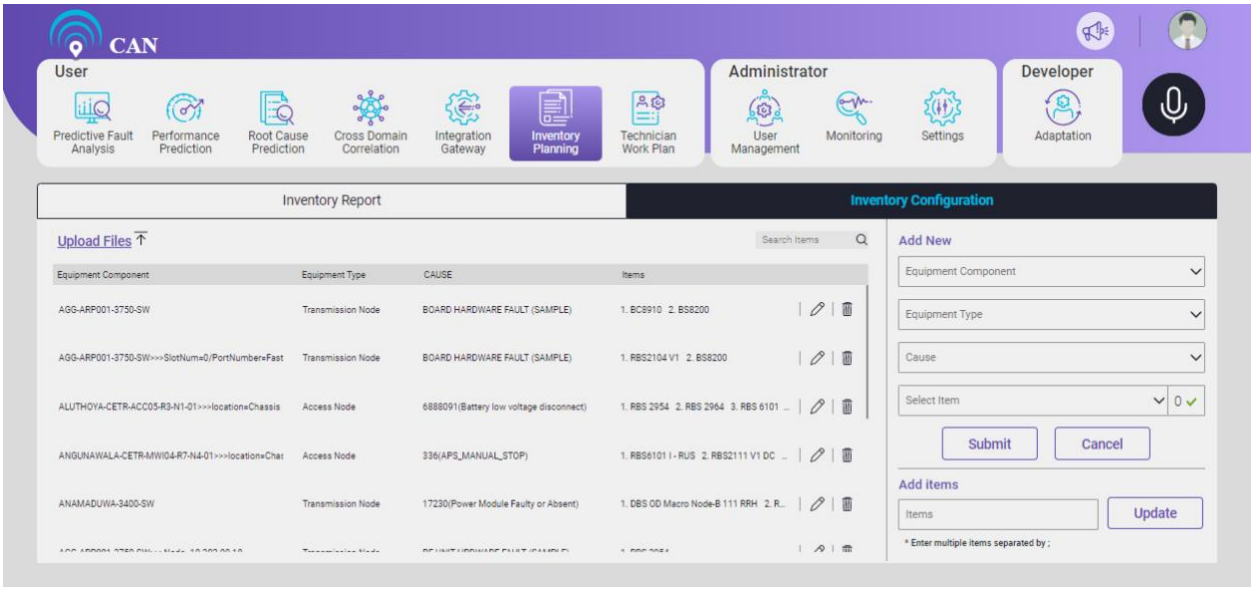


Figure 8.2 - Inventory Configuration Screen

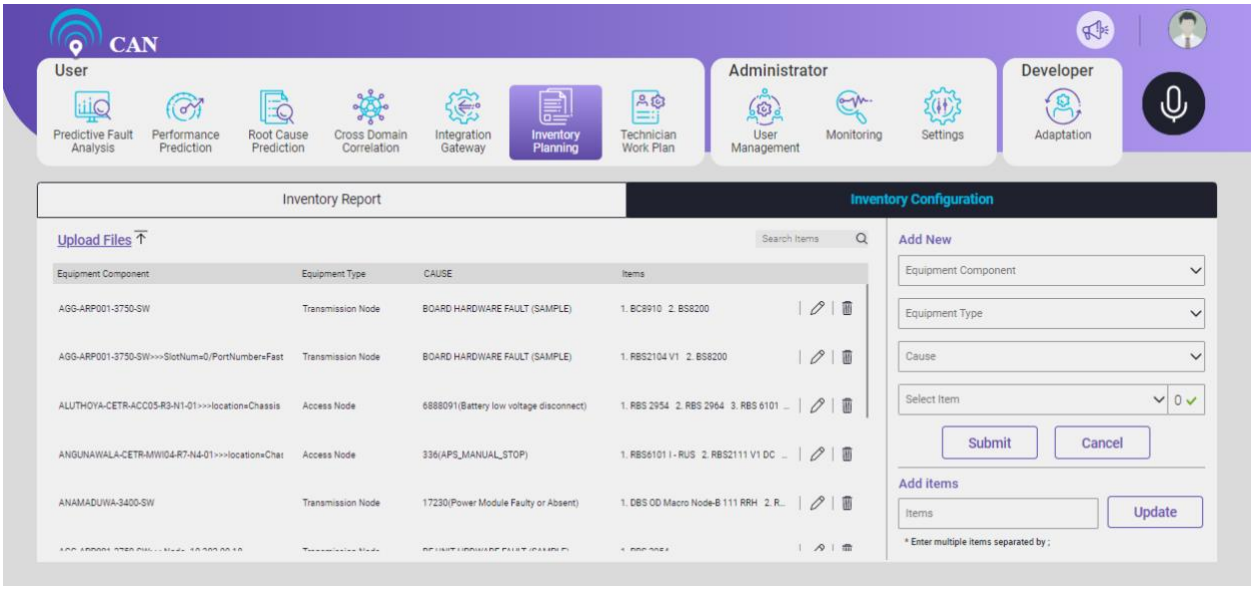


Figure 8.3 - New Equipment Item Addition Screen

To Add New Inventory Configuration

1. Write the Equipment Component, Equipment Type and Cause attributes in the text box or select them from the drop down.
2. Select the **item** attribute from the drop down menu (User can select multiple items at a time).
3. Click the **Submit** button to Add New Inventory Configuration.
4. To cancel the selection, click the **Cancel** button.

Note: If user want to Add New item, User can Add Items attribute in the Add Items text box. Click Update button to add the new Item.

To Update the Existing Inventory Configuration

1. Click the edit icon and edit the respective field. User can make the changes manually or choose from the existing options.
2. To save the changes, click the save icon .
3. Similarly, to delete an **Inventory Configuration**, select and delete the **Inventory Configuration**.

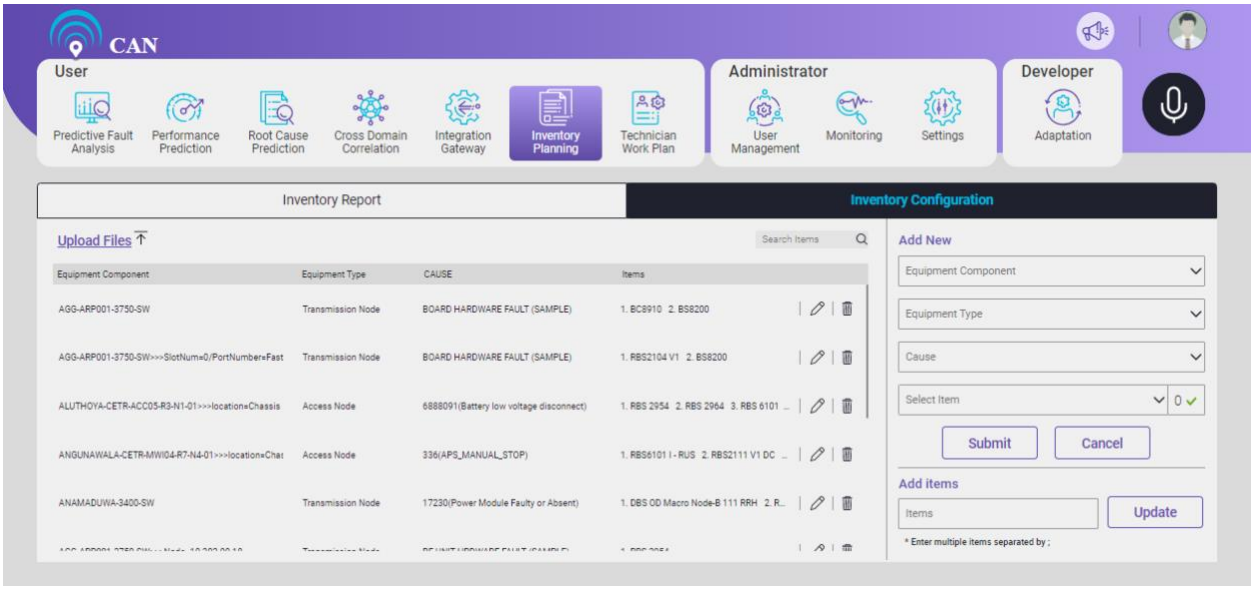


Figure 8.4 - Update or Delete Equipment Item Screen

User can also search the inventory items in the search item box.

To upload the file, click the 'Upload Files' icon on the left side of the screen. A screen will open where you can drag and drop the inventory file in XLSX format with Equipment Component, Equipment Type, Cause and Items information.

Note: Upload files facilitates the upload of multiple Inventory Configurations at a time.

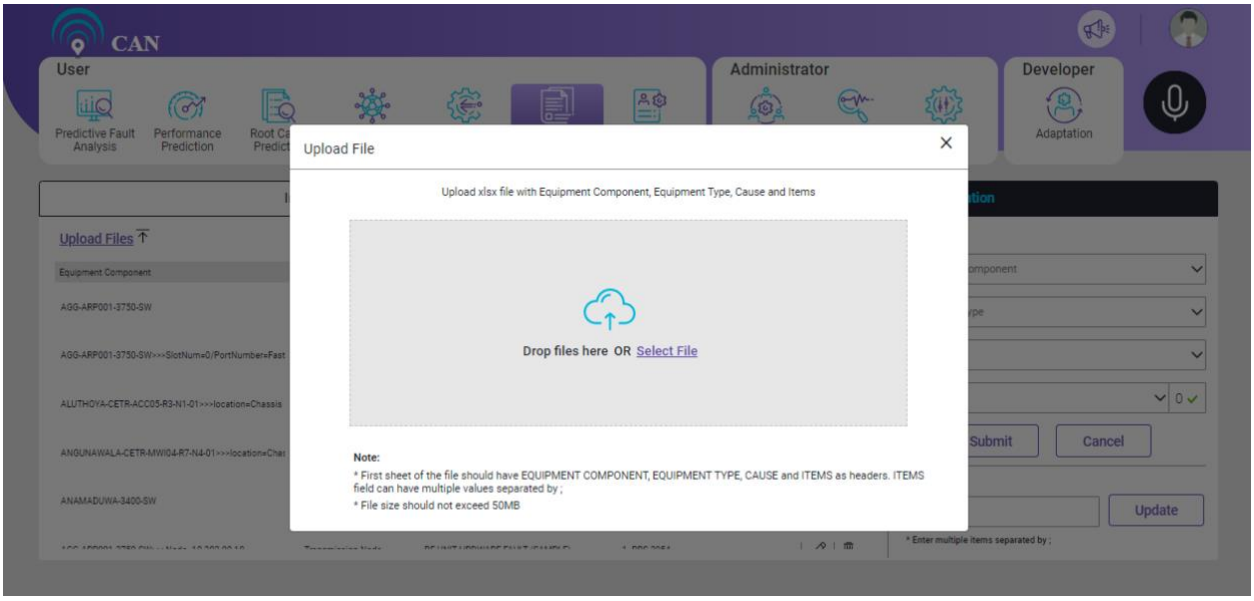


Figure 8.5 - Upload File Screen

9. TECHNICIAN WORK PLAN

Technician Work Plan provides option to assign the tickets to recommended technicians and shows the history of faults resolved by technicians. CAN identifies the right technician for particular issue and recommends such technician whenever similar incidents are predicted based on the ticket resolution history.

User can access the screen from the dashboard home. The Technician Work Plan tab has two tabs: **Recommendations** and **Resolved alarms**.

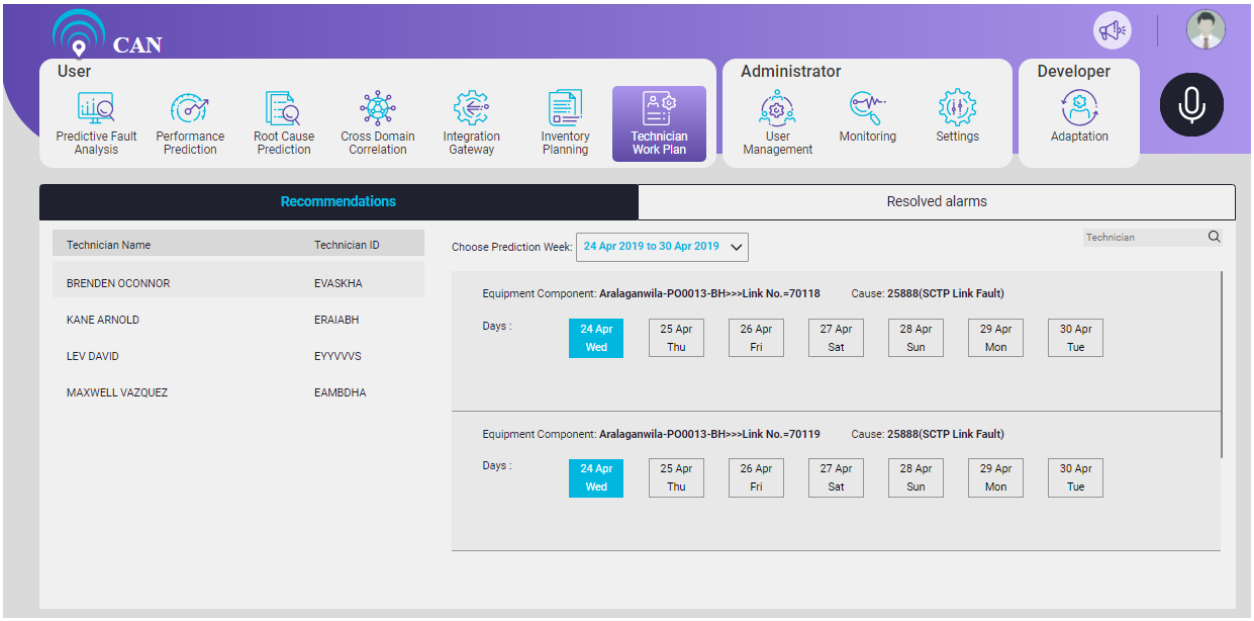


Figure 9.1 - Technician Work Plan

Recommendations

Click the ‘Recommendations’ tab. Choose a week from the “**Choose Prediction Week**” drop down menu. The screen displays a list of technicians with Technician Name and Technician ID who are most suitable to solve the predicted faults which can occur in the prediction week.

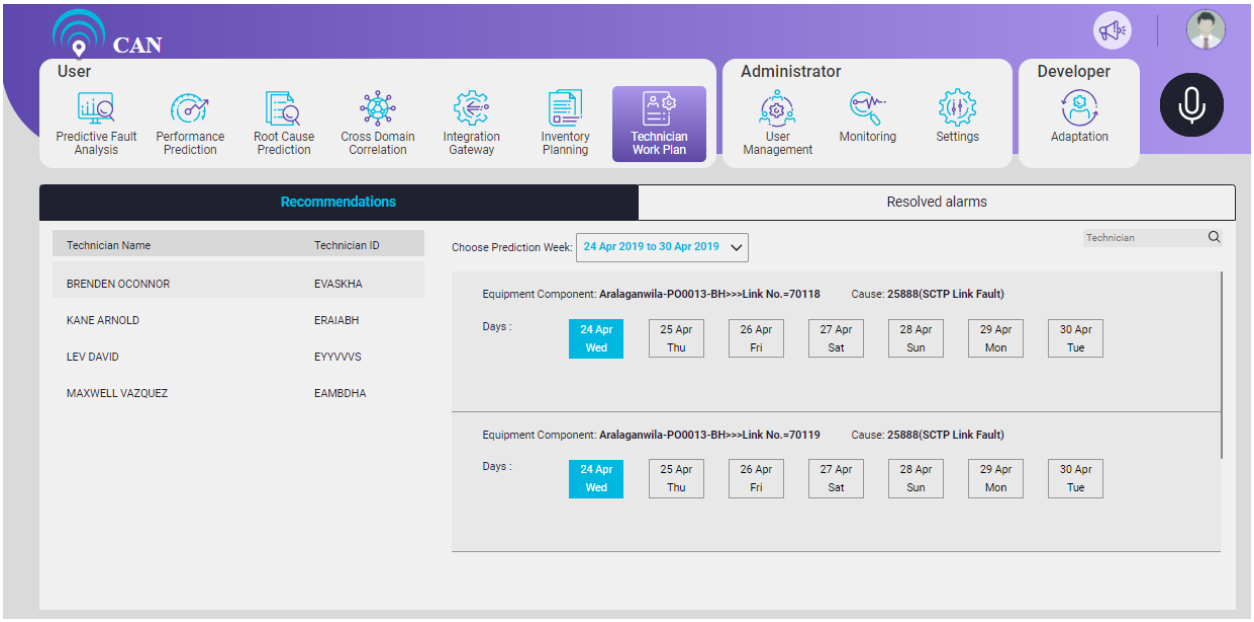


Figure 9.2 - Recommendations

When user clicks the date, a screen pops up displaying the details of Predicted fault details and Prediction Action Tracking.

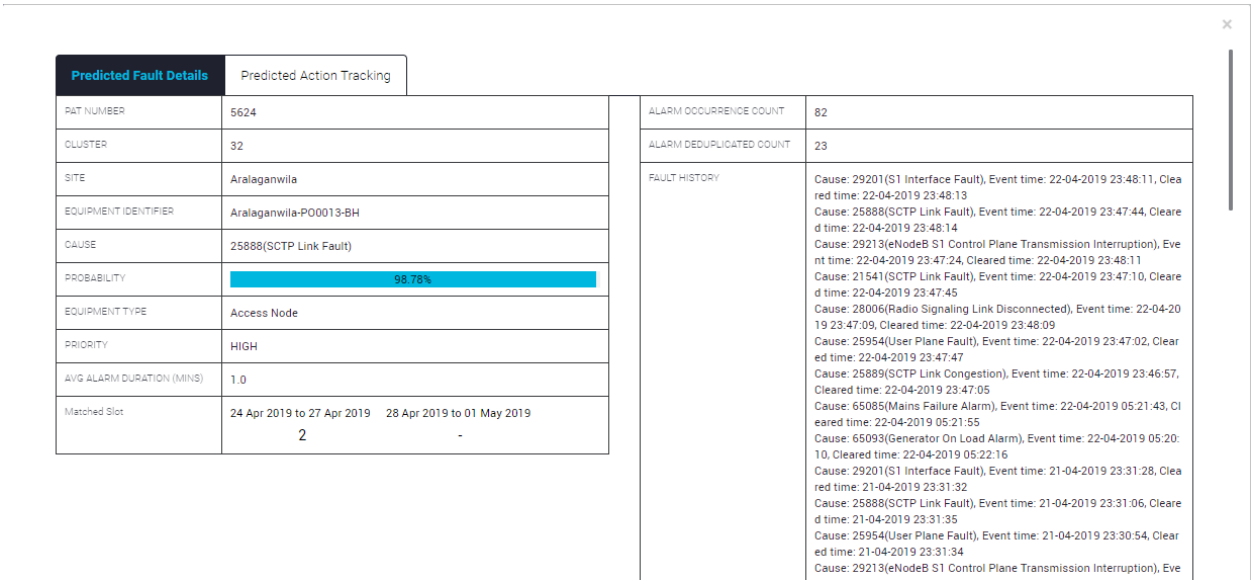


Figure 9.3 - Predicted Fault Details

When user click the **Predicted Action Tracking** tab, the screen displays the **Recommended Technician**. If certain technician is not available, user can allot the work to the next most suitable technician available.

Click the **Update** button to update the **Current Technician**.

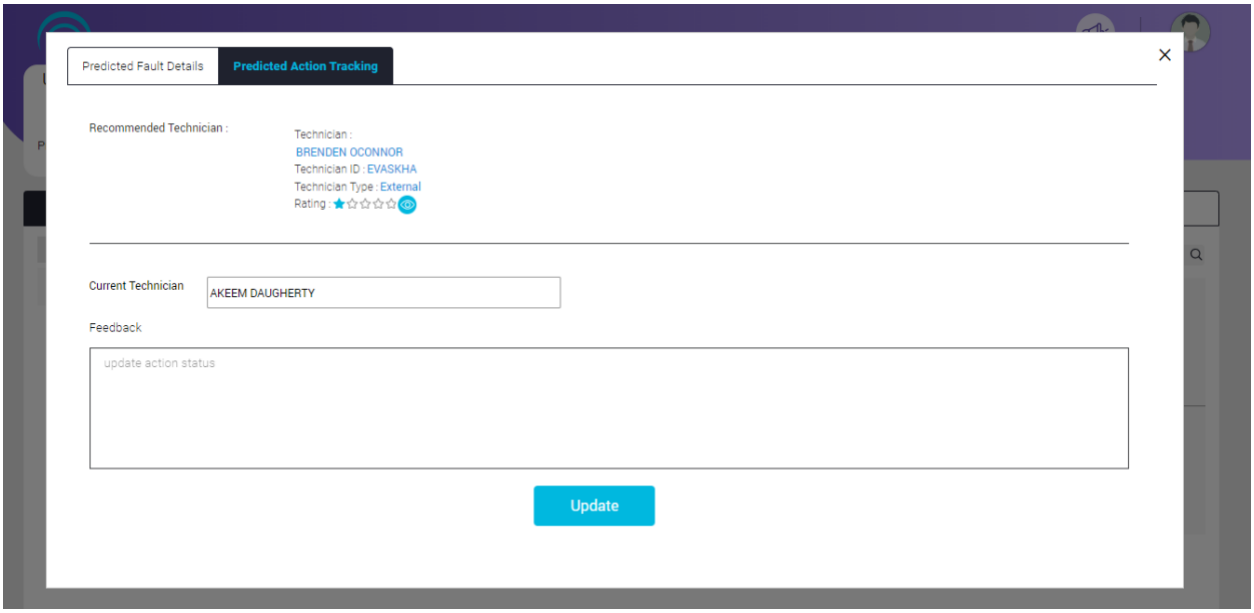


Figure 9.4 - Predicted Action Tracking

Resolved Alarms

Click the **Resolved alarms** tab on the screen.

The screen displays the Technician's Name, their ID and the resolved alarms information mapped to their name.

On the screen, in the Search box, select the name of the technician from the drop down menu. The screen displays all the resolved alarms mapped with technician's name.

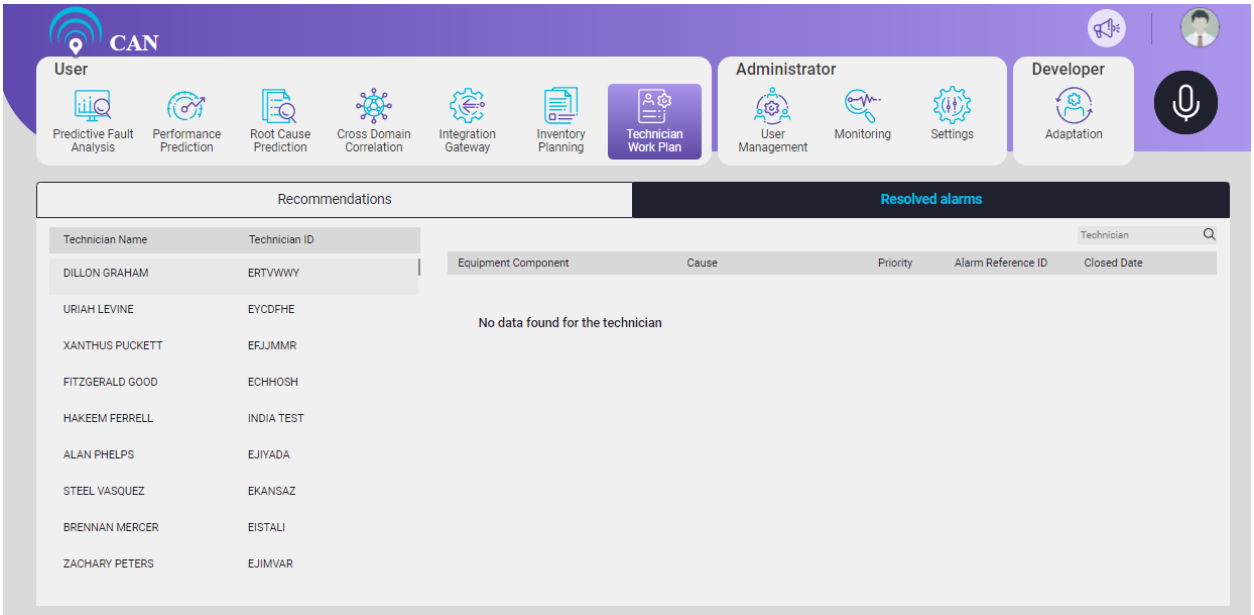


Figure 9.5 - Resolved Alarms

Page Intentionally Left Blank

10. ANNOUNCEMENT

This screen is useful for the administrators at the NOC. The **Announcement** tab generates a continuous stream of latest predictions that can be eventually projected on big screen for the information and necessary actions of related teams.

To view the announcements, click the **Display Announcements** button.

User can use the toggle button  to remove the prediction from the announcement list.

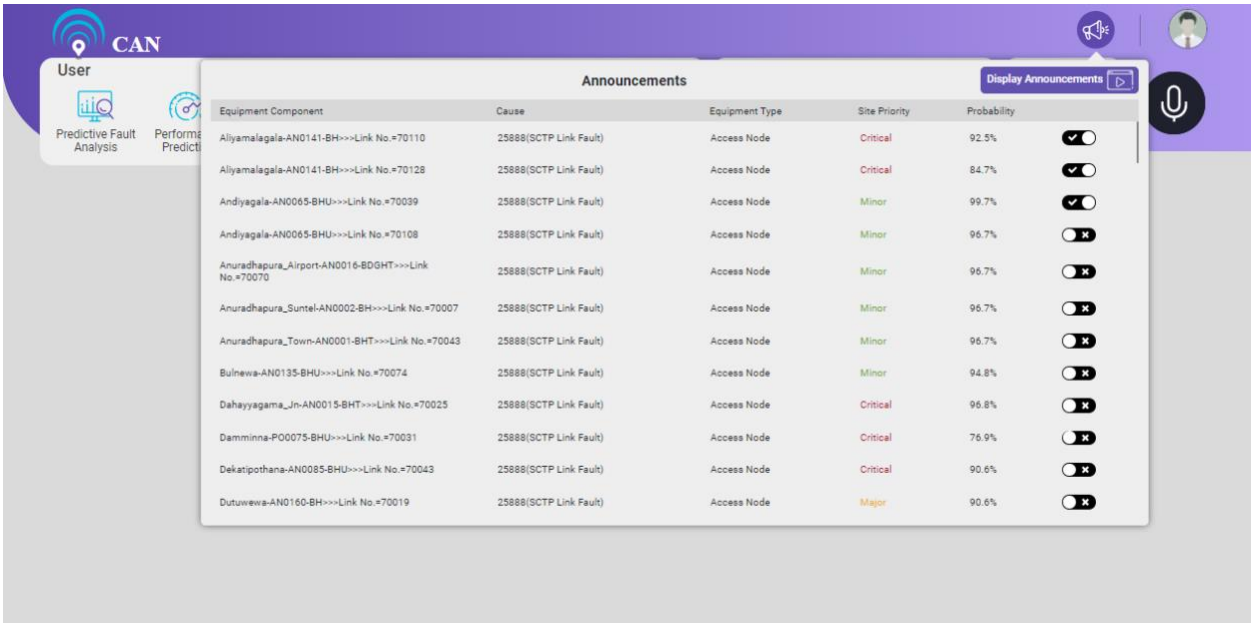
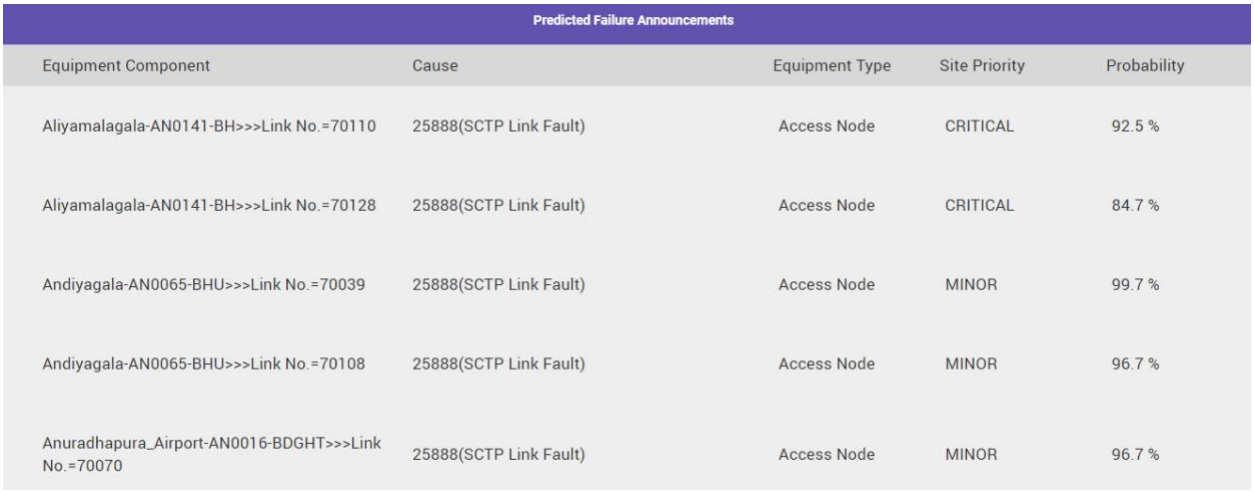


Figure 10.1 - Announcement Home Page

The below screen displays the Predicted Failure Announcements.



Predicted Failure Announcements

Equipment Component	Cause	Equipment Type	Site Priority	Probability
Aliyamalagala-AN0141-BH>>>Link No.=70110	25888(SCTP Link Fault)	Access Node	CRITICAL	92.5 %
Aliyamalagala-AN0141-BH>>>Link No.=70128	25888(SCTP Link Fault)	Access Node	CRITICAL	84.7 %
Andiyagala-AN0065-BHU>>>Link No.=70039	25888(SCTP Link Fault)	Access Node	MINOR	99.7 %
Andiyagala-AN0065-BHU>>>Link No.=70108	25888(SCTP Link Fault)	Access Node	MINOR	96.7 %
Anuradhapura_Airport-AN0016-BDGHT>>>Link No.=70070	25888(SCTP Link Fault)	Access Node	MINOR	96.7 %

Figure 10.2 - Display Announcement Screen

11. USER MANAGEMENT

User management helps to control the user access.

Roles supported are Super Admin, Admin, Circle Manager, Zone Lead and others. Each role has following accesses:

Modules		Admin	Circle Manager	Zone Lead	Others
User	1. Predictive Fault Analysis	Yes	Yes	Yes	Yes
	2. Performance Counter	Yes	Yes	Yes	Yes
	3. Root Cause Prediction	Yes	Yes	No	No
	4. Cross Domain Correlation	Yes	Yes	Yes	Yes
	5. Integration Gateway	Yes	Yes	Yes	Yes
	6. Inventory Planning	Yes	Yes	Yes	Yes
	7. Technician Work Plan	Yes	Yes	Yes	Yes
Administrator	1. User Management	Yes	No	No	No
	2. Monitoring	Yes	Yes	No	No
	3. Settings	Yes	No	No	No
Developer	1. Adaptation	Yes	No	No	No

Table 1 : User Roles

User Management module has three tabs:

- Manage Role
- Manage Users
- View Logs

Manage Roles

This tab allows to add, delete, search and modify the Existing Roles.

User can use the search icon to search the Existing Roles.

To Add New Role

1. Write the Role Name in the **Role Name** text box.
2. Select the Role Category from the drop down menu.
3. Select the applicable Circle from the **Choose circle** drop down menu.
4. Select the cities from the **Choose cities** drop down menu.
5. Click the **Submit** button to add the New Role.

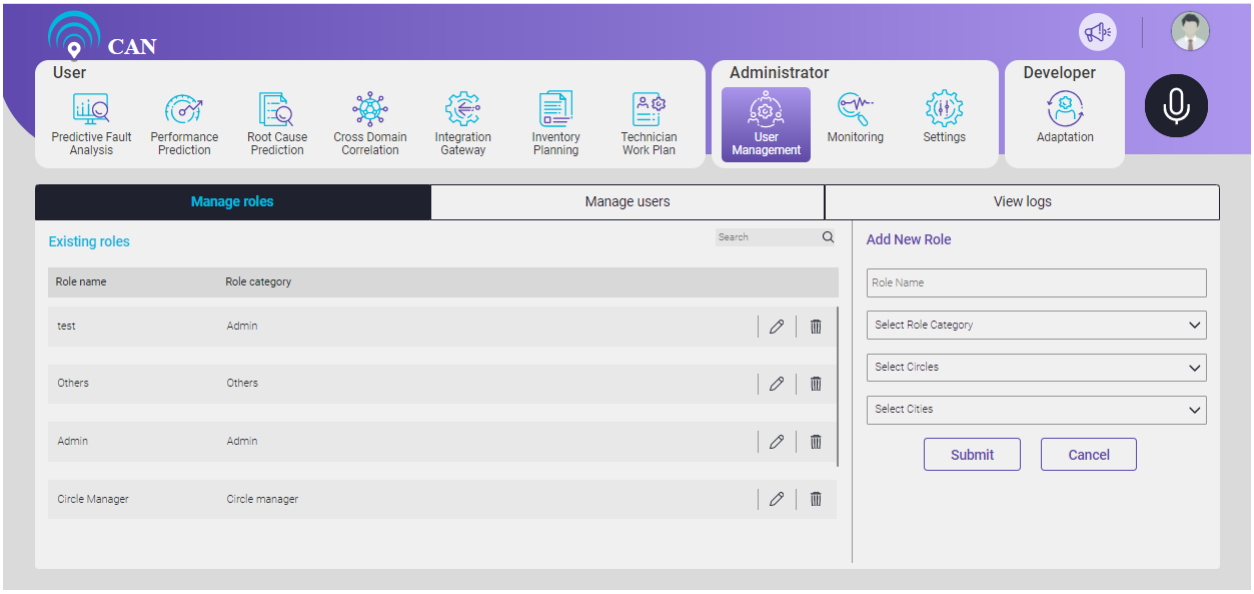


Figure 11.1 - Manage Roles

To Edit the Existing Roles

1. Click the edit icon .
2. Edit the fields you want to edit. Select the appropriate “Role category”, “Choose circles”, “Choose cities” from the drop down menus to update.
3. Click the update icon to save the changes. If user will not save the changes, the changes will not get saved.
4. Click the delete icon to delete the Existing Role.

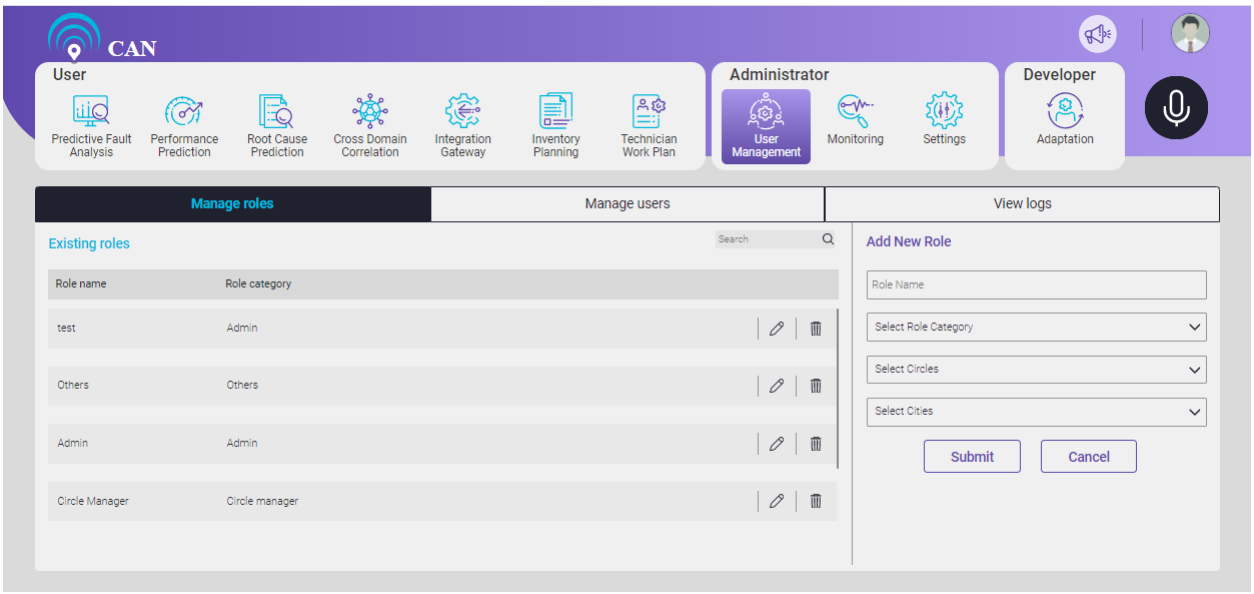


Figure 11.2 - Manage Roles of Existing Users

Manage users

The screen displays the details of existing users of CAN. The details include User Name, Email Id, Role assigned to user, Expiry Date of a particular user, Status of the user. The functionality of this screen allows to add a new user, modify the existing user details and delete the existing user.

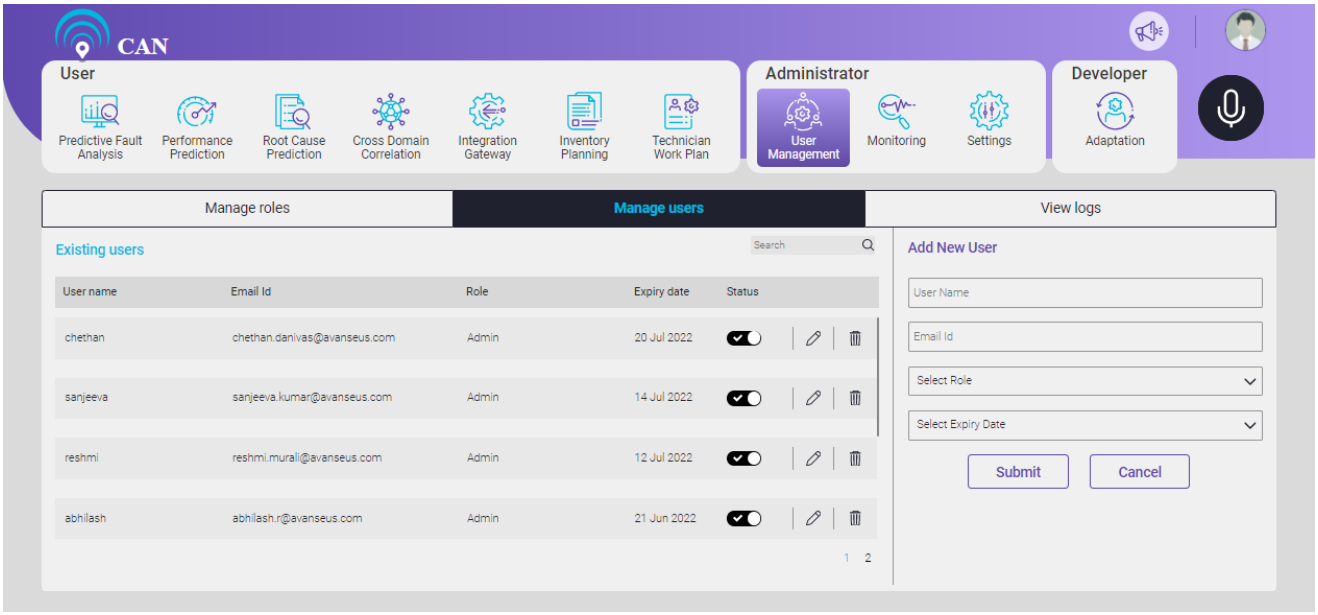


Figure 11.3 - Add New Users

To Add New User

1. Type the User Name in the **User Name** text box.
2. Type the Email ID of the user in the **Email ID** text box.
3. Select the appropriate role from the drop down menu.
4. Select the tenure for the access to user from the drop down.
5. Click the **Submit** button.

To Edit the Details of Existing Users

1. Click the edit icon .
2. Edit the respective fields you want to edit.
3. Click the update icon to save the changes. If user will not save the changes, the changes will not get saved.
4. Click the toggle button to resume the existing user or suspend the user.
5. When the suspended user will be resumed access, you need to select the Duration for the resumed Role access from the drop down menu. The access duration can be given for One week, One month or One year.
6. Click the delete icon to delete the Existing Role.

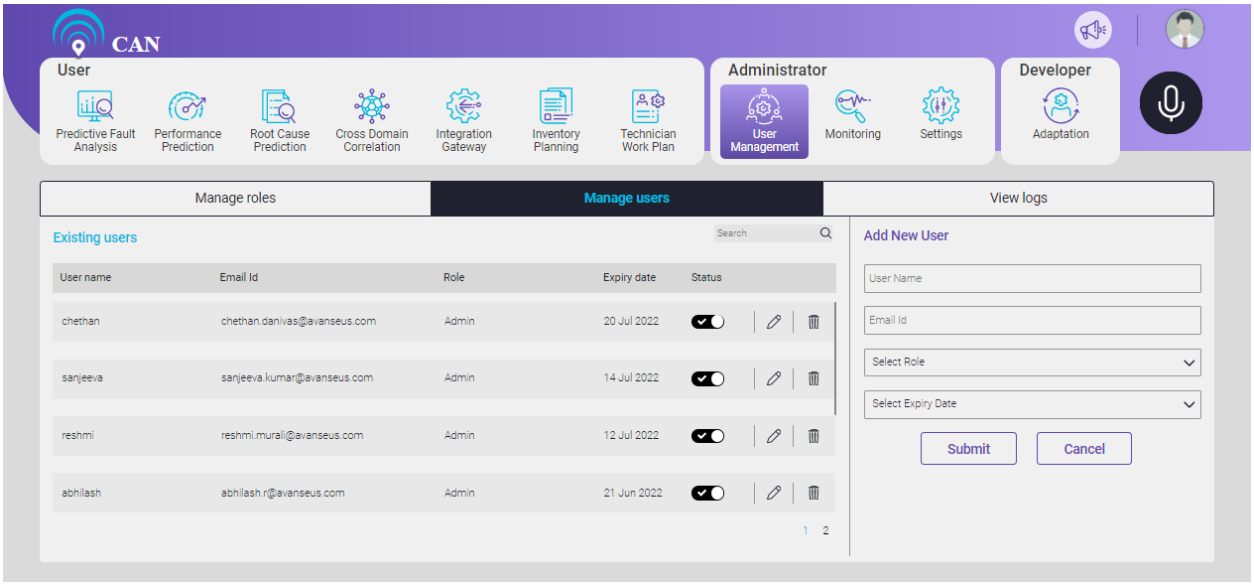


Figure 11.4 - Manage the Existing Users

View Logs

This screen displays up-to-date CAN log activity from various users. User can search for a particular activity based on the User Name, From Date, To Date, Activity Type (all, log in, log out, password modification, Failed Login, User creation, User modification, Role creation, Role modification, Security log access) and Location.

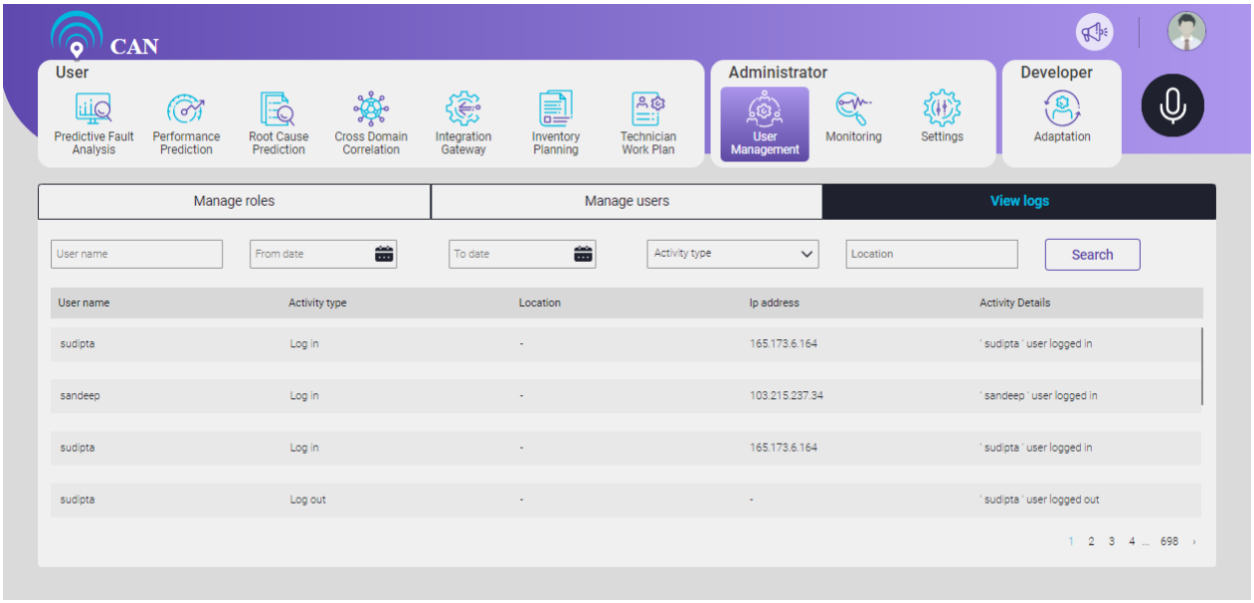


Figure 11.5 - View Logs

Page Intentionally Left Blank

12. MONITORING

Monitoring allows the user to receive the information on the system operation. This tab has two options: **Data Collection Audit** and **Notification Handler**.

Data Collection Audit

This screen has two filters: Period and Data Source.

There are three Periods available:

- Current month,
- Current with previous month and
- Current with previous 2 months.

The data sources available are:

- All
- Alarms
- Tickets
- Work Order
- Performance Counter
- Splunk
- Others

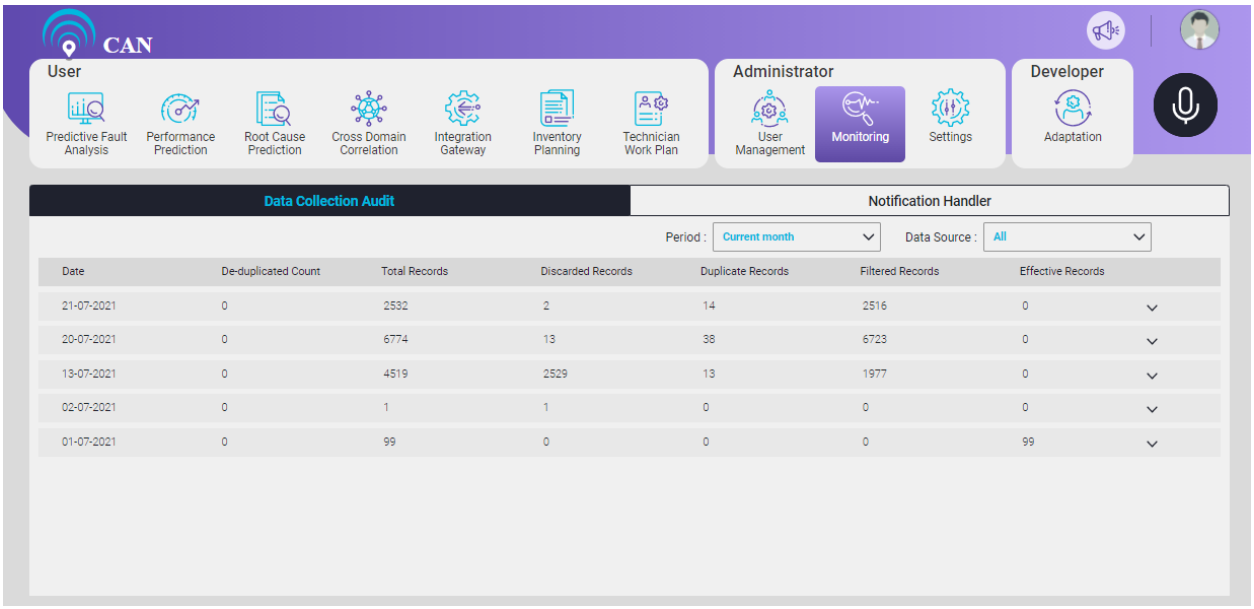


Figure 12.1 - Data Collection Audit Screen with Periods

This screen displays the **Date**, **De-Duplicated Count**, **Total Records**, **Discarded Records**, **Duplicate Records**, **Filtered Records** and **Effective Records** on a daily basis (for each period and data source combination).

The screen will display the data based on the selected period and data source combination. For **OTHERS** data source, the screen will not display De-Duplicated Count and Filtered Records.

For each period, if the files are present for more than 5 days, then the screen will display pagination and for each page, the screen will display 5 rows. If total number of pages is more than 10, then after 9, dots will appear up to the last page. User can click on the dots; one input box will appear. User can search for a particular page with the appropriate input. When you click previous and next arrow, the corresponding page information's will be displayed.

User can click each row to see the details of **File Parsed Info**, **File Parsed Status**, **Start Time**, **End Time**, **Time Difference** (in HH: MM: SS format) with previously mentioned count stats for file on a daily basis.

If for "ALL" data source, multiple data sources are there for that particular day, then all will appear and the data sources will appear as multiple tabs. On click of each tab, file information's will appear for that particular data source. If only one data source is there for that particular day, then only that data source name will be displayed like header. Each case, total number of file count for the particular data source will appear on the right hand side of the expanded area.

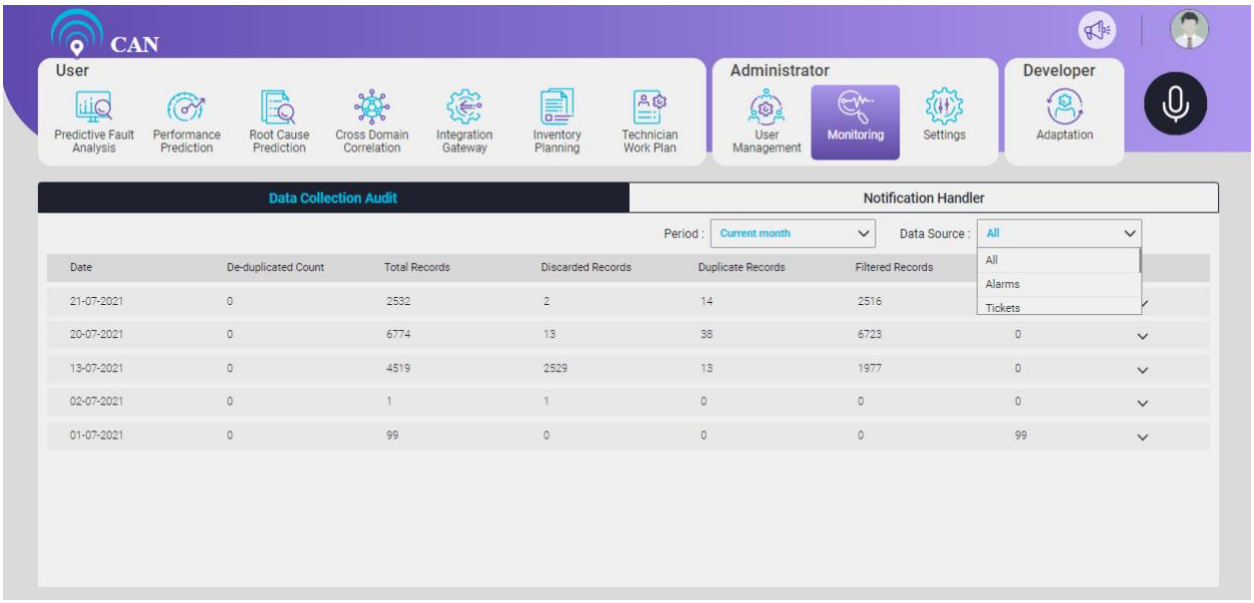


Figure 12.2 - Data Collection Audit Screen with Multiple Data Sources

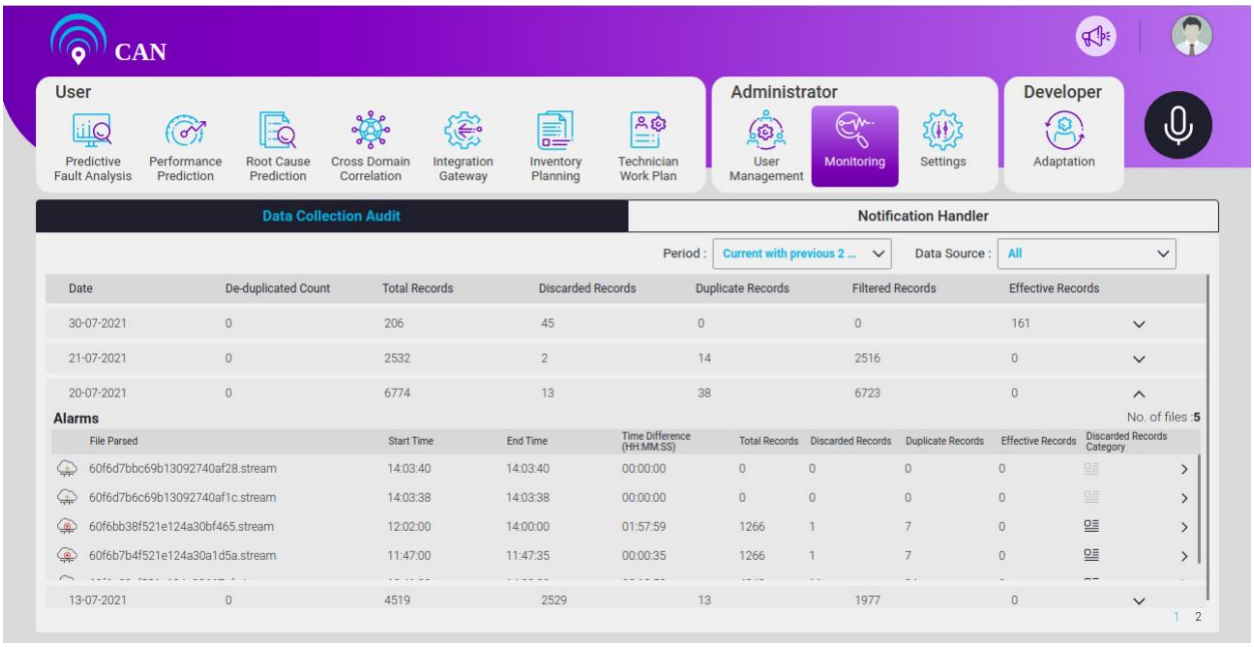


Figure 12.3 - Data Collection Audit Screen

To view the information on **Discarded Records Category**, click the icon .

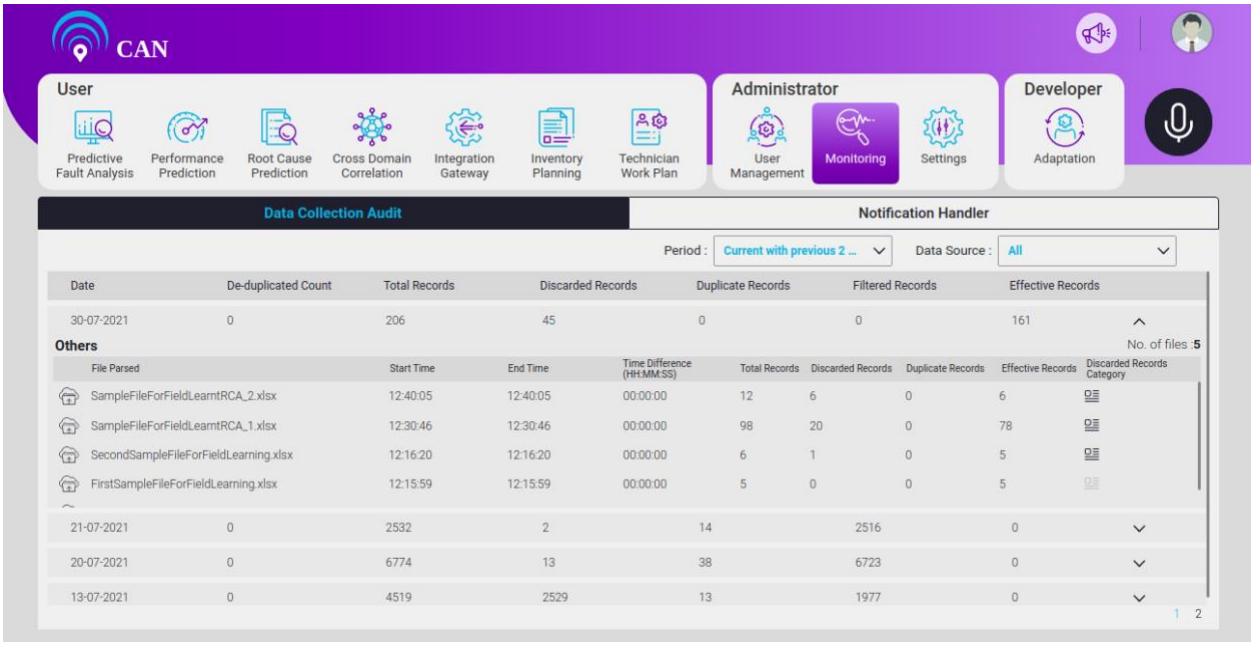


Figure 12.4 - Discarded Records Category

Discarded Category includes counts of Preprocessor Rejected, Post processor Rejected, No Office Code No Equipment, No Equipment Component, No Cause, No Creation Date, No Category, No Zone, No Priority, No Nation, No Equipment Vendor, No Equipment Type, No performance Counter Equipment Component, No Performance Cause, No Source, No Restriction, No Time, No Category, Others, No Ticket ID, No Ticket Creation Date, and Error.

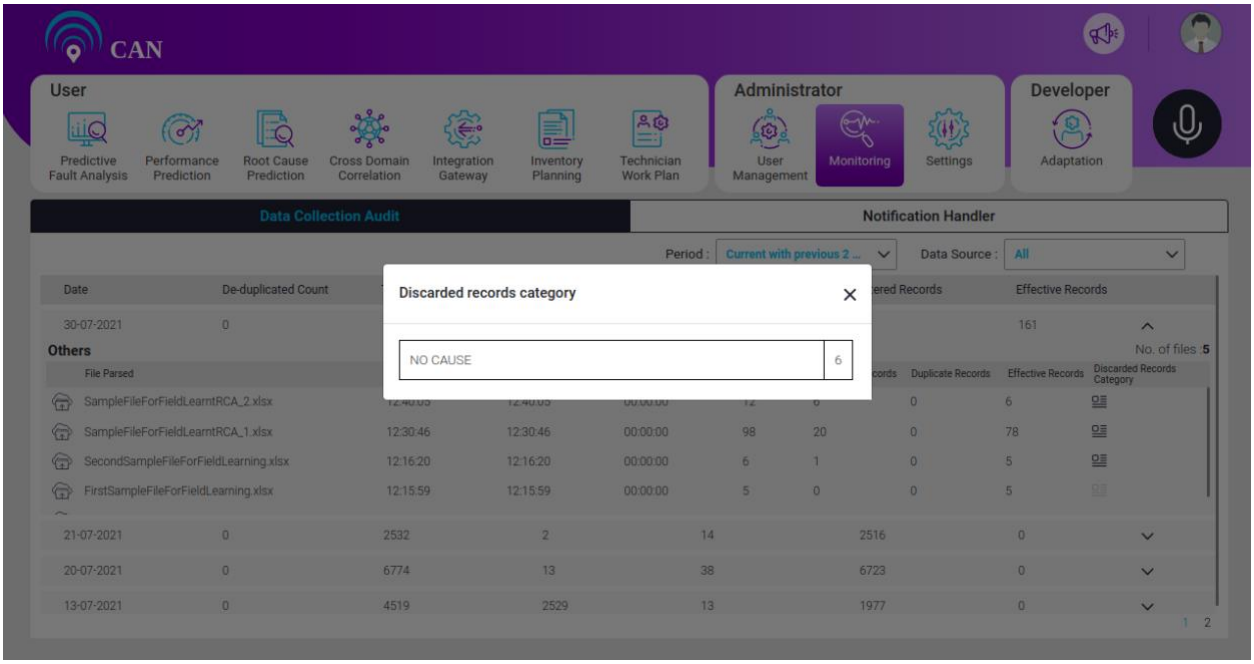


Figure 12.5 - Discarded Record Category

Parsed records coming from batch processing (Non Kafka) are indicated using the icon . This icon is called as file based collection icon.

Parsed Kafka details are displayed under **Alarms** Data Source. The Kafka details can be viewed in:

- Live Streaming Data - It represents the data that is live streaming. This icon is used to show live streaming data.
- Paused Streaming Data - It represents the data whose streaming status is either paused or completed. This icon is to show the paused streaming data.

Each Kafka row has a unique streaming ID and it is the combination of streaming chunks.

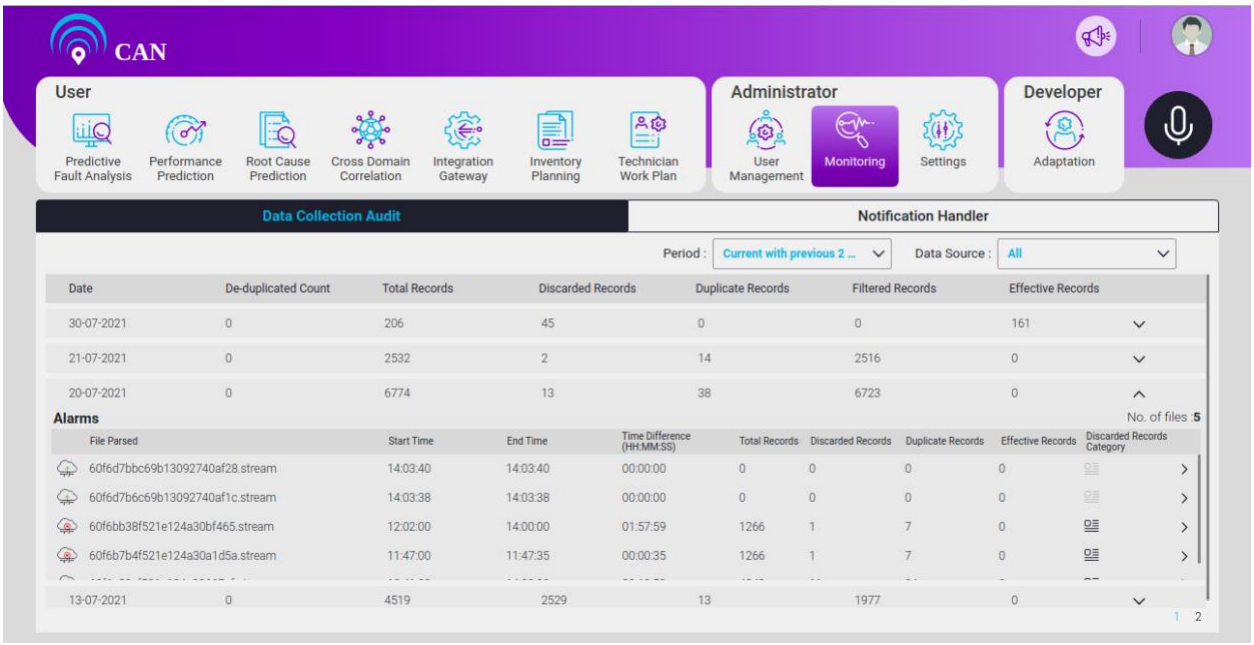


Figure 12.6 - Kafka Paused Streaming Data

To view the details of the Streaming Chunk, click the icon ›. When you click ›, a pop up appears. The pop-up screen shows the details of these chunks.

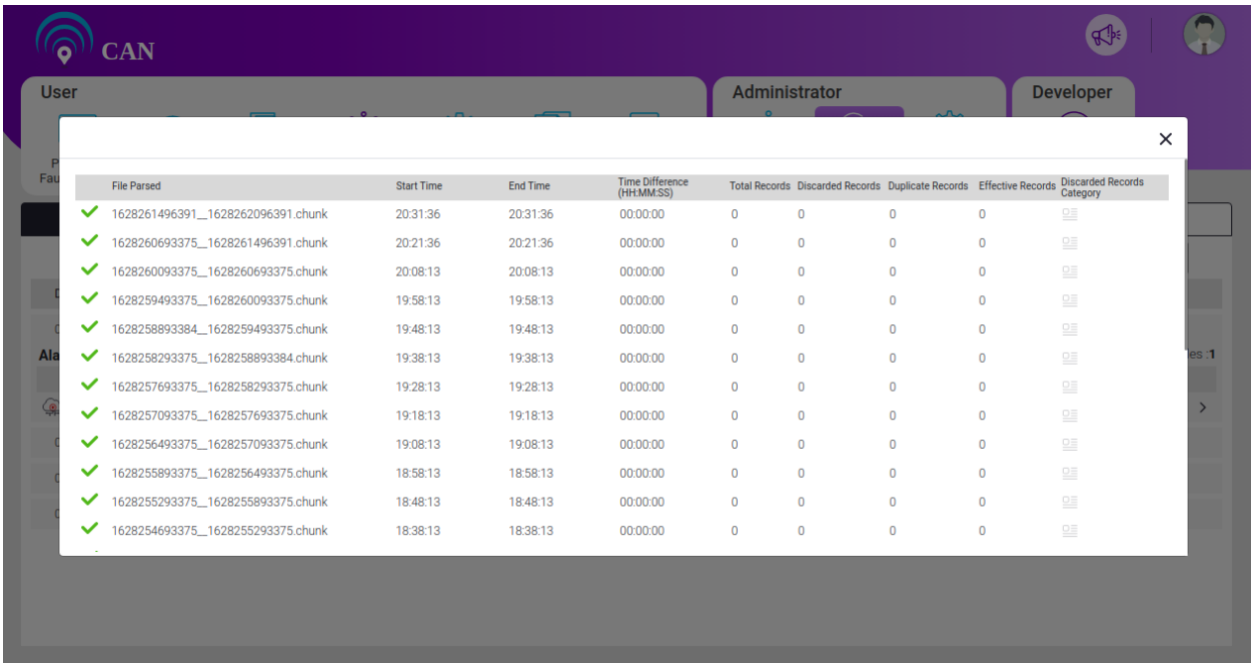


Figure 12.7 - Kafka Paused Stream Data Details Screen

Click the close button to close the pop up screen.

Notification Handler

This screen is used to configure success and failure emails for various email groups. When enabled, notification about various processes such as Data Collection, File Availability, Alarm archival etc. will be sent to mail ids listed in the mail group.

If enabled, then red star mark * will appear for the mandatory fields of the corresponding section and if disabled, then star mark will not appear.

User can select multiple mail groups at a time for each section. Based on the available mail groups, the screen will display. User can edit only one section at a time and after modification, user has to update the configuration, otherwise new changes will not reflect.

By default, edit option will be there. After going to edit mode and adding at least one mail group for a particular section, and if email subject and email body are present, then save icon will appear. User can save and proceed for the other sections.

On saved mode, user can only go through the saved mail group names on hover of the particular mail group area. On edit mode, after addition/deletion of a mail group name, the existing count will be populated and will appear at the right hand side of the corresponding mail group area with a green tick mark ✓.

On edit mode, if user will deselect all the mail groups for at least one of the success and failure mail group section or at least one of the email subject and subject body is empty in success or failure mail section, update icon will disappear.

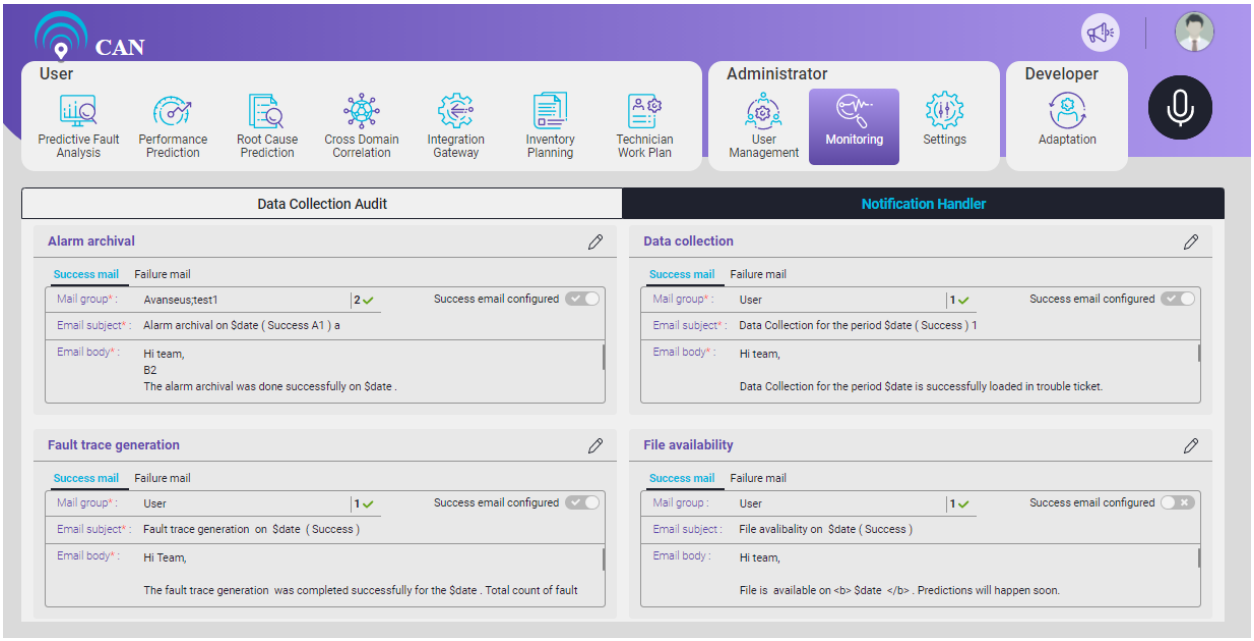


Figure 12.8 - Notification Handler

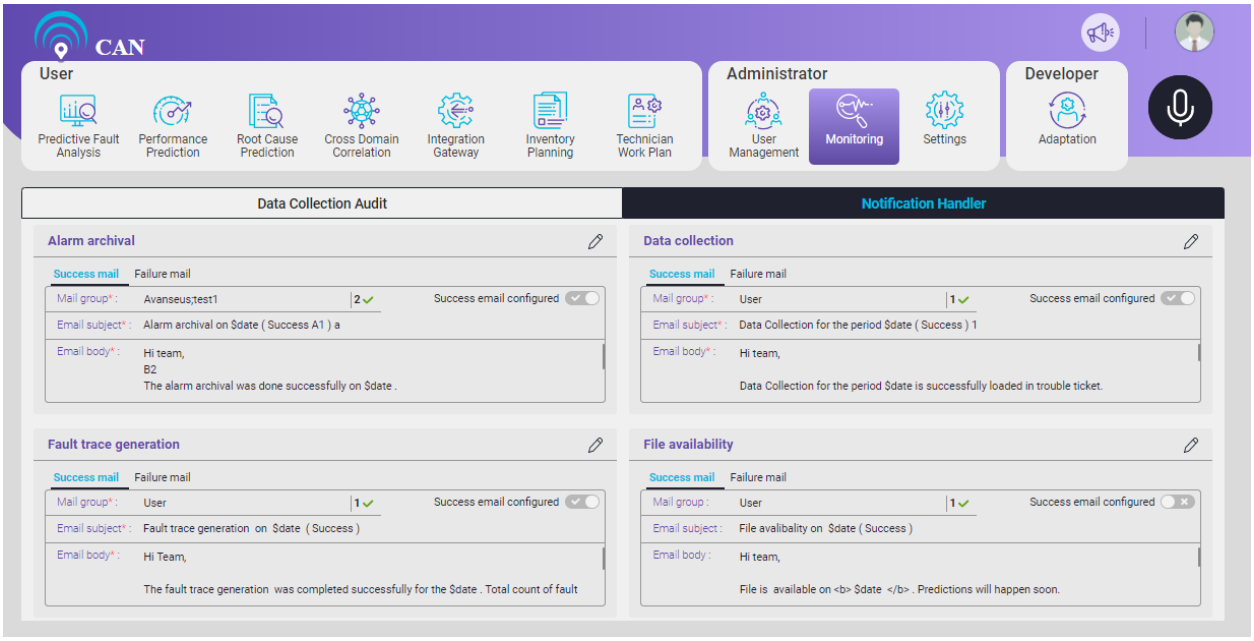


Figure 12.9 - Success Mail Template

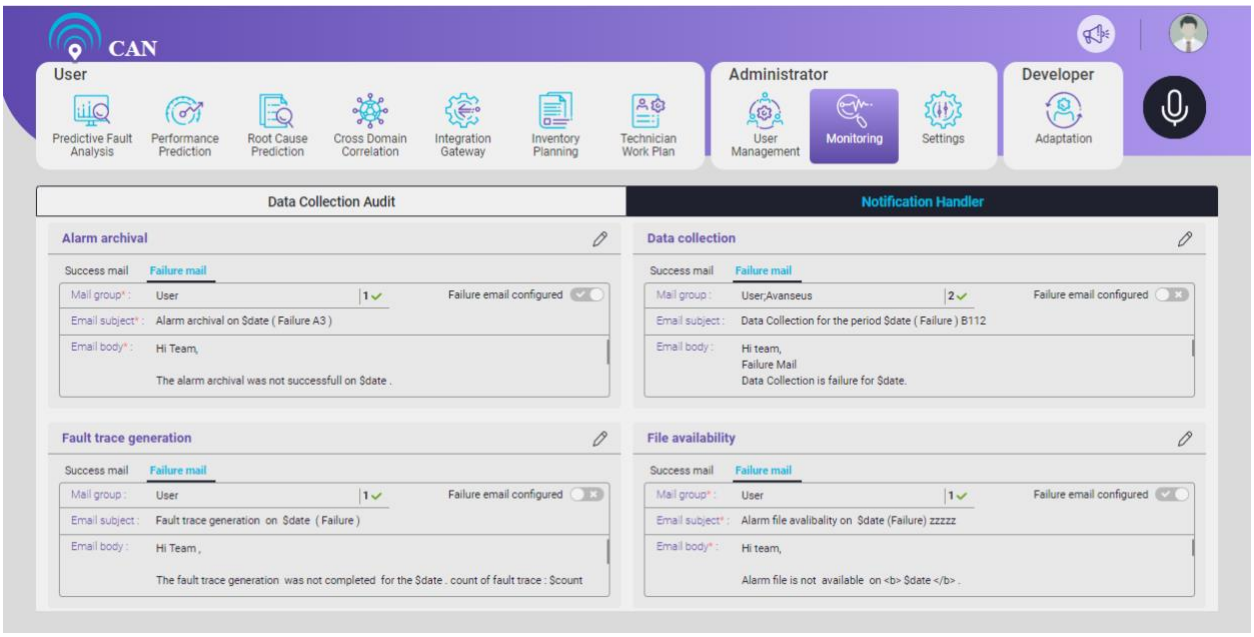


Figure 12.10 - Failure Mail Template

13. SETTINGS

Users can visit the settings page to modify the application level configuration.

To modify the application level configuration, click the **Settings** tab.

Settings are classified under five tabs:

- **Cause Management** - Manage the Causes relevant Configurations by giving them an alias by setting in Domain field, Network Type, Categorise them as INFRA, HARDWARE, TRANSMISSION, CONFIGURATION, EXTERNAL or TEST and provide a slot to totally remove them from prediction generation by unchecking in Service Impact checkbox.
- **Announcement Exclusion Rules** - Useful at NOC for administrators and network fault resolution team to get real time notifications/announcements of the major and top priority predicted faults. This is a focal point for network troubleshooting, supervision, monitoring and management.
- **Technician Availability** - This helps to record the technician availability in real time for work assignment.
- **Mailing List** - The mailing list is used to configure the mail ids of the users into groups to send them the prediction report and other important reports.
- **GIS Update** - This screen is used to view and edit the latitude and longitude of the equipment. Validated the same against the geo coding API.
- **Priority Management** - This screen is used to view and update the site priority of the corresponding office code.

Cause Management

Cause Managements enables the user to manage the Cause by providing the vectors related to specific Cause. This tab enables user to define the depth of each Cause by providing the Cause domain, the Network Type where this Cause is valid, whether it is service impacting or not, whether it is a priority Cause as per user and what kind of Cause category that the particular Cause belongs to. This enables the CAN engine to show the prediction output appropriately assigning the adequate importance based on the gravity of the Cause.

User will use Schedule Job Button whenever there is an update in Cause attribute. User will click the **Schedule Update Job** button, when user want to update the Cause attributes in Alarm and Predicted Fault Table.

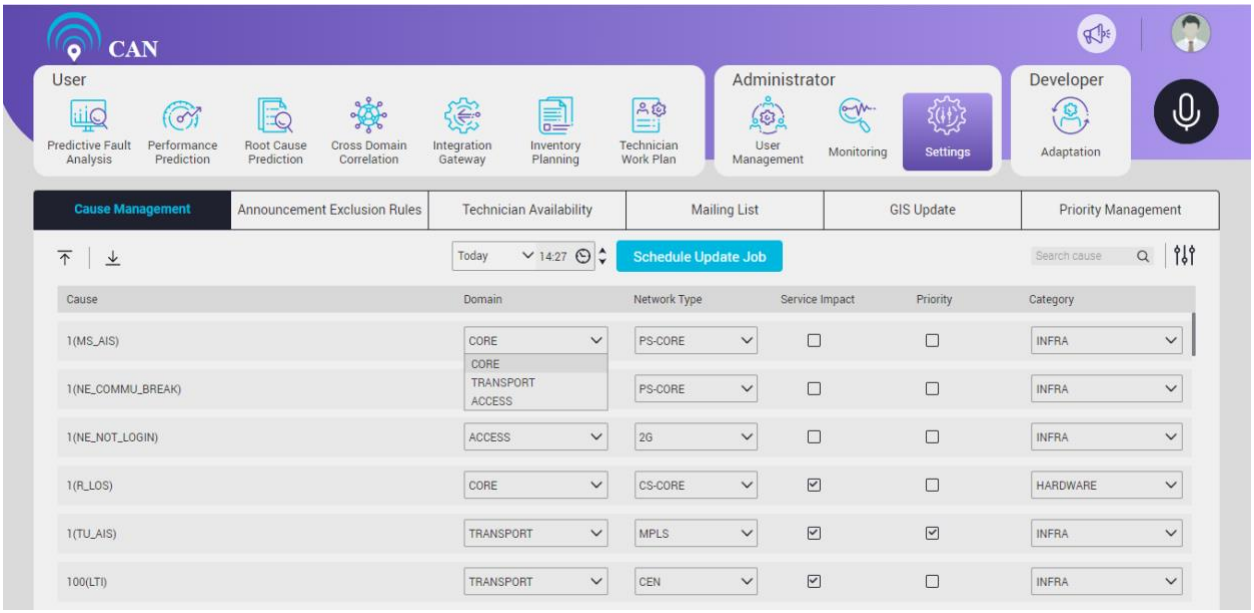


Figure 13.1 - Cause Management

To Filter the Cause Details

1. Select the **Domain** from the drop down.
2. As per your selected domain, **Network Type** will be displayed. Select the applicable **Network Type** from the drop down.
3. Check the **Service Impact** and **Priority** radio buttons (Yes or NO).
4. Select the **Category** from the drop down.
5. Click the **Apply** button**.**
6. To reset the filter**,** click **Reset Filter.**

NOTE: User can select any of the parameter i.e. Domain, Network Type, Service Impact, Priority and Category and click Apply to see the filtered result.

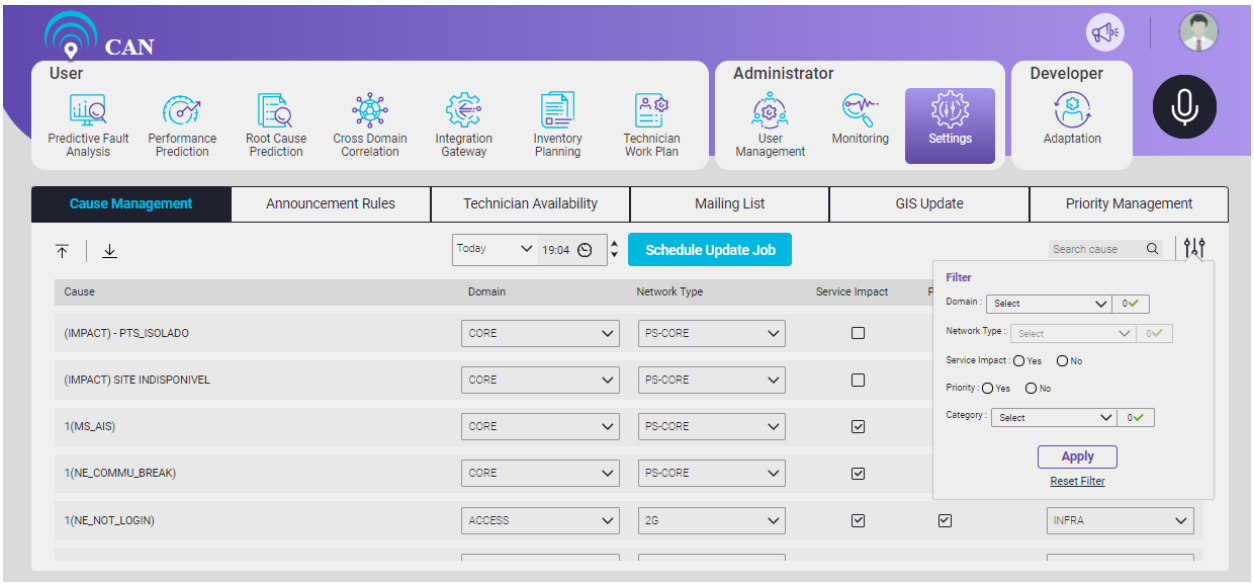


Figure 13.2 - Cause Management Filter

User can download the details of pre-configured alarm causes for cause management.

To upload the file, click the Upload Files icon on the left side of the screen. A screen will open where you can drag and drop the Cause detail file in XLSX format with details of CAUSE, DOMAIN, NETWORK TYPE, SERVICE IMPACT, PRIORITY and CATEGORY.

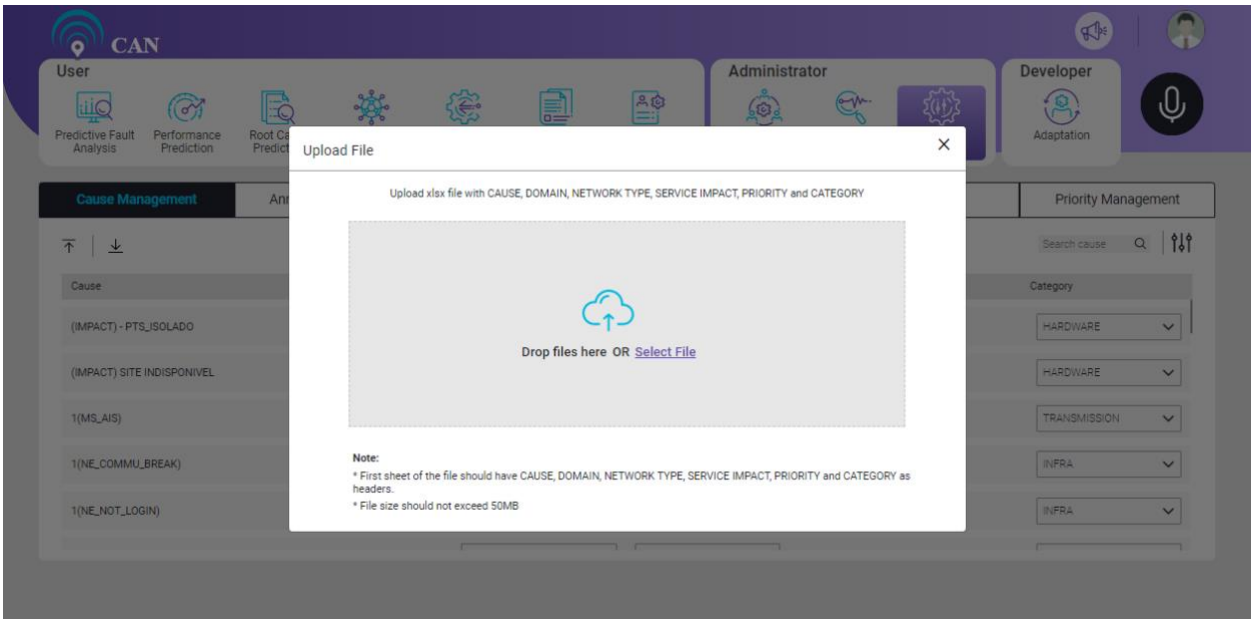


Figure 13.3 - Cause Management Upload Files

User will click the Schedule Update Job button, a pop to Confirm Action with a message “Do you want to schedule the update action” will appear on the screen.

Click the **Yes** button to schedule the job or click the **No** button.

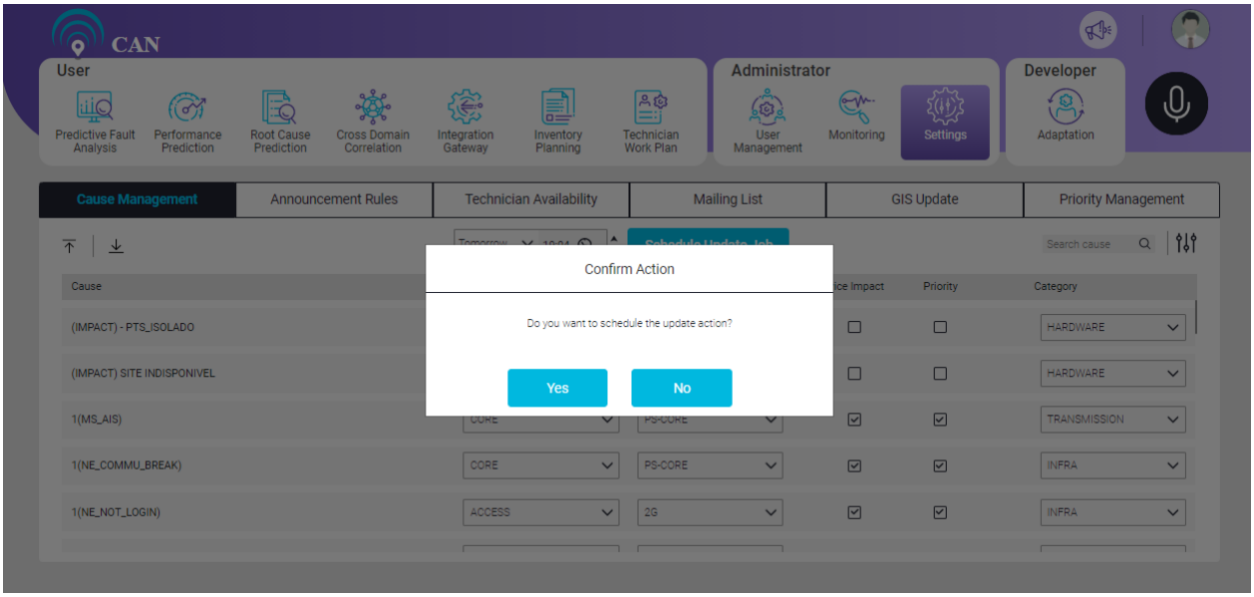


Figure 13.4 - Confirm Action for Schedule Update Job

User can schedule the job only after 10 minutes from the current time otherwise a message "**Please select appropriate time with at least 10 minutes ahead from the current time**" will appear on the screen.

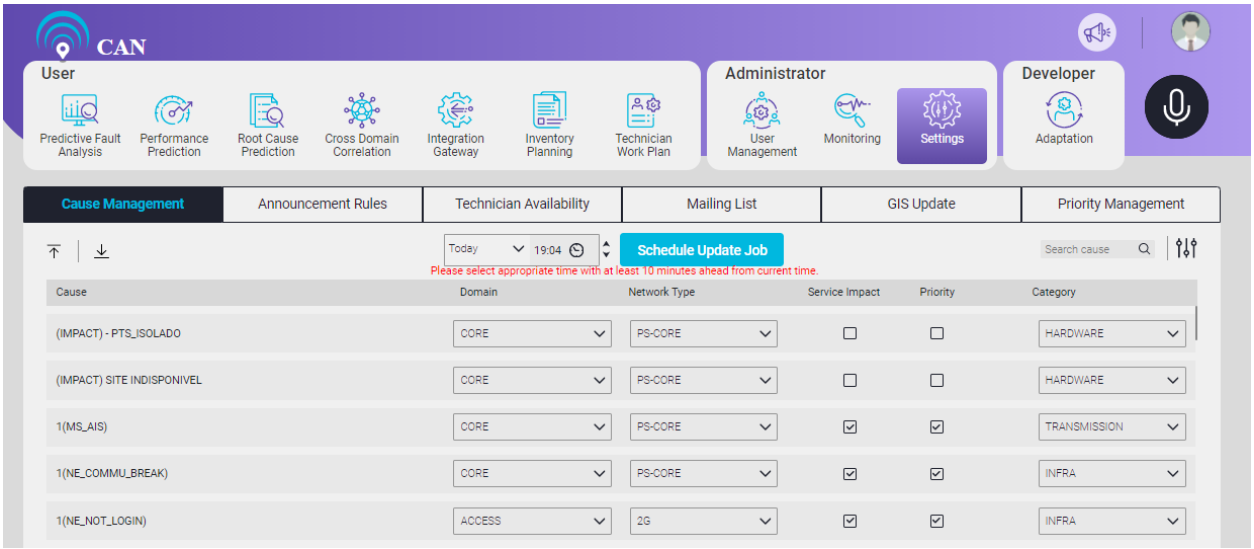


Figure 13.5 - Schedule Update Job

Announcement Rules

This screen is useful at NOC for administrators and network fault resolution team to get real time notifications/announcements of the major and top priority predicted faults. This is a focal point for network troubleshooting, supervision, monitoring and management. This screen is maintained in order to create rules to exclude certain predicted faults for the announcements.

User can create and modify the rules in the same way as that of Alarm Exclusion Rules screen.

User can use the **Search** text box to search any particular Rule applicable to Announcement Exclusion.

User can use the Reorder icon or to reorder the Rules up or down as per the priority. User can decide the Priority of the Rule.

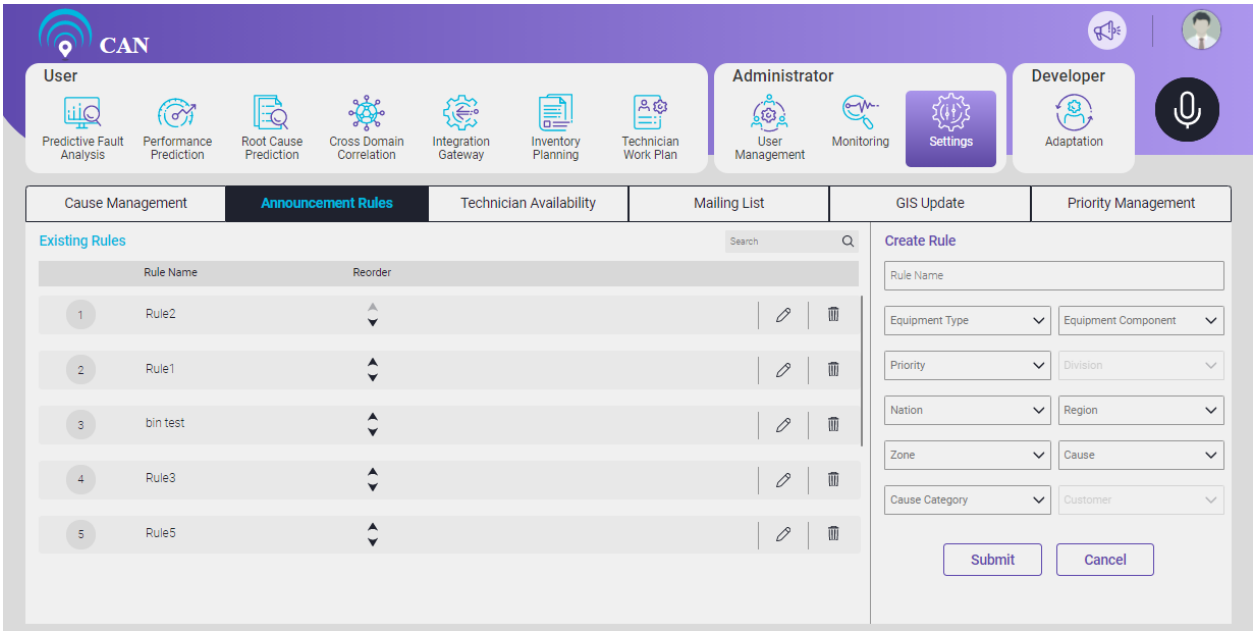


Figure 13.6 - Reordering the Rule

To Create New Rule

1. Go to **Create Rule** section, write the Rule name in the **Rule Name** text box.
2. Select the **Equipment Type**, **Equipment Component**, **Priority**, **Division**, **Nation**, **Region**, **Zone**, **Cause**, **Cause Category** and **Customer Information** from the drop down menu.
3. After selecting the appropriate components, click the **Submit** button to create a New Rule.

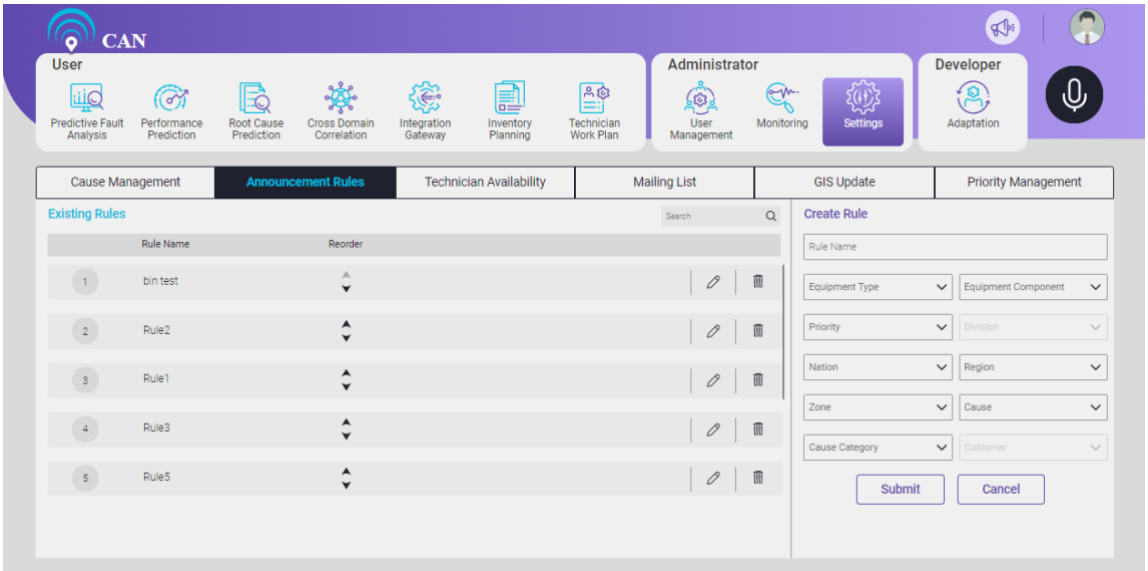


Figure 13.7 - Rule Configuration for Announcement Exclusion

To Edit the Existing Announcement Rule

1. Under Existing Rules section, click the edit icon .
2. Update the **Equipment Type**, **Equipment Component**, **Priority**, **Division**, **Nation**, **Region**, **Zone**, **Cause**, **Cause Category** and **Customer Information from the drop down** as required.
3. Click the save icon to save the changes.
4. Click the delete icon to delete the **Existing Rule**.

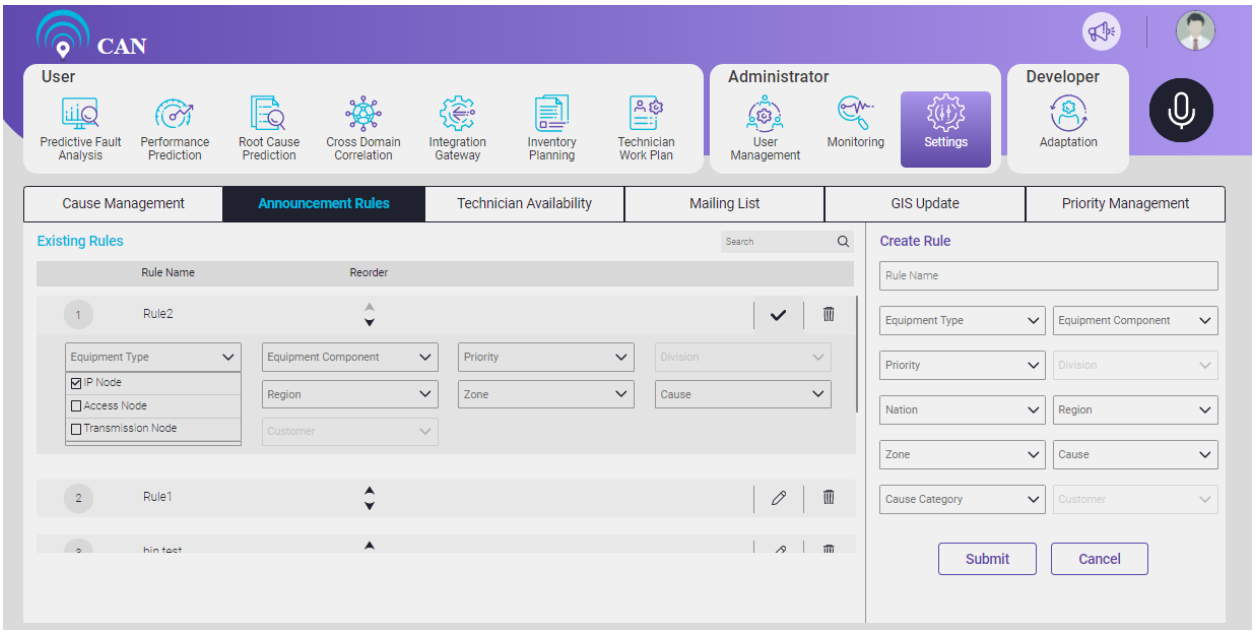


Figure 13.8 - Editing Existing Rules Configuration

Technician Availability

This screen helps to check the availability of technicians. A list of technicians is available here along with their type - either External or Internal - with their ids. User can search specific technicians in the Search bar. The toggle switch gives the real time availability of the Technician. The availability of the technician can be updated with the toggle switch.

User can use the **Search** text box to search the technician with his name or ID.

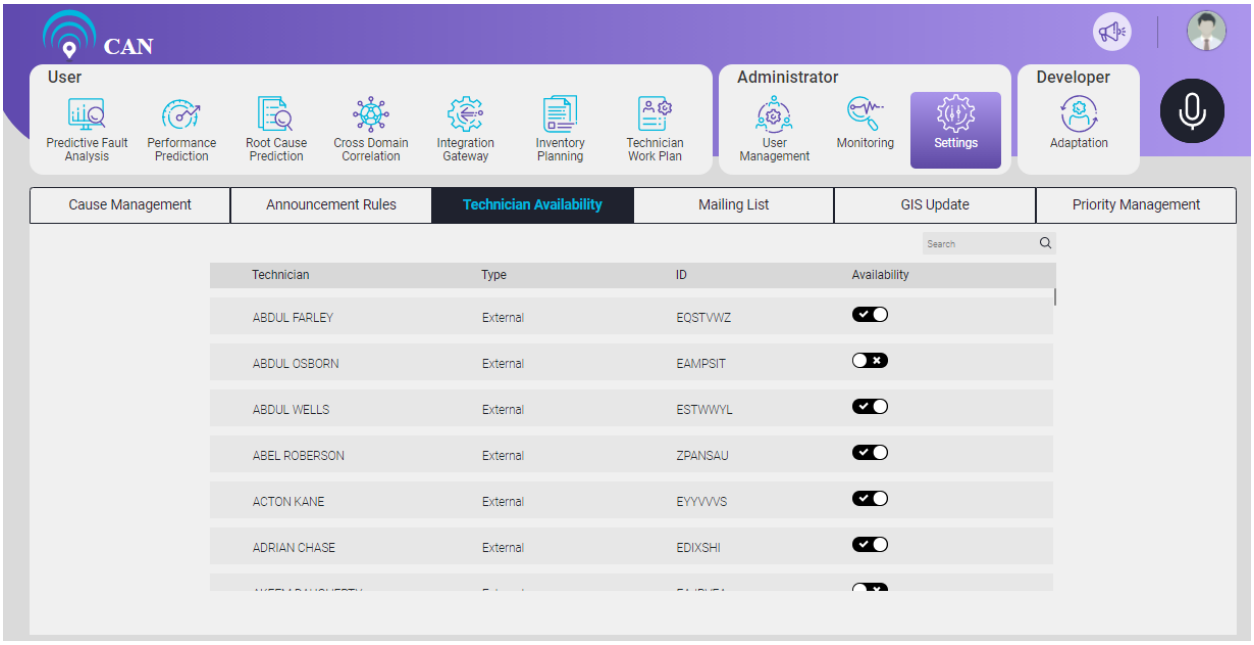


Figure 13.9 - Technician Availability Screen

Mailing List

Mailing list comprises of the groups with individual email ids of the end users, responsible to act on the Predicted Faults. Other important application related mails will also be sent to this mailing list.

To Create New Mailing Group

1. Go to **Create Group** section, Write the Group Name in the **Group Name** text box.
2. Add the new id in the next text box, Click add icon ⊕ to add new id.
3. Click the **Submit** button to add the New Group name.

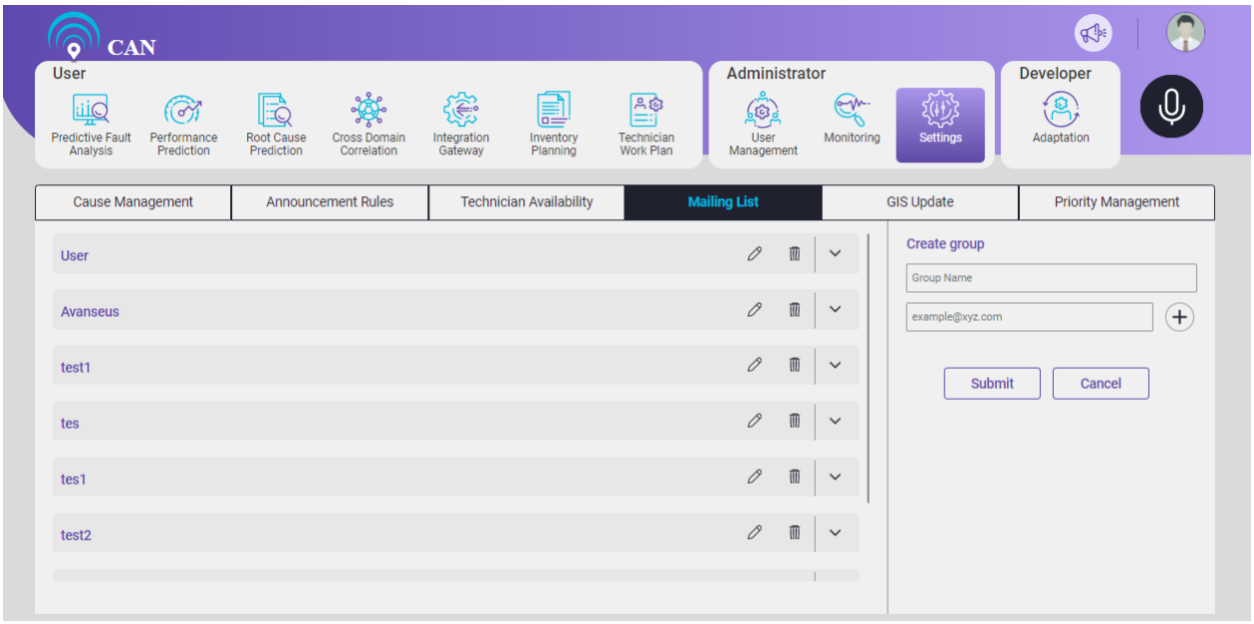


Figure 13.10 - Mailing List

To Edit an Existing Mailing Group

1. Click the edit icon .
2. Write the Email id in the text box.
3. Click the **ADD** button to add the email id.
4. Click the save icon to save the changes.

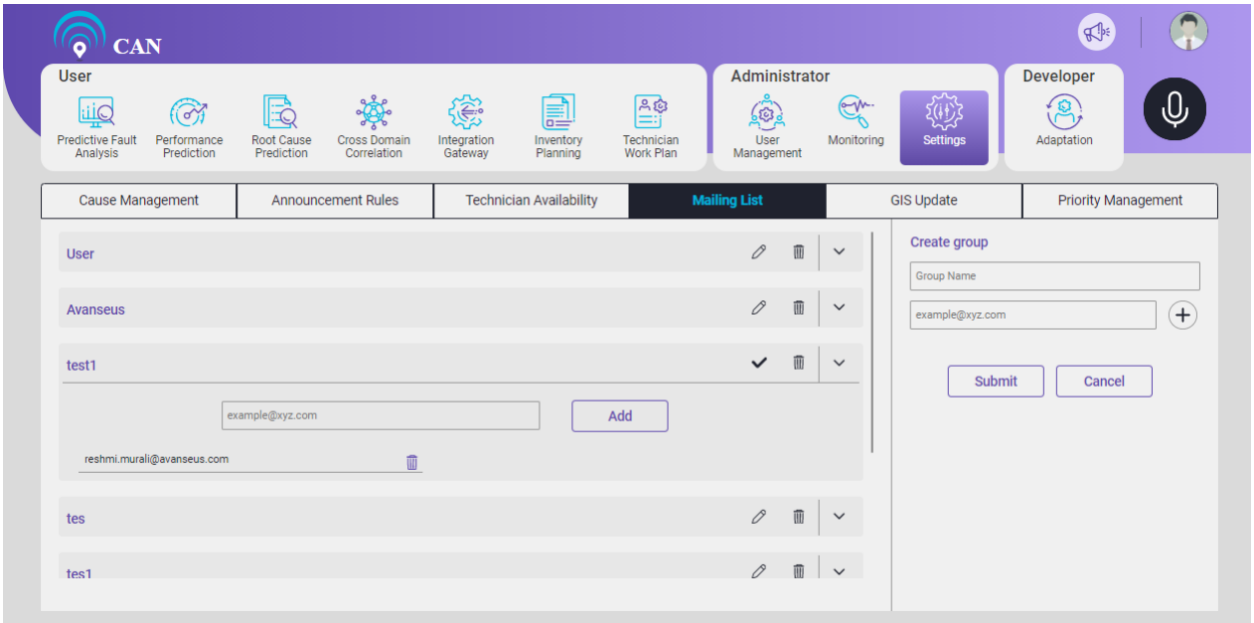
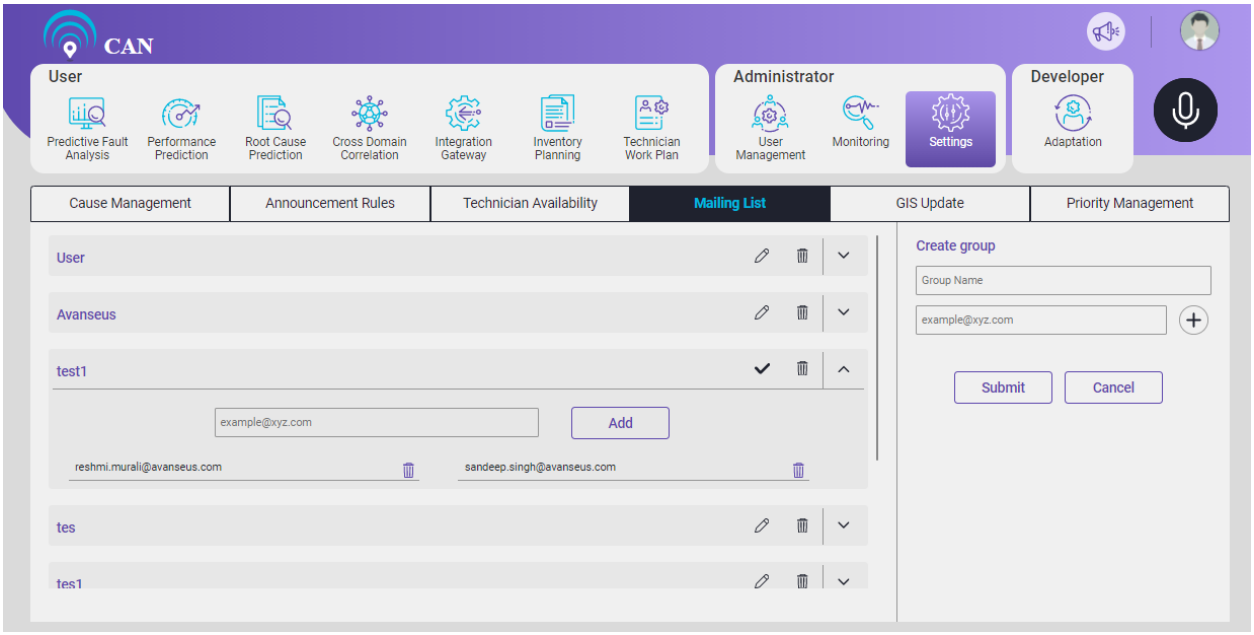


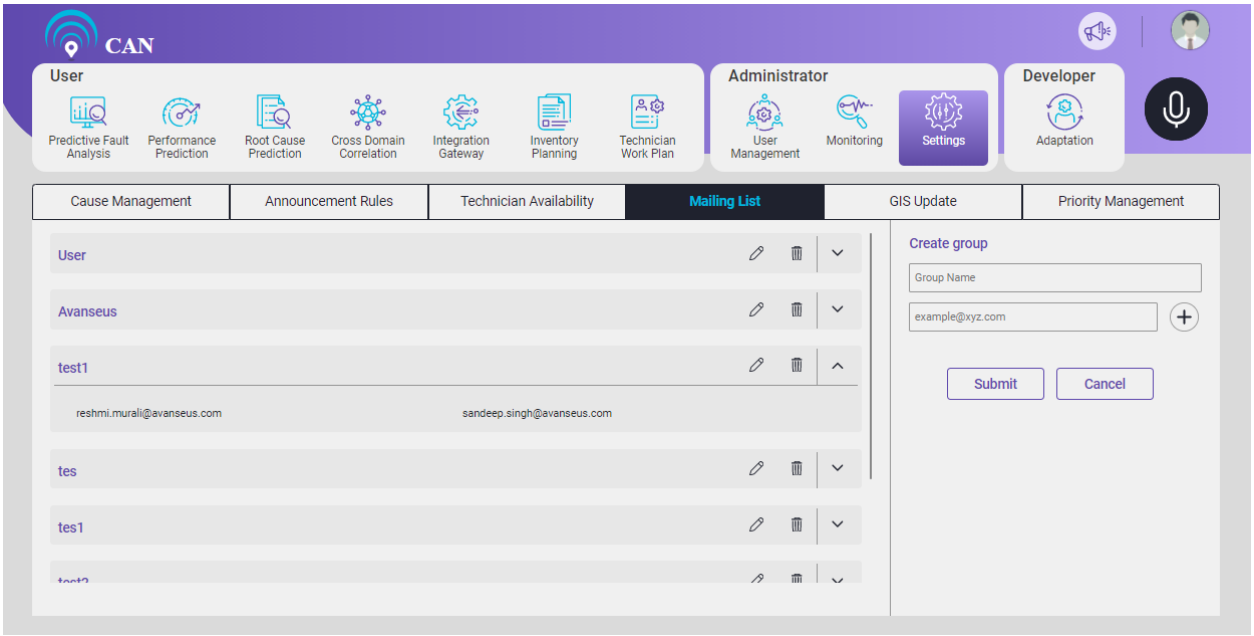
Figure 13.11 - Mailing List Edit Section

5. User can add multiple mail id's in one Mailing list. User can click the delete icon to delete the newly added email id or the existing mail id. Click the save icon to save the changes.



Click the delete icon to delete the **existing Mailing List**.

Click to see the details of the Mailing List.



GIS Update

This screen helps to view and configure the equipment along with appropriate Latitude and Longitude. These (Latitude and Longitude) must be valid as per the geo-coding API. The first column displays the list of equipment and one can scroll down to access the entire list.

User can use the **Search** text box to search any Equipment Component.

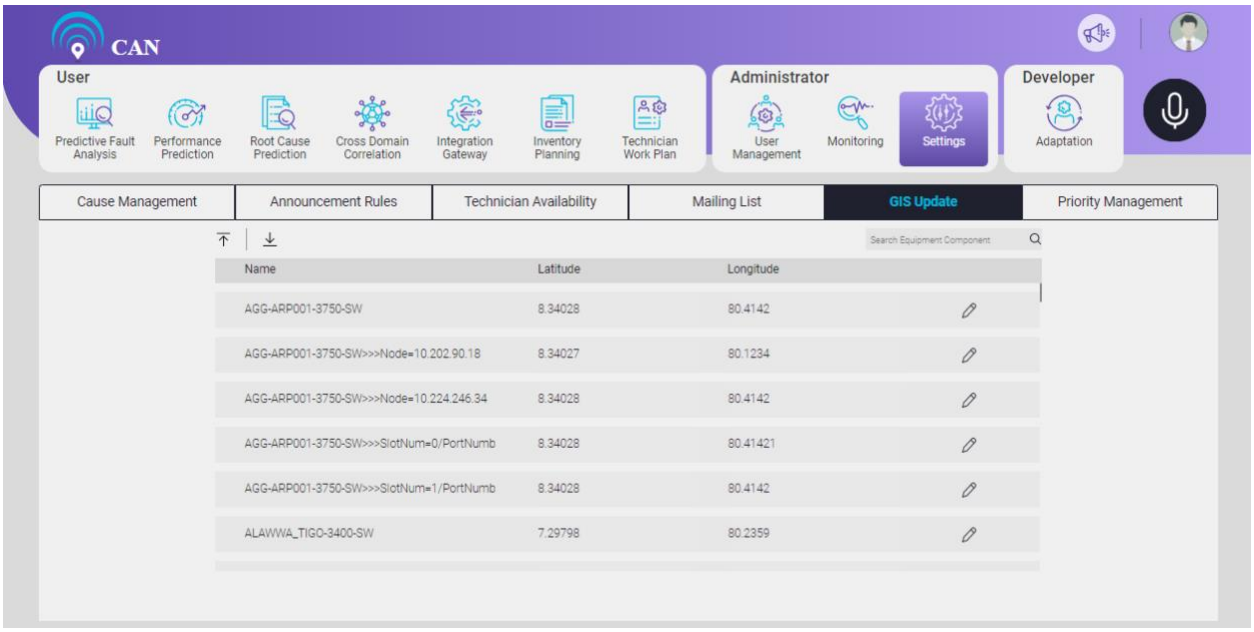


Figure 13.12 - Equipment Component Configuration

To edit any of the equipment details, click the edit icon . User can only edit the Latitude or Longitude.

To download the equipment details, click the download icon .

To upload or update equipment details, click the upload icon . Either select the file from a location or drag and drop the file.

Note:

- **First sheet of the file should have EQUIPMENT COMPONENT, LATITUDE and LONGITUDE as headers.**
- **File size should not exceed 50MB**

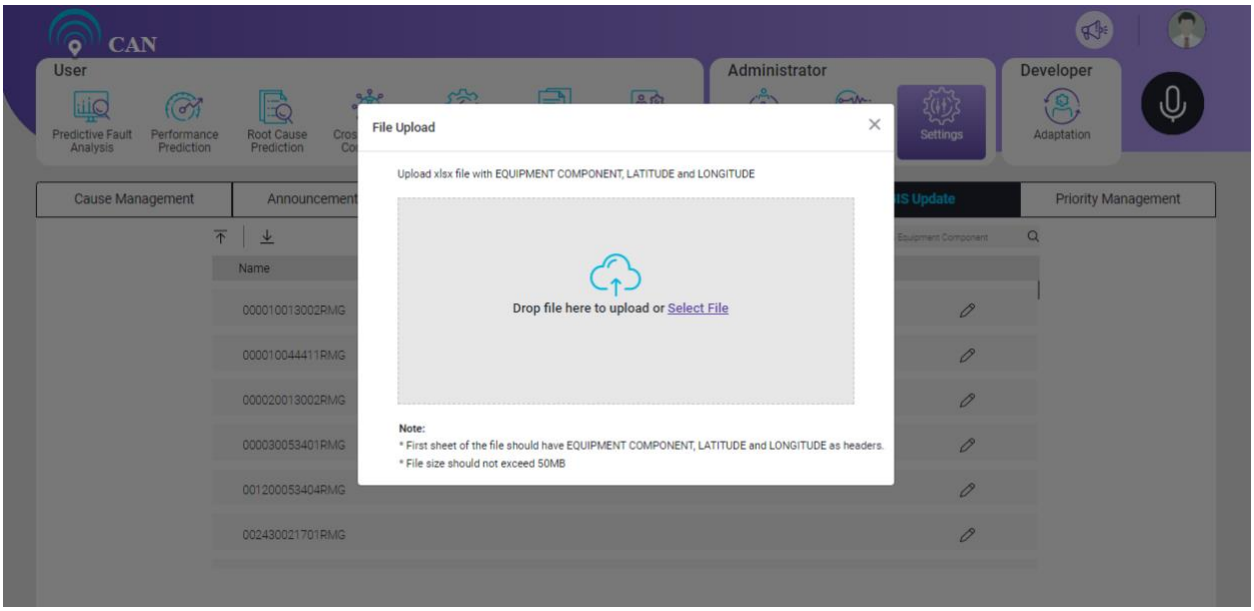


Figure 13.13 - Uploading/Updating Equipment Details

Priority Management

This screen helps to prioritize the Site Priority for the office codes.

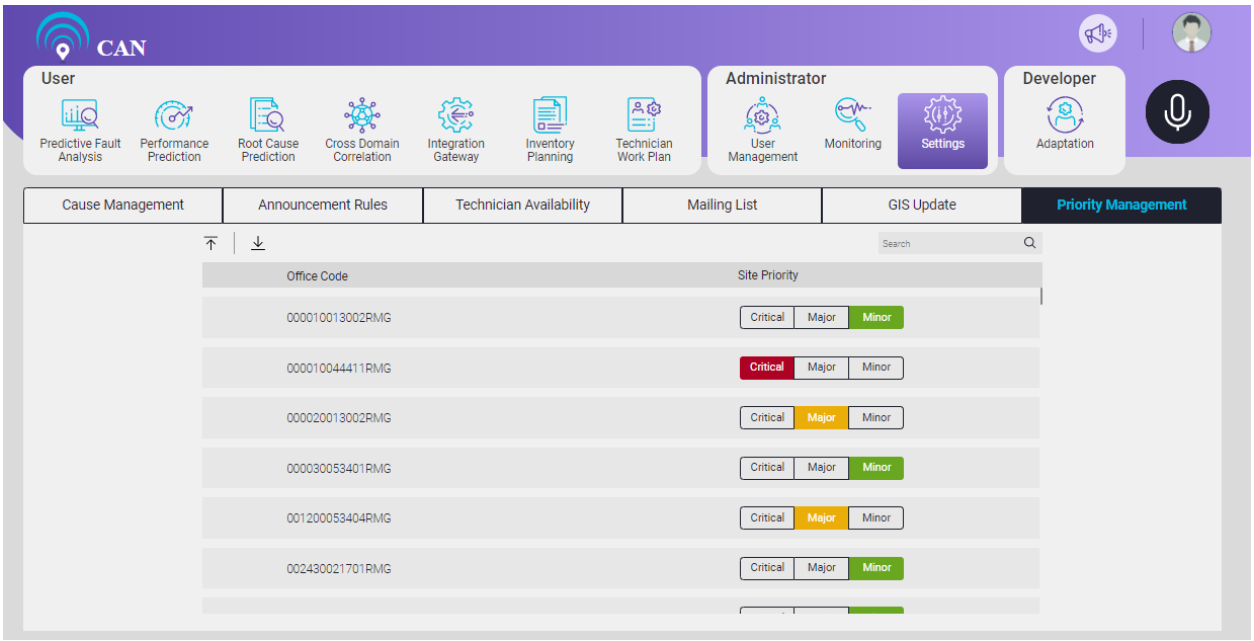


Figure 13.14 - Priority Management Screen

The first column displays the list of office codes and second column displays the corresponding site priority. User can scroll down to see the entire list.

User can use the **Search** text box to search any particular office code name or any particular site priority.

To update the site priority, click the appropriate category. “**Critical**” will be marked in red, “**Major**” will be marked in yellow and “**Minor**” will be marked in green.

To download the office code list with the corresponding site priority, click the download icon .

To update multiple site priorities, click the upload icon . User can select a xlsx file from a location or drag and drop the xlsx file.

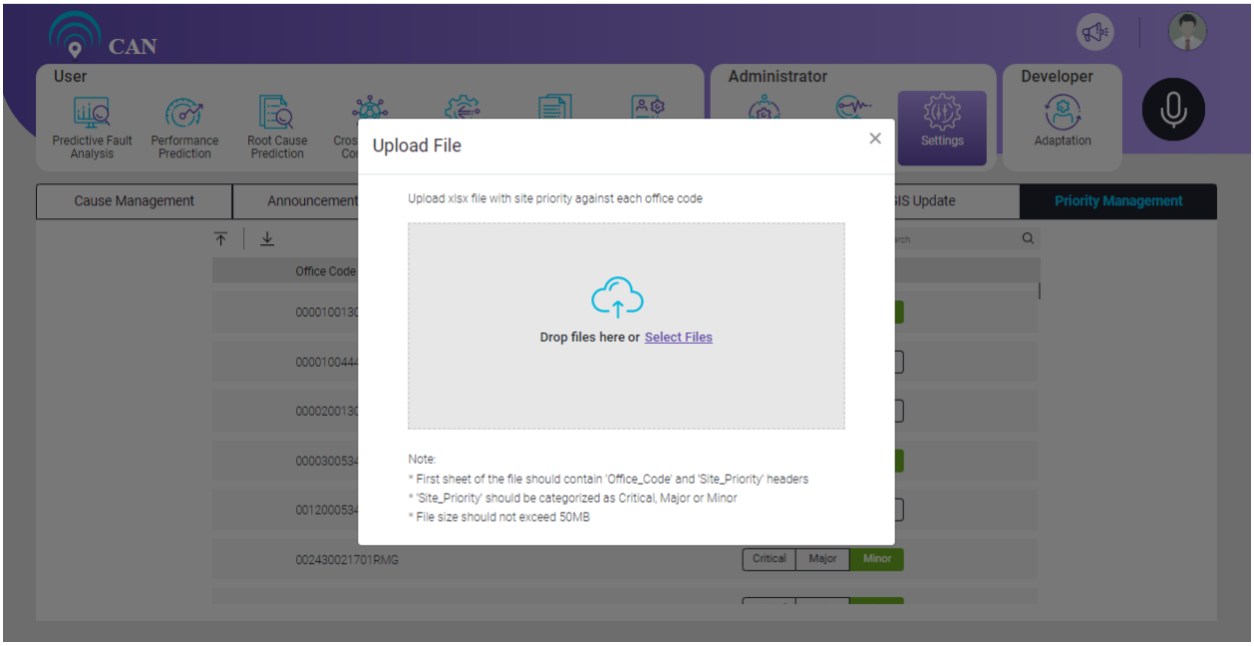


Figure 13.15 - Upload File Option

Note:

- **First sheet of the xlsx file should contain Office_Code and Site_Priority headers.**
- **Site_Priority should be categorized as Critical, Major or Minor.**
- **File size should not exceed 50MB.**
- **If the file contains error entries, those entries will appear in the upload pop up. User can view and download the file with error entries.**

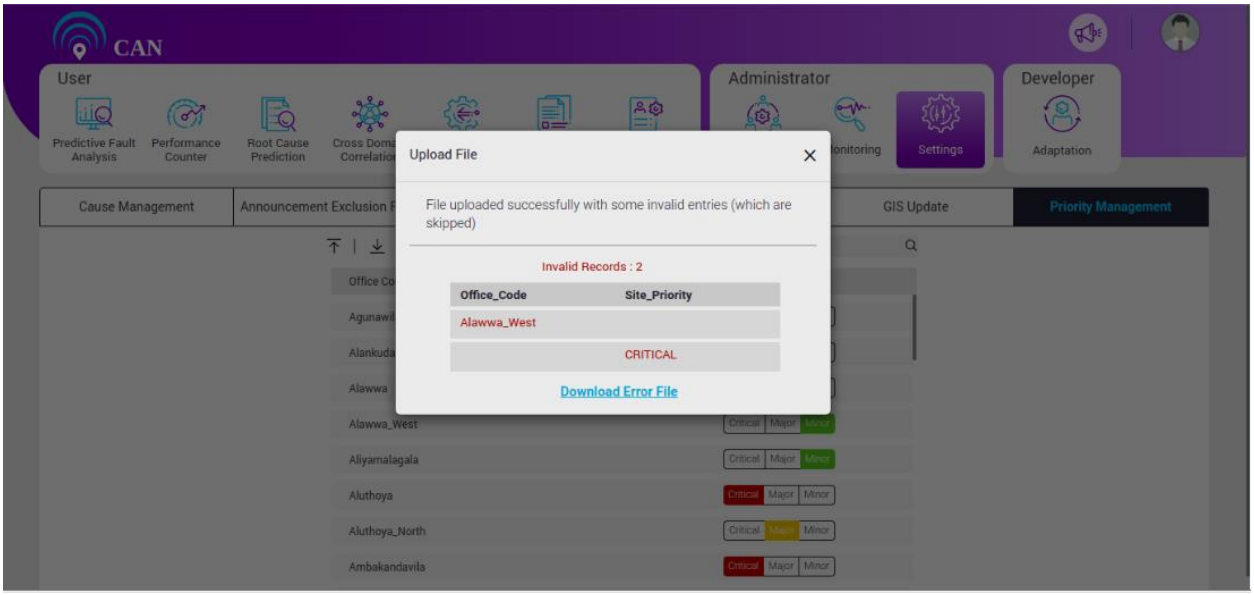


Figure 13.16 - File Uploaded with some Invalid Entries

Page Intentionally Left Blank

14. ADAPTATION

Adaptation helps to integrate new data sources and refine prediction output based on expert knowledge. The features of the Integrated Development Environment are:

- Java code syntax validation
- Java code keywords coloring
- Java code compilation on the fly
- Displaying errors in-line with the code & overall status of the code compilation in top right corner
- Highlighting tokens when the cursor is moved on them
- Auto-completion of API methods when dot operator is used on pressing Ctrl+Space
- Auto-indentation of code on pressing Ctrl+I
- Feature where template code is made non-editable.

The **Adaptation** screen has below tabs:

- Parser - User can set the Configurations related to loading client data files here. Three options fall under this category.

  1. Pre-processor
  2. Parser
  3. Post-processor

- File Collection & Configuration - User can set the Configurations required to pull files from remote sources.
- Prediction Assignment - It is used for prediction load distribution.
- Filter Configuration - User can configure the rules to filter and optimize predictions here.
- Post Prediction Process - User can upload the customizable code to be executed post prediction.
- Report Configuration - The result of Prediction in Excel format is made configurable.
- Advanced configuration - Developer related Configurations.
- Alarm Inclusions/Exclusions - Allows user to configure alarm filters.
- Resource Configuration - Allows user to upload master data files which can be later used to fetch some information.
- ROE Configuration - It helps to identify the root cause of a prediction based on multiple alarm parameters.
- Performance Configuration - Performance Configuration gives information on threshold configuration based on the KPI's.
- Integration Configuration - It is to integrate CAN with 3-party software (BMC Remedy, Weather Integration and Splunk).

Input Mapper

Input Mapper has three tabs:

- Pre Processor
- Parser
- Post Processor

Pre-Processor

Pre-Processor screen is used to process the data before mapping it to CAN field. This is helpful when some data needs to be excluded from data load or some input data value needs to be modified before mapping it to CAN field.

To save a pre-processor user need to give name and description and write a java code (similar to that of writing Parser Java code) inside the text area.

This code will implement IPreprocessor interface which provides record object as parameter. Record object is a key value pair of header name (In case there is no header name, its convention starts with 0 as 1st column,1 as second column and so on) and header value.

User can see a list of saved pre-processor Configurations at the right top corner.

By default, Pre-processor is in edit mode.

Click the SampleProcessor on the right side of the screen.

The orange tick on the screen describes the warnings in the code. Click the **Update** button to update the changes in the code. User can hover on the orange tick to see the Error, Warning and Info details of the code.

User can click the **Save** button to save the code with warnings.

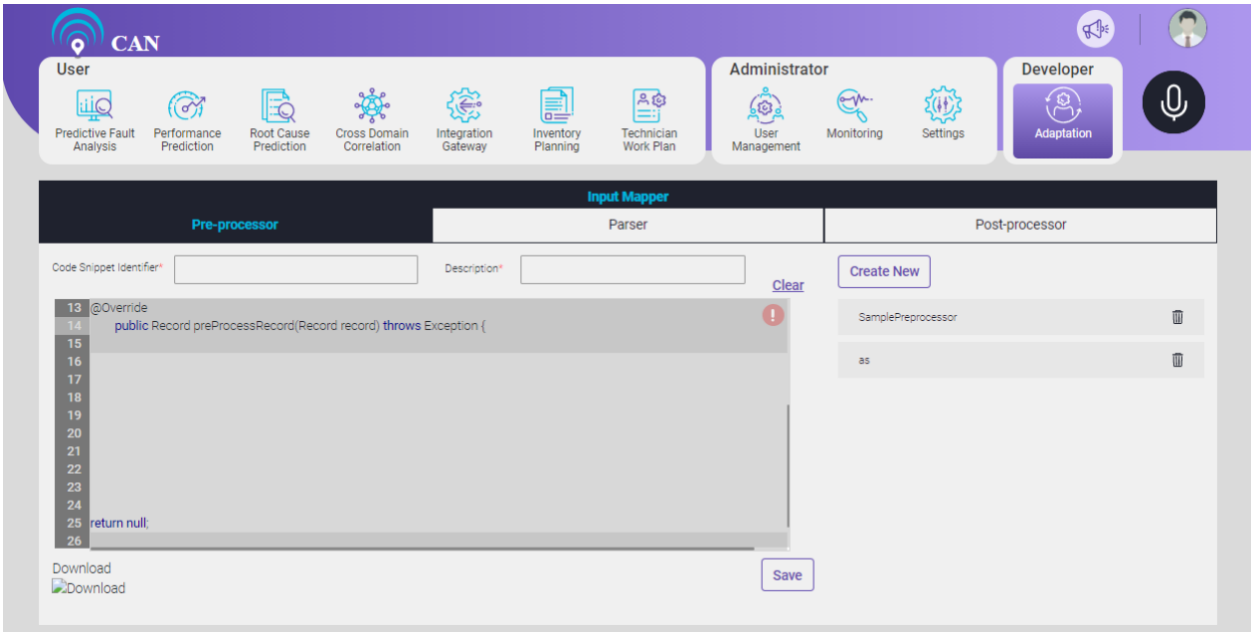


Figure 14.1 - Pre Processor Screen with Warnings

The red color exclamatory mark on the screen describes the Error in the code. User can hover on the red exclamatory mark to see the number of Errors in the code.

The **Update** button gets disabled in case of the error in the code.

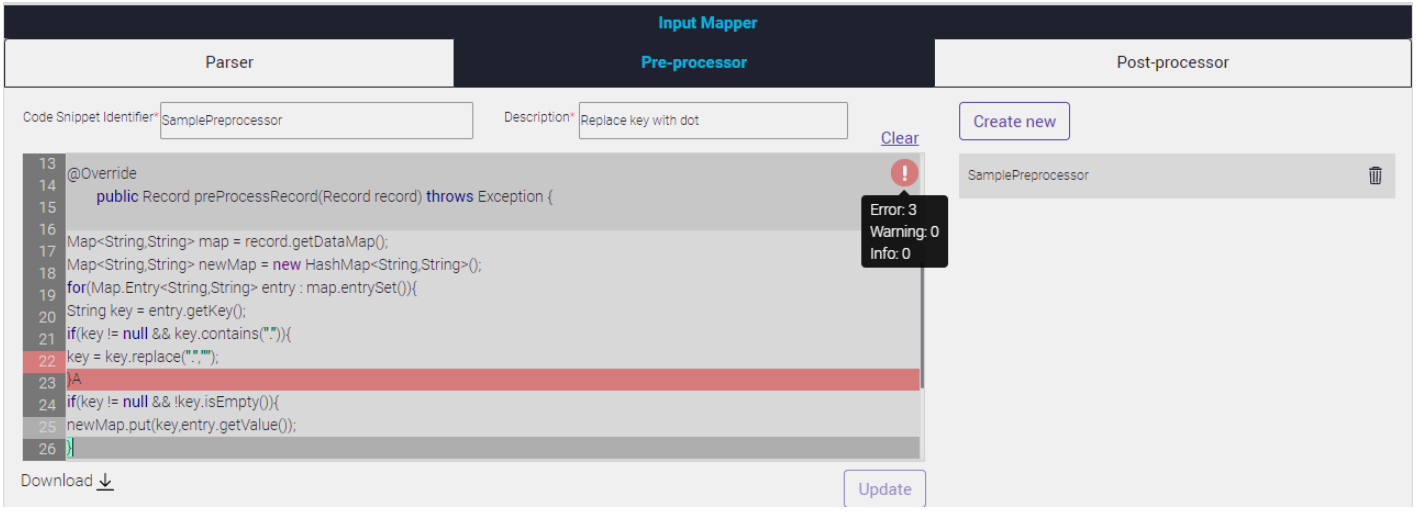


Figure 14.2 - Pre Processor Screen

User can hover on the errors and can see the details of the error. User can also edit and delete the error.

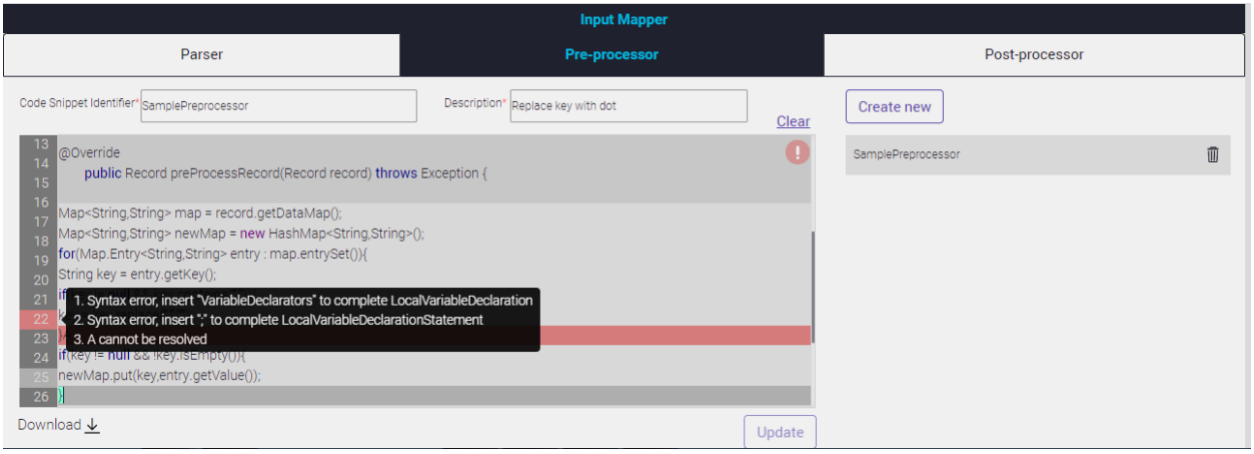


Figure 14.3 - Pre Processor Screen with details of Error

To Create a New Pre-Processor Configuration

1. Click the **Create New** button.
2. Write the **Name of the Code Snippet Identifier** and its **Description** in the respective text boxes.
3. Write the suitable code for the Pre-Processor Configuration.
4. Click the **Save** button to save the new Pre-Processor configuration.
5. To delete the Saved Configurations, click the delete icon .

Parser

Parser is available under the Adaptation Screen on the main home screen. Its function is to map the client input data with the CAN model. These two data structures need to be in sync to generate the results. A client input data file should be synced with the CAN fields.

The data sources are: Alarm, Ticket, Work order, Performance Counter, Splunk and others.

To Add New Parser Configuration

1. Click the **Add New Mapping** button.
2. Fill all the details in File Level Info. File level Info contain fields that includes Name, Description, Pre-processor, Post-processor, Page size, Header, and File Type specific details.
3. The usual format of File Type is XLSX, DELIMTED, CUSTOMDELIMTER, CUSTOM.
    - In XLSX file type, Sheet Names should be specified. Add multiple sheet names and separate them with colon (:). Empty Sheet names field will consider all the sheets in the file.
    - In DELIMITED file type, Delimiter (single character that separates 2 columns) and Escape Character fields needs to be recognized from input file and set accordingly. Row delimiter in this case is by default new line character (\n).
    - In CUSTOM file type, a popup provides an option to upload java file. This java file must contain code for parsing custom files formats. This code implements ICustomFileParser interface.
    - In CUSTOMDELIMITER file type, column delimiter (multiple character that separates 2 columns), row delimiter (multiple character that separates 2 rows) and escape character needs to be set.
4. Page size defines batch size of records to be parsed at once while parsing input data.
5. Pre-processor and post-processor is auto completed that already have existing pre and post processor Configurations.
6. Set the toggle button  to select the Header in the file.
7. Besides the File level info, a tabular view is present which helps in mapping client data with CAN conventions. This contains Mapping Name and CAN Fields under Mapping Fields. Mapping Names are the header names found in input files. CAN Fields are standard conventions maintained in CAN. These configurations are customizable and can be added or deleted as per client requirements.
8. User can add additional CAN fields in the table. To add the additional CAN field in the table, click the 

button. The screen displays a pop-up of standard CAN fields for selected data source, user can select the appropriate field. If input parsing requires a new field that is not part of standard CAN fields, user can add new field i.e. custom fields. To add custom field, click and select the Custom option in CAN field pop-up.

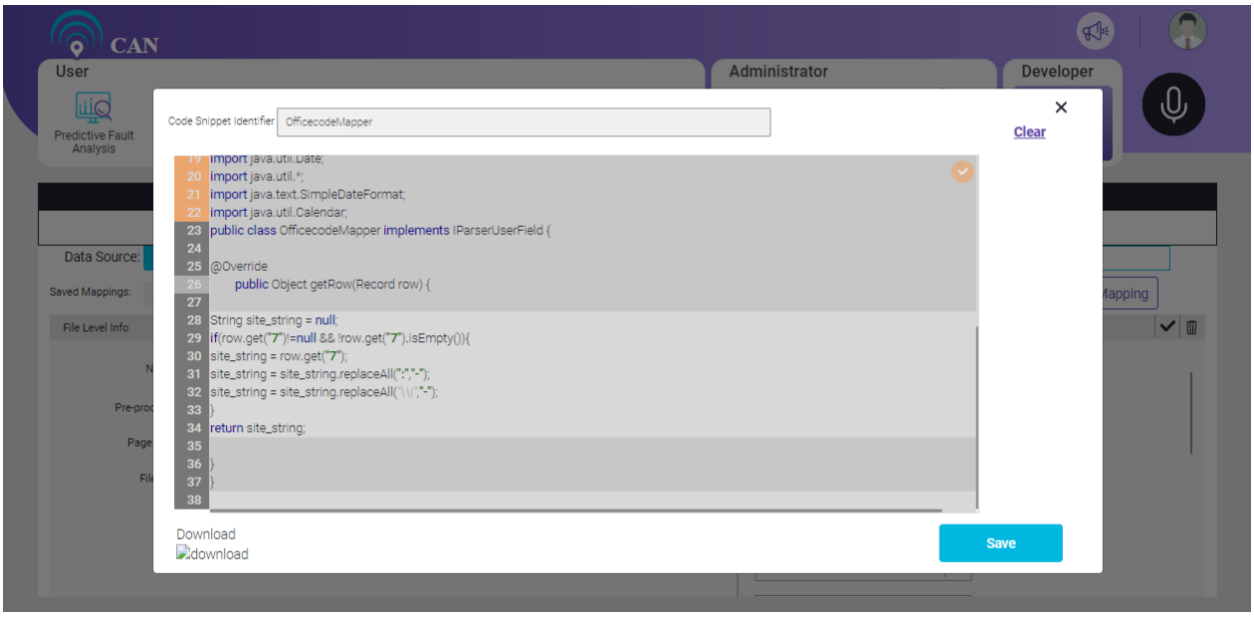
To Edit the Existing Mappings:

1. Click the edit icon  beside the Mapping fields. All the fields of File Level Info and Mapping fields are now available for editing.
2. Click the edit icon  on the Mapping Name column, a pop up opens up on the screen. User can write the corresponding java mapping code in the text area. It will automatically get compiled. The

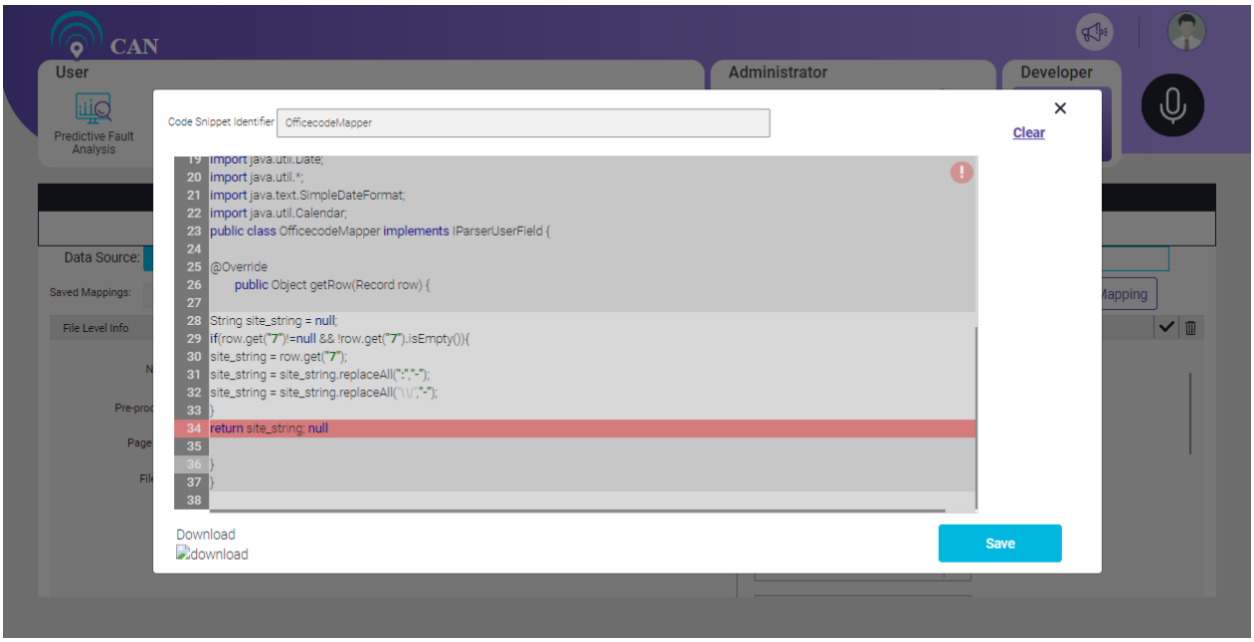
green tick on the right side of the screen confirms the correct code. The code will automatically compile. To save the code, click the **Save** button.

3. Click the save icon ✔ to save the New Mapping. In case, user is editing the existing mappings this icon ✔ will appear as Update icon.

Note: User can also download the code. To download the code, click the download icon Download **.**



In case the code is not correct then the screen will show the exclamatory mark in orange color. This represents error in the code. The **Save** button will get disable and will not allow user to save the code. User need to delete the error in order to save the code.



To delete the existing parser configuration within Saved Mappings section, click the delete icon.

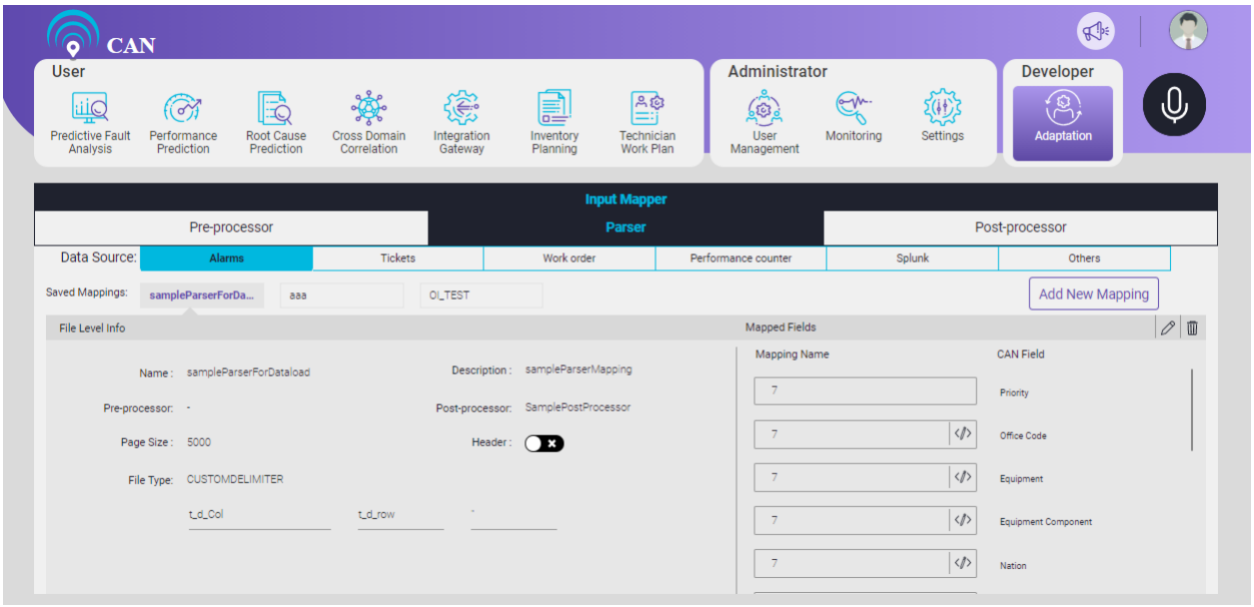


Figure 14.4 - Parser Screen

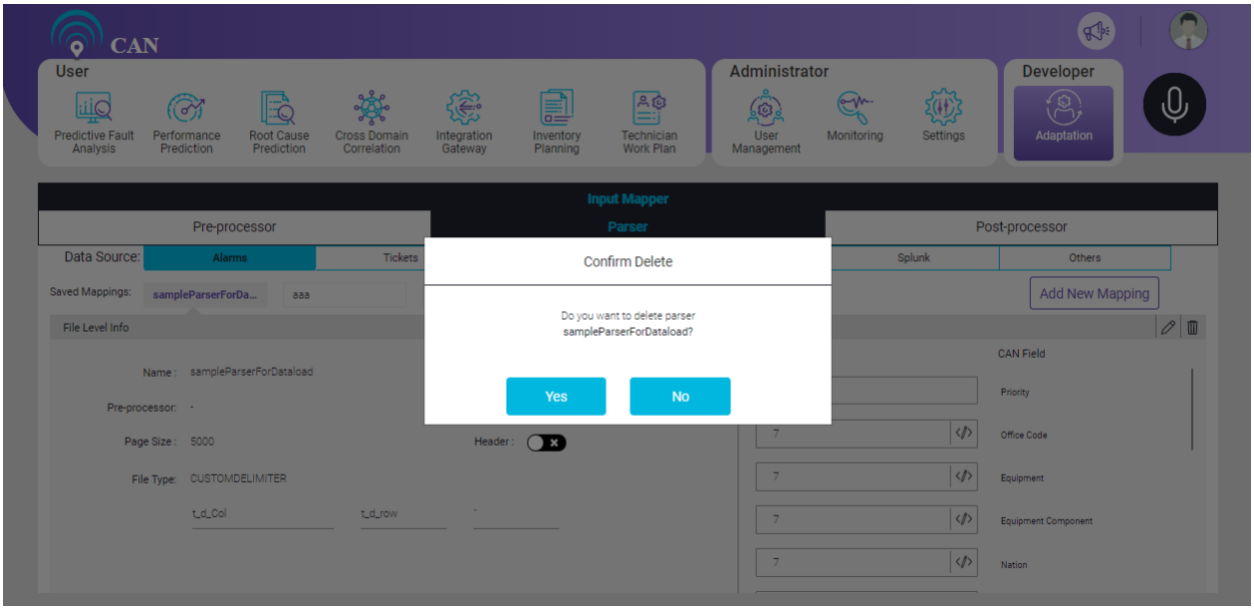


Figure 14.5 - Parser Screen to Delete the Configuration

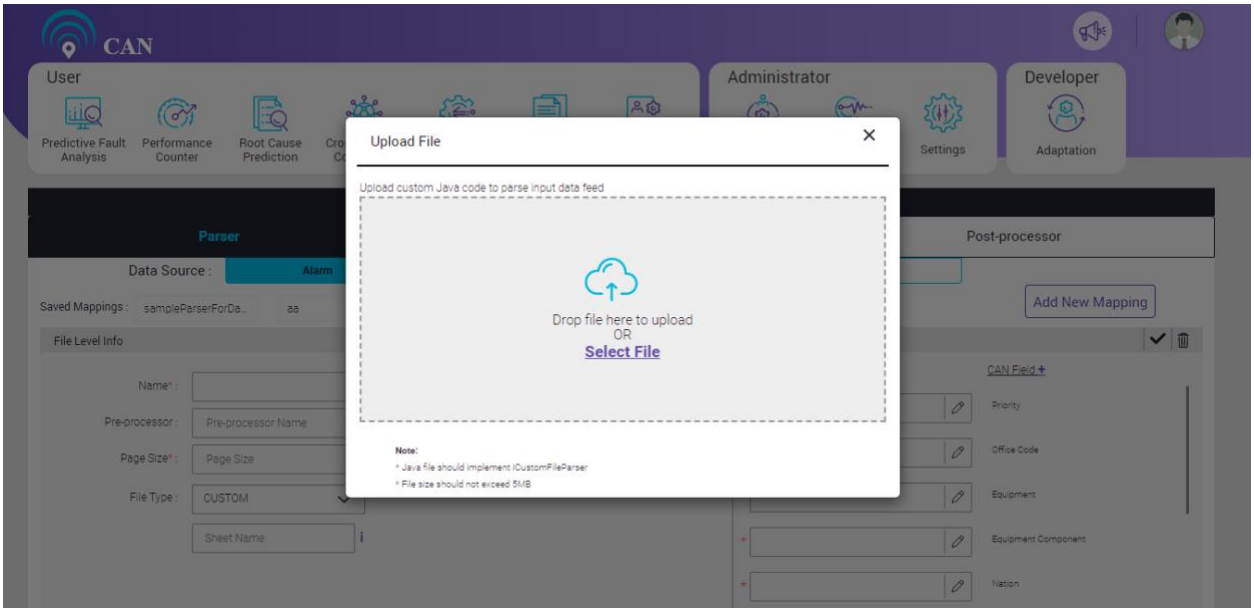


Figure 14.6 - Custom File Upload

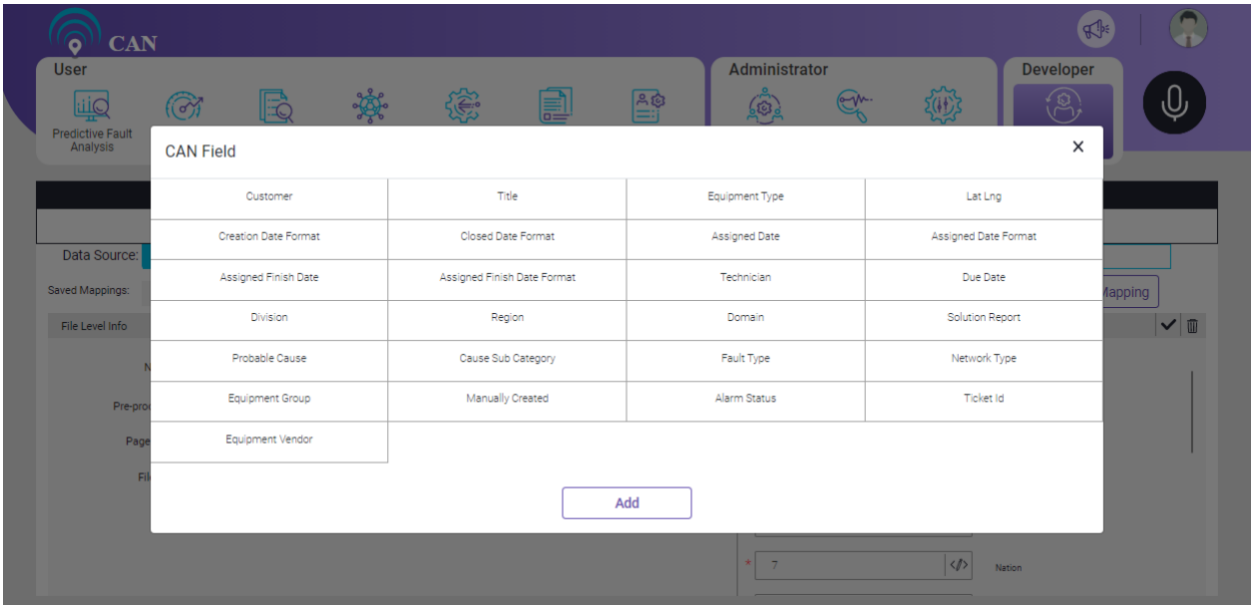


Figure 14.7 - CAN Fields

Post-Processor

Post-processor is used to modify or discard the data after parsing and just before loading of the data.

Post Processor screen looks and functionality is almost similar to Pre Processor screen.

Code snippet written here will implement IPostprocessor interface which provides a map of troubleTicket object as parameter.

By default, the Post processor will be in edit mode.

The red color exclamatory mark on the screen describes the Error in the code. User can hover on the red exclamatory mark to see the number of Errors, Warnings and Info details in the code.

The "**Save**" button gets disabled, if there is error in the code.

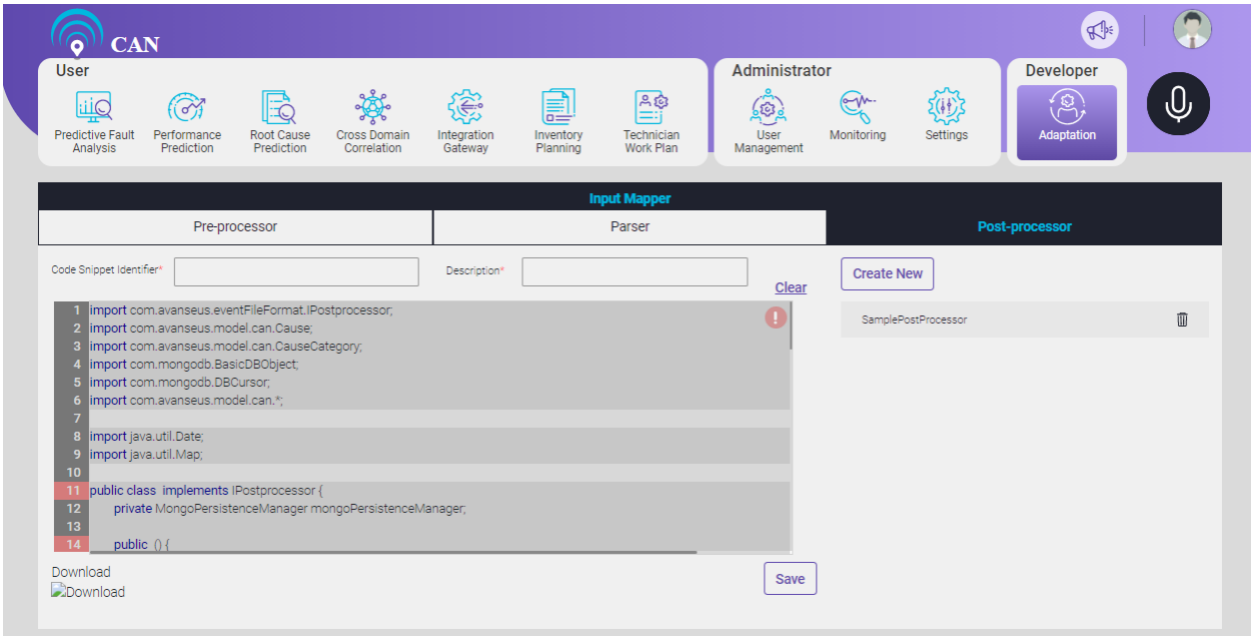


Figure 14.8 - Post Processor Screen with Warnings in the code

User can hover on the errors and can see the details of the error in the code. User can also edit and delete the error in the code.

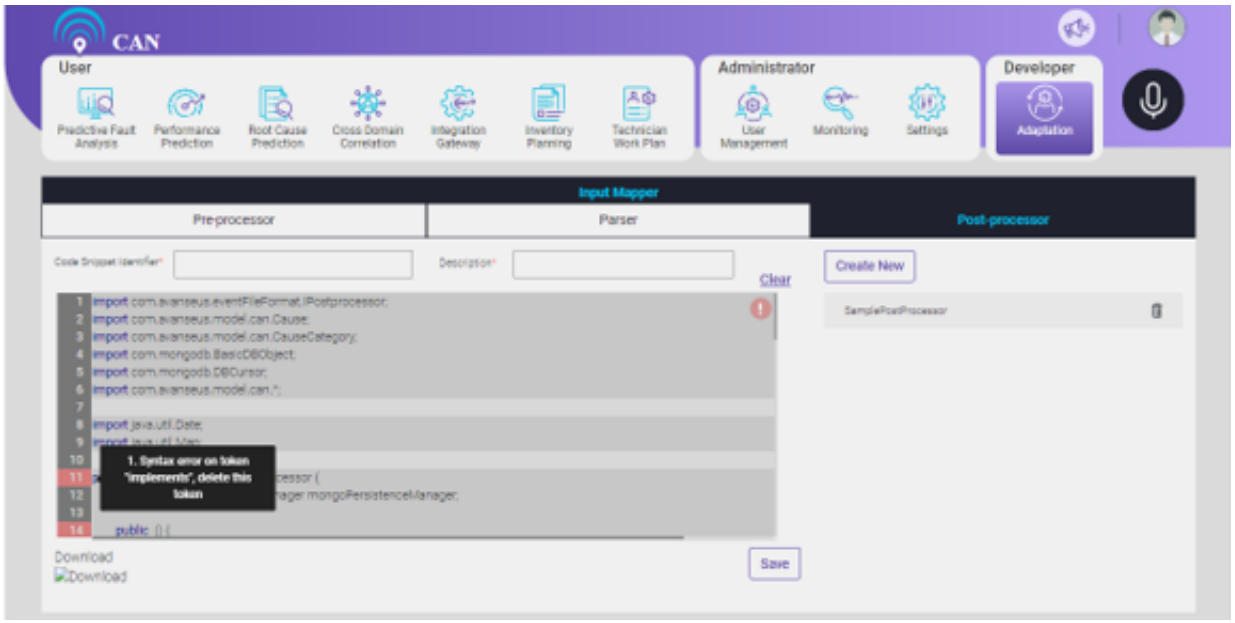


Figure 14.9 - Post Processor Screen with details of Error in Code

To Create a New Post-Processor Configuration

1. Click the **Create New** button.
2. Write the **Name of the Code Snippet Identifier** and its **Description** in the respective text boxes.
3. Write the suitable code for the Post-Processor Configuration.
4. Click the **Save** button to save the new Post-Processor configuration.
5. To delete the saved configurations, click the delete icon .

Data Collection & Configuration

Data Collection screen include configurations that are applicable to collect the data files from the remote source. Remote sources include following interfaces:

- SFTP
- FTP
- GITHUB
- EMAIL
- CUSTOM
- KAFKA

User can add, edit and delete a Data Collection Configuration and also specify the active collection time cron for the next job.

The icons used to indicate the configurations are as follows:

- The active file that perform batch processing (non Kafka) is represented by icon.
- The inactive file that perform batch processing (non Kafka) is represented by icon.
- The active file that perform stream processing (Kafka) is represented by icon.
- The inactive file that perform stream processing (Kafka) is represented by icon.

To Add a New Data Collection Configuration

1. Go to the **Configure New Collection** section on the right side of the screen.
2. Write the File Name in the **File Name** text box.
3. Write the Description in the **Description** text box.
4. Select the appropriate interface from the drop down menu.
5. To activate or de-activate the File Collection status, use the toggle button .
6. Click the **Submit** button to configure the New File Collection.

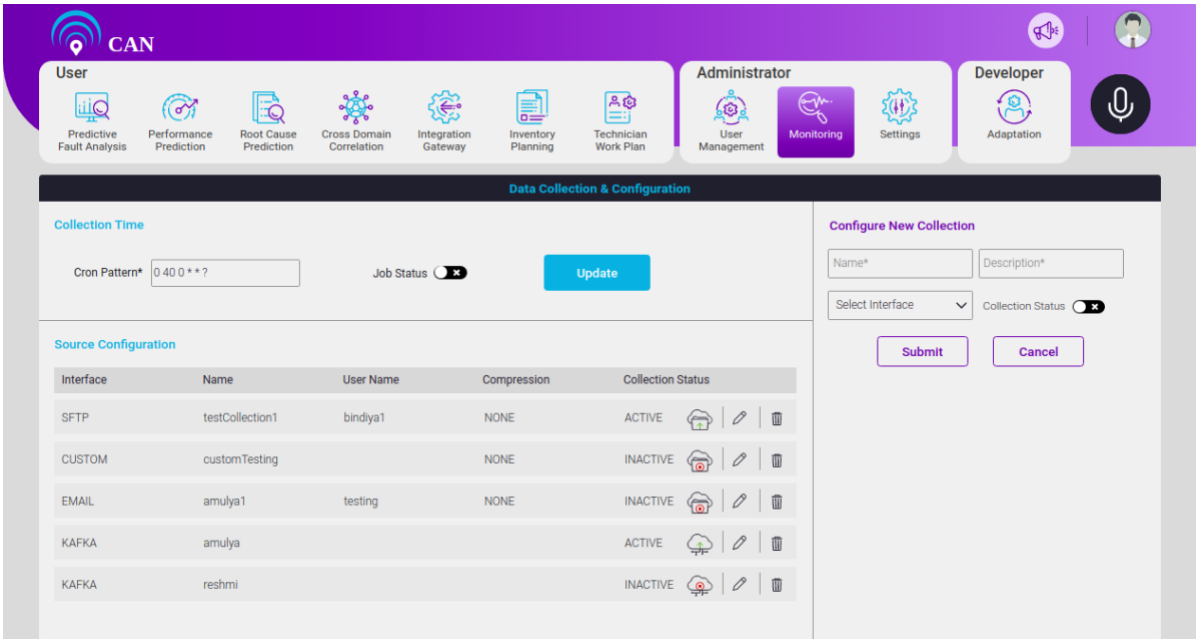


Figure 14.10 - Data Collection Configuration Screen

To Edit the Existing Source Configuration

1. Click the edit icon in the Source Configuration.
2. User can edit the Interface, File Name, User Name, Compression and Collection Station fields.
3. Click the update icon to save the changes. If user will not save the changes, Data Collection Configuration screen will not reflect the changes.
4. To delete the new **Data Collection Configuration**, click the delete icon .

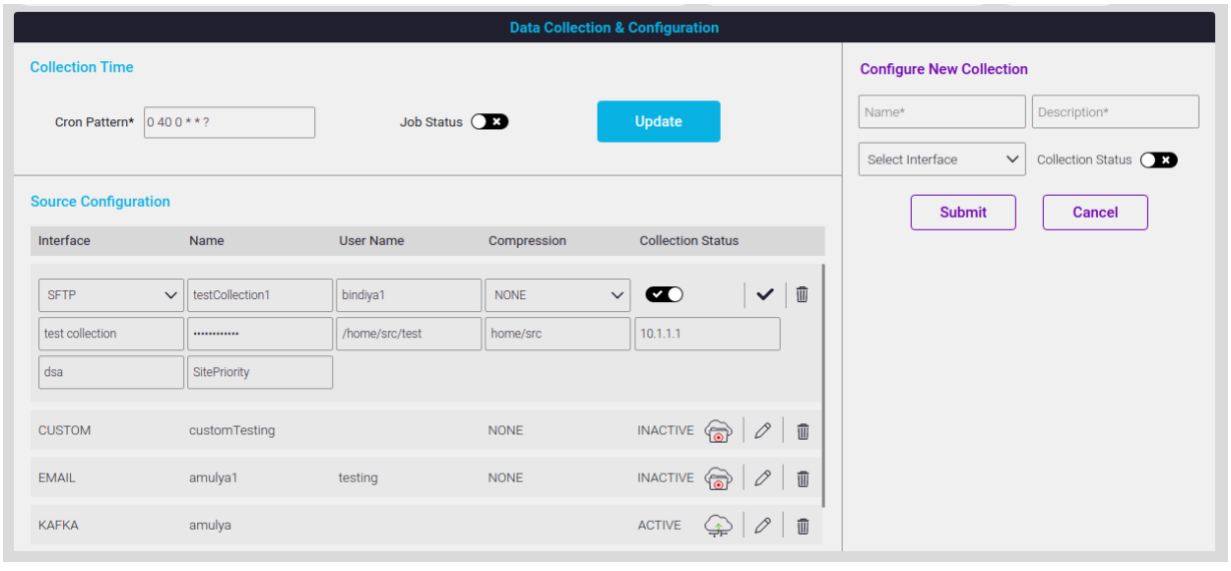


Figure 14.11 - Data Collection Configuration Edit Option

Data Collection Configuration fields that are common to all interface type are as follows:

- User can write the Specific Name and Description for every Data Collection Configuration.
- All of these pre mentioned interface types require authentication information such as Username and Password.
- File name pattern can be regex pattern that will match with multiple files.
- Each configuration is provided with various compression formats such as ZIP, GZ, TAR, TARGUNZIP, TARZIP and NONE. Compressed files will be decompressed before parsing.
- This configuration also requires mapper information to be set that will be autocompleted from the saved parser configurations.

SFTP and FTP

In SFTP/FTP interface, apart from above mentioned fields user must specify IP address of SFTP/FTP location, source root path (relative path of file location on SFTP/FTP) and source archive folder path (relative path of archive folder on SFTP/FTP).

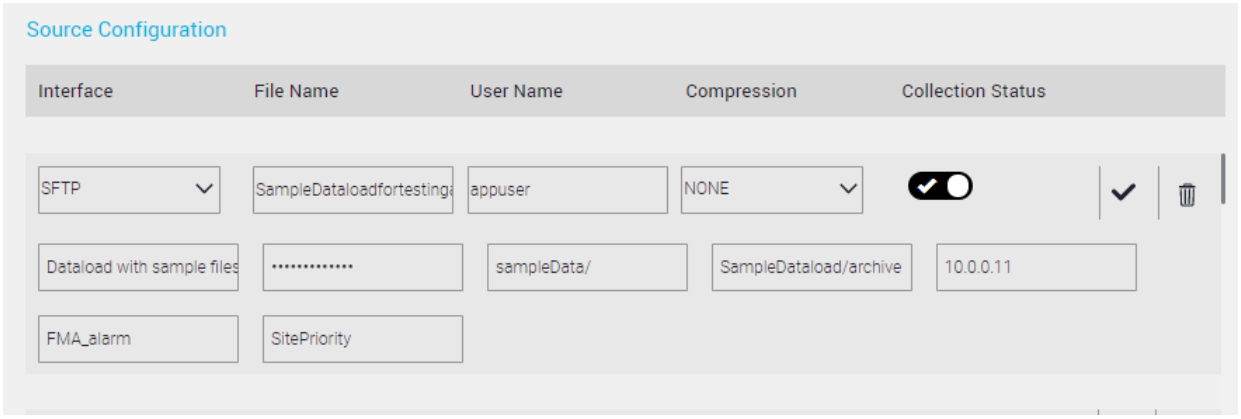


Figure 14.12 - SFTP/FTP Interface Configuration

GITHUB

In GITHUB interface, apart from the above mentioned fields user must specify URL of GITHUB location, source root path (absolute path of file location on GITHUB), source archive folder path (absolute path of archive folder on GITHUB) and source directory (location where git is cloned).

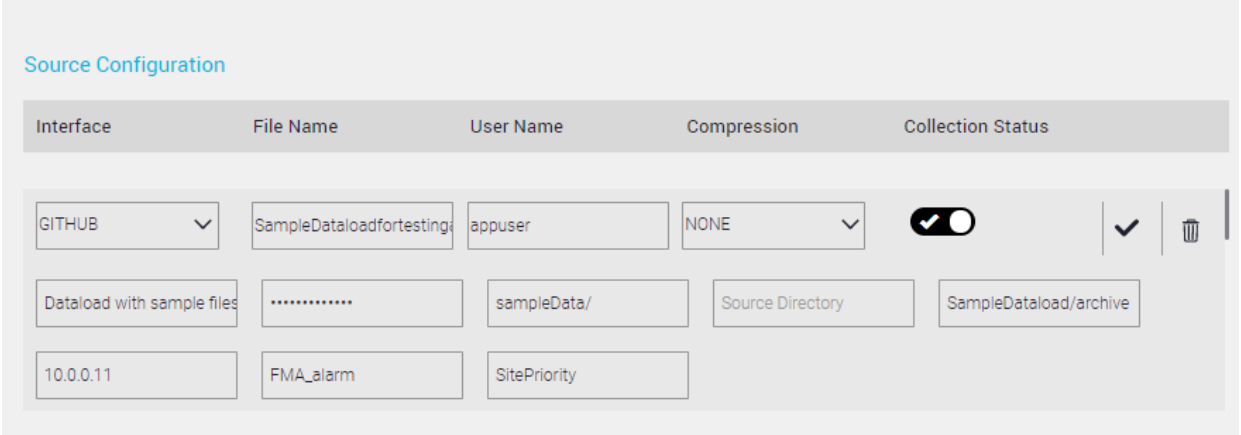


Figure 14.13 - GITHUB Interface Configuration

EMAIL

In the EMAIL interface, apart from the above mentioned fields, user must specify protocol (IMAP /POP3S), mail server name, port number, source archival folder path (relative path of archive folder). Instead of file name pattern, user must specify mail attachment (file) name pattern and search string for both email subject and body.

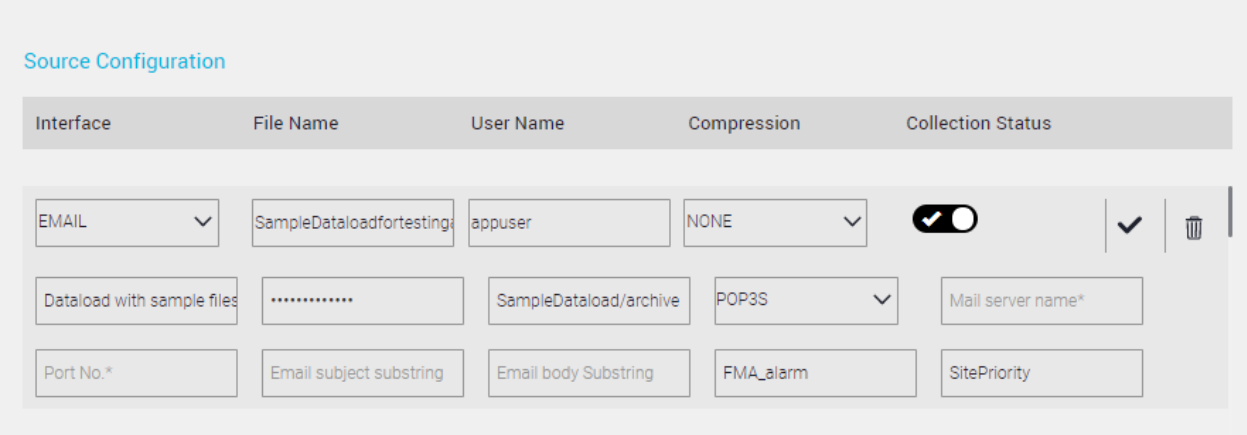


Figure 14.14 - EMAIL Interface Configuration

CUSTOM

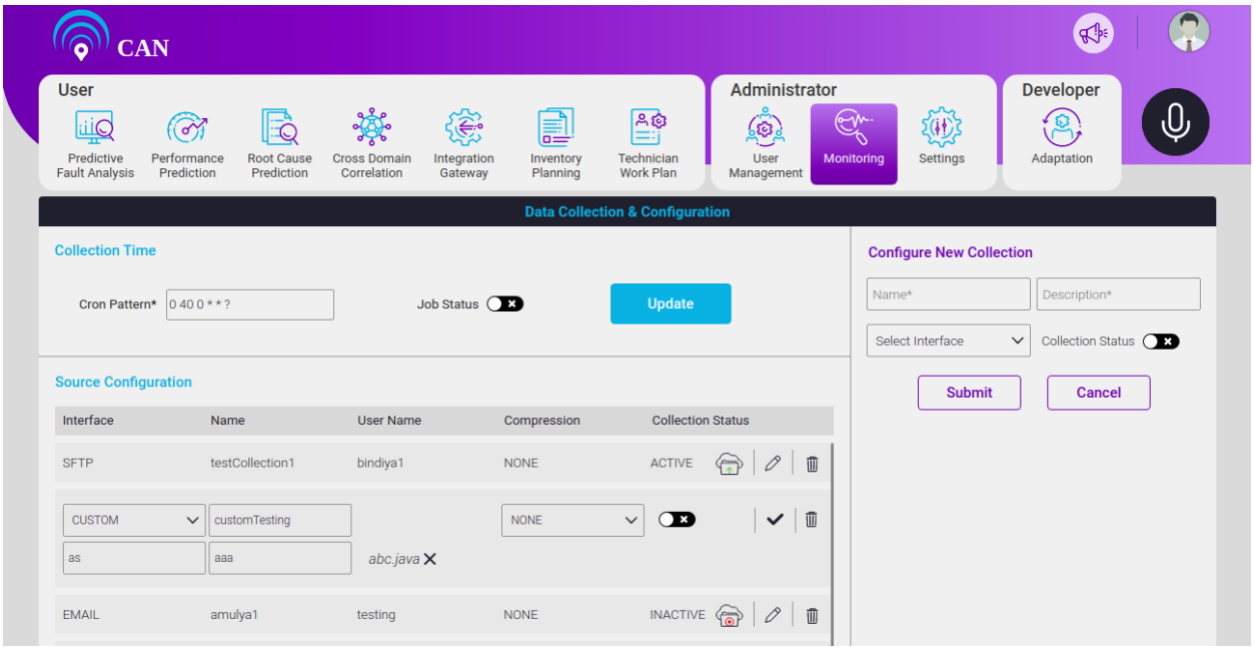


Figure 14.15 - Custom Interface Configuration

KAFKA

In the Kafka interface, apart from above mentioned fields user must specify bootstrap servers and topic name. User can connect through bootstrap servers to establish the initial connection to the Kafka cluster. We will get the data from the configured Topic.

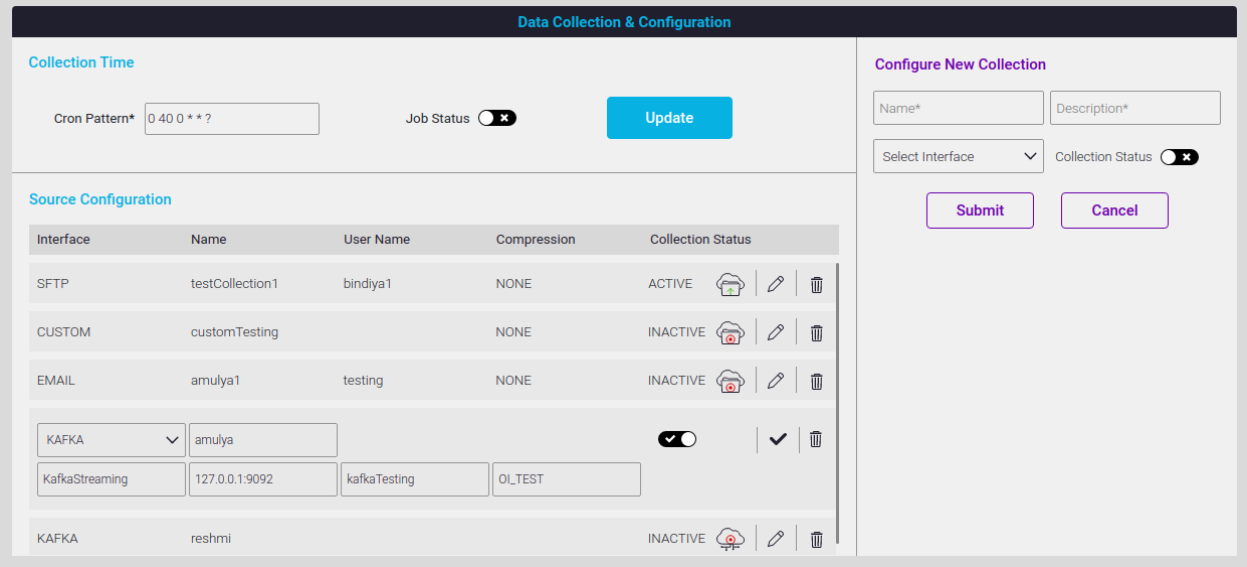


Figure 14.16 - Kafka Interface Configuration

Filter Configuration

This screen can be accessed under the **Adaptation** tab. It provides features to manage predicted fault filtration rules. The predicted fault generation is widely split into two phases, namely:

(a) Generation of initial set of predicted faults

(b) Generation of final set of predicted faults.

The filtration rules created in this screen is basically applied on the initial set of predicted faults to derive at the final set. The filtration rules are based on the rules discovered from past history of alarms and its patterns as well as manually entered ones which collectively provide an appropriate set of predicted faults to act upon. These rules also help in improving the overall accuracy of prediction and mainly to optimize the prediction results.

To Add New Filter Rule

1. Click </> icon, a screen will pop up. Write the name of the Code Snippet Identifier and its description in the respective text boxes. Click the **Save** button.
2. To download the new rule, Click the **Download** icon Download.

To Add New Rule Configuration for Predicted Fault Filtration

1. Select the **Rule Name** from the drop down.
2. Select the **Key type** from the drop down.
3. Select the **Key value** from the drop down.

4. After selection of Key value, **Add New Key** will get activated.
5. Click **Add New Key** to add multiple Key Type and Key Value.
6. Click **Submit** to add the New Rule for Filter Configuration.
7. Click **Cancel** if you don't want to add the New Rule.

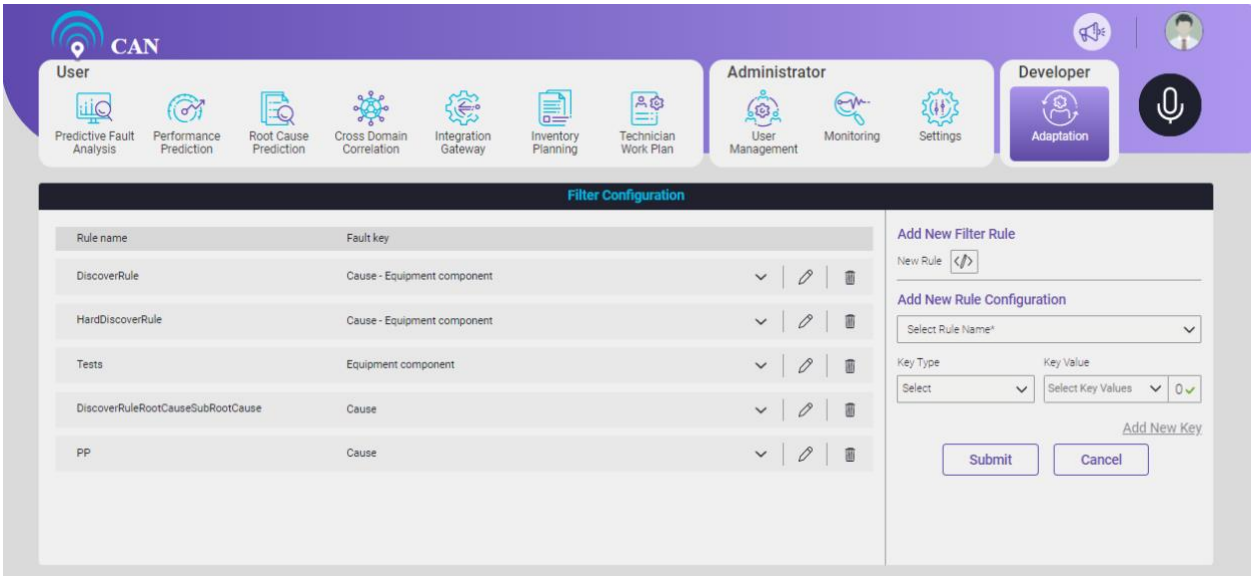


Figure 14.17 - Filter Configuration Home Page

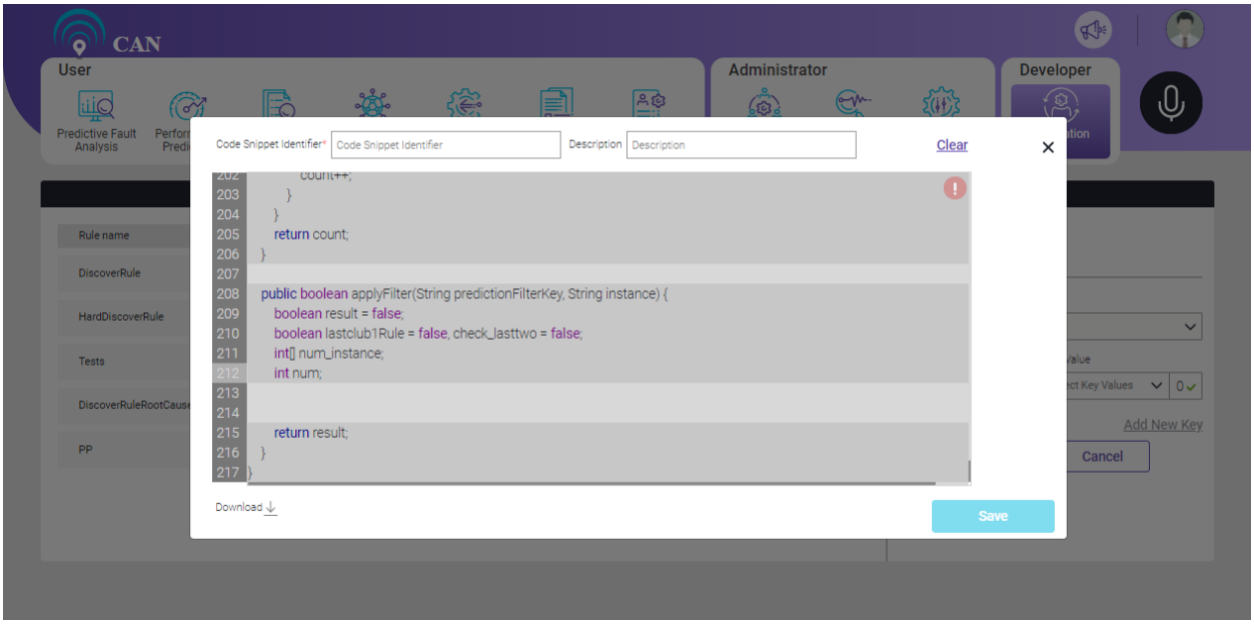


Figure 14.18 - Create Predicted Fault Filtration Rules

To view the details of existing **Rule**, click the more icon .

To view the existing code, click the Rule name.

To Edit the Existing Rule Name

1. Click the edit icon .
2. To edit the existing code, click the existing **Rule name**. A screen will pop up to update the code.
   - Update the code and click **Update**.
   - User can click the clear option to delete the existing code.
   - User can also download the Rule java file. Click the **download** icon to download the Rule java file.
   - Click the **Close** button to close the screen.
3. Select the **Key Type** from the drop down to add the new fault key. You can add multiple Key types at a time.
4. Click **Add New option** to add new input box to select Key Value from the drop down.

Note: After addition of New Option "Add New" option will gets disable. Once you select the Key Value from the drop down Add New option will re-enable.

5. Click the **Delete** icon to delete the Key Value.
6. Click the **Update** icon to save the changes.
7. Click the delete icon to delete the existing Rule.

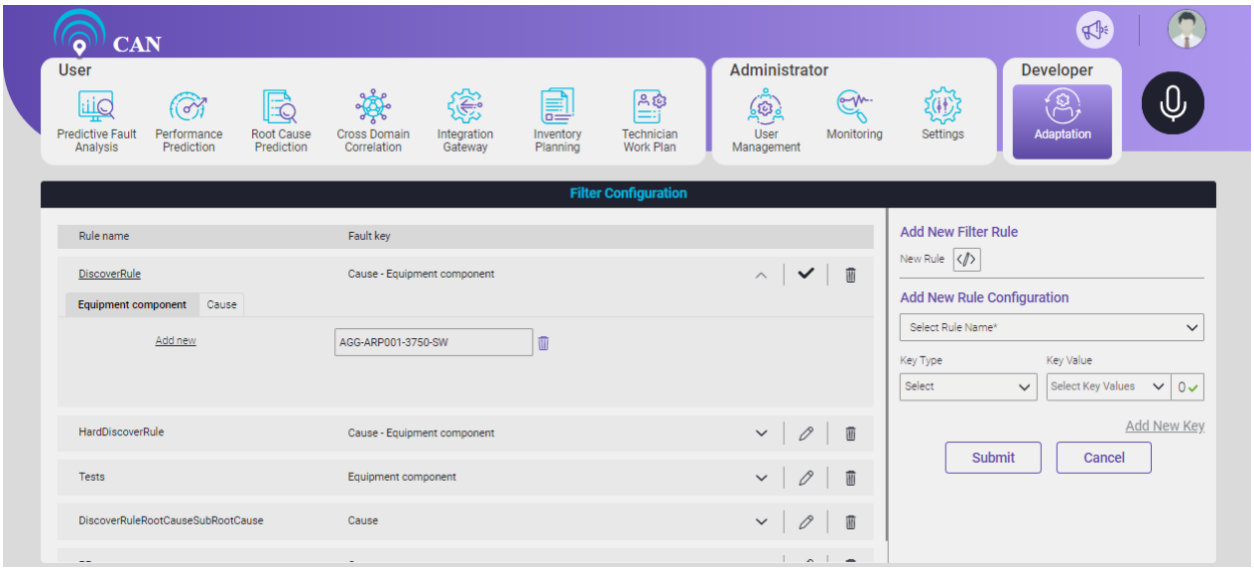


Figure 14.19 - Modifying Predicted Fault Filtration Rules

Post Prediction Process

A file needs to be uploaded that contains java code to enrich predicted information with customized data. This java file should implement **IPostPredictionProcess**.

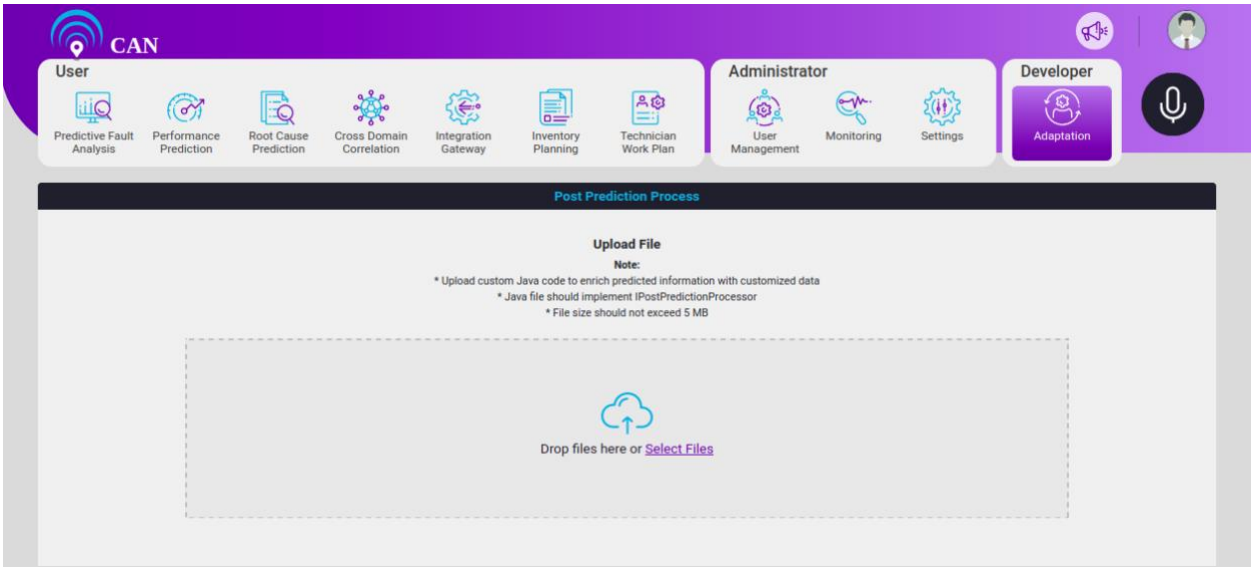


Figure 14.20 - Post Prediction Process

User can upload the java file. User can drag and drop the java file to upload or can select the file to upload.

Below is the screen to show the uploaded java file.

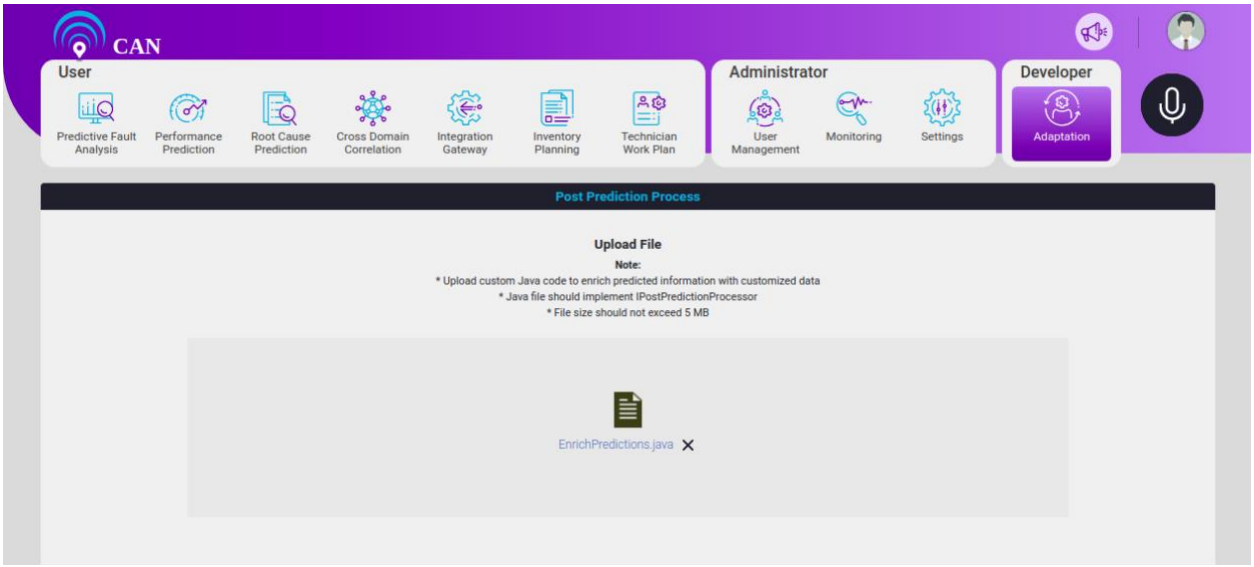


Figure 14.21 - Java File Upload

User can download the java file. To download the java file, click the file name.

To delete the java file, click the delete icon ✕.

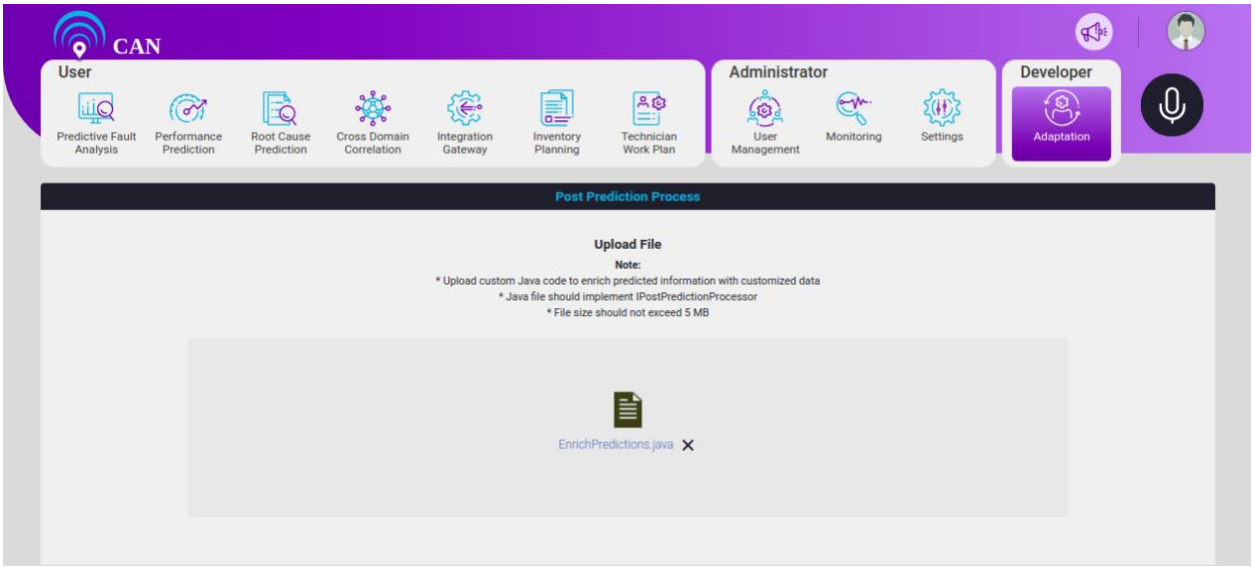


Figure 14.22 - Java File Download/Delete Option

When you click the delete icon, a Confirm Delete message pops up asking “Are you sure you want to delete?”. Click the **Yes** button to delete the java file. Click the **No** button to keep the java file.

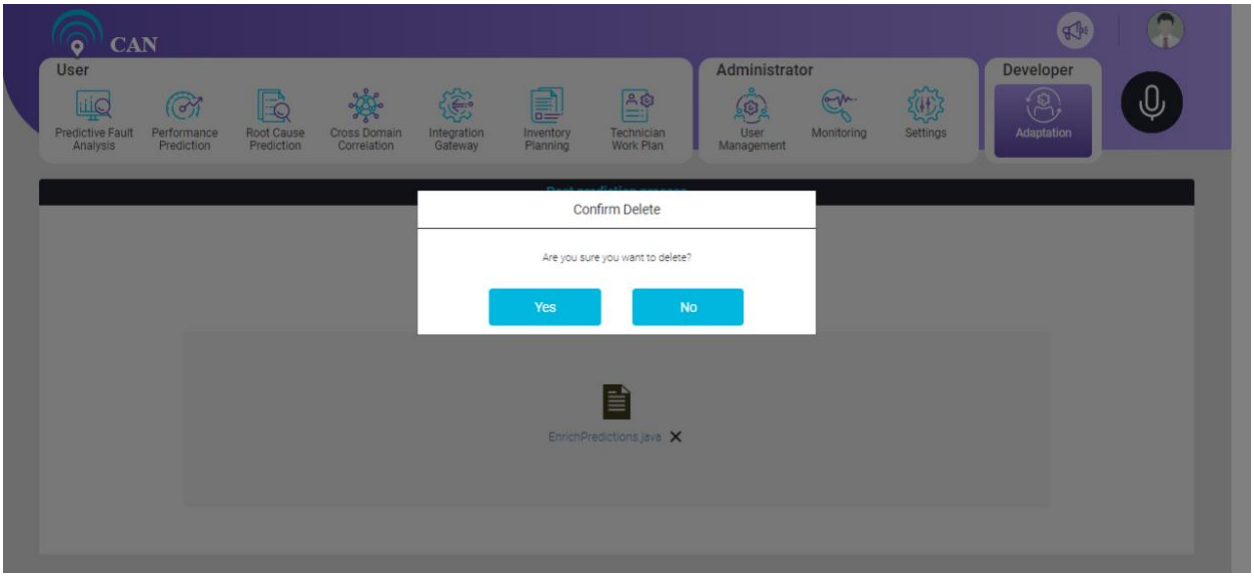


Figure 14.23 - Java File Delete Confirmation Message

Report Configuration

Prediction results are generated as an excel report. This screen allows user to configure fields which they wish to see in the excel report.

There are 2 configurations under this:

- Page Configuration
- Excel Report

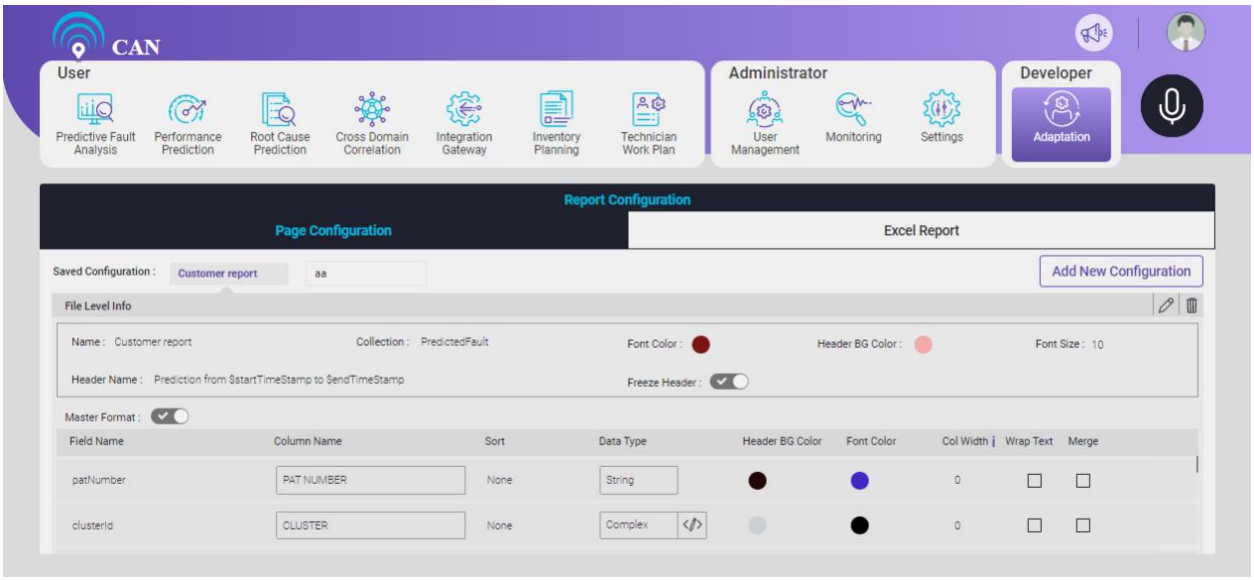


Figure 14.24 - Existing Page Configuration

Page Configuration

Page Configuration screen has configured all the Columns that are required to appear in every sheet of a prediction report and are customizable. It allows user to set excel sheet formats and excel sheet styles accordingly.

There is a list of pre-existing configuration names. User can click any of the existing configurations, the screen will display the saved contents of corresponding configuration. User can edit the existing configuration, if required.

To Edit the Saved Configuration

1. Click the edit icon .
2. To edit the **Column Name,** click the icon . A screen will pop up to update the code. Update the code and click the **Save** button.
3. Select the appropriate **Data Type** from the drop down.
4. If user want to add new row, user can click **Add New** button.
    a. Click the **Add New** button.

       Note: MERGE and SORT options are disabled as RoE is active. Manually merging or sorting of columns is not valid if RoE is active

    b. User can configure few other parameters to set each column of the prediction report The parameters are as follows:
        i. Field Name - Name of the field as it is in prediction result table i.e. Predicted Fault table as per CAN convention.
        ii. Column Name - Name of the column which user wishes to see in report.
        iii. Sort - Column values can be sorted as Ascending, Descending and None.
        iv. Data Type - Select the Data formats like String, Number, Percent, Complex and Drop down. If user selects the complex data type, Edit icon appears next

to that. When the user clicks this icon, a popup (which is similar in functionality with respect to parser screen) comes up.

v. Header BG Color - User can decide background color for column header.
vi. Font Color - User can decide font color for column values.
vii. Column Width - Sets width of column, here value 0 indicates auto resizing of column.
viii. Wrap Text - If checked, text contents of each cell in that column will be wrapped.
ix. Merge - Allows multiple adjacent cells to be combined into a single larger cell when values are similar.
x. Sequence - User can change the column sequence with move up or move down button. User also have the drag and drop option to move the column up or down.

5. After editing the required fields, click the update icon to save the existing configurations. If user will not save the changes, Page Configuration will not reflect the changes.
6. If any of the pre-existing configuration isn't required, click the delete icon.

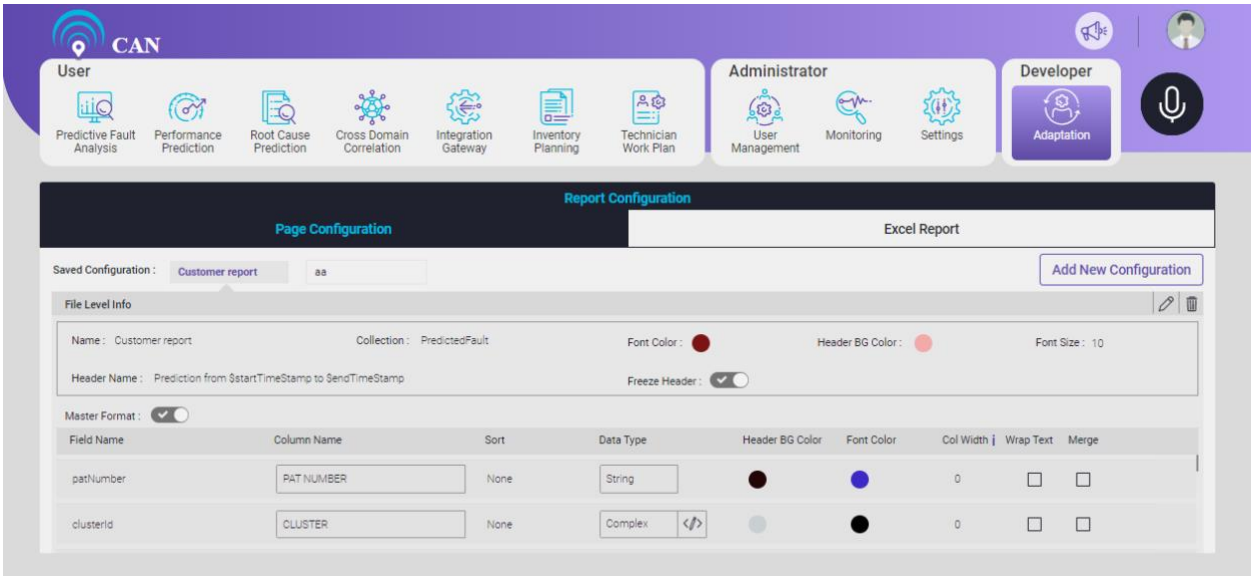


Figure 14.25 - Existing Page Configuration

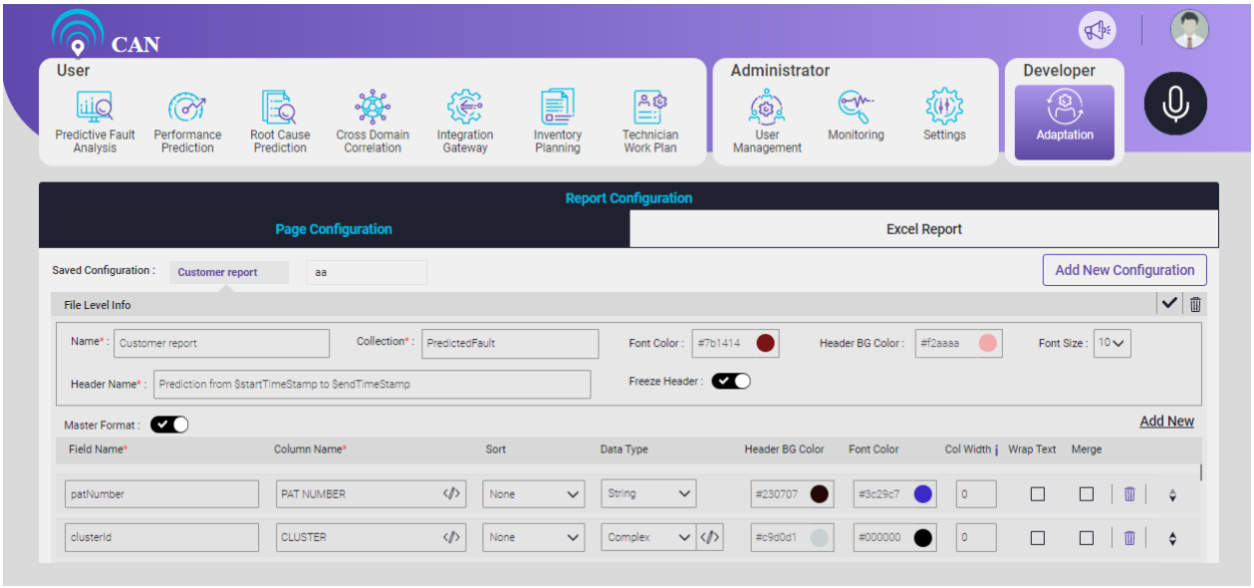


Figure 14.26 - Create New Page Configuration

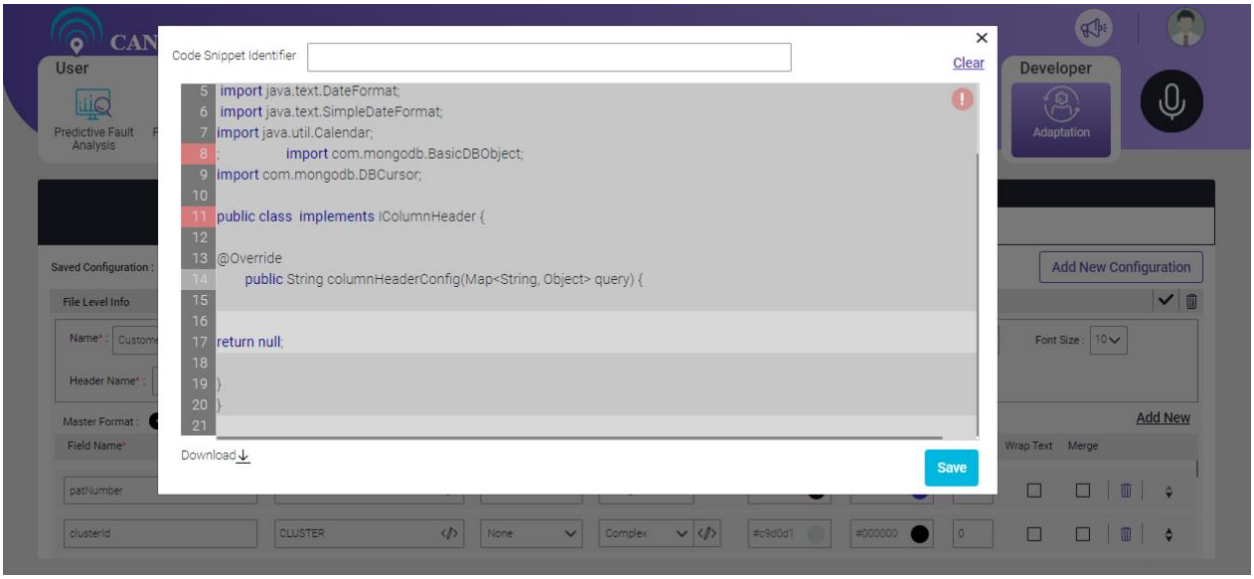


Figure 14.27 - Code Snippet Text Area

By default, **Freeze Header** toggle button will be ON. If it is ON, then the first two rows of report will freeze when the report will be generated.

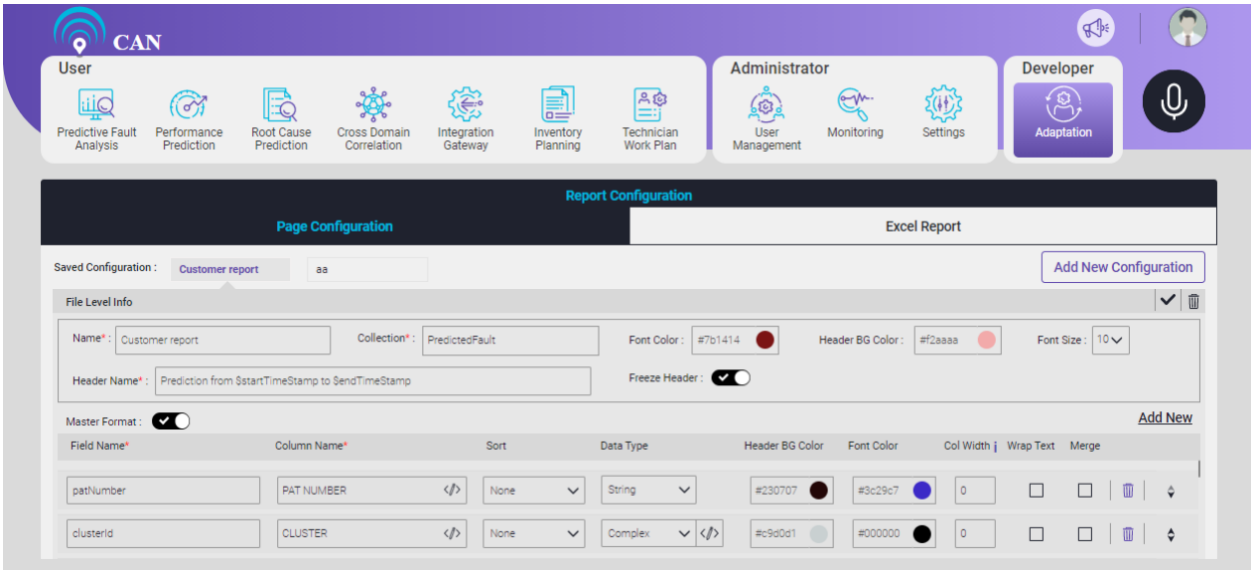


Figure 14.28 - Freeze Header Button

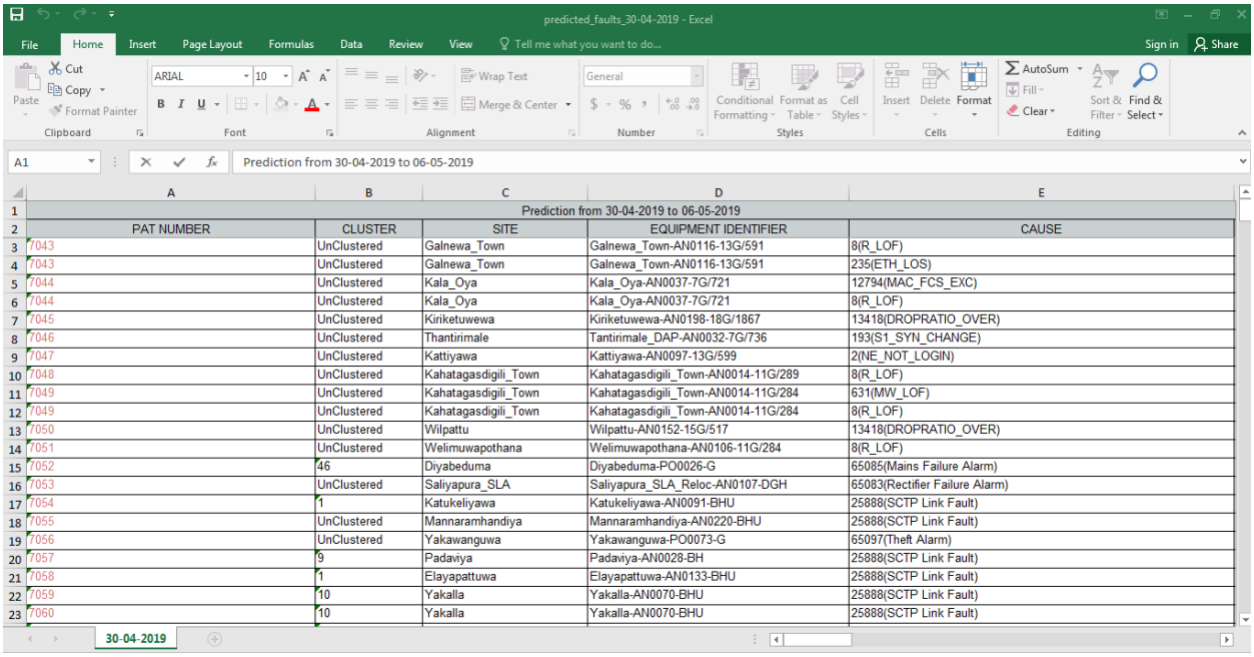


Figure 14.29 - First Two Rows Freeze

To Create a New Configuration

1. Click the **Add New Configuration** button.
2. Give a new name to the configuration. User is allowed to set excel styling features like Font Color, Header Background Color, Font Size. User is also allowed to set the Header Name that appears as first row in the Excel Report.
3. If user want to add new row, user can click **Add New** button for Column Configuration.
    a. Click the **Add New** button.

Note: MERGE and SORT options are disabled as RoE is active. Manually merging or sorting of columns is not valid if RoE is active

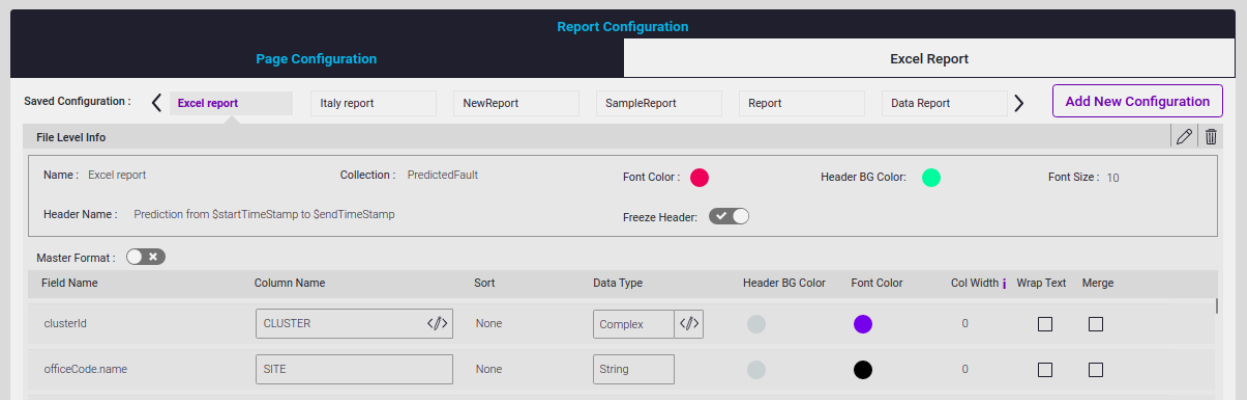
b. User can configure few other parameters to set each column of the prediction report The parameters are as follows:
   i. Field Name - Name of the field as it is in prediction result table i.e. Predicted Fault table as per CAN convention.
   ii. Column Name - Name of the column which user wishes to see in report.
   iii. Sort - Column values can be sorted as Ascending, Descending and None.
   iv. Data Type - Select the Data formats like String, Number, Percent, Complex and Drop down. If user selects the complex data type, Edit icon appears next to that. When the user clicks this icon, a popup (which is similar in functionality with respect to parser screen) comes up.
   v. Header BG Color - User can decide background color for column header.
   vi. Font Color - User can decide font color for column values.
   vii. Column Width - Sets width of column, here value 0 indicates auto resizing of column.
   viii. Wrap Text - If checked, text contents of each cell in that column will be wrapped.
   ix. Merge - Allows multiple adjacent cells to be combined into a single larger cell when values are similar.
   x. Sequence - User can change the column sequence with move up or move down button. User also have the drag and drop option to move the column up or down.

4. Click the save icon to save the New configurations. If user will not save the changes, Page Configuration will not reflect the changes.

There is a Master Format toggle button . If enabled, this configuration generates the matching report.

There is one Freeze Header toggle button , If enabled, the header on the excel file will get freeze and other columns can be scrolled.

In case of more Saved configurations, user can click icon to navigate to right and click icon to navigate to left side of the screen.



Excel Report Configuration

Page Configuration tab is specific to column configurations of every single excel sheet whereas Excel Report tab helps to create the sheet configurations.

On top portion of this screen, a **'Add New Configuration'** button is available to create new configuration. There is a list of pre-existing configuration names.

Click any of the existing configurations to display the saved contents of that corresponding configuration.

User can modify the existing configuration, if required. If any of the pre-existing configuration isn't required, user can delete the existing configuration.

A switch to activate and deactivate excel report configuration is also available.

User can generate the Prediction report in accordance with active configuration. User can also write success and failure mail templates. Success mail will be attached with Prediction report.

To Edit the Existing Configuration

1. Click the edit icon .
2. Write the Configuration Name, Percentage Format, Excel Report Name.
3. Select the Date Format and Font Name from the drop down. User can also write the date in the **Date Format** by select **Add New Date Format** from the drop down.
4. User can edit the Success Email Template and Failure Email Template.
5. Click the **Add New Mapping** button to add new mappings to the existing configuration.
    a. Click the **Add New Mapping** button. User can also modify or delete the existing sheet configuration.
    b. Sheet configuration contains the following fields:
        i. Sheet Name - Name of the sheet to appear in Prediction report.
        ii. Page configuration type - It can be Basic or File Upload type.
        iii. Page configuration - Allows to choose saved Page Configuration from auto completion.
        iv. Query - User can write a MongoDB query to filter prediction results appearing in various sheets. Query can be written within a popup and it will be validated before saving or updating the configuration. Refer the link https://docs.mongodb.com/manual/ for Mongo DB user manual.
        v. Sequence - User can change the column sequence with move up or move down button. User also have the drag and drop option to move the column up or down.
6. Click the update icon to save the changes. If the user will not save the changes, Excel Report will not reflect the changes.
7. Click the **delete** button to delete the existing configuration.

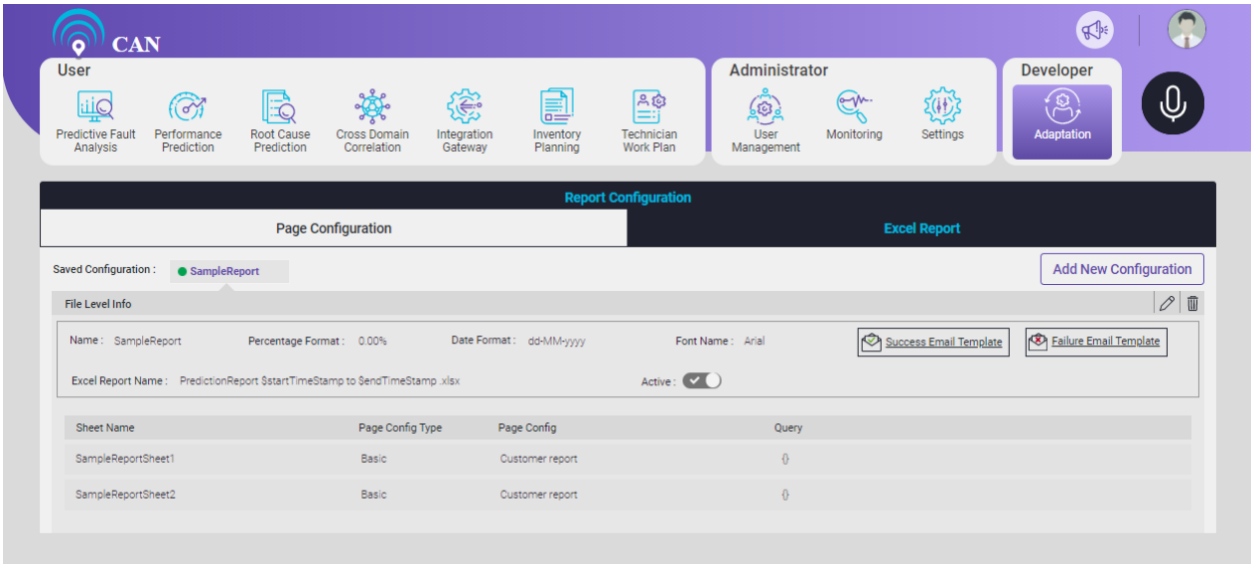
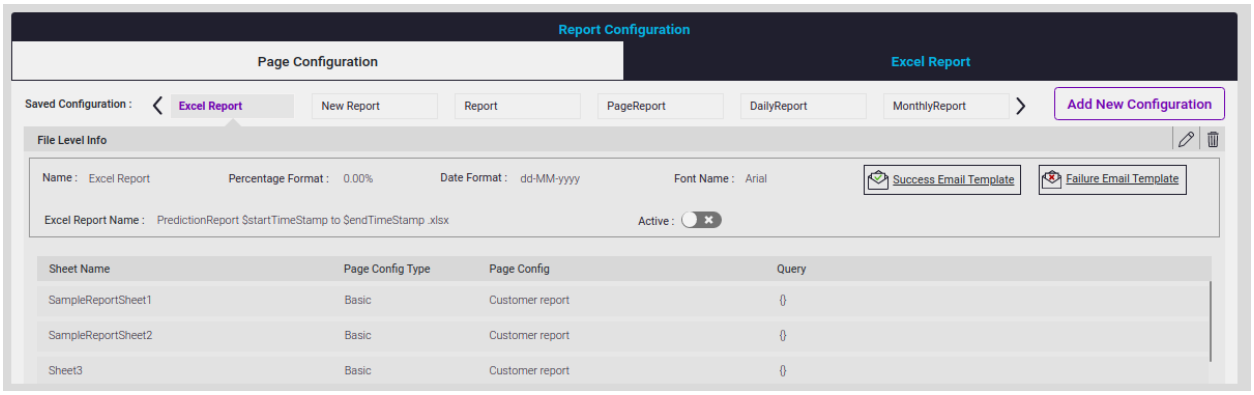


Figure 14.30 - Existing Excel Report Configuration

In case of more Saved configurations, user can click › icon to navigate to right and click ‹ icon to navigate to left side of the screen.



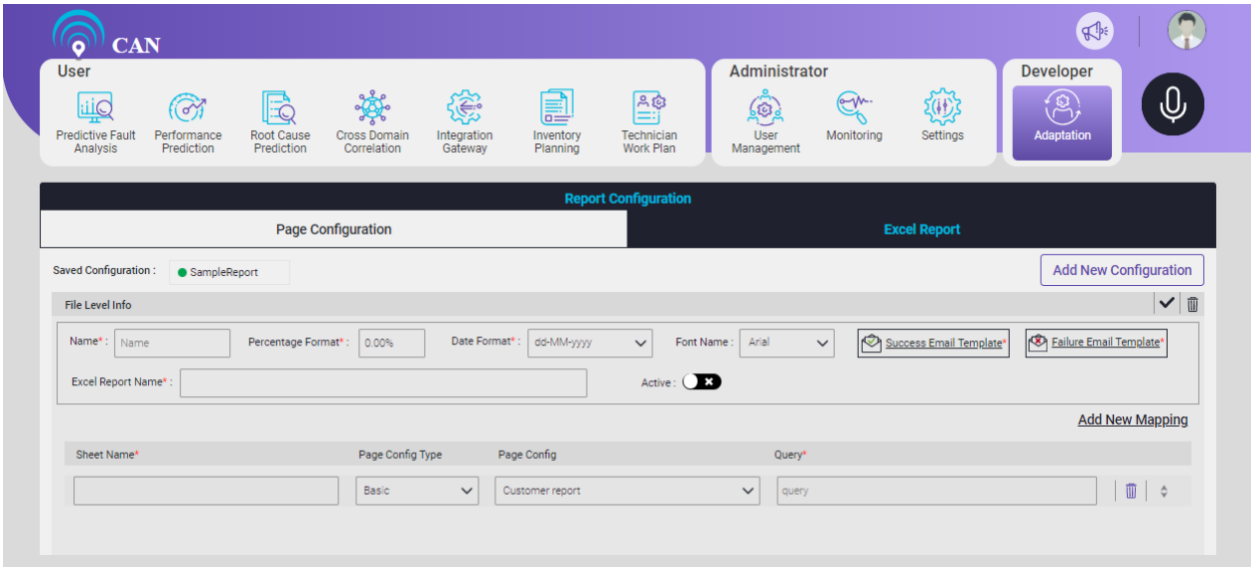


Figure 14.31 - Create New Excel Report Configuration

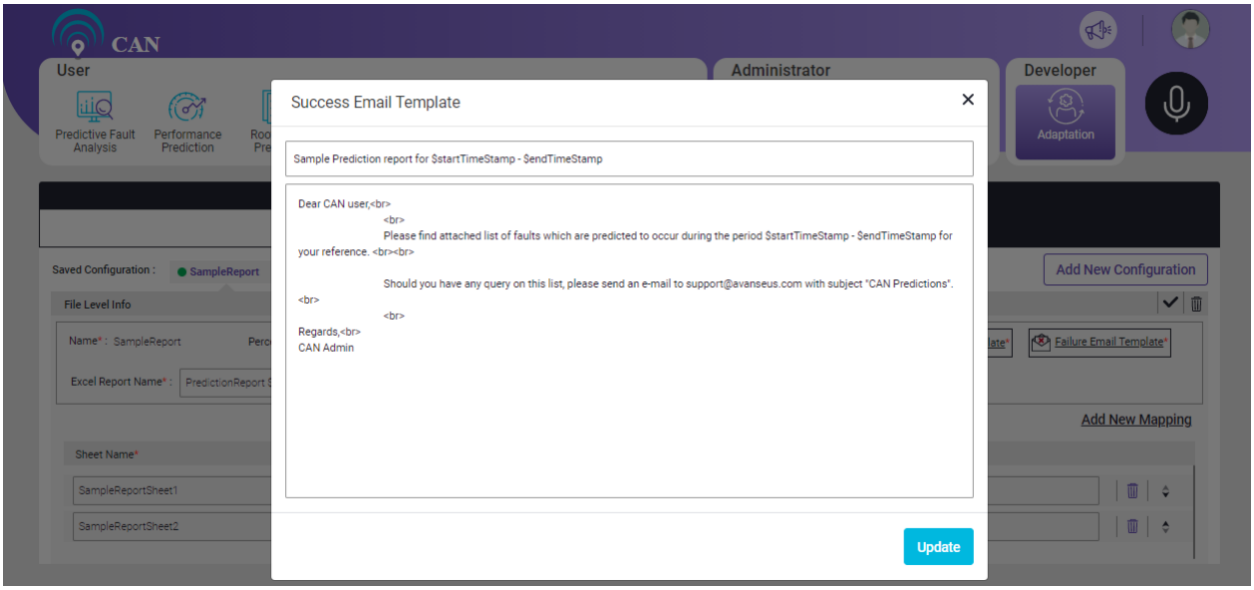


Figure 14.32 - Email Template

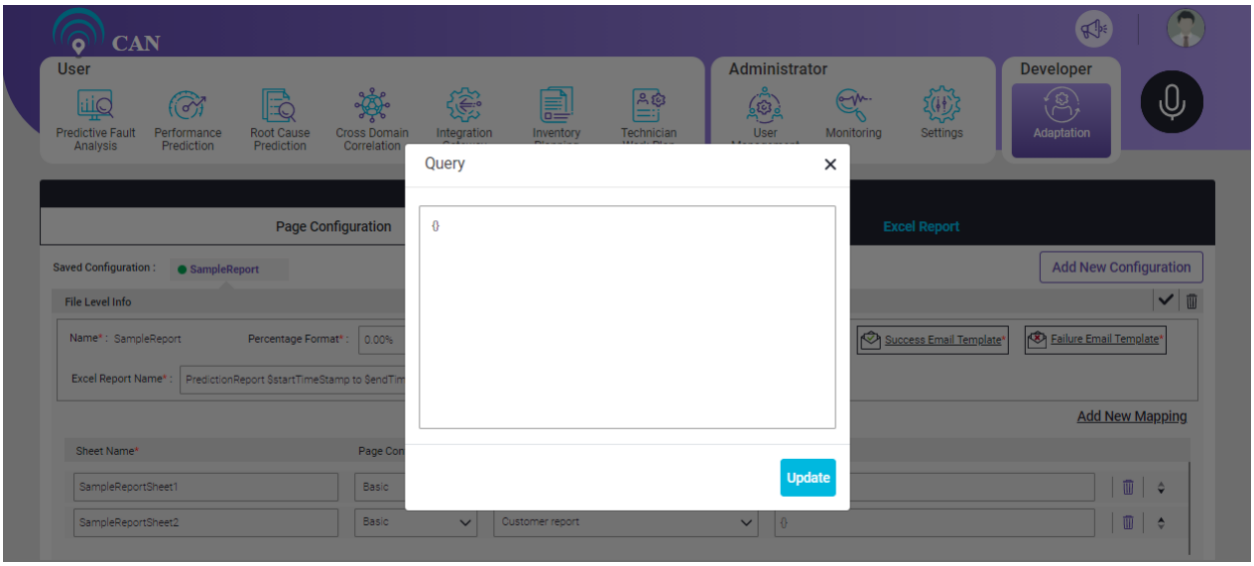


Figure 14.33 - Query Snippet

To Create a New Configuration

1. Click the **Add New Configuration** button.
2. Write the Configuration Name, Percentage Format, Excel Report Name.
3. Select the Date Format and Font Name from the drop down. User can also write the date in the **Date Format** by select **Add New Date Format** from the drop down.
4. **Activate** or **Deactivate** the Excel Report from the toggle button.
5. Click the **Add New Mapping** button to add the New Mappings to the New Configuration.
    a. Sheet configuration contains the following fields:
        i. Sheet Name - Name of the sheet to appear in Prediction report.
        ii. Page configuration type - It can be Basic or File Upload type.
        iii. Page configuration - Allows to choose saved Page Configuration from auto completion.
        iv. Query - User can write a MongoDB query to filter prediction results appearing in various sheets. Query can be written within a popup and it will be validated before saving or updating the configuration. Refer the link https://docs.mongodb.com/manual/ for Mongo DB user manual.
        v. Sequence - User can change the column sequence with move up or move down button. User also have the drag and drop option to move the column up or down.
6. Click the save icon ✔ to save the New configurations. If user will not save, then the changes will not be reflected in the Excel Report Configuration Page.

Alarm Inclusions/Exclusions

This screen is to save an Inclusion and Exclusion rule. User can transfer the data between **Alarm** and **Alarm_all** Table based on the rule.

After the transfer of the data:

Alarm Table will have all the documents which belongs to Inclusion rule.

Alarm_all will have all the documents which does not belong to Inclusion rule.

To enable/disable the Alarm inclusion/exclusion, Click the **Enable/Disable** toggle button.

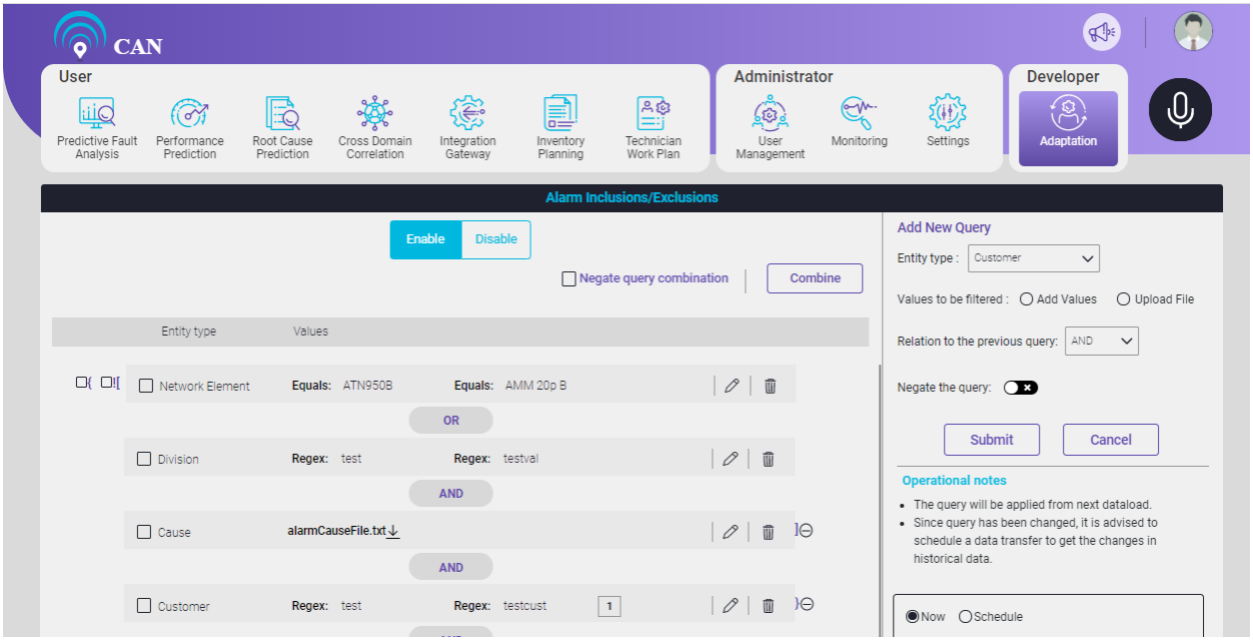


Figure 14.34 - Alarm Inclusion/Exclusion Toggle Switch

To Add New Query for the Alarm Inclusion/Exclusion

1. Select the Entity Type from the drop down menu.

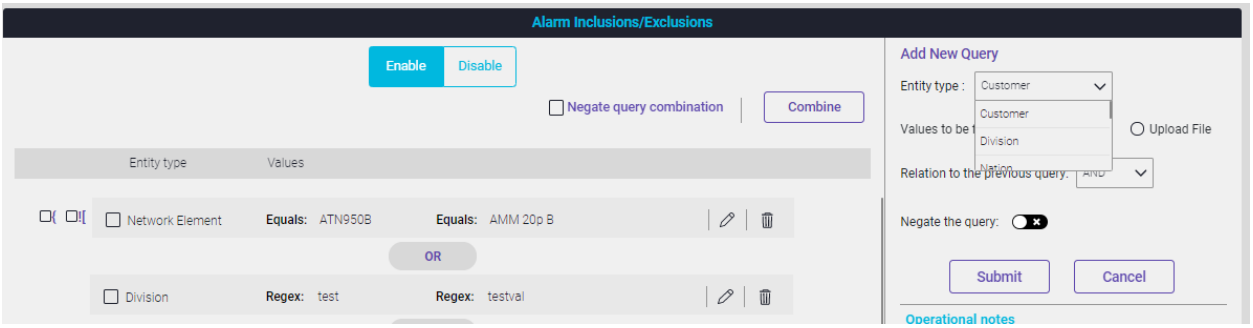


Figure 14.35 - Alarm Inclusions/Exclusions Entity Types

Note: When user selects the Entity type as “Custom”, user needs to write the “Entity Name” too in the text box. The Entity Name* must be an existing key from the alarm table. See the below image for more clarity.

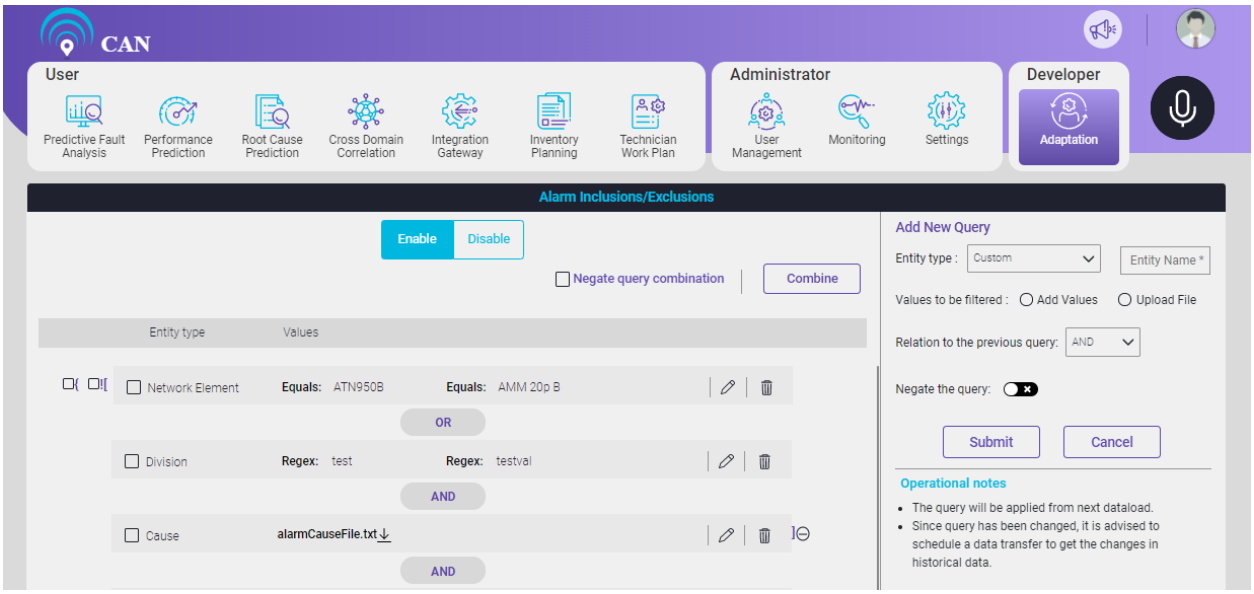


Figure 14.36 - Alarm Inclusions/Exclusions Entity Types

2. User can add values in two different ways:
3. User can also upload less than 5 values manually. To upload more than 5 values, click the Upload File radio button.

To Add Manually

1. Select the radio button with Values label.
2. Put the values in the fields and click **Update** button to add it.

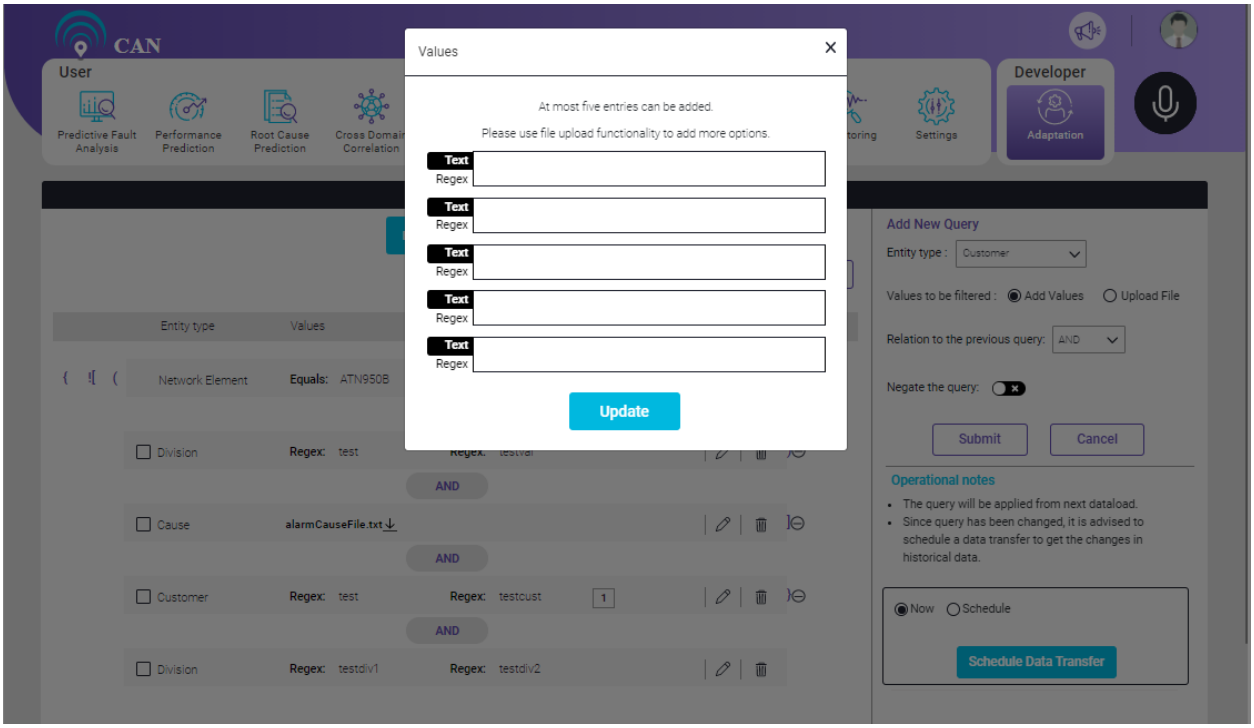


Figure 14.37 - Values

Note: For the text values, keep the toggle switch as “Text”, for Regular Expression (Regex), Click the toggle switch for Regex.

Upload File

Select the Upload File radio button, a pop will come to upload the file. User can drag and drop the file to upload or can select the files from the desktop.

Every line should have unique entity type values in that text file.

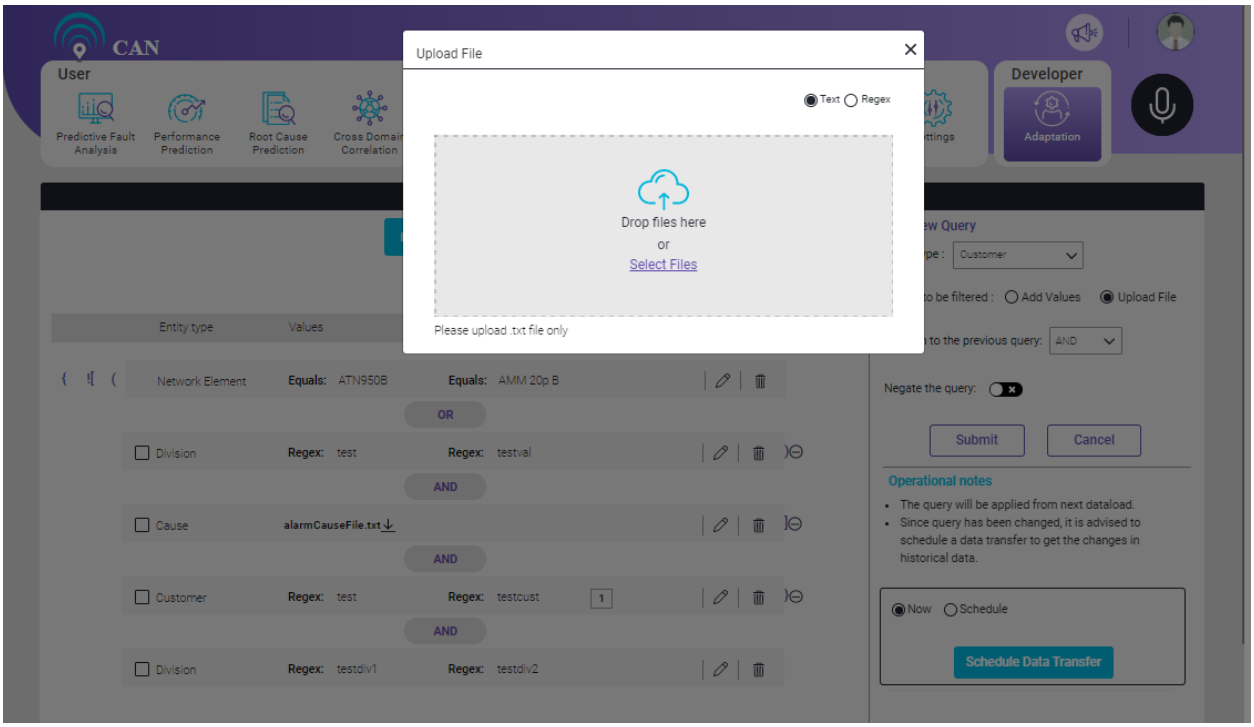


Figure 14.38 - File Upload

Note: For the text values, keep the toggle button as "Text", for Regular Expression (Regex), Click the toggle button for Regex.

3. To add a relation to the previous query, select one operator from the Relation to the previous query drop down menu.

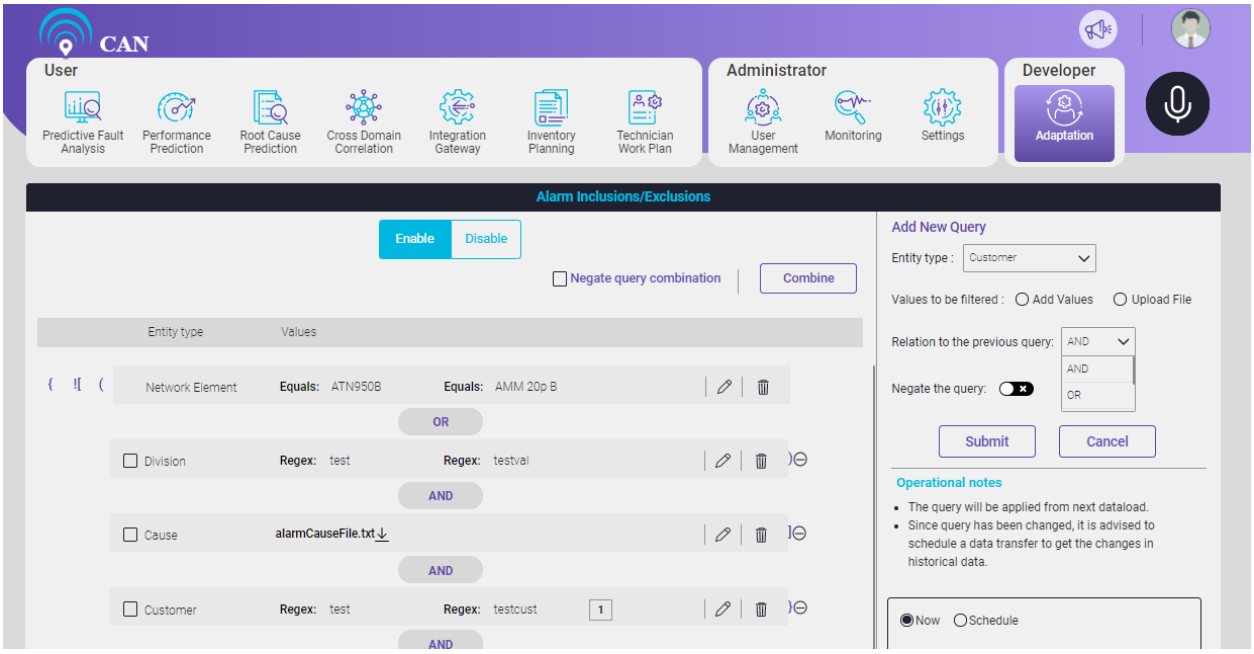


Figure 14.39 - Relation to the previous query

4. To negate a query, click “**Negate the query**” toggle button.

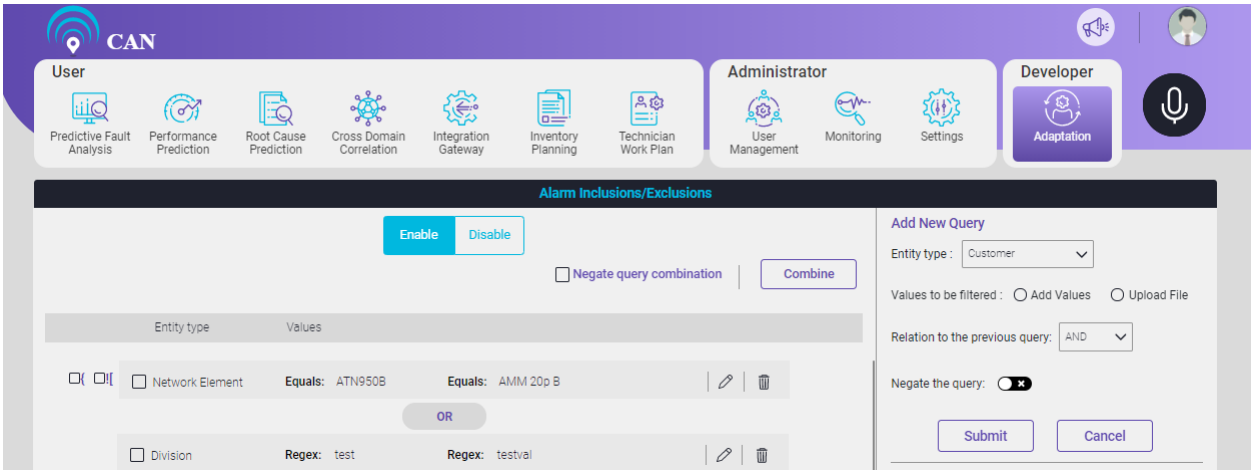


Figure 14.40 - Negate the query

Note: If no query is there then operator cannot be selected.

5. To save the query, click the **Submit** button.

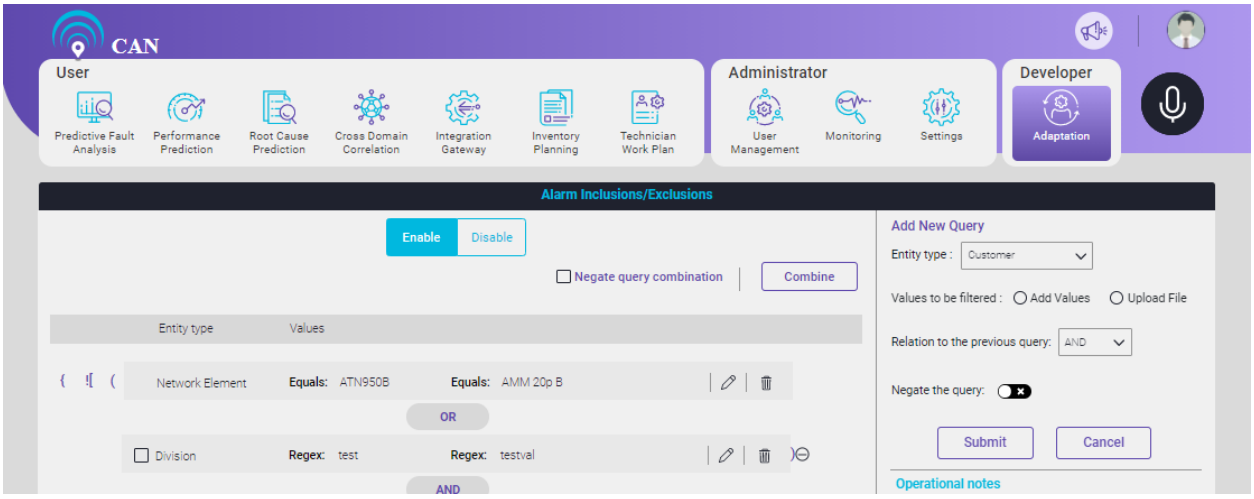


Figure 14.41 - Add New Query

Edit:

User can modify the Values. To modify the values, click the edit icon .

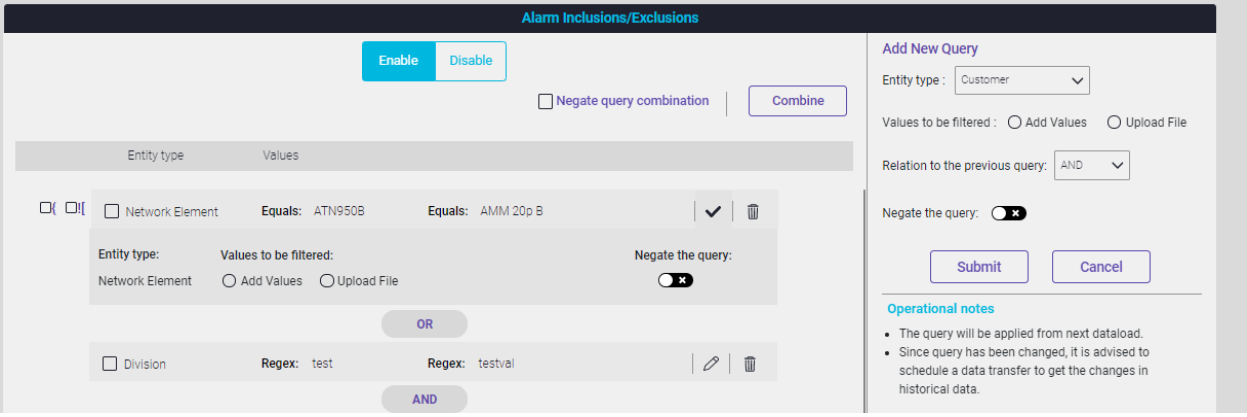


Figure 14.42 - Edit Query

To save the changes, click the save icon .

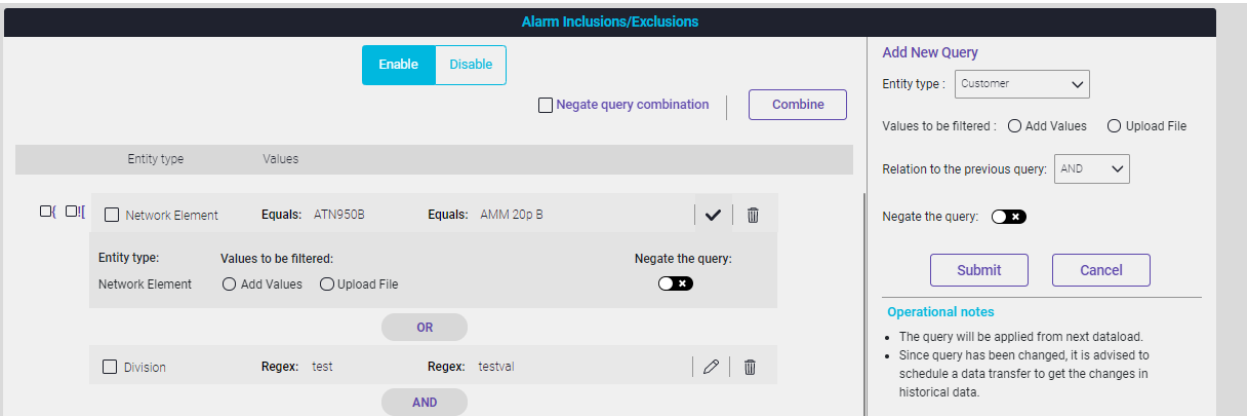


Figure 14.43 - Save Icon

Delete:

To delete a query, click the delete icon .

Figure 14.44 - Delete a sub query

One dialog box will appear.

To confirm the deletion, click the **Yes** button, otherwise click the **No** button.

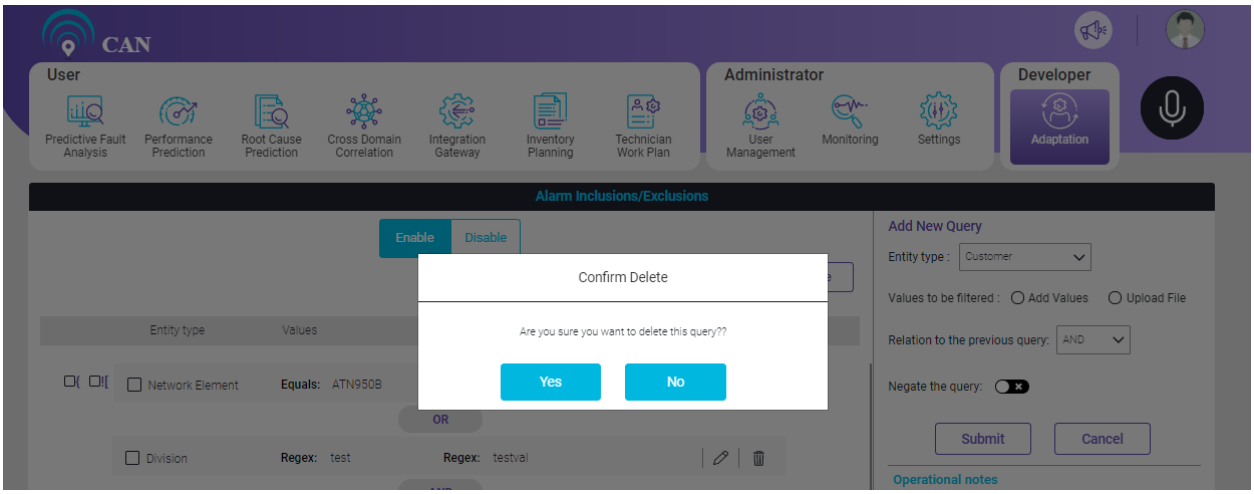


Figure 14.45 - Deletion Confirmation Message

To combine the sub queries, select the checkboxes corresponding to the particular sub queries and click the **Combine** button.

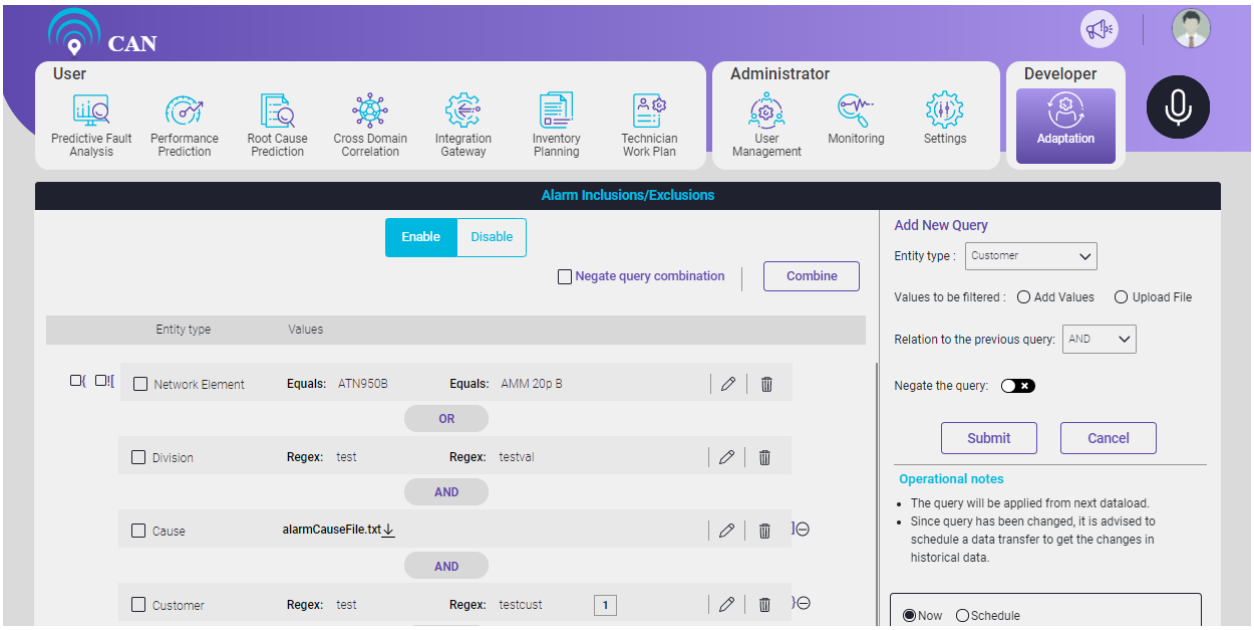


Figure 14.46 - Combination of Queries

Note: To negate the combination select the checkbox “Negate query combination”.

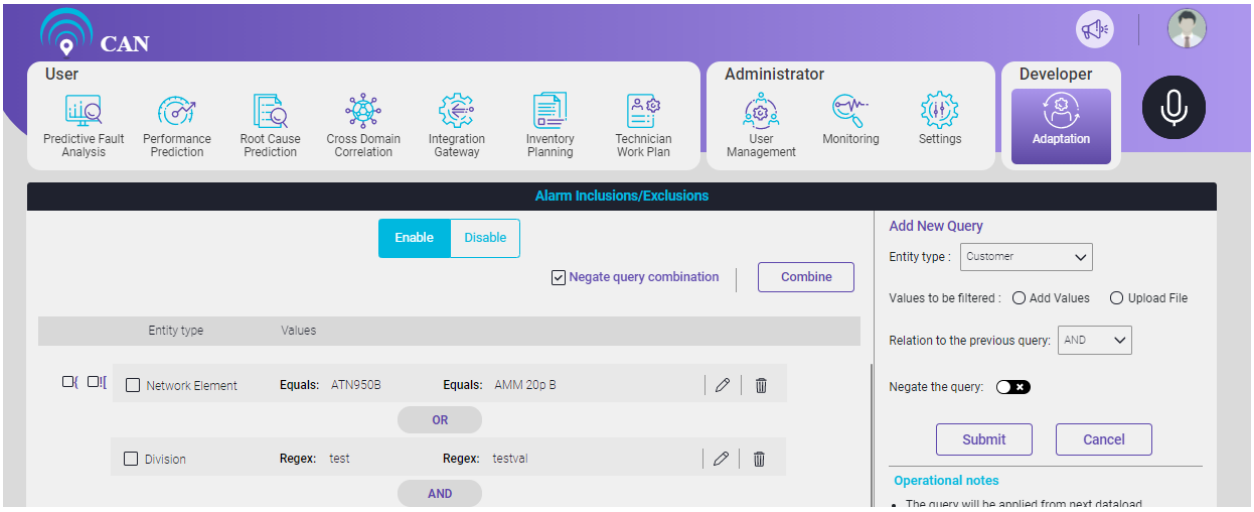


Figure 14.47 - Negate Query Combination

“Operational notes” section present on the right bottom of the screen conveys the information to the user regarding the query for the next data load.

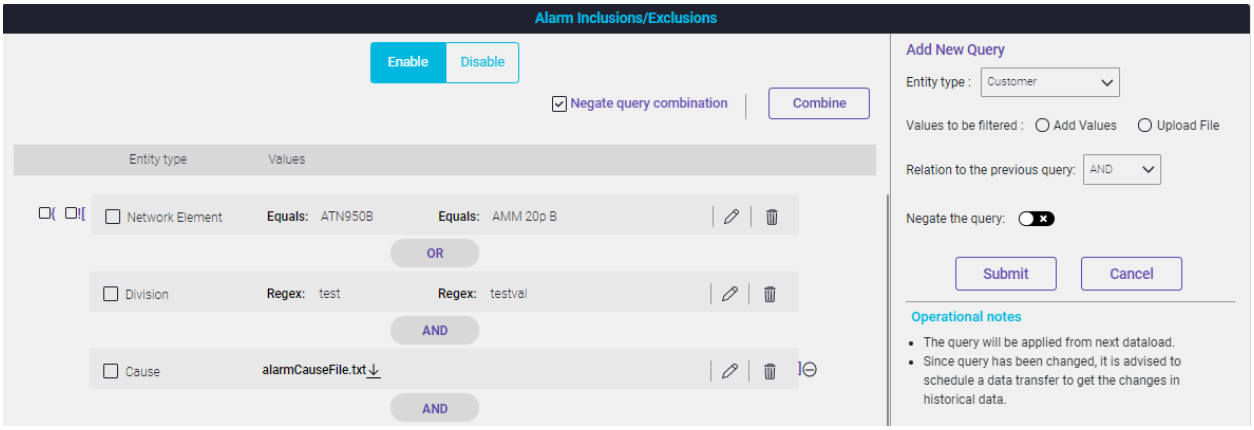


Figure 14.48 - Operational Notes

To Schedule a Job:

1. To schedule the job immediately, select “Now” radio button and click the “**Schedule data transfer**” button.

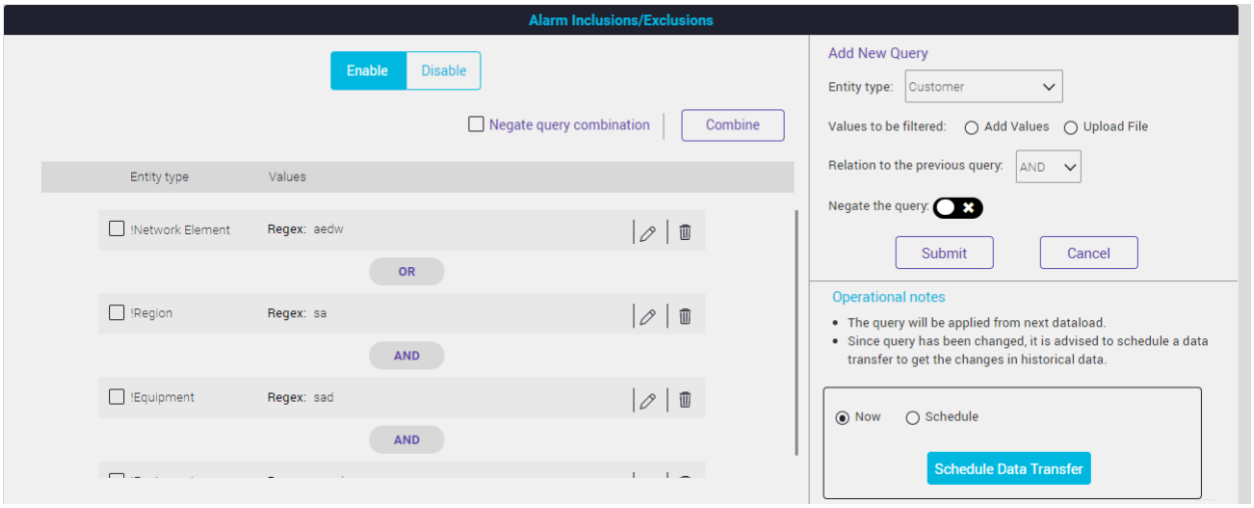


Figure 14.49 - Job Scheduler

2. During the data transfer process, user will be able to do any modification in the query with the below constraints:
    - The query will be applied from next dataload.
    - Since query has been changed, it is advised to schedule a data transfer to get the changes in historical data.
3. To cancel the data transfer, click the "**Cancel Data Transfer**" button to cancel the process.

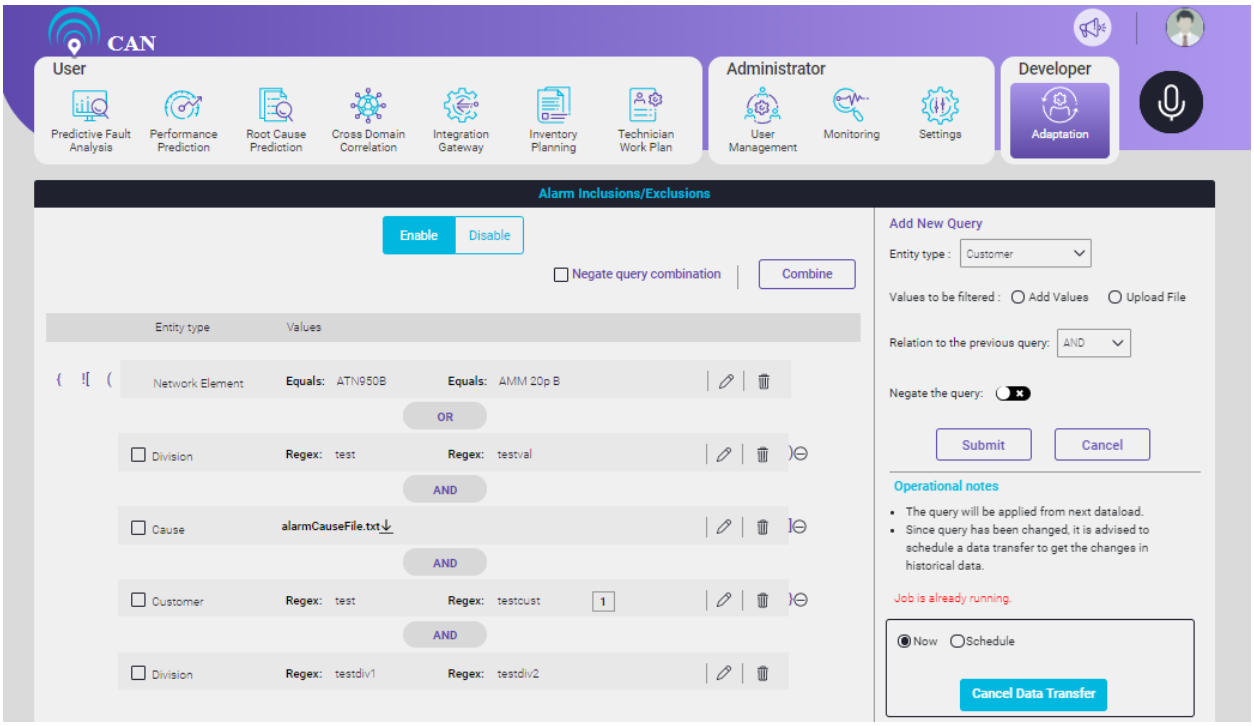


Figure 14.50 - Cancel Data Transfer

4. When user clicks Cancel Data transfer, the confirmation box pops up with “**Continue**” and “**Cancel**” option where the user must choose the appropriate action.
5. Click the “**Continue**” button, to cancel the data transfer.
6. Click the “**Cancel**” button, to let the job run.

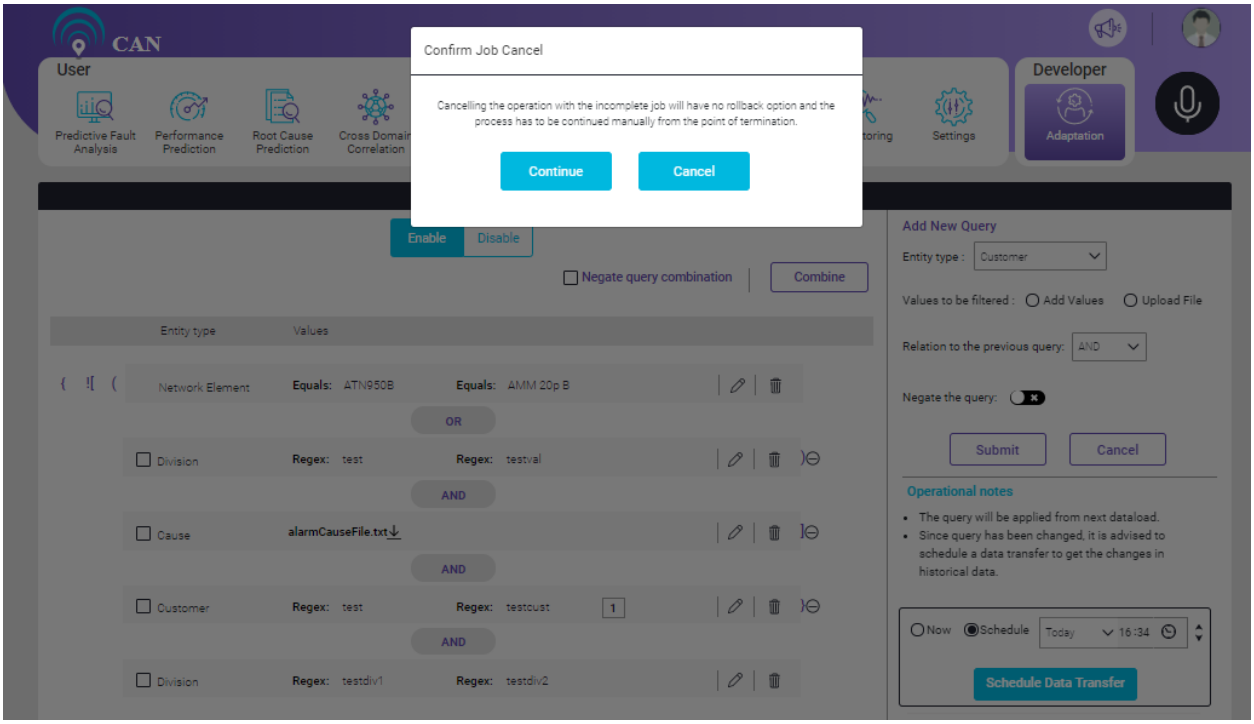


Figure 14.51 - Cancel data transfer

To Schedule the Job Later:

1. Select the “**Schedule**” radio button and select a day from the drop down menu,
2. Select the time from the time menu and click the “**Schedule Data Transfer**” button.

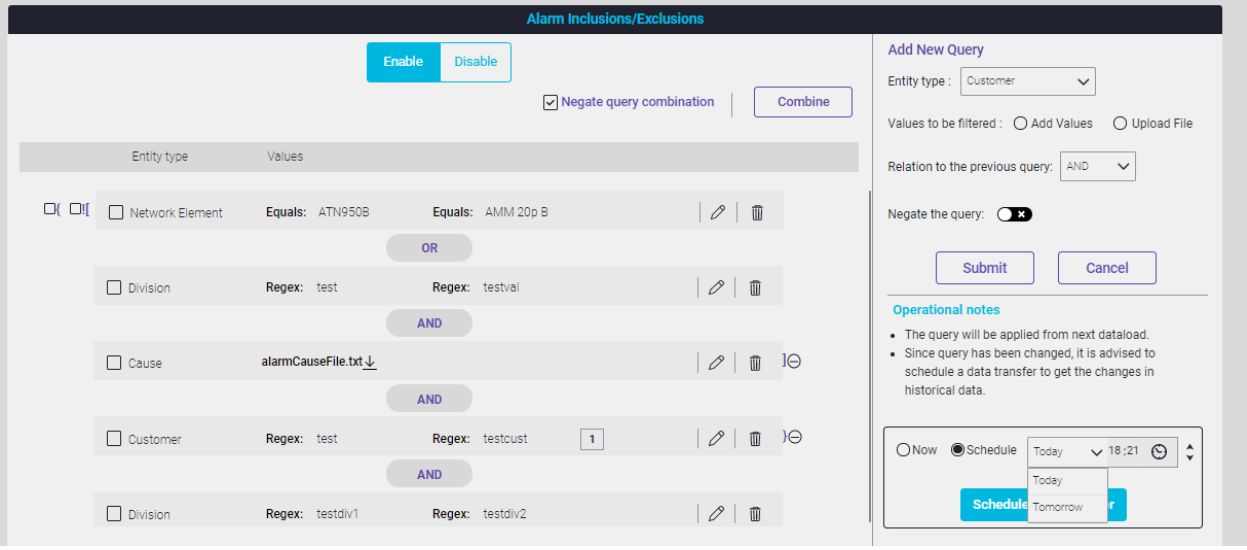


Figure 14.52 - Job Scheduler

Resource Configuration

This screen is found under the Adaptation on the main home screen. Its function is to upload and parse the customer specific data which cannot be mapped with the CAN model. A client input data file should be synced with the mapper present in parser screen. This resource data can be used as an add-on during data load or after prediction (Eg: In post Prediction process to attach some information to prediction).

To Add New Resource Configuration

1. Write the Resource name in the "**Resource**" text box.
2. Select the Mapper name in the "**Mapper**" text box. The text box gives the suggestions of the Mapper names.
3. There is an option to upload the Resource Files. User can select a file or drag and drop to upload. This file should be of specified format in selected Parser Mapping and should not exceed 100 MB.
4. Click the **Submit** button to add the New Source Configuration.

NOTE: User can upload multiple files and the progress bar displays the percentage of the file upload. Progress bar disappears once upload is complete and user clicks the mouse somewhere outside the selected resource region.

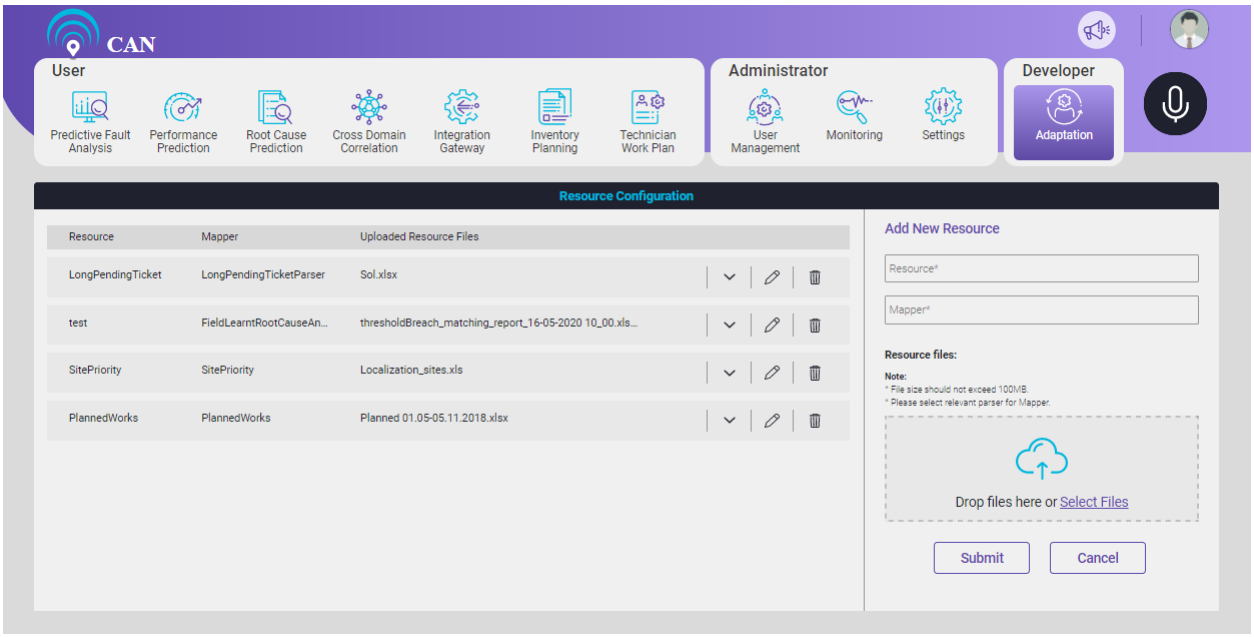


Figure 14.53 - Resource Configuration Screen

5. To see the details of the Resource, click more icon .

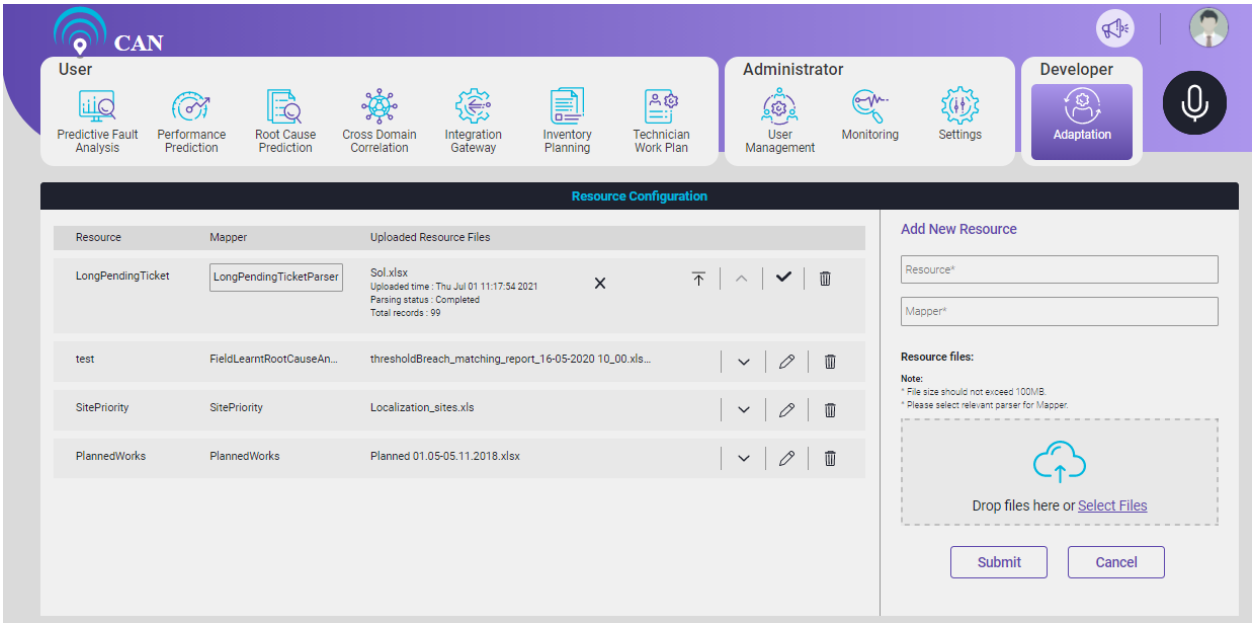


Figure 14.54 - Resource Configuration Screen

To Edit the Existing Resource Configuration

1. To edit the existing Resource Configuration, click the edit icon .
2. To delete the Uploaded Resource Files, click the **delete** button .

3. To upload the new Resource File, click the upload icon . When user clicks the upload icon, a pop screen to upload the resource file opens. User can select a file or drag and drop to upload.
4. Click the **Update** button to save the changes.
5. To delete the existing resource configuration, click the delete icon .

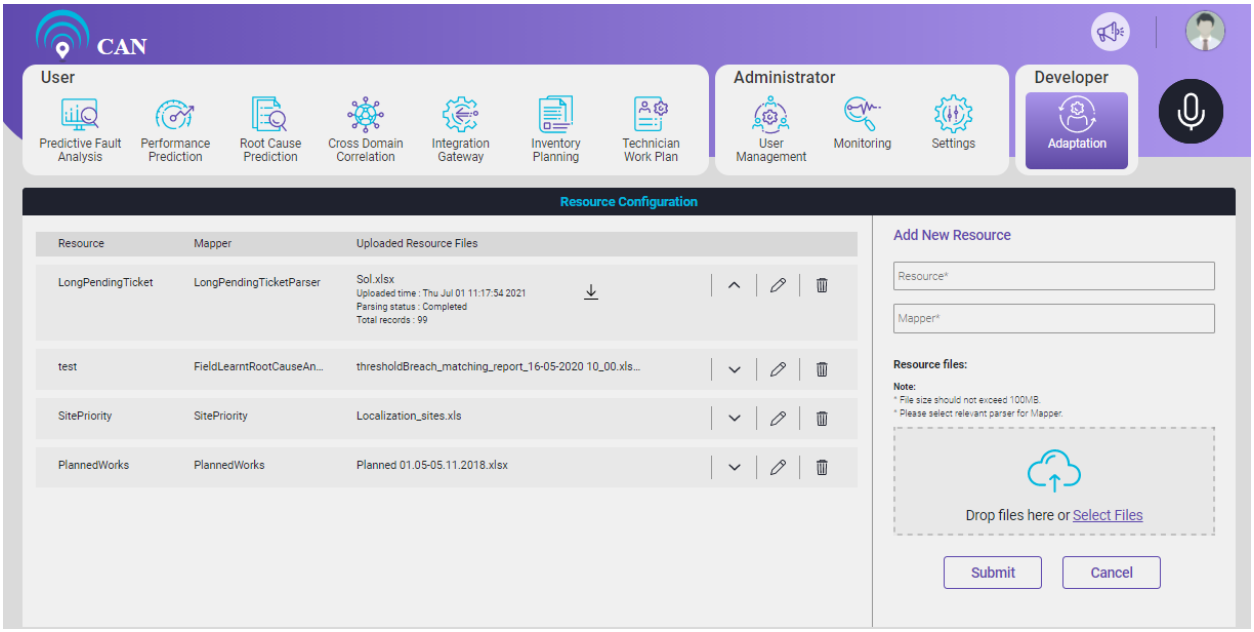


Figure 14.55 - View More Information of Resource Files

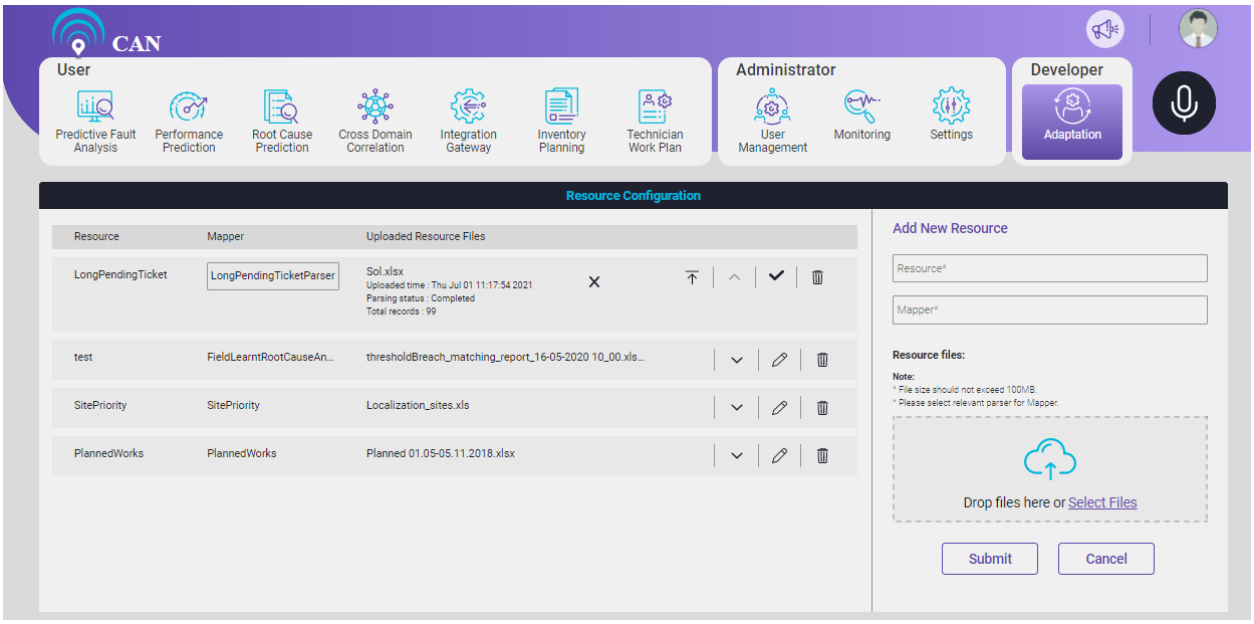


Figure 14.56 - Edit Existing Resource Files

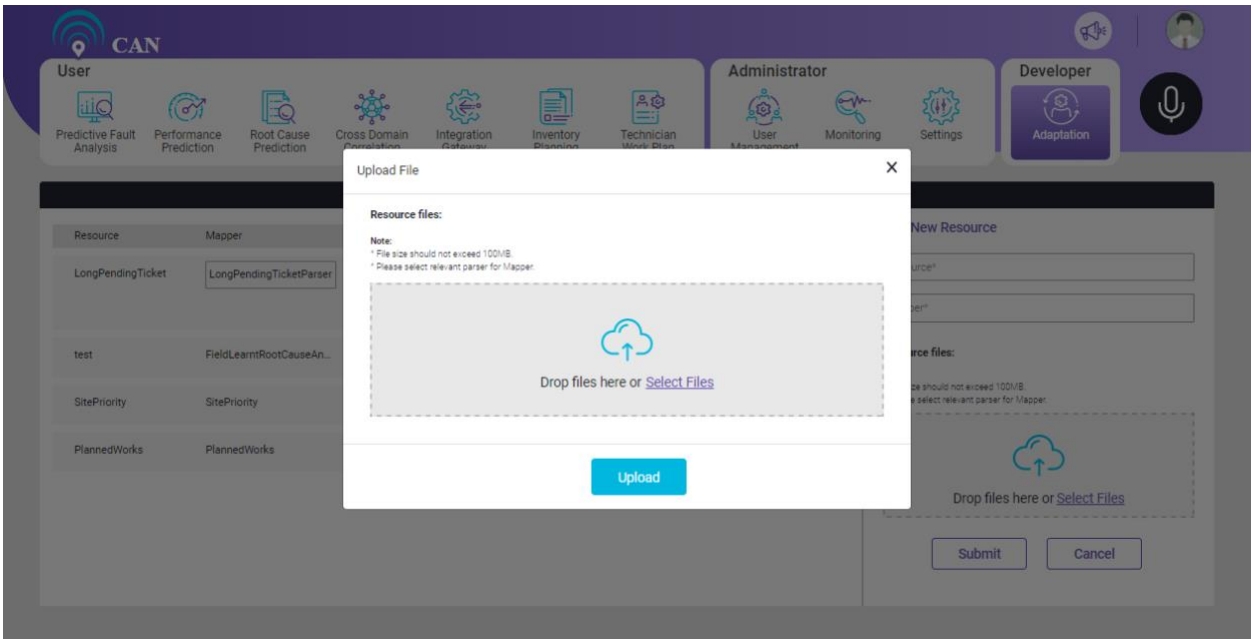


Figure 14.57 - Upload Resource Files

Advanced Configuration

Developers use this screen to configure prediction algorithm settings and General settings.

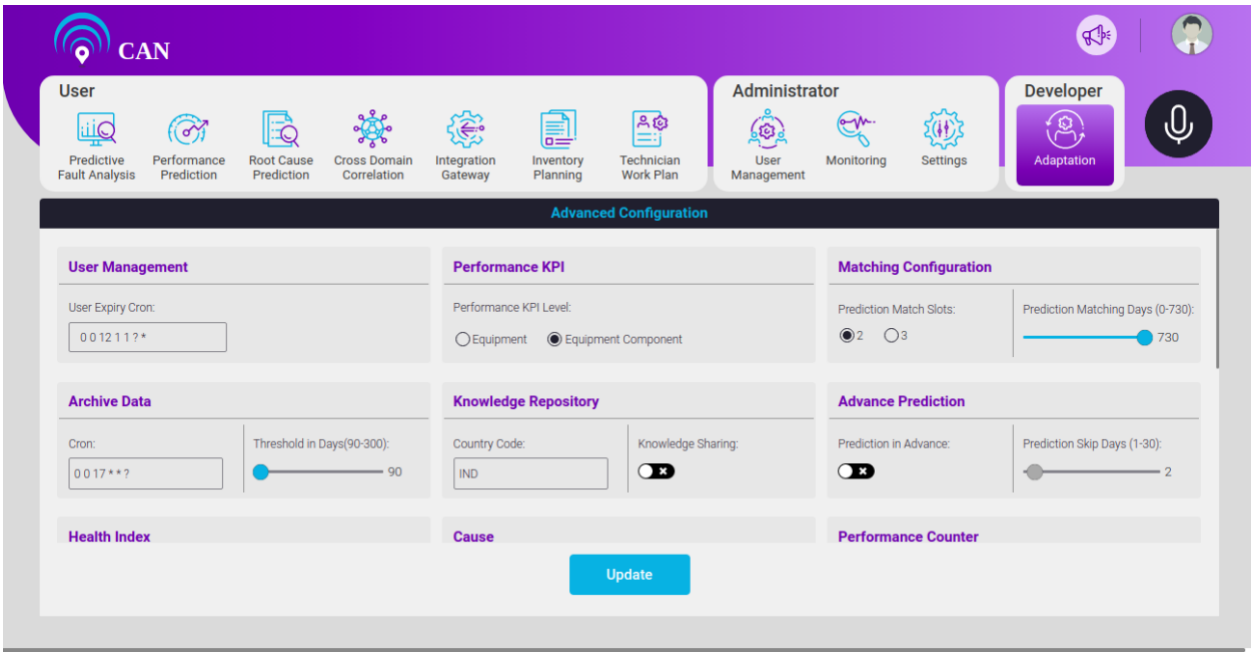


Figure 14.58 - Advanced Configuration

Advanced Configuration includes the following:

User Management

- User expiry Cron - This Cron checks the validity date of the user.

Performance KPI

- Performance KPI Level - Level at which the prediction for performance counter will happen.

Knowledge Repository

- Country Code - It shows the ISO code of a country. Example - The ISO code for India is IND or IN.
- Knowledge Sharing - This toggle button is used to enable knowledge sharing capability across all CAN deployments around the world.

Matching Configuration

- Prediction Match Slots - Decides the number of slots to be matched.
- Prediction Matching (Days) - Number of history days to be considered for matching from current day. It is mainly used for cross validation that will be performed for history dates.

Advance Prediction

- Prediction in Advance - Toggle switch to enable or disable advanced prediction.
- Prediction Skip Days - Slider that specifies number of days to be skipped for running predictions. This provides clients some buffer time to take action by sending future prediction reports.

Archive Data

- Cron - Cron pattern to schedule the archival process.
- Threshold in days - Set a slider with name Threshold in days to maintain the number of days of data in Trouble Ticket Table required to run the predictions. Older data that doesn’t fall under this set threshold will be moved to Archival table.

Health Index

- Offset - To find the minimum of non-failure probabilities.
- Scaling Factor - To find the average of failed probabilities. Divide the average value by 6. It will be the Scaling Factor.
- Warning Level - Threshold at which equipment's health is about to get deteriorated.
- Critical Level - Threshold at which equipment's health has deteriorated.

Cause

- Domain - User have a drop down to Add or Delete the domain. Domain value should be CORE or TRANSPORT or ACCESS or as per the customer data.

- Network Type - User have a drop down to Add or Delete the Network Type. The Network Type will depend on the domain. **NetworkType** should be relevant to domain and it should be unique across all the domains.
- Priority - The toggle button to set the priority.
- Service Impact - The toggle button to select the service impact.
- Category - User can configure the category as per the requirement. User have the option to Add or Delete the Cause category. INFRA and HARDWARE Category are set as default.

Performance Counter

- Data Availability (Mins) - Frequency of data availability in performance counter data.
- Prediction Interval - The period for which prediction is being made e.g. 14 days.
- Bit Sequence Length - Number of history days to be covered for prediction input.
- Slot Length - Number of days a single unit represents in the prediction input.
- Prediction Time - The enumerated data type to define the type of prediction to be done. It can take 3 values namely: ALARM, KPI and SUPERPOSED.

Visual Preferences

- Displayable Causes - Predictive Fault Analysis screen displays the filter causes as top causes. User can perform an auto search for ease of use.
- Feedback Configuration - User can choose to display the Technician feedback in fault details popup.
- Historical Faults (Days) - Fault Analysis screen displays the maximum number of closed alarm days.
- Default Representation - Select the Map view or Tabular view for the Default representations of faults.
- Display Cause Categorization - If any categorization exists, top faults can be categorized by enabling or disabling the toggle button.
- Group Tickets - When it is toggled to YES, alarms in Failure Analysis are grouped.

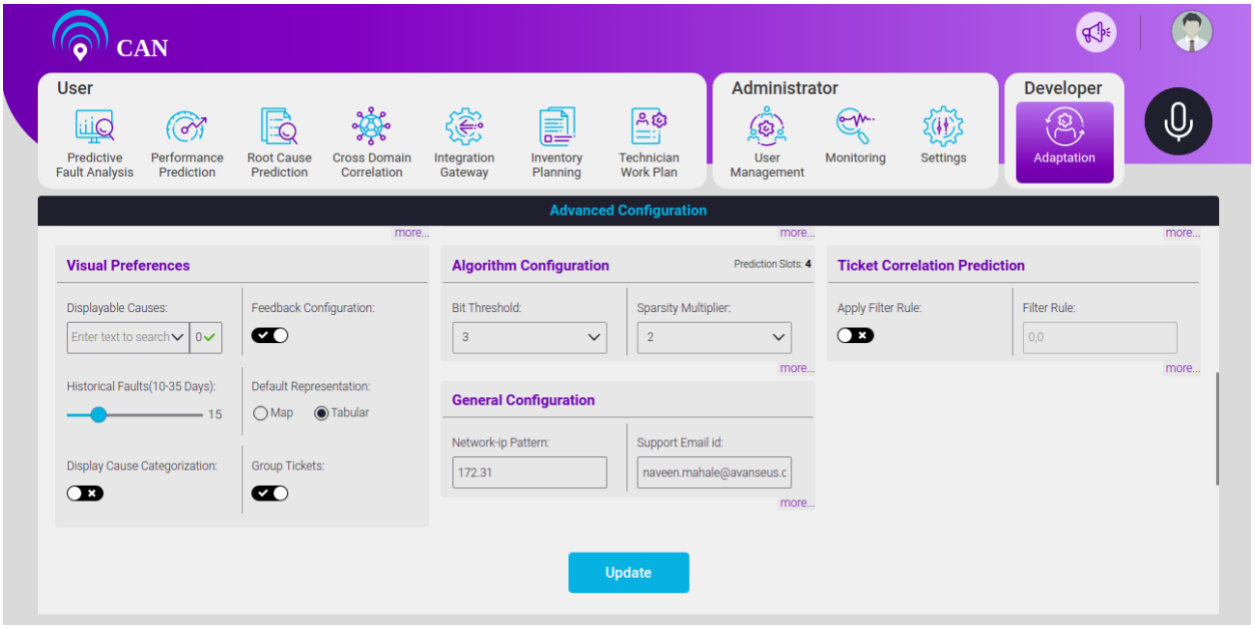


Figure 14.59 - Visual Preference Screen

Algorithm Configuration

- Bit threshold - Minimum threshold number of faults in input data in order for a fault sequence to be eligible for prediction. Please note that fault sequence is smoothened before being considered for prediction.
- Sparsity multiplier - Multiplier to go back more in history as part of variable horizon.
- Probability threshold - Probable threshold of the fault occurrence.
- Prediction Interval days - The period for which prediction is being made e.g. 7 days.
- Bit sequence length - Number of history days to be covered for prediction input.
- Slot length - Number of days a single unit represents in the prediction input.
- Display precision - In order to format the decimal values of probability in prediction report
- Prediction onset - Start day of the prediction in a week. 1 represents Sunday & 7 represents Saturday.
- Calculated prediction slots - Number of units to be considered as prediction output.

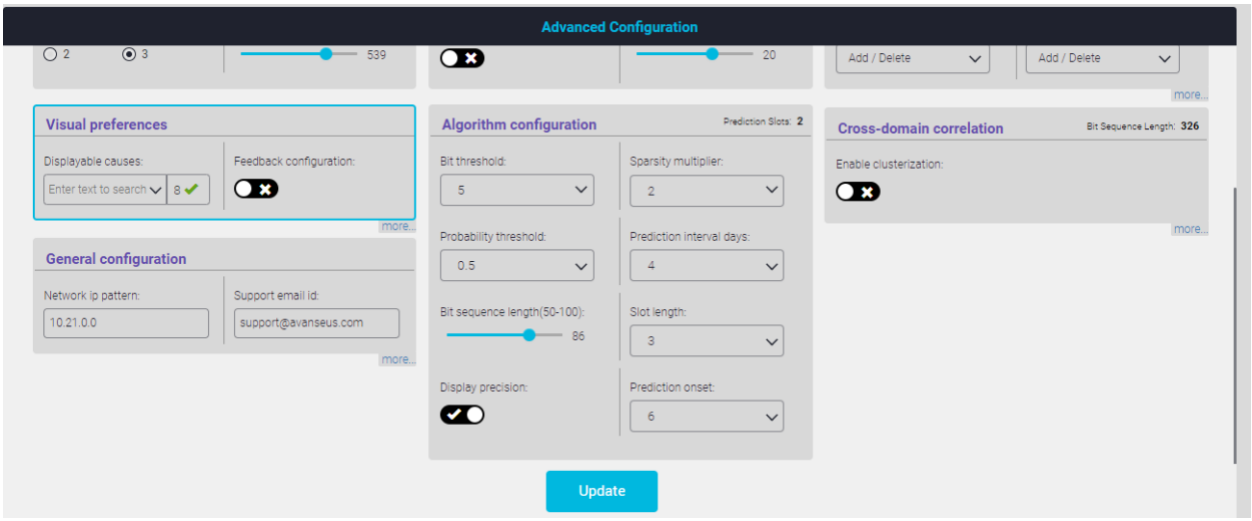


Figure 14.60 - Algorithm Configuration Screen

Cross-Domain Correlation

- Enable clusterization - Enable clusterization switch decides whether to display the configuration part or do the clustering.

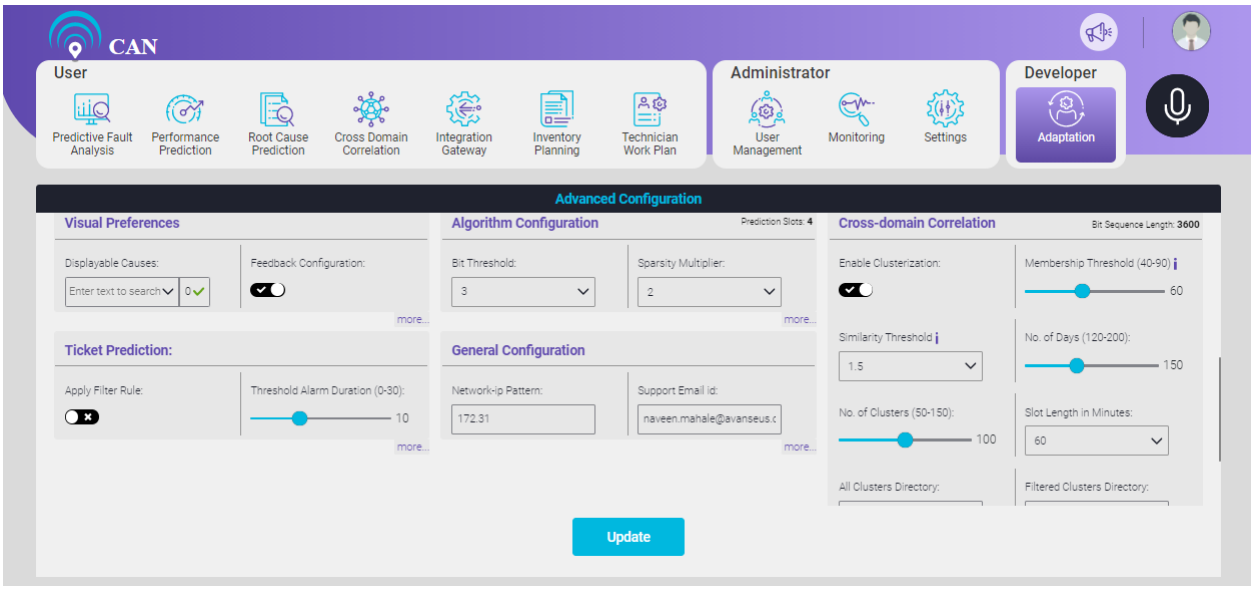


Figure 14.61 - Cross Domain Correlation Screen

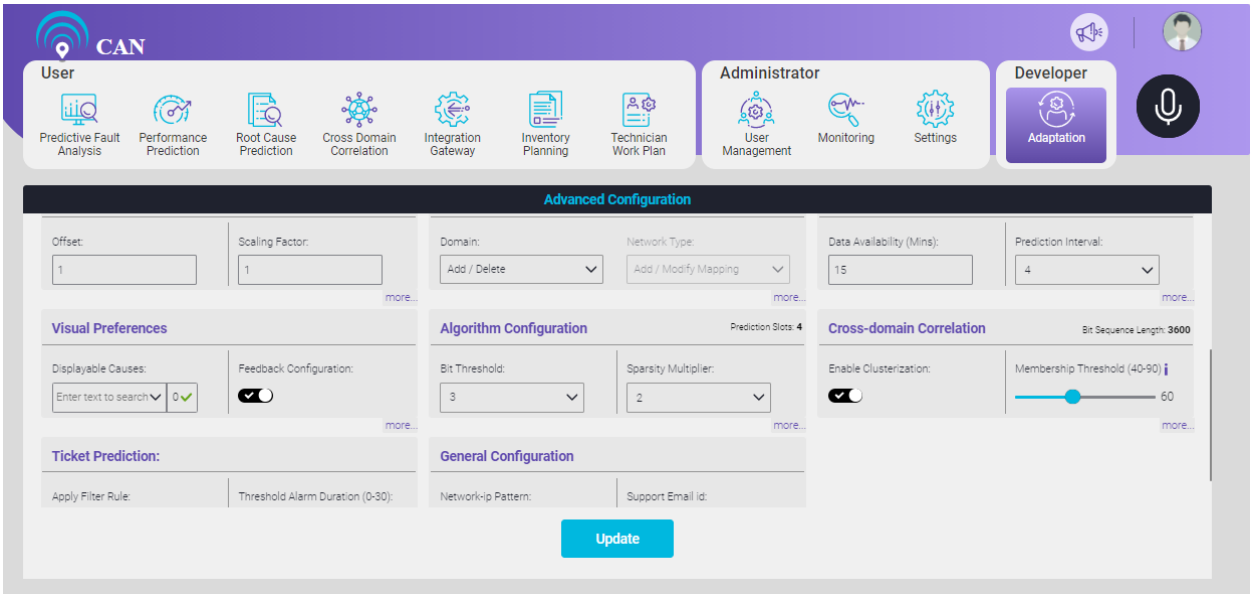


Figure 14.62 - Enable Clusterization Switch

- Membership threshold - It displays the percentage of faults where “Similarity threshold” are within the specified limits. User can select the value moving the slider between the min value and max value i.e. (40% to 90% respectively).
- Similarity threshold - It displays the percentage of interrelated faults occurring together across the same or different sites. User can select the value using arrow keys. (Range is 0.5 - 3).
- No. of days - User can select the No. of days to run the cluster. User can select the values using slider between the min value and max value i.e. (120 to 200 respectively).
- No. of clusters - It allows the user to select maximum No. of clusters for each zone. User can select the values using slider between the min value and max value i.e. (50 to 150 respectively).

Note: Slot length in minutes - It allows the user to select the number of hours from the drop down menu. User can select a slot from the drop down menu. The slot divides the day into different hours.

- Directory for all clusters - Relative path of the folder in which cluster details will be saved as a file.
- Directory for filtered clusters - Relative path of the folder in which filtered cluster details will be saved as a file.
- Cron - It runs the “Cross-domain correlation” automatically at specific time.
- Calculated bit sequence length - Length of bit sequence which will be generated after checking whether faults have occurred or not in each slots for total no. of days.
- [Calculated bit sequence length = 1440*(No of days)/ ((Slot Length in minutes) *60)].

Ticket Correlation Prediction

- Apply Filter Rule - Use the toggle switch to enable the Filter Rule. User can change the Filter Rule once the toggle switch is in Enable mode.
- Filter Rule - User will use the Filter Rule to improve the overall accuracy of prediction and mainly to optimize the prediction results.

- Manual Threshold Alarm Duration - This is the alarm duration to get considered during the Manual Ticket Correlation Prediction. User can slide the slider to set the duration of the alarm (0-30) minutes.
- Slot Length - Number of days a single unit represents in the prediction input.
- Bit Sequence Length - Number of history days to be covered for prediction input.
- Prediction Interval Days - The period for which prediction is being made e.g. 14 days.
- Bit Threshold - Minimum threshold number of faults in input data in order for a fault sequence to be eligible for prediction.
- Auto Threshold Alarm Duration - This is the alarm duration to get considered during the Auto Ticket Correlation Prediction. User can slide the slider to set the duration of the alarm (0-2) minutes.
- Manual Ticket Correlation Level - It correlates the alarms and tickets. The Corelation level for Manual Ticket Corelation prediction.
- Threshold Probability - Probable threshold of the fault occurrence.

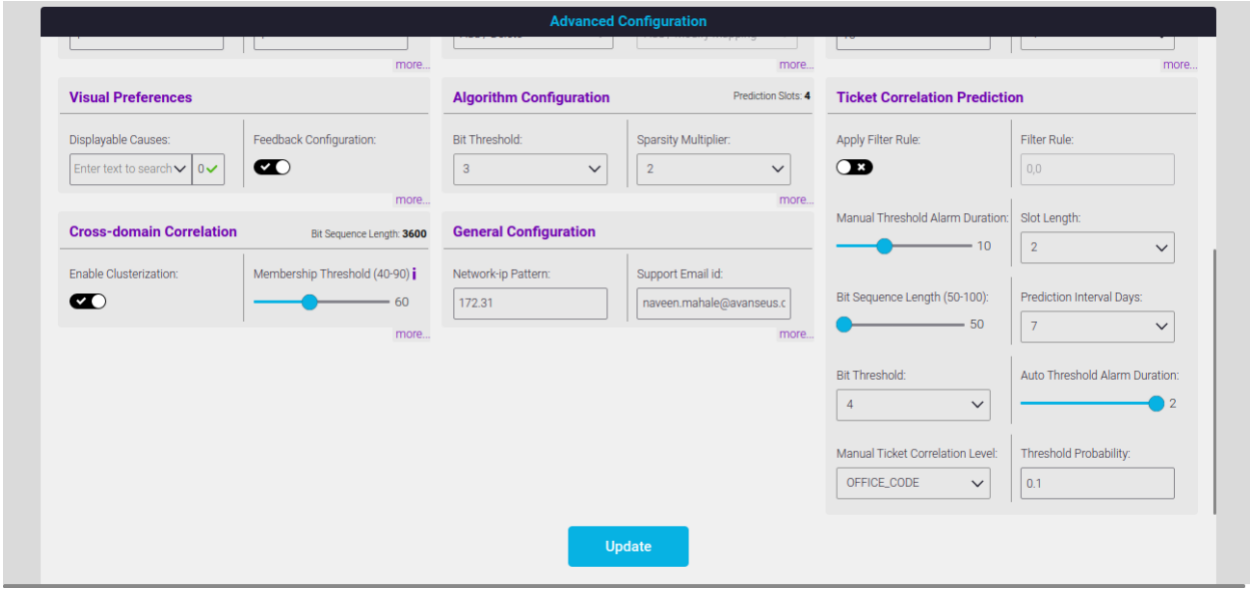


Figure 14.63 - Ticket Correlation Prediction

General Configuration

- Network IP pattern - IP pattern prefix where the prediction process needs to bind.
- Support email id - Mail id of CAN support team.
- Fault data type - Input data (Alarm, Ticket, etc.)
- Customer - Customer name for whom the reports would be generated.
- Alarm collection - Cron to initiate UI table population on a daily basis.
- Recommend technical query execution - Decides whether or not to run Technician related queries.
- Alarm collection days - Number of days of data to be maintained for rendering UI.
- Cause based precision coverage - It displays the Number of top faults in Predictive Fault Analysis and Fault Analysis screen.

- Deduplicated count - Cron to calculate Deduplicated count for alarms and tickets on a daily basis.
- Recommendations - Number of recommendations needs to be shown during report generation.
- Fault key separator - Key separator or delimiter in prediction input data.
- Display inventory - Switch that decides whether to display Inventory table or not in Inventory Planning screen.
- Expected day date format - It decides the day date format.

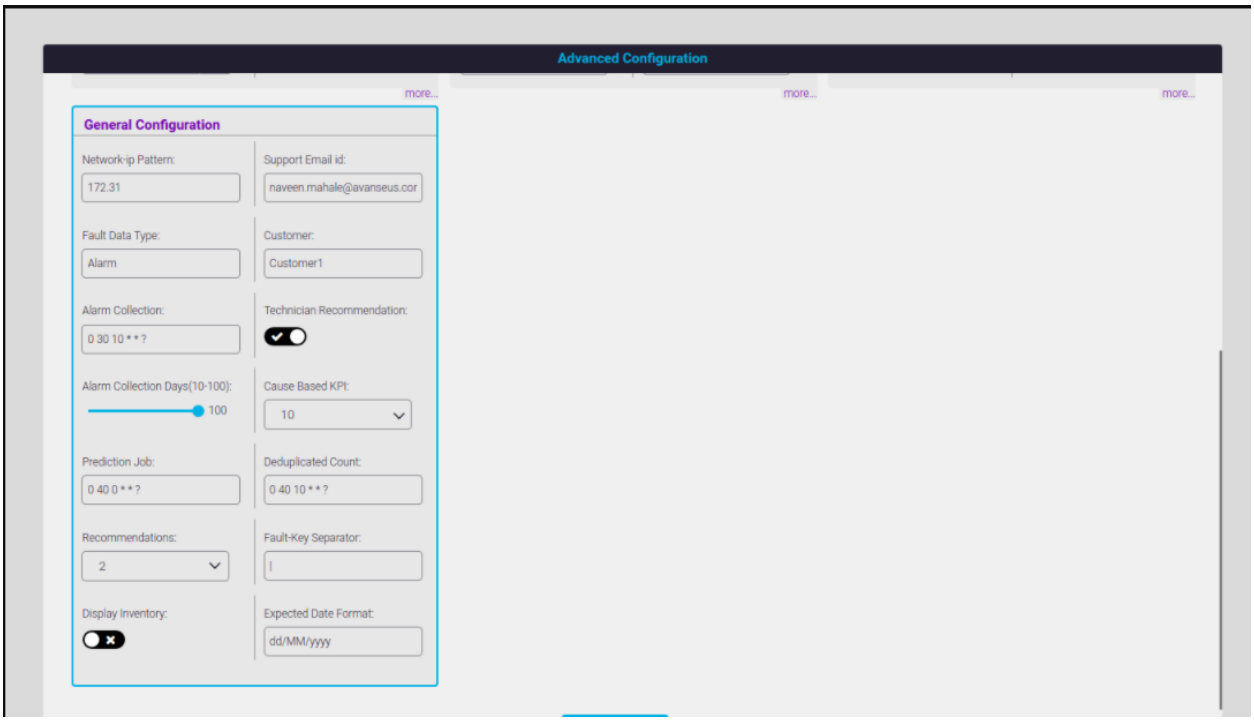


Figure 14.64 - General Configuration

RoE

Return on Effort (RoE) index based prediction shortlisting is a way of selecting a particular subset of predicted faults which are more impactful or likely to happen and highlighting them in the prediction report. This impact or likelihood of faults are determined by taking cumulative effects as measured by weight indices of different parameters like fault history, ticket history, alarm occurrences etc.

By default, some policies are configured under policy configuration, those can be used during RoE configuration.

RoE configuration consist of 2 tabs:

- Policy Configuration: User can create or modify policies, under each policy user can configure different RoE parameters with their respective limits and weightages.
- Sheet Configuration: Different sheets from prediction report where RoE needs to be applied are sconfigured.

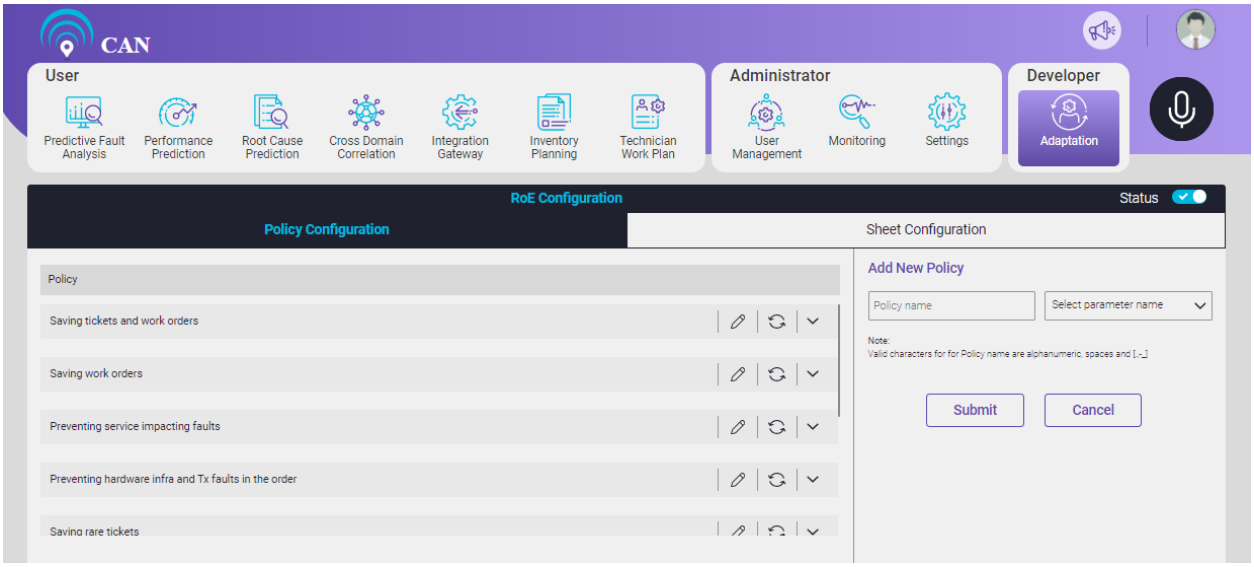


Figure 14.65 - Default RoE Weightage Configuration

Policy Configuration

To Add New Policy Configuration for ROE

1. Write the **Policy Name** in the Policy Name text box.
2. Select the name of parameter from the **Select parameter name** drop down menu.

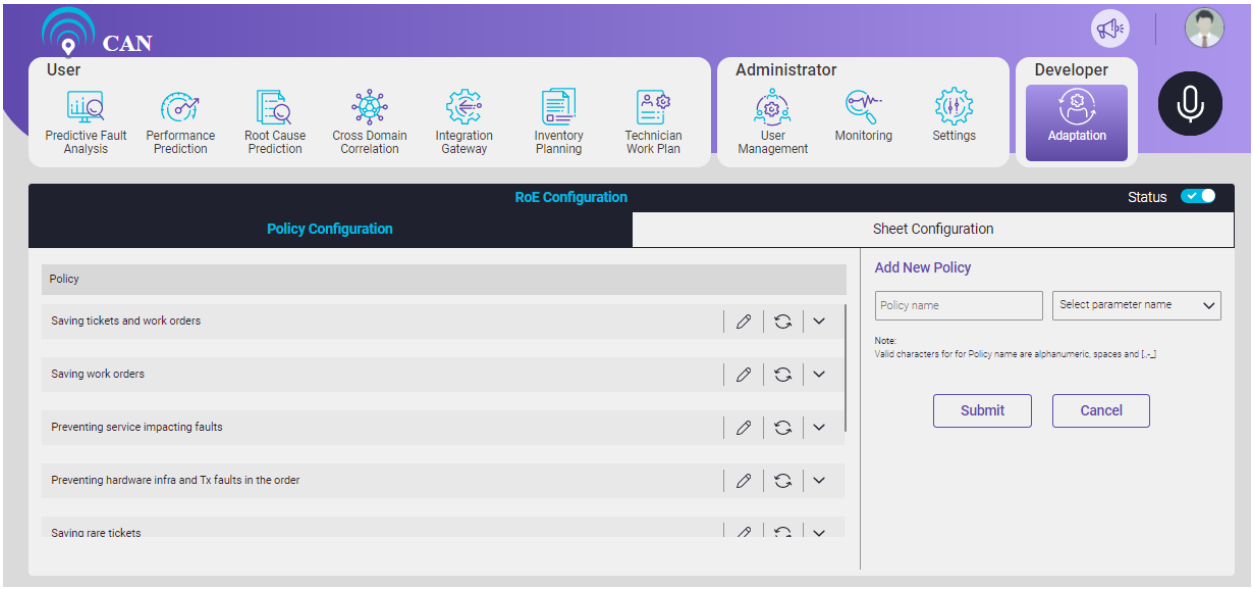


Figure 14.66 - Policy in Policy Configuration

3. Click the Parameter value icon </>.

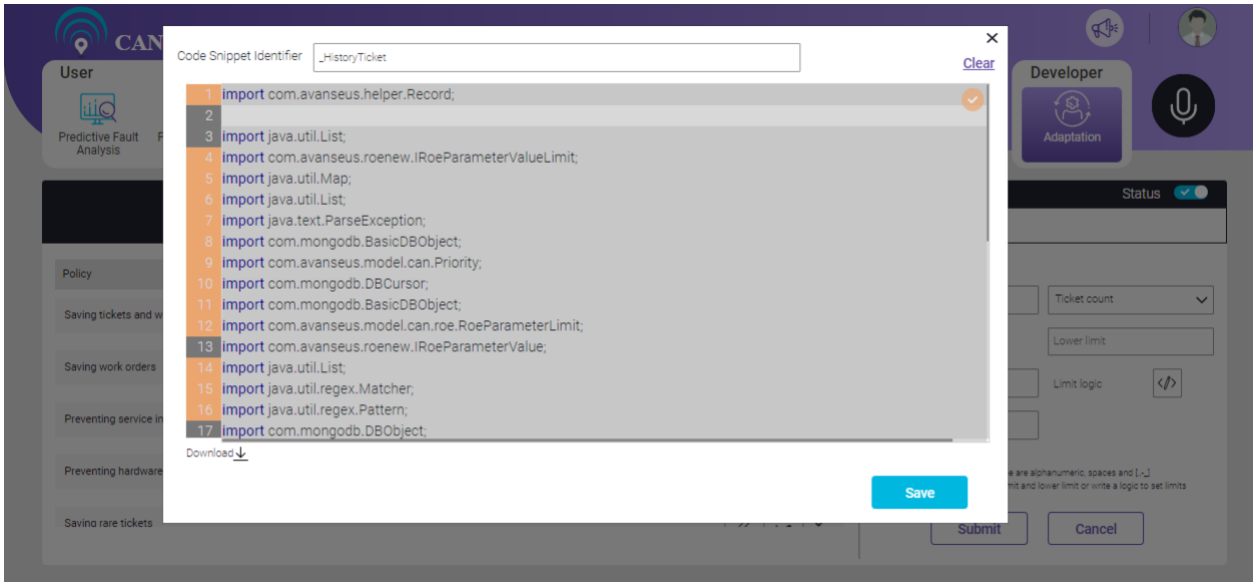


Figure 14.67 - Code Snippet for Parameter Value

Note: Parameter value code snippet is not mandatory.

User can write a valid class name and corresponding code in text area to fetch the parameter value. To save the code, click the **'Save'** button.

User need to write a logic to fetch the value of a parameter. This is not a mandatory field. User can directly access the value using parameter name from Predicted fault, then code is not required. User need to write logic to fetch the value when the value cannot be fetched directly by the parameter name. A default code for an **Alarm count, Ticket count, Ticket correlation, Work order count, Priority, Cause category,** and **Service impacting** is already present.

Sample java code to fetch parameter value

```
List<String> historyTickets = (List<String> ) dbObject.get("historyTickets");
Double count = null ;
if(historyTickets!=null){
    count = Double.valueOf(historyTickets.size());
}

return count;
```

Figure 14.68 - Logic to Fetch Number of Tickets

Note: The java code will implement IRoeParameterValue interface which provides "dbObject" as parameter.

This implementation needs code snippet. It doesn't require class definitions. In the implementation return statement is mandatory which expects user to return a "Double" value.

Code snippet written within text area overrides the **fetchValue** method.

4. Set the lower limit of parameter value.
5. Set the upper limit of parameter value.
6. Click the Limit Logic </>, a popup opens.

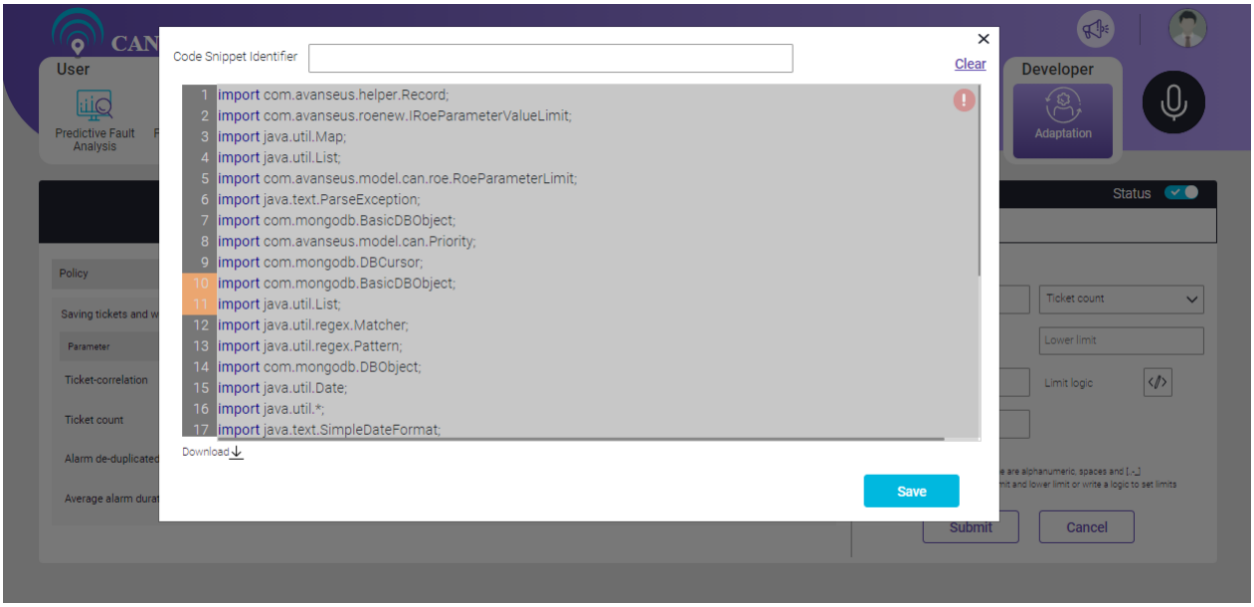


Figure 14.69 - Code Snippet for Parameter Limit

Code snippet written within text area overrides the **setLimits** method.
To set the limits (both upper and lower limit), user can write a valid class name and corresponding code in the text area. User must save this code. To save the code, click the **'Save'** button. Once the code is saved the upper and lower limit fields are disabled and the values set in the code is taken into consideration for weight index calculation.

Sample java code to set limit logic

The java code will actually implement IRoeParameterValueLimit interface which provides predictedFaultCursor as parameter and expects RoeParameterLimit as return type.

```
RoeParameterLimit roeParameterLimit = new RoeParameterLimit();
roeParameterLimit.setLowerLimit(0.0);
roeParameterLimit.setUpperLimit(4.0);
return roeParameterLimit;
```

7. Assign **Weightage** to each parameter such that sum of them equals 1.0.
8. Click the **Submit** button to Add New Policy.

To Edit New Policy Configuration for ROE

1. Click the modify icon on the left side of the screen to edit the New policy configuration.
2. Edit the Parameter value, Lower Limit, Upper Limit, Limit Logic, Weightage.
3. Click update icon to save the changes.
4. If user want to revert the changes of the Parameter, user can click .

Note: Revert option is available only for default policies and its default parameters.

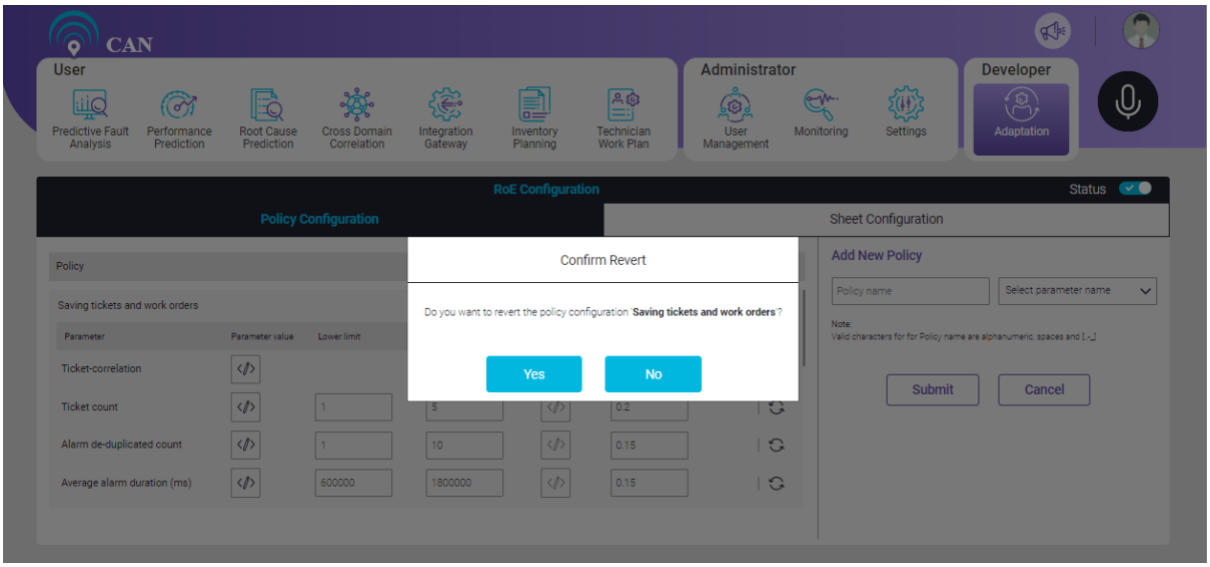


Figure 14.70 - Revert Confirmation Message

5. User can use the delete icon to delete the particular parameter row in the User added New Policy.

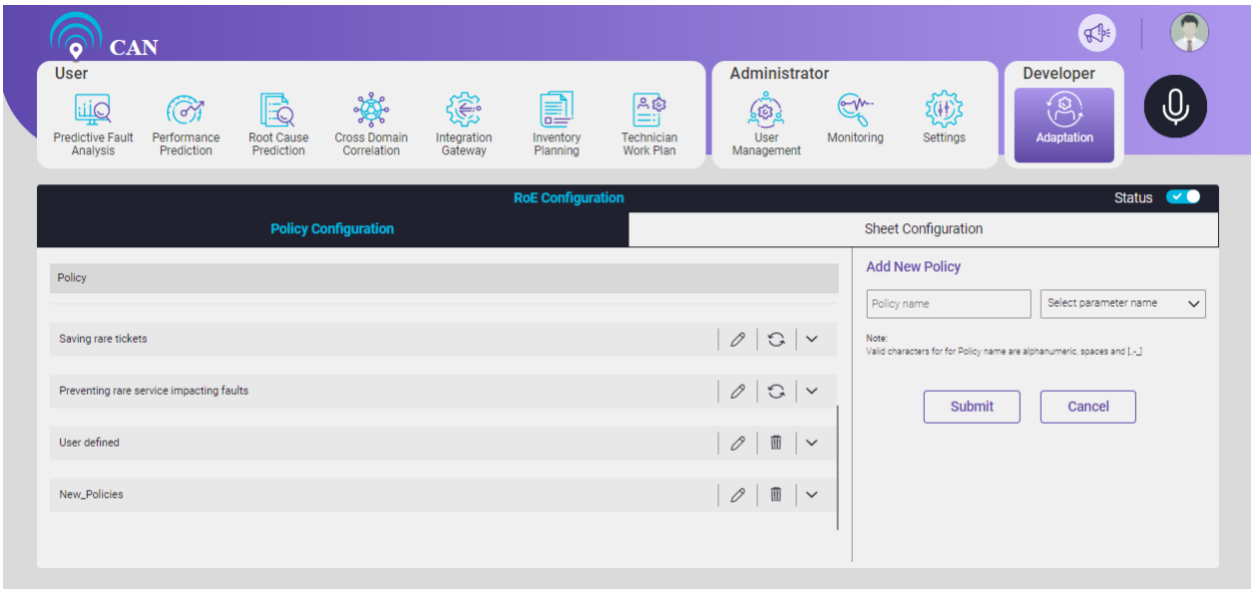


Figure 14.71 - Delete Icon in User Added New Policy

6. Click **Yes** button to delete the Newly Added New Policy. Click **No** if you don't want to delete.

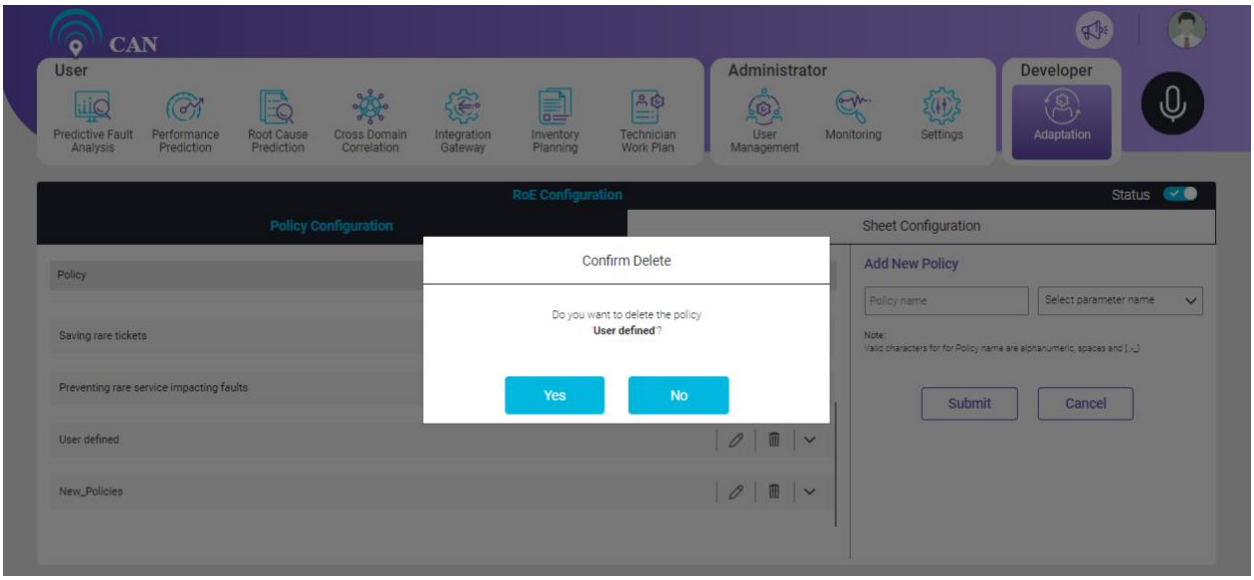


Figure 14.72 - Delete Confirmation Message

To enable/disable RoE, use the toggle button.

Sheet Configuration

By default, no sheets are configured in Sheet Configuration tab.

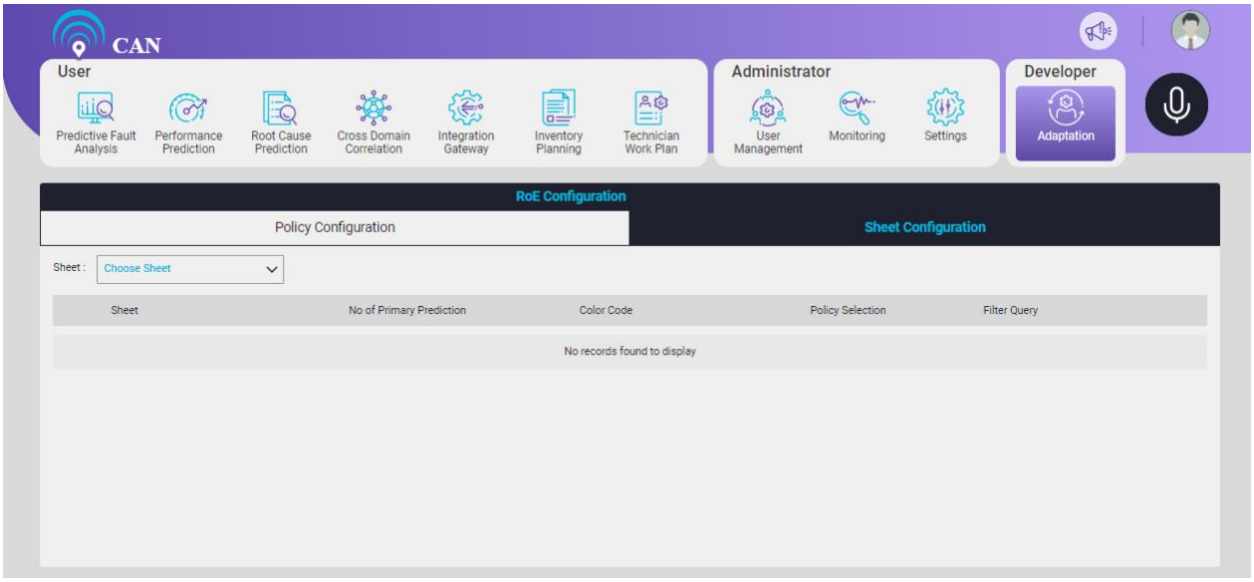


Figure 14.73 - Default View of Sheet Configuration Tab

User can choose the sheet from the drop down menu. Select any of the sheet to save a default configuration.

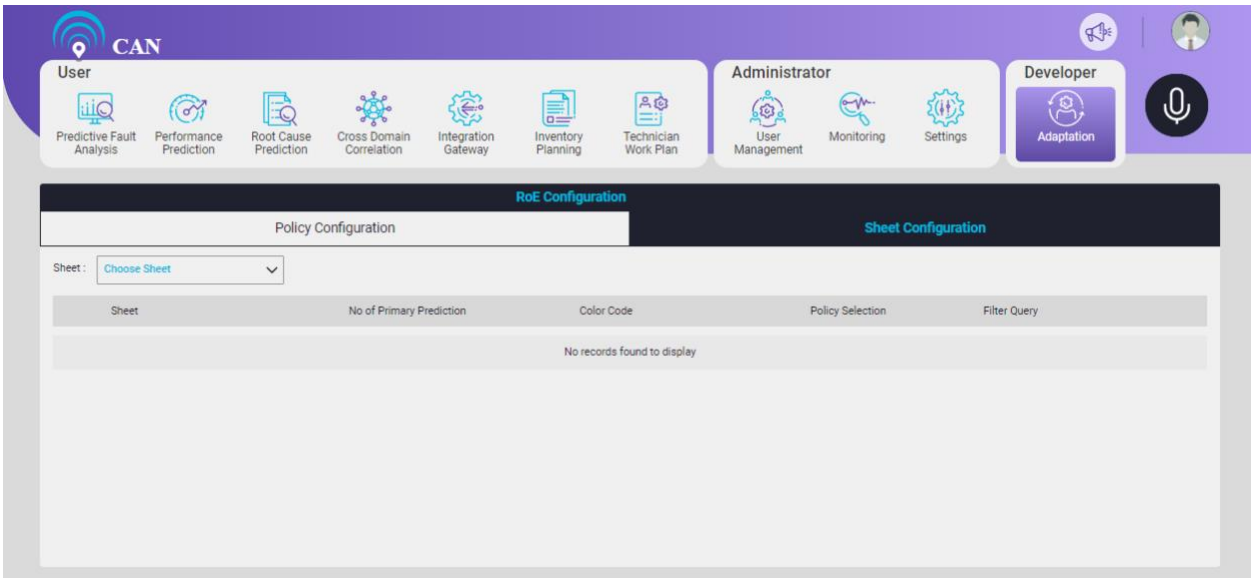
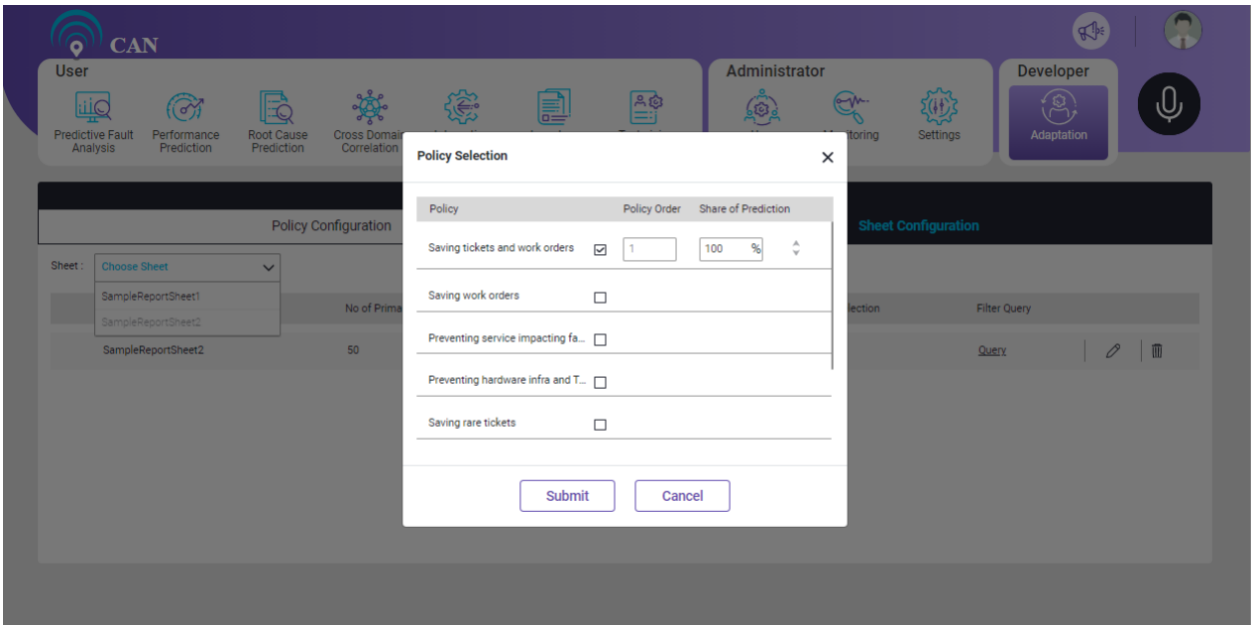


Figure 14.74 - Drop Down to Choose Sheet

When you select the sheet, the below screen will pop up. You can select the Policy and edit the details of **Policy Order** and **Share of Prediction.**



User can see the details of the Policy Selection. To see the details, under **Policy Selection**, click **Policy**.

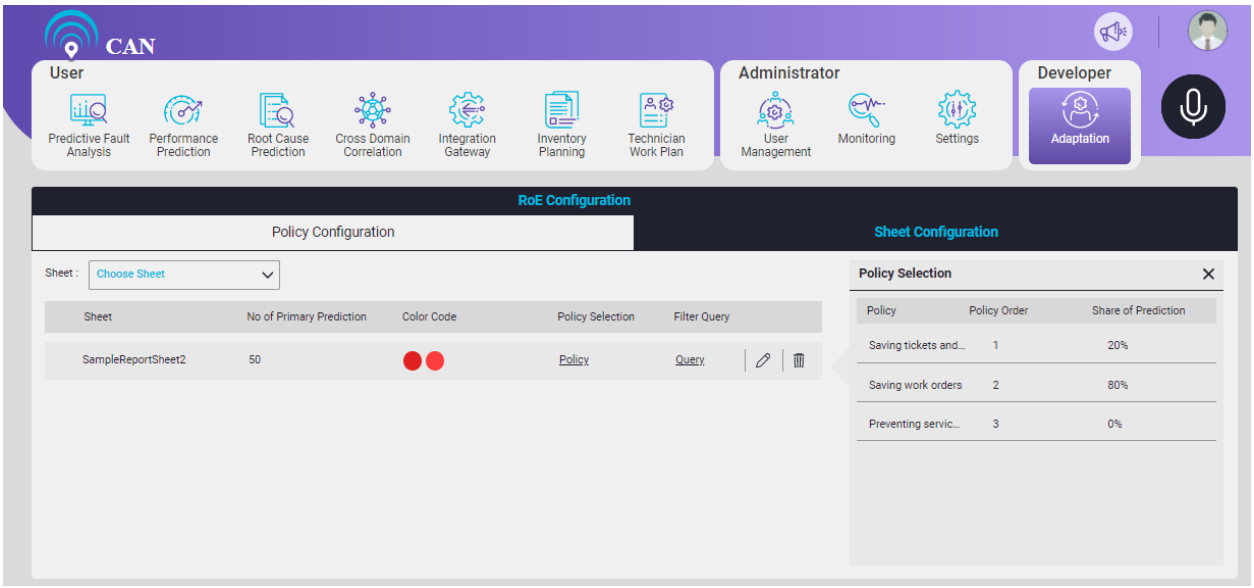


Figure 14.75 - Policy Selection Details

To delete the configuration of the sheet, click the delete icon .

When you click the delete icon, the below screen will pop up. Click **Yes** to confirm the delete command.

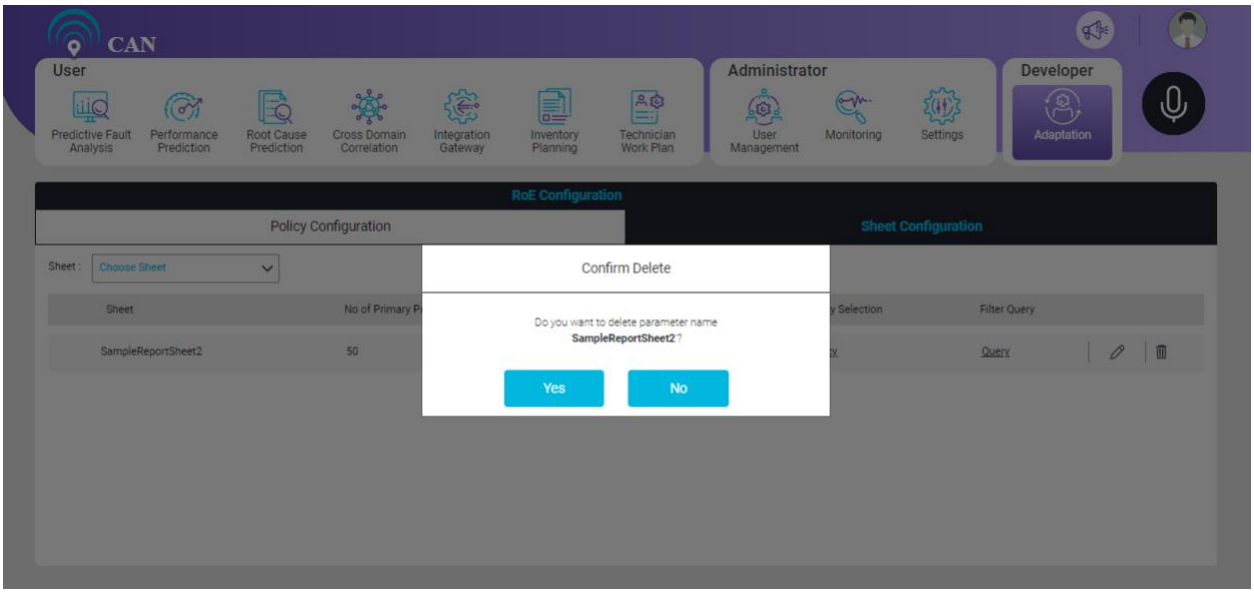


Figure 14.76 - Delete the Configuration for SampleSheet2

Configurations provided in this tab are:

1. Filter query: User can add single or multiple queries.
2. No. of primary prediction: Total number of primary predictions required to be colored in the prediction report.
3. Color code: Color of primary prediction rows of prediction report.

When multiple queries are added then predictions in the prediction report appear based on the sequence of added queries.

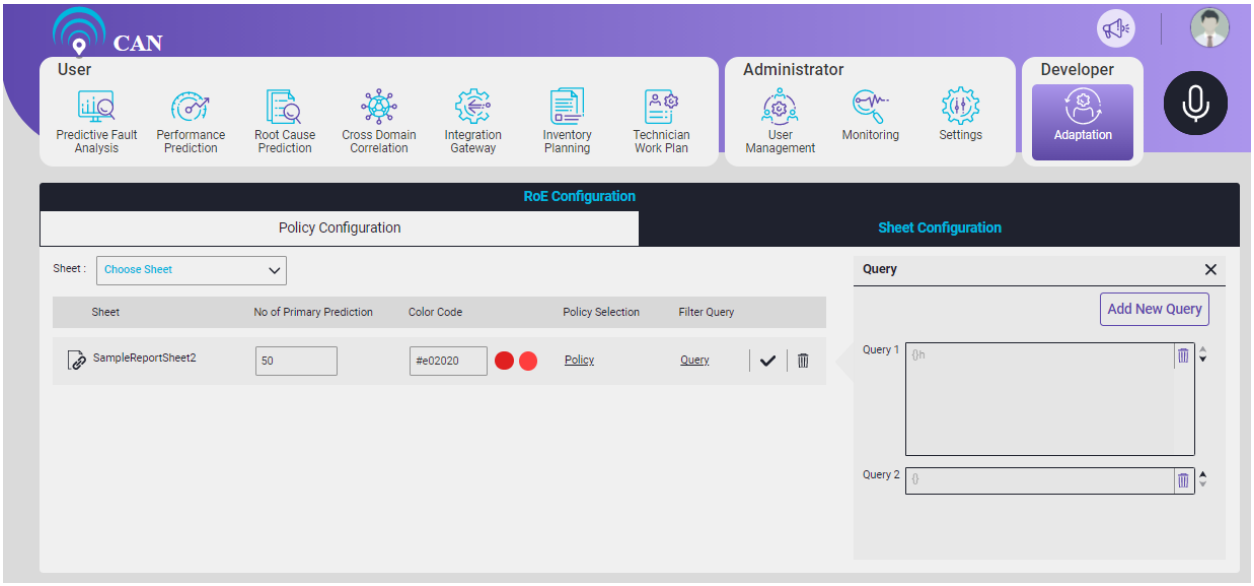


Figure 14.77 - Multiple Filter Query Configured

The above figure displays two filter query. Predictions in report will first appear based on the first query and then the second query.

Note: The second color box's color changes automatically with lesser intensity as that of first color box to indicate the color of secondary predictions.

User can add multiple queries. To add multiple queries, click the Add new query button. Once a new text box appears, click the text box to open a pop up. User can write json query in the text box. All the keys of json query must be enclosed within double quotes.

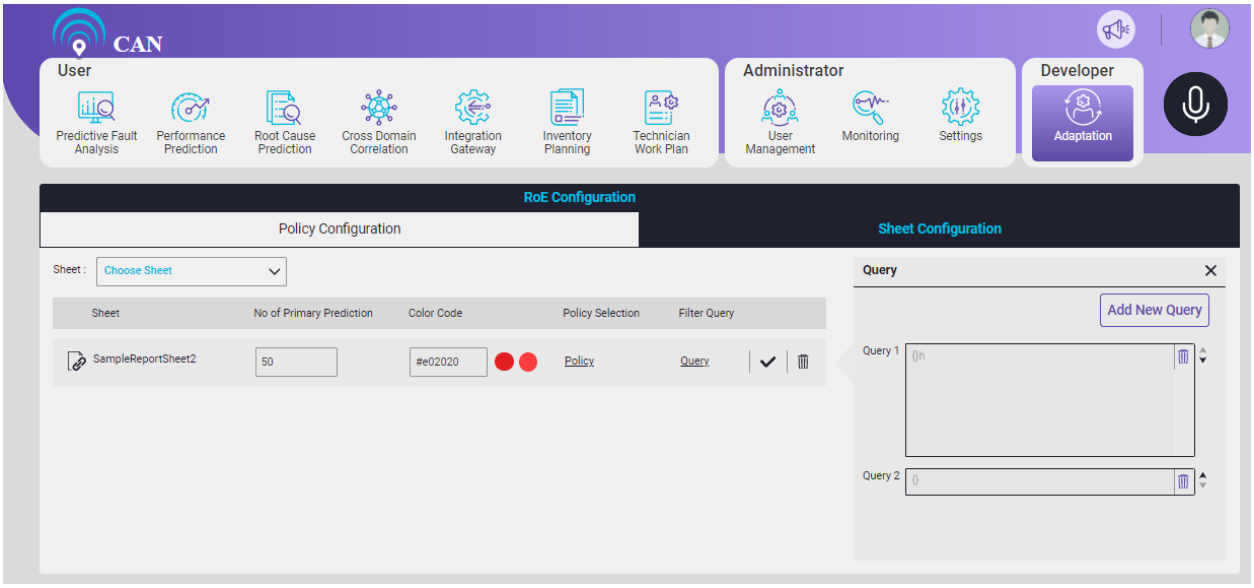


Figure 14.78 - Pop up to Write Query in json Format

Linking

RoE can also be extended from a parent sheet to another sheet of prediction report if the total number of primary predictions appearing in the parent sheet is lesser than the number specified in the configuration.

Linking feature is available for all the sheets in excel report. To link multiple sheets to a parent sheet, use the linking icon . When the user clicks the link icon, the screen displays all sheets available for linking on the left hand side and the list of all sheets already linked on right hand side.

When no sheets are available the screen displays a message "No sheets linked". A sheet can link only those sheets which are appearing later in prediction report. For example: if Test1, Test2, Test3, Test4, Test5, Test6 is the sequence of the sheets in excel report then Test1 can be linked to Test2, Test3, Test4, Test5, Test6. Test2 cannot be linked to Test1 but can be linked to Test3, Test4, Test5 and Test6.

To link sheets from the pool of available sheets, click the sheet name. The sheet moves to linked sheet names from available sheet name list.

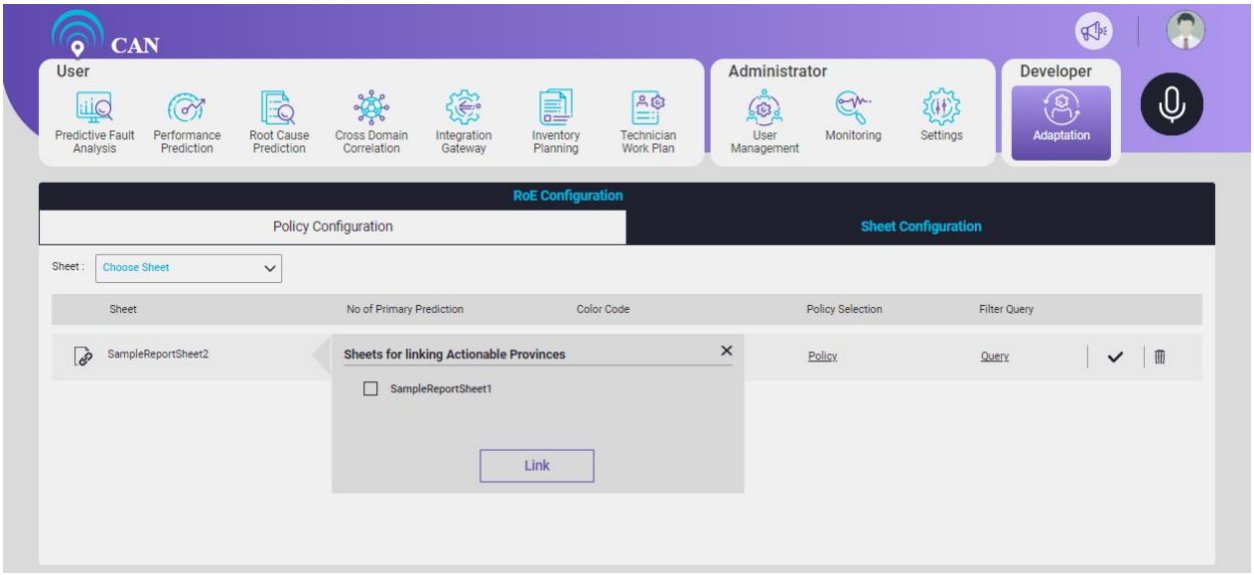


Figure 14.79 - Linked sheets

Select the sheets to be linked, click the **Link** button to link the sheets.

Performance Configuration

Performance Configuration gives information on threshold configuration based on the KPI's.

Individual component can have many KPI's parameters.

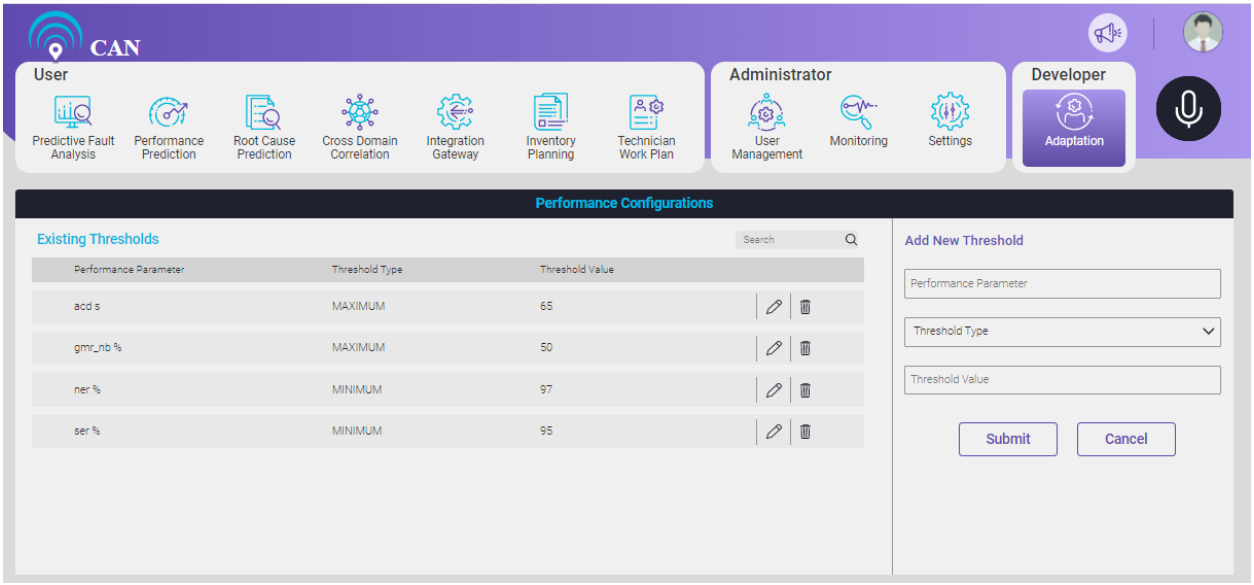


Figure 14.80 - Performance Configuration Screen

To Add New Threshold

1. Write the Performance Parameter in the **Performance Parameter** text box.
2. Select the Threshold Type to Maximum or Minimum from the **Threshold Type** drop down menu.

3. Write the **Threshold Value** in the Threshold Value text box.
4. Click the **Submit** button to Add New Threshold. Click the **Cancel** button if you don't want to Add New Threshold.

To Edit the Existing Threshold

1. Click the edit icon .
2. Change the Threshold Type or Threshold Value.
3. Click the save icon to save the changes.
4. Click the delete icon to delete the particular Performance Parameter.

Integration Configuration

Integration Configuration has four tabs:

- BMC Ticket Configuration
- ServiceNow Configuration
- Weather Configuration
- Splunk Configuration

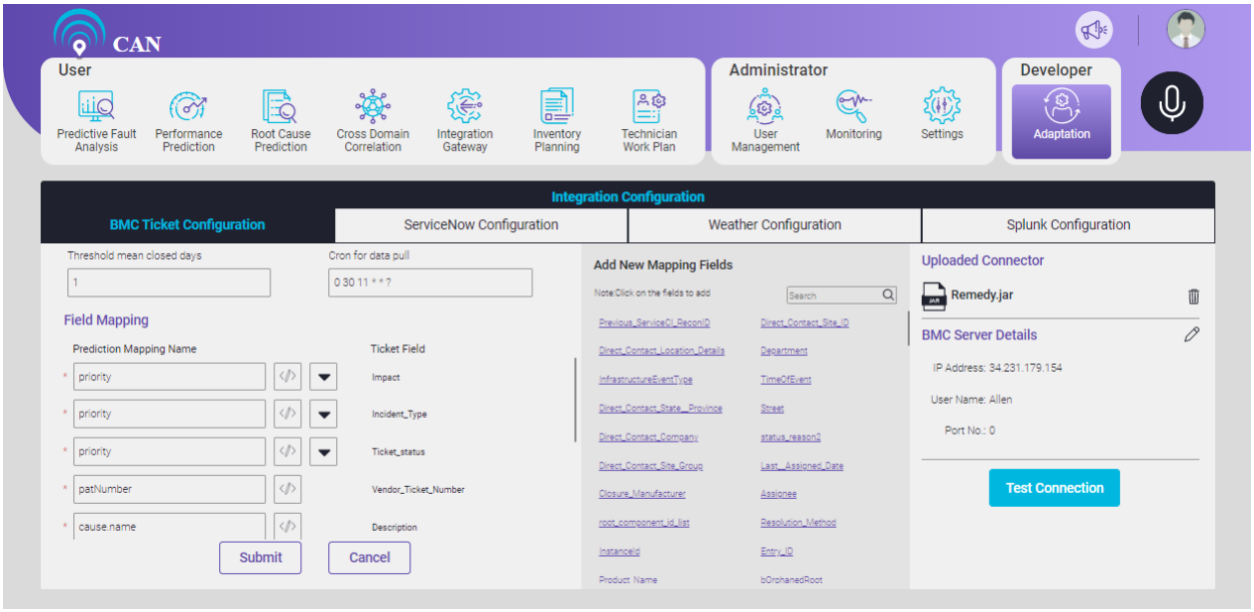


Figure 14.81 - Integration Configuration Screen

BMC Ticket Configuration

By default, no BMC Ticket is configured in the BMC Ticket Configuration.

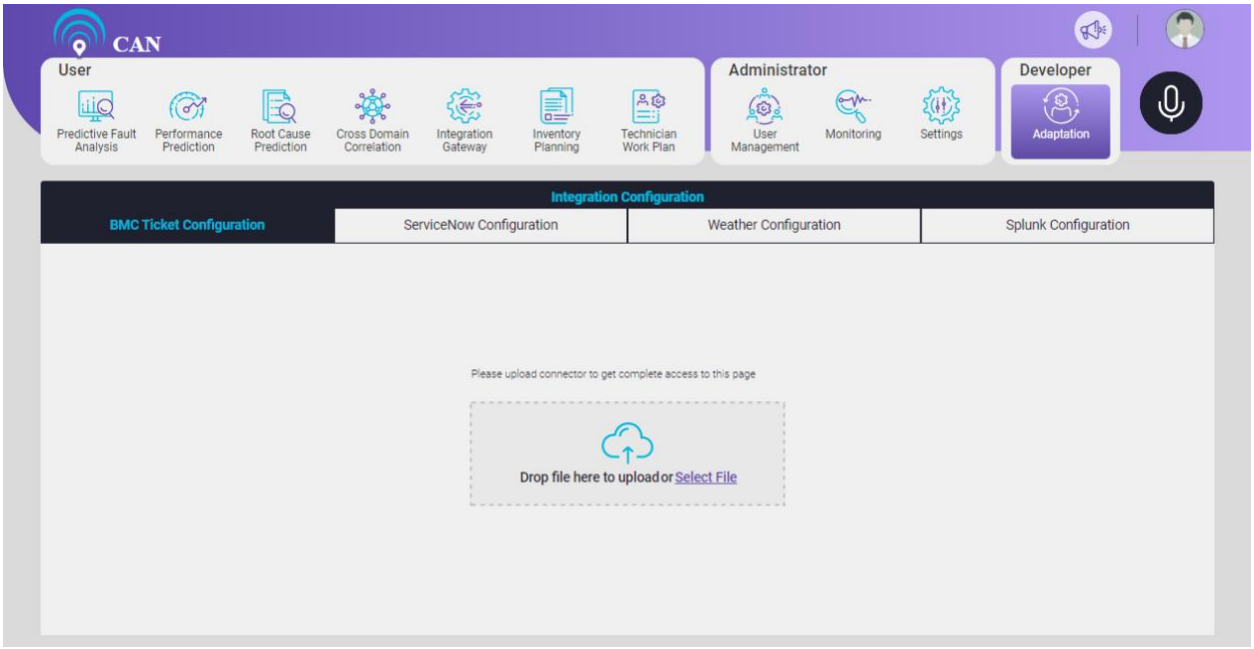


Figure 14.82 - BMC Ticket Configuration Screen

User need to upload the connector (Remedy.Jar) file to get the complete access of the page.

User can upload the file. To upload the file, user can drag and drop the file or select the file to upload.

To Configure the BMC Ticket

1. Connect to the BMC remedy by uploading the connector (.jar) file.
2. In the BMC server details, click the edit icon .
    a. Write the IP Address in the IP Address text box.
    b. Write the user name (For example - Allen) in the User Name text box.
    c. Write the Password in the Password text box.
    d. Write the Port No. in the Port No. text box.

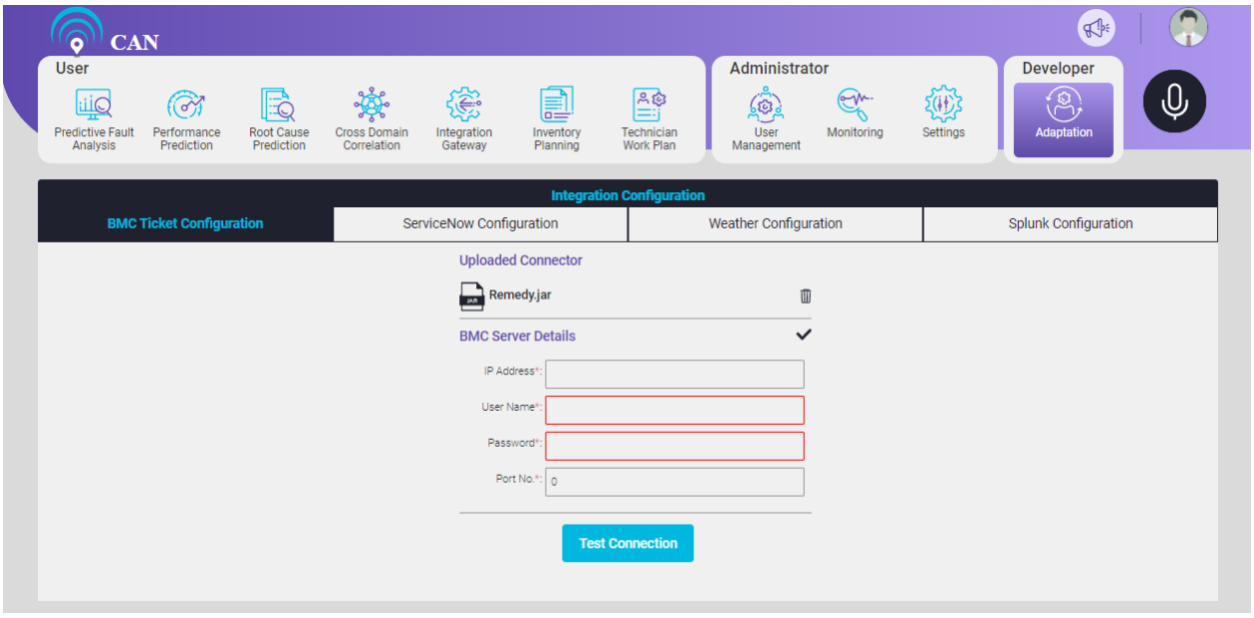


Figure 14.83 - BMC Server Details

3. Click the **Test Connection** button.

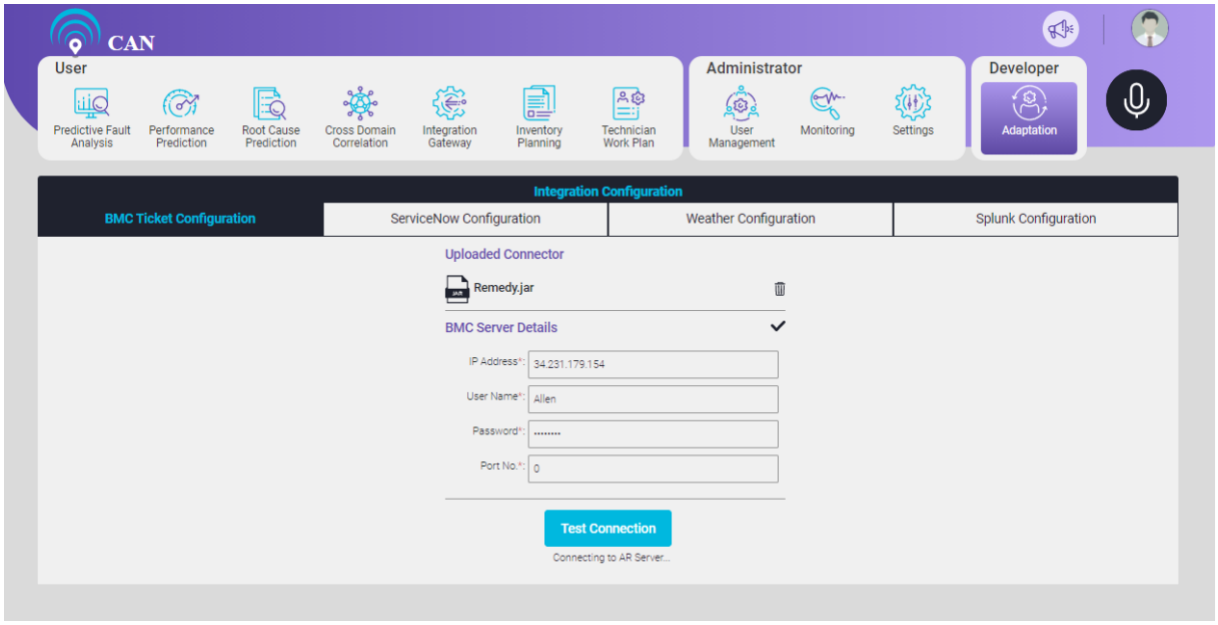


Figure 14.84 - BMC Ticket Test Connection

In BMC ticket configuration we map the prediction fields to BMC tickets.

BMC Integration screen shows **Field Mapping** components on the left side of the screen and **Add New Mapping Fields** on the centre of the screen.

We map the fields or add the new mapping fields as per the customer's requirements.

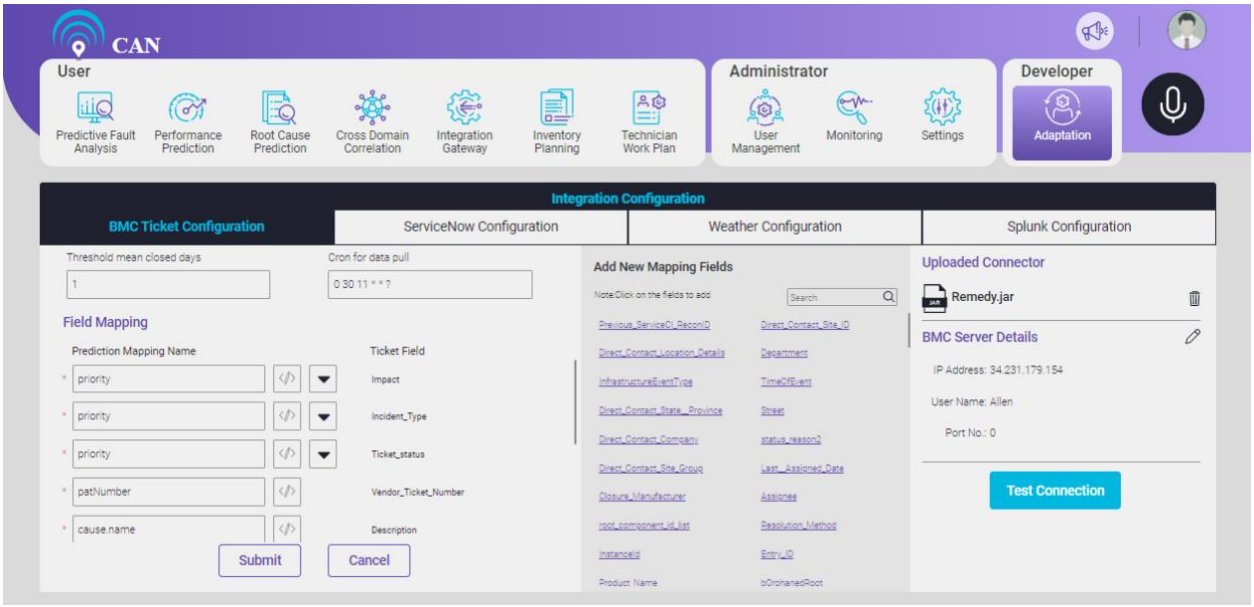


Figure 14.85 - BMC Ticket Configuration Screen

Click the icon </> to edit the mapping codes. User can see the saved configuration. User can write the corresponding java mapping code in the text area. It will automatically get compiled. Click the **Save** button to save the changes.

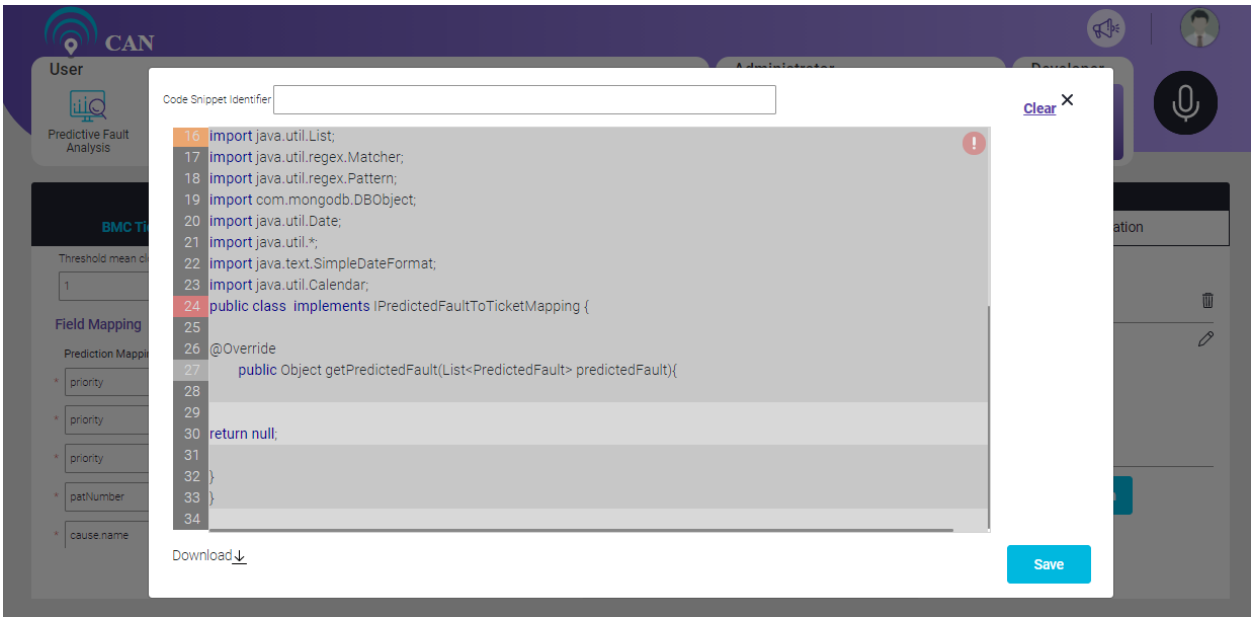


Figure 14.86 - BMC Ticket Configuration Code for Mapping

Click the drop down to edit the details of the **Dropdown Configuration**. Click the **Save** button to save the changes.

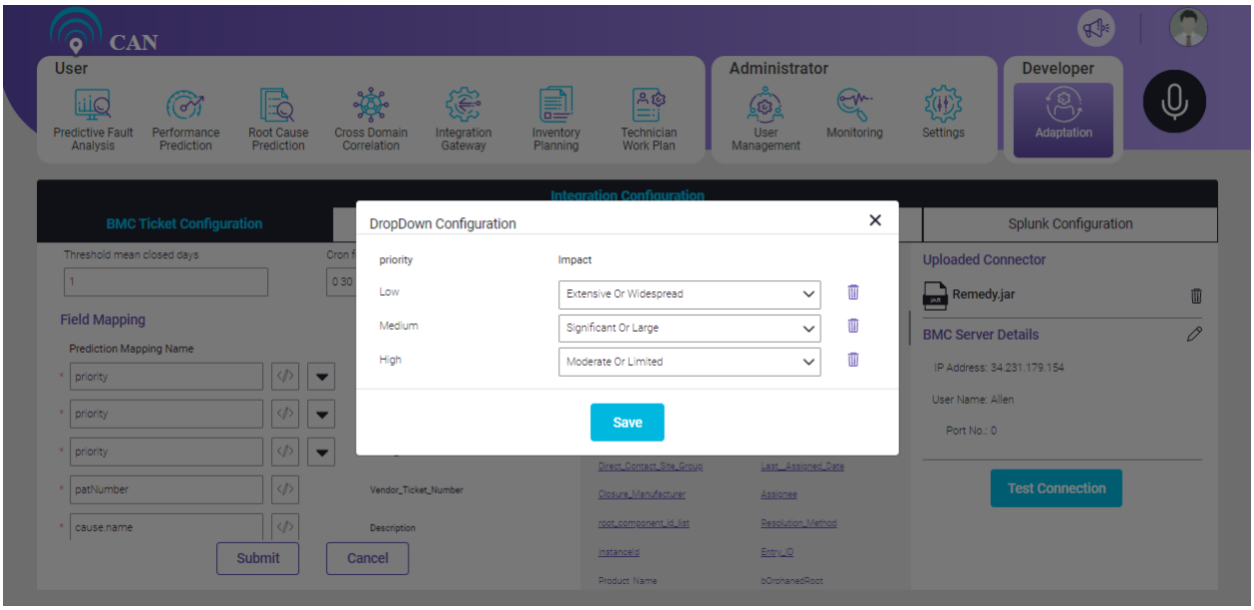


Figure 14.87 - Dropdown Configuration Screen

ServiceNow Configuration

By default, no information is configured in the ServiceNow Configuration screen.

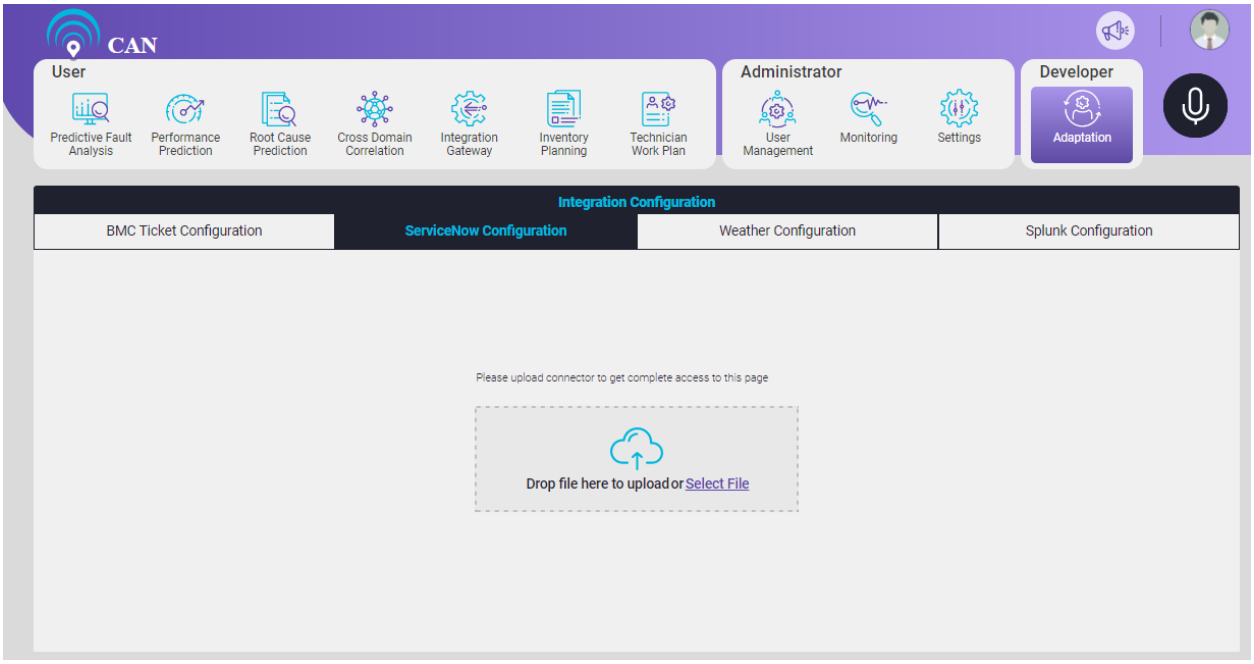


Figure 14.88 - ServiceNow Configuration Screen

User need to upload the connector (Servicenow.Jar) file to get the complete access of the page.

User can upload the file. To upload the file, user can drag and drop the file or select the file to upload.

To Configure the Service Now configuration

1. Connect to the ServiceNow by uploading the connector (.jar) file.
2. In the **ServiceNow server** details, click the edit icon .
    a. Write the IP Address in the IP Address text box.
    b. Write the user name in the **User Name** text box.
    c. Write the Password in the **Password** text box.

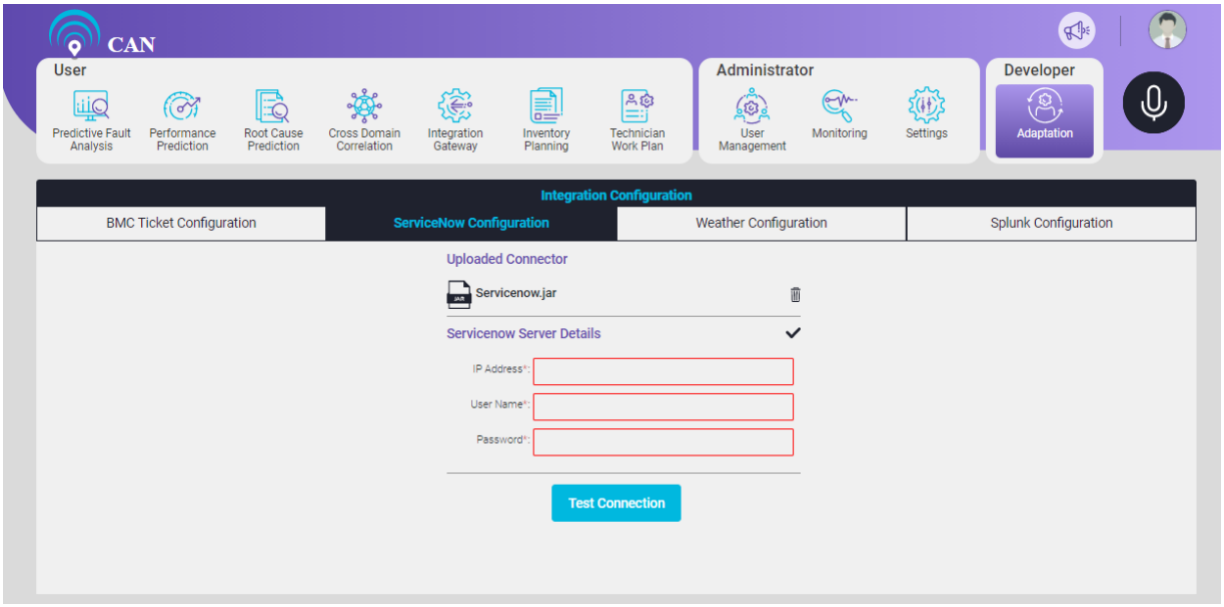


Figure 14.89 - ServiceNow Server Details

3. Click the **Test Connection** button.

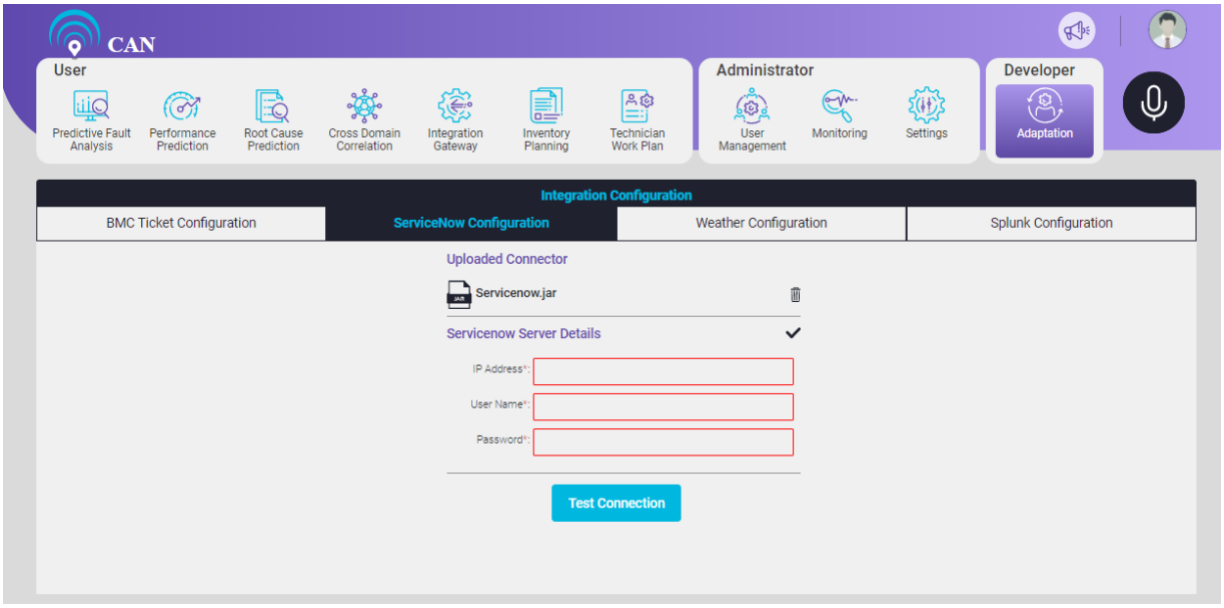


Figure 14.90 - ServiceNow Test Connection

In **ServiceNow** configuration we map the prediction fields to ServiceNow.

ServiceNow Integration screen shows **Field Mapping** components on the left side of the screen and **Add New Mapping Fields** in the centre of the screen.

We map the fields or add the new mapping fields as per the customer's requirements.

There is a search icon to search the mapping fields. User can search and add the Mapping fields.

The screen also shows the data **Threshold mean closed days** and **Cron for data pull**.

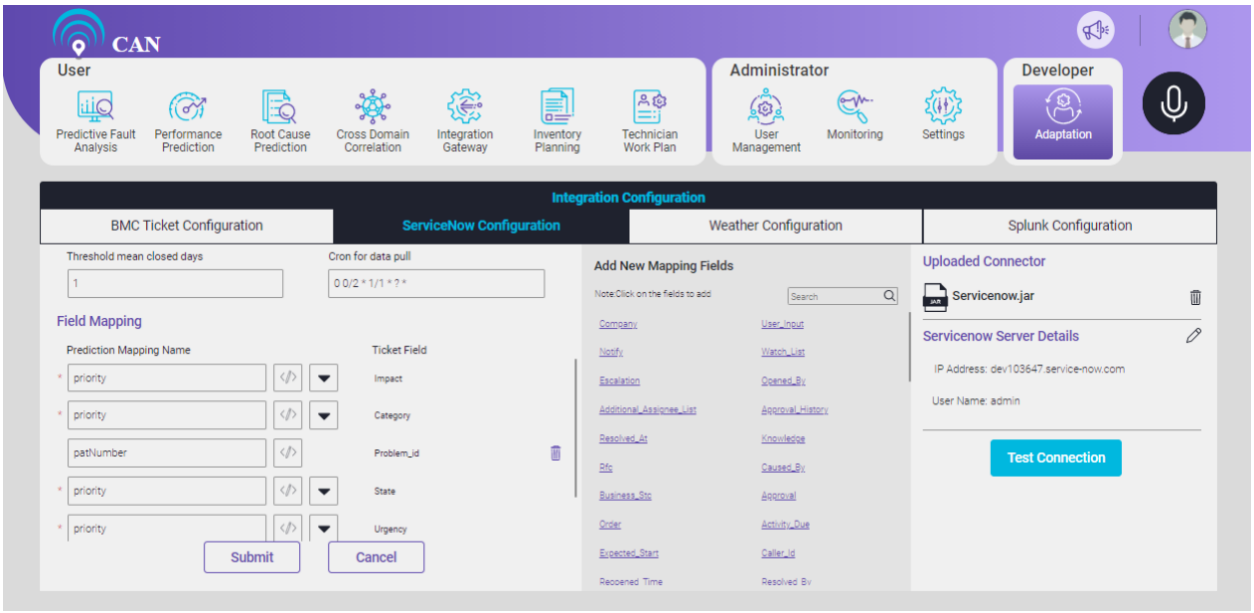


Figure 14.91 - ServiceNow Configuration Screen

To Edit the New Field Mapping Fields

1. Click the icon </> to edit the mapping codes. User can see the saved configuration. User can write the corresponding java mapping code in the text area. It will automatically get compiled. Click the **Save** button to save the changes.

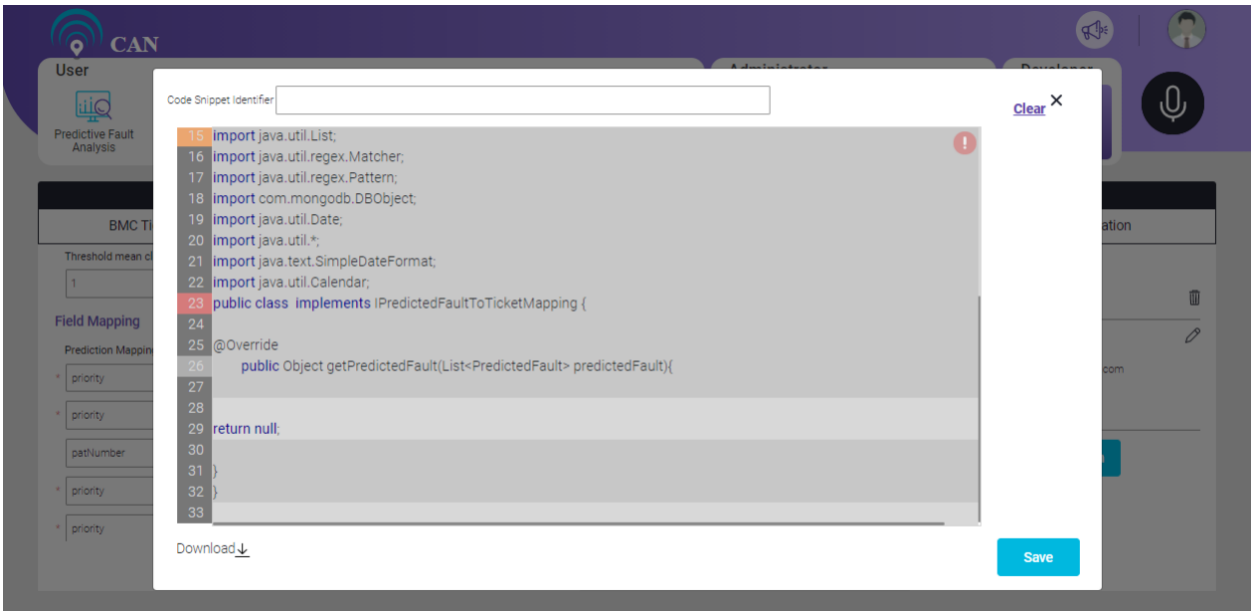


Figure 14.92 - ServiceNow Configuration Code for Mapping

2. Click the drop down to edit the details of the **DropDown Configuration**. Click the **Save** button to save the changes.

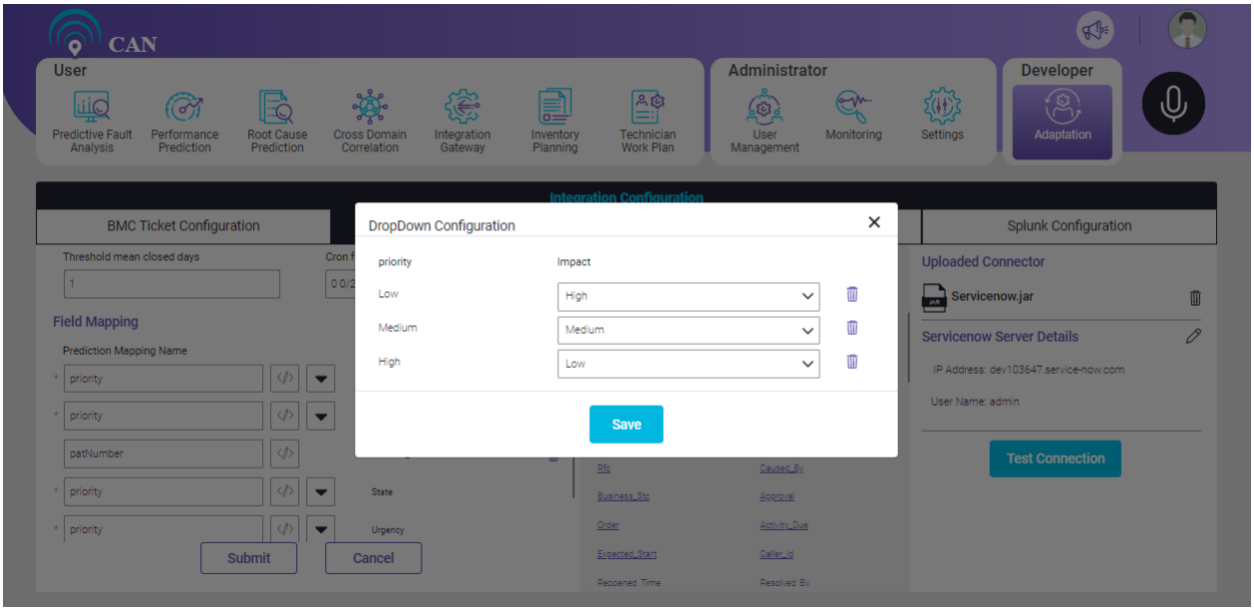


Figure 14.93 - DropDown Configuration Screen

Weather Configuration

By default, no information is configured in the Weather Configuration screen.

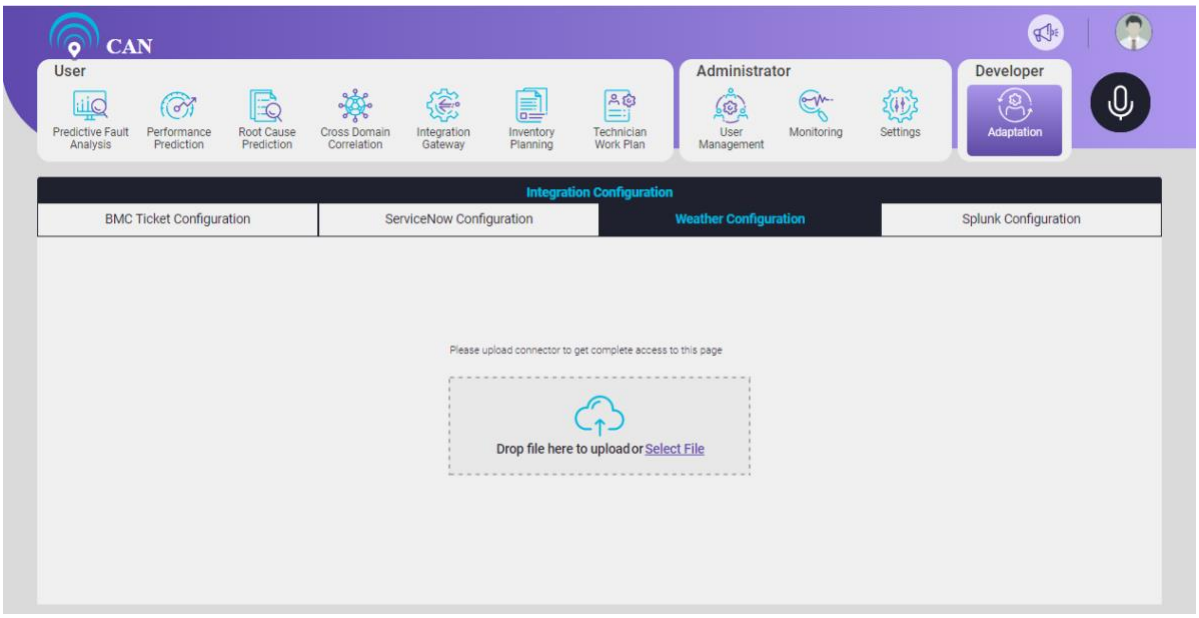


Figure 14.94 - Weather Configuration Screen

User can upload the file. To upload the file, user can drag and drop the file to upload or select the file to upload.

To Configure the Weather Configuration

1. Upload the connector (.jar) file. Currently, CAN supports **OpenWeatherMap** service for the weather data.
2. Write the API URL details “http://api.openweathermap.org/data/2.5/forecast” in the API URL field.
3. Write the APP ID in the APP ID field. Click the **Save Details** button.

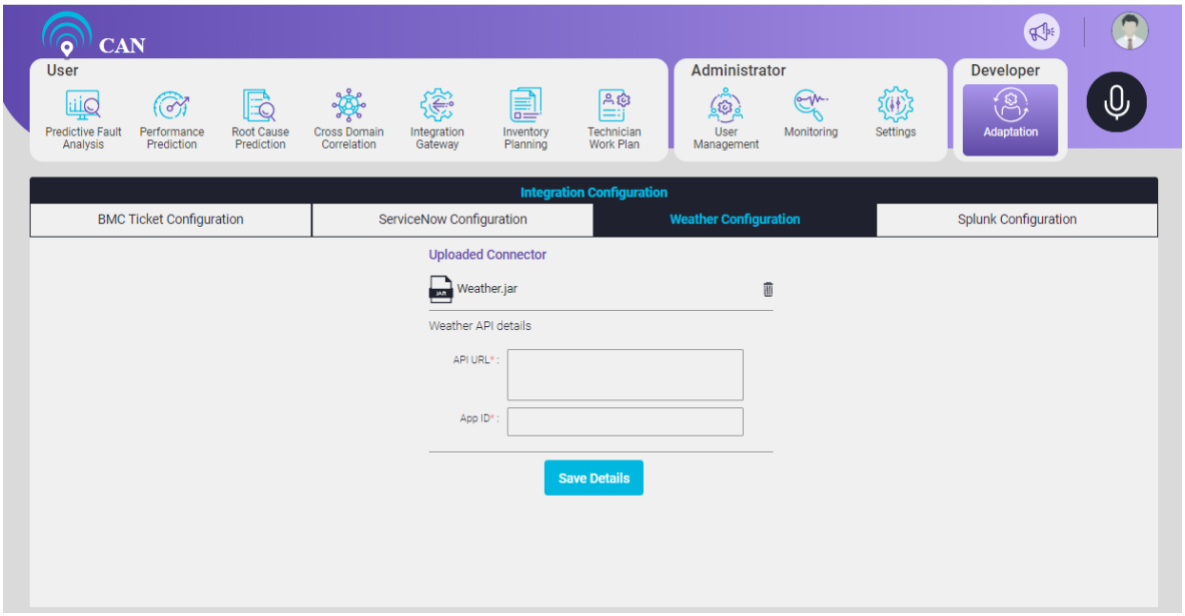


Figure 14.95 - Weather API Login Page

The Weather Integration screen will display the following components:

- Zone
- Latitude
- Longitude
- City Borders

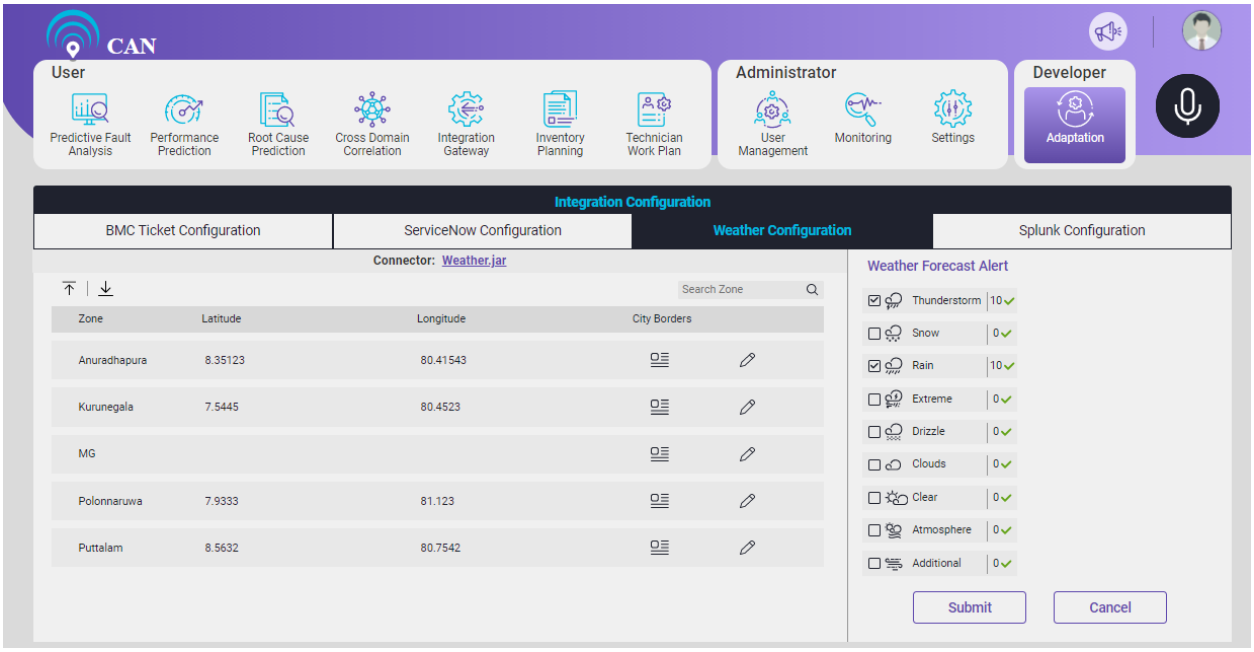


Figure 14.96 - Weather Integration Components

Click the edit icon to update the Latitude and Longitude information only.

User can upload the file. To upload the file, click the upload icon . We can update Latitude, Longitude and City Borders all the three information.

User can drag and drop the file to upload or can select the file to upload.

Click the download icon to get the zone details.

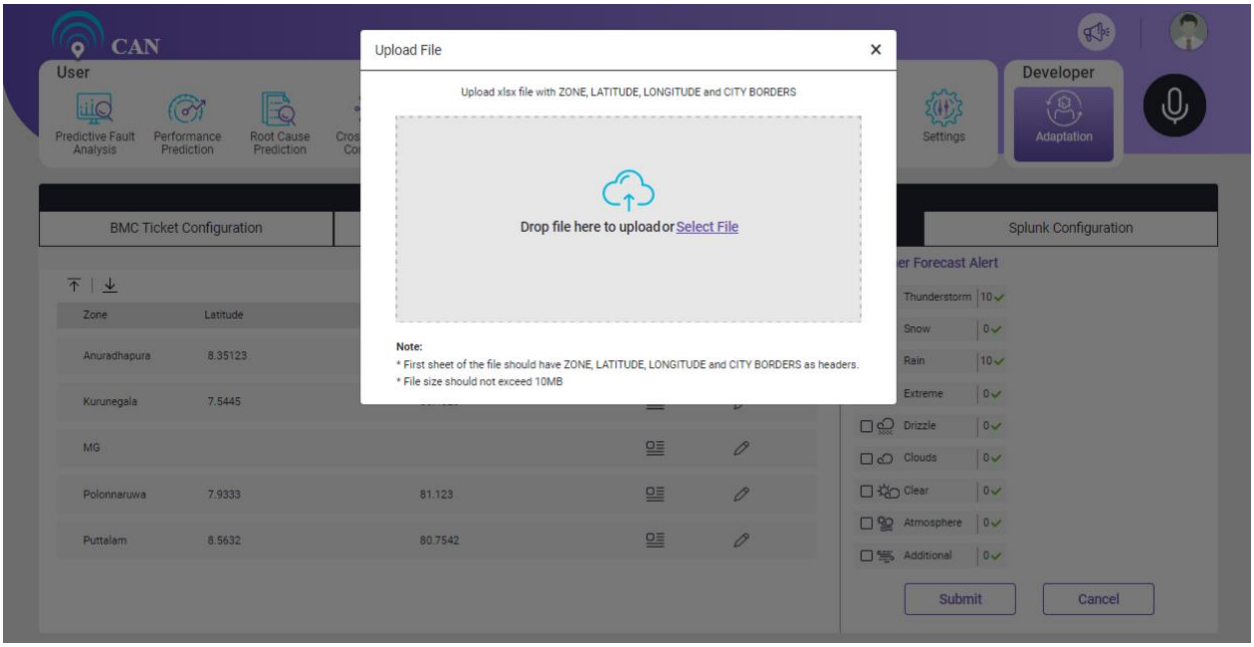


Figure 14.97 - Weather Integration File Upload

User can see the required weather forecast alerts on the right side of the screen.

There are many weather alerts under weather forecast alerts. User/Technician can select the required alerts according to his interest.

The weather alerts available in the weather Forecast alerts are (all these fields have checkboxes):

- Thunderstorm
- Snow
- Rain
- Extreme
- Drizzle
- Clouds
- Clear
- Atmosphere
- Additional

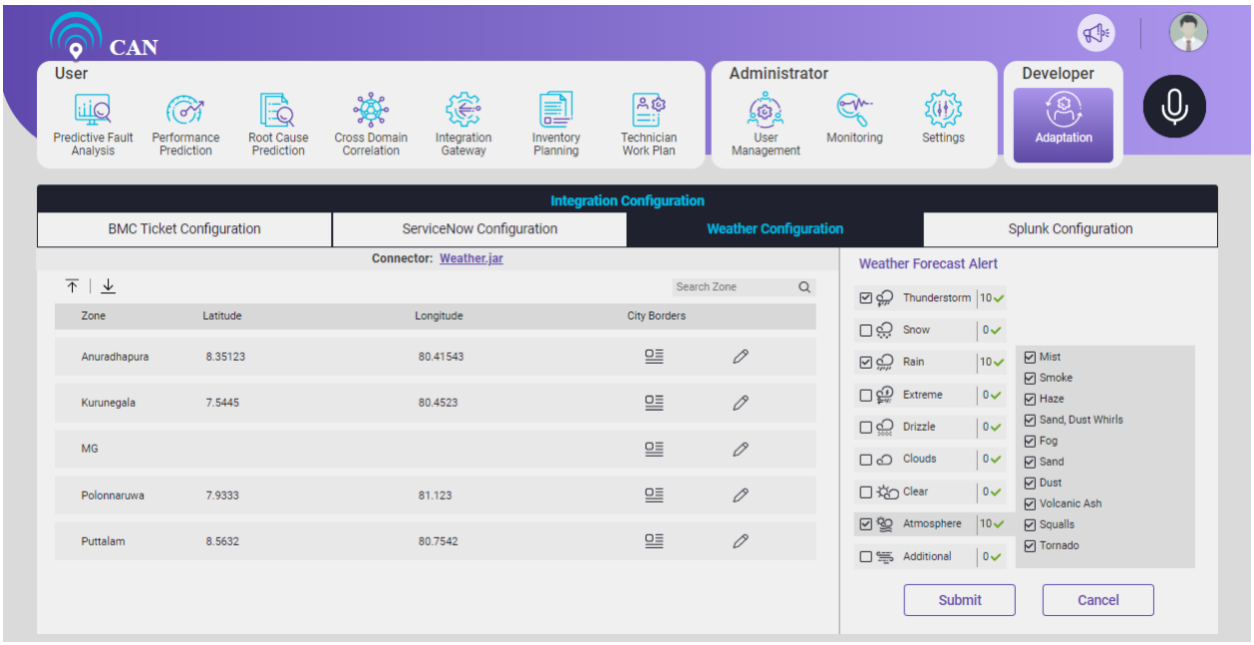


Figure 14.98 - Weather Forecast Alerts

Each of the Weather Forecast Alert fields have the sub fields.

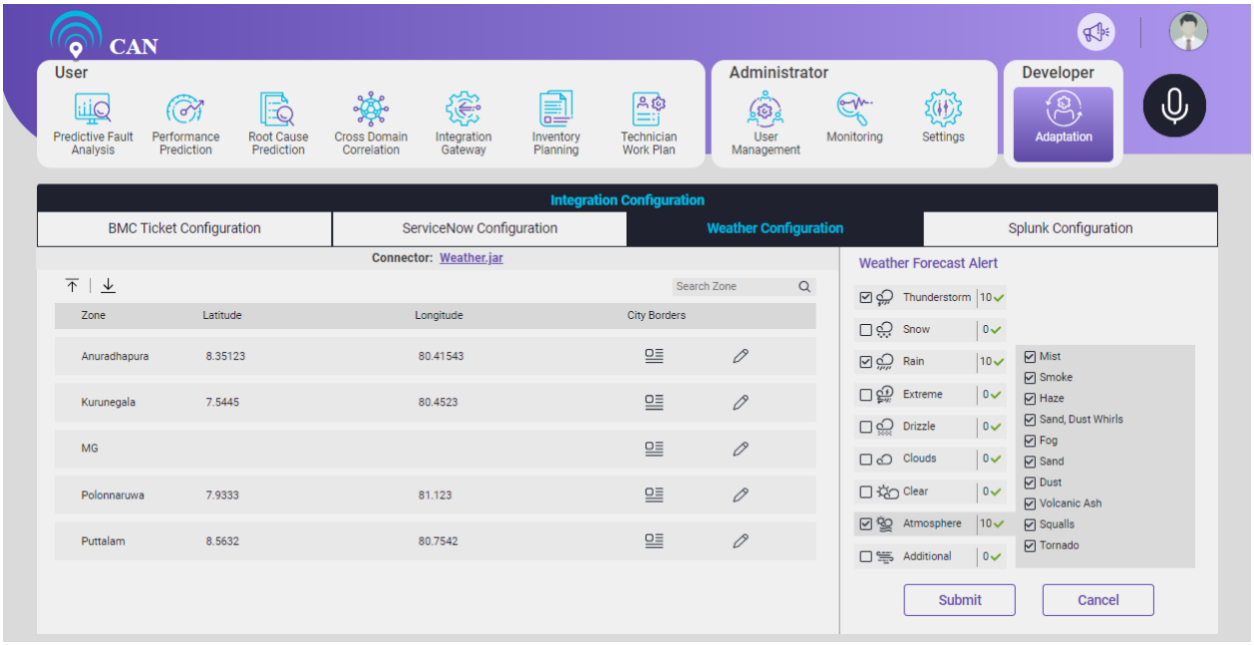


Figure 14.99 - Weather Forecast Alerts (Subfields)

Splunk Configuration

By default, no Splunk is configured in the Splunk Configuration tab.

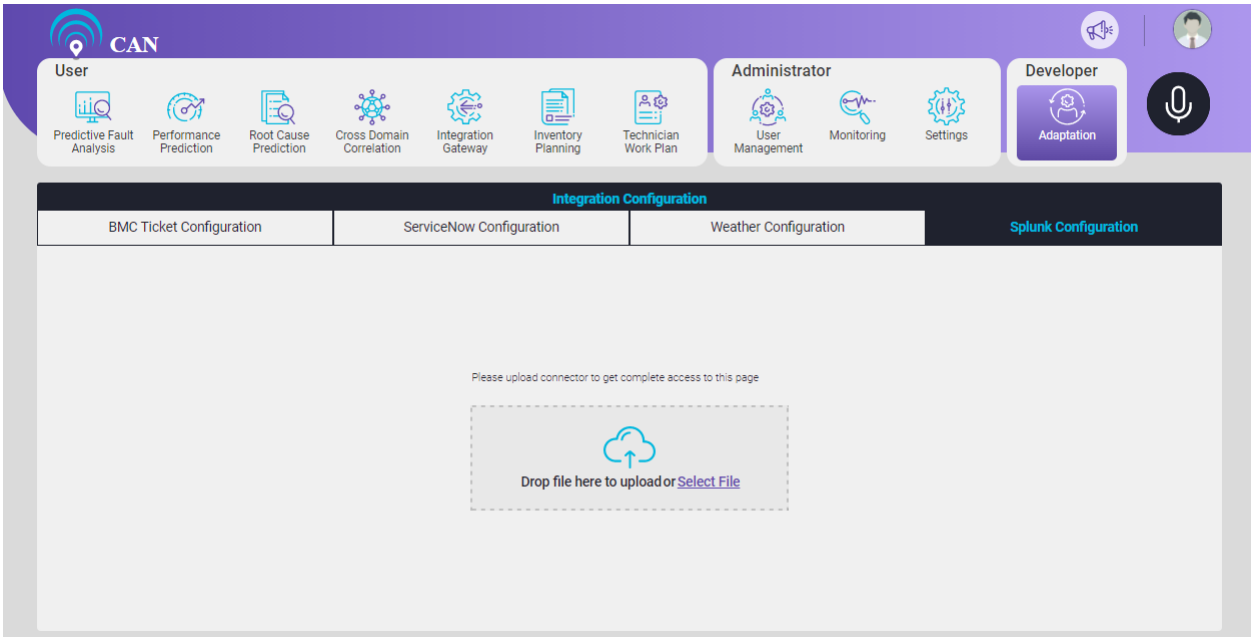


Figure 14.100 - Splunk Configuration Screen

User need to upload the connector (**Splunk.Jar**) file to get the complete access of the page.

User can upload the file. To upload the file, user can drag and drop the file or select the file to upload.

To Configure the Splunk

1. Connect to the Splunk by uploading the connector (Splunk.jar) file.
2. In the Splunk server details, click the edit icon .
    a. Write the IP Address (For example - 127.0.0.1) in the IP Address text box.
    b. Write the user name (For example -avanseus) in the User Name text box.
    c. Write the Password (Avanseus$0) in the Password text box.
    d. Write the Port No. in the Port No. text box.

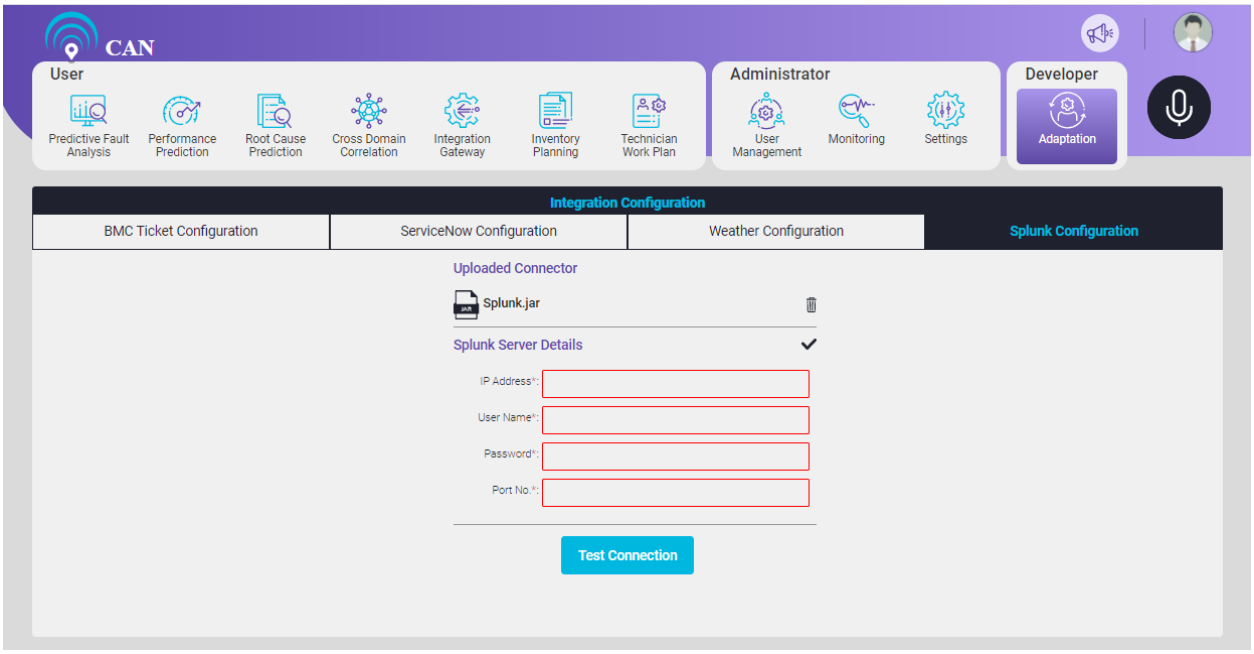


Figure 14.101 - Splunk Server Details

User can delete the Splunk.jar files. To delete the Splunk.jar file, click the delete icon .

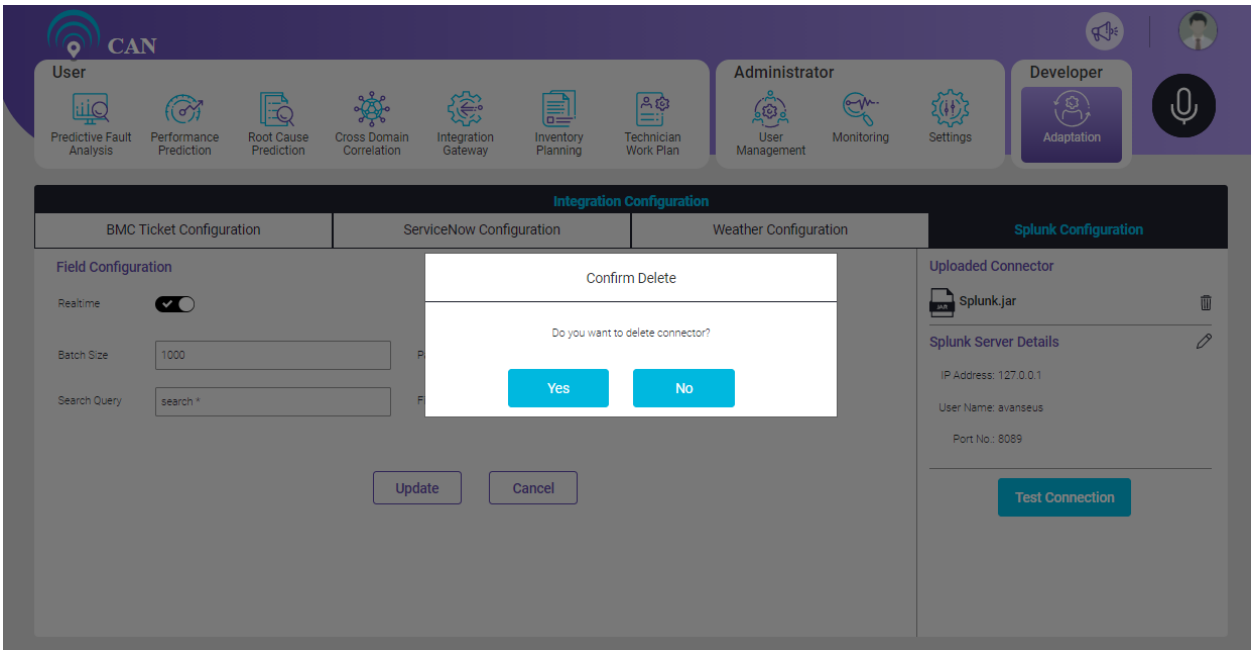


Figure 14.102 - Splunk Uploaded Controller

Field Configuration have two options:

- Realtime
- Cron for Batch Pull

User needs to set the toggle button to ON to select the Realtime.

In the “**Realtime**”, user can pull the data with some delay.

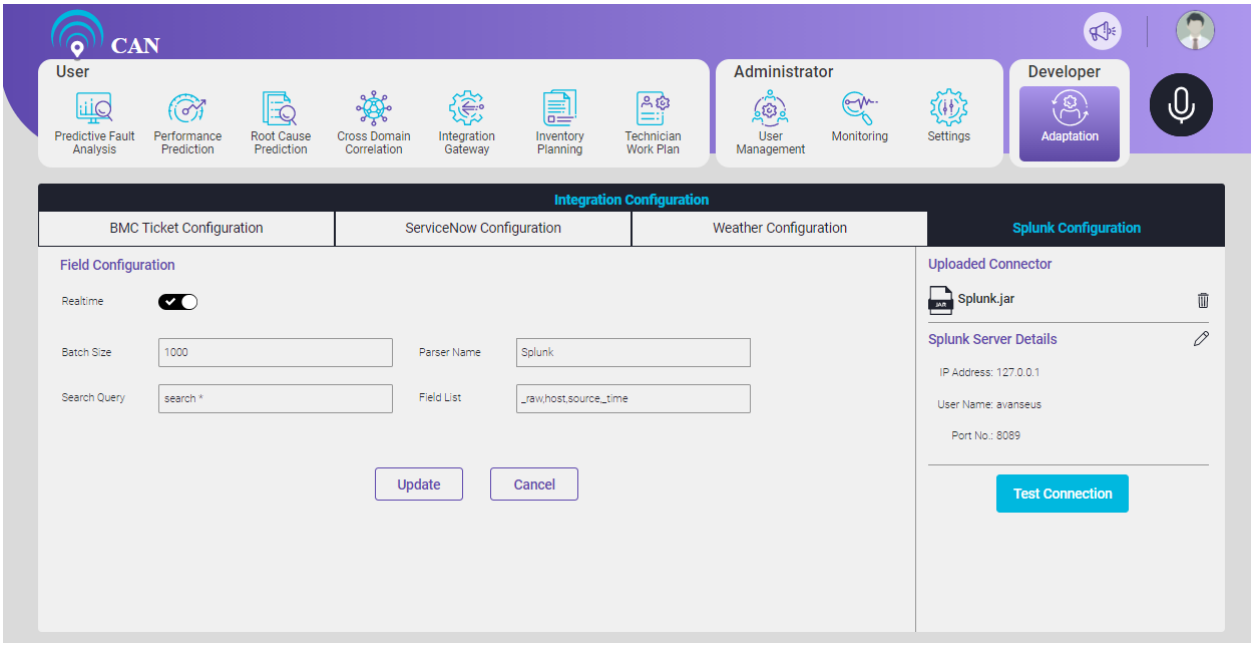


Figure 14.103 - Field Configuration - Realtime Toggle Button

User need to set the toggle button to OFF to select the “**Cron For Batch Pull**”. User can pull the Splunk details using the coupler at some point of the day (For example at 12 O clock).

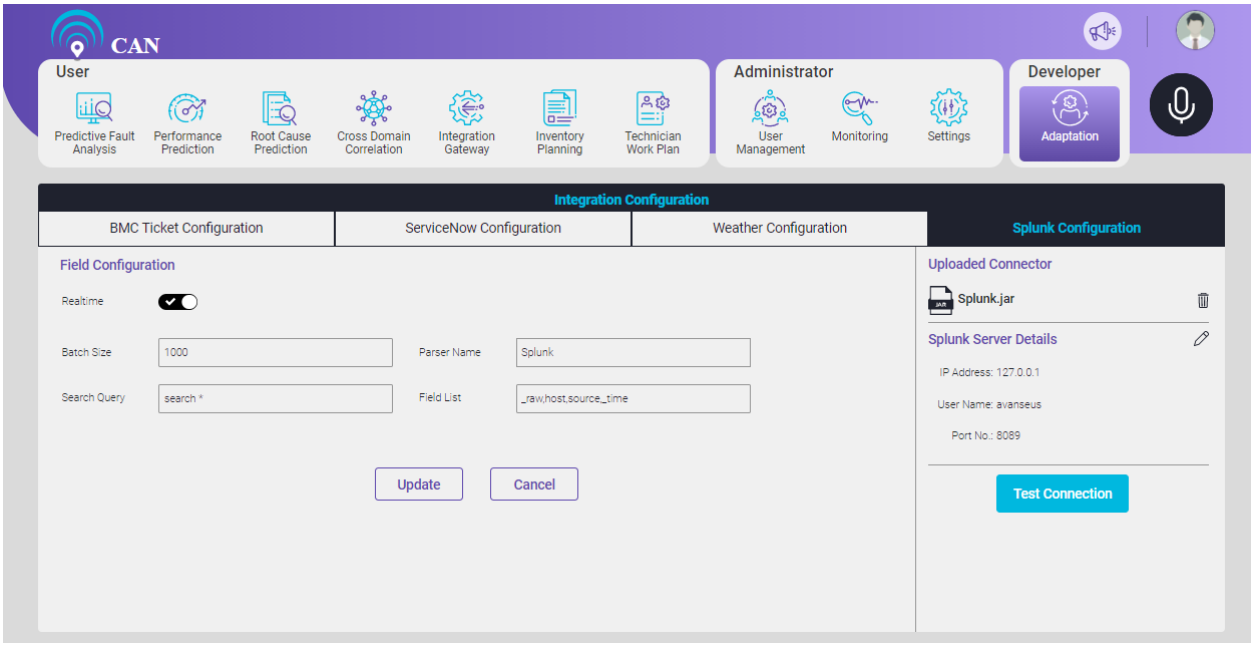


Figure 14.104 - Splunk Configuration Screen

User can write the Search Query in the search query text box.

By default, the Splunk Search Query text box have **Search*** written as query. **Search*** will contain all the pre default values in the backend.

User can write the Search Query in the search query text box.

To edit the Splunk Search Query, click the **Splunk Search Query** Search box, a screen will pop up.

1. User can edit the query as per requirement.
2. Click the **Update** button to save the query.

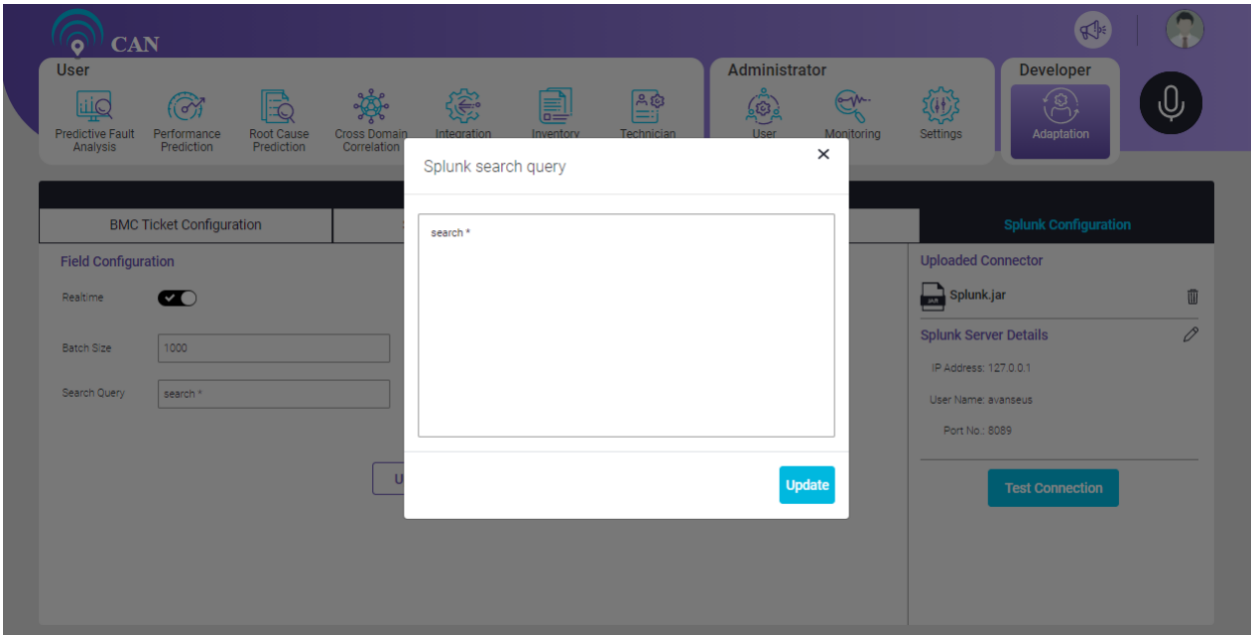


Figure 14.105 - Splunk Search Query

User can add the **FieldList** in the Field List text box.

To add the Field List, Click the **FieldList** text box, the **FieldList** screen will popup.

1. User can edit the Field List as per the requirement.
2. Click the **Update** button to save the Field List.

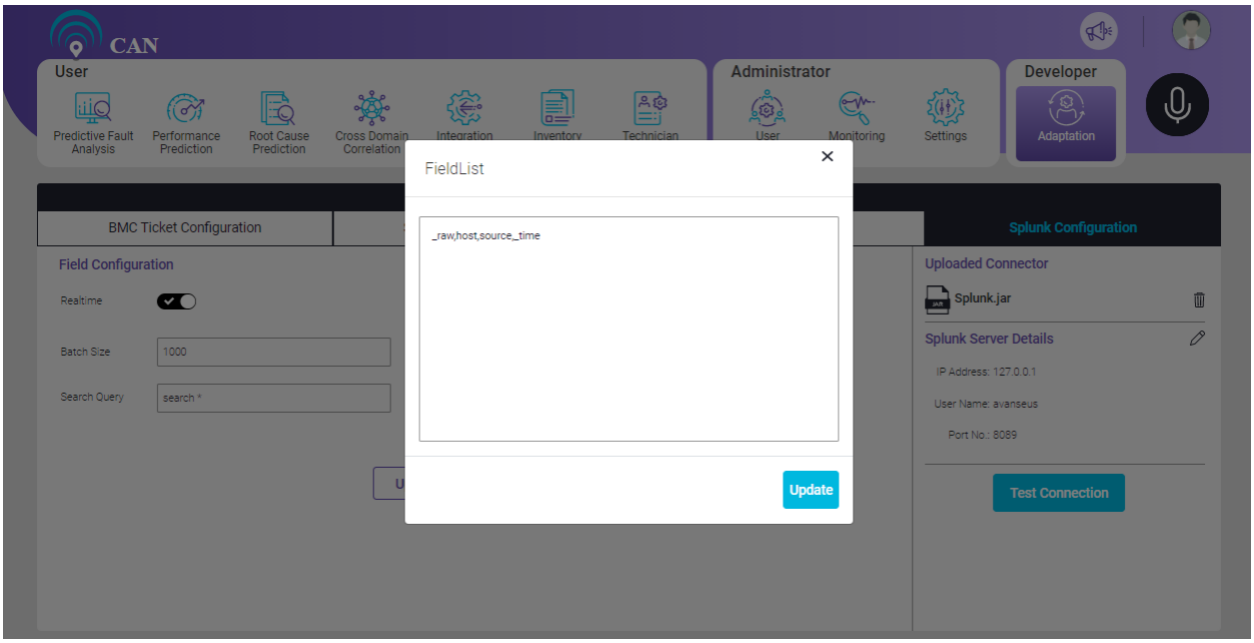


Figure 14.106 - Splunk Field List

15. VBI (Voice Based Interaction)

The VBI (Voice Based Interaction) allows the user to ask queries related to Prediction Data. Voice based Interface to fetch relevant (supported) set of queries on fault predictions.

VBI provide answers to user's queries in the voice form as well as it also displays the query result on the screen. The queries must be in US English or IN English.

Pre-Requisites:

- The VBI module supports the Chrome browser. VBI module will not work in any other browser. If the chrome browser is not used the speech icon will not appear on the screen.
- Ask question in a moderate speed (not too slow, not too fast) to make sure that the system is able to understand the voice command.
- If you are using the system microphone, you shouldn't ask questions from long distance.
- Ask question spontaneously with correct pronunciation (if you are not spontaneous, it will detect pause and it will try to execute that much).
- For the current release, no conversation with the system and speech-to-text will allow US English and Indian English and text-to-speech will allow US English.
- Internet connection is required. Otherwise, tooltip will display "Service is unavailable", when the user will click the speech icon with adequate animation.

A user can ask query irrespective of the CAN screen he is working on. When user makes a query, if the query is valid, then it navigates the user to Predictive Fault Analysis screen to display the filtered results for the current prediction week. If the query is ambiguous or misunderstood, multiple suggestions will be displayed as per the query. If the query is wrong or not valid, the system will respond in voice but the screen will not show any message.

If there is ambiguity in voice command, the screen displays the probable commands and asks the user to choose from the options.

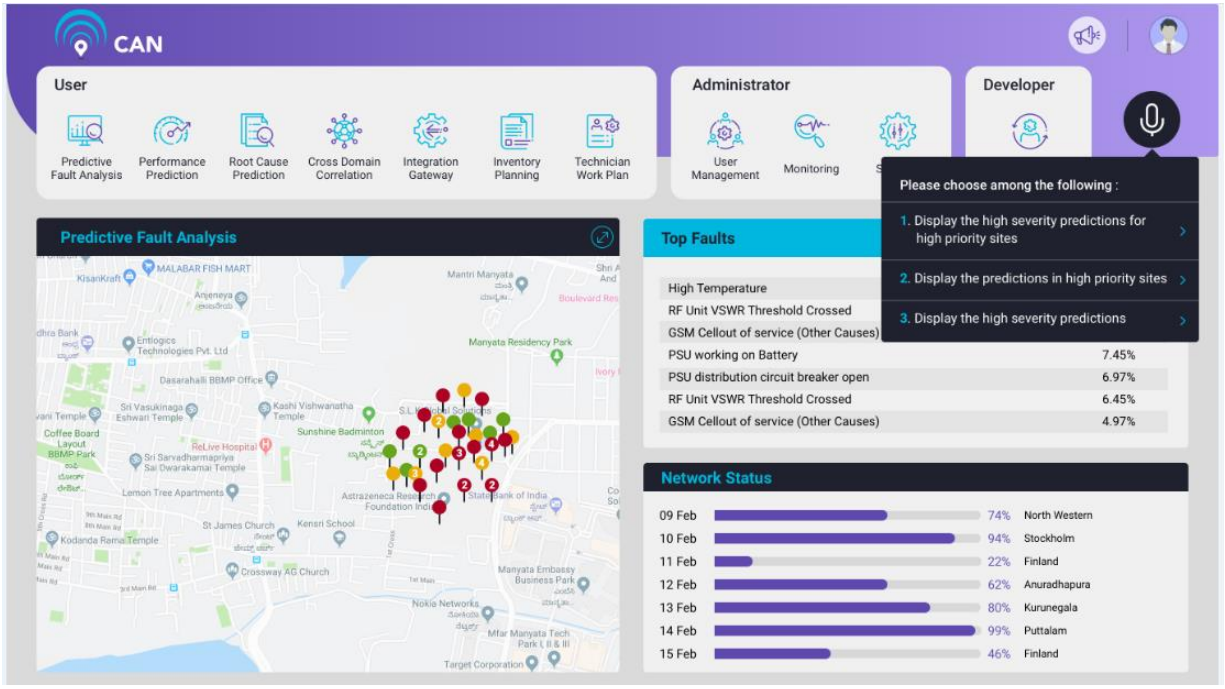


Figure 15.1 - VBI Icon

The speech icon has the below properties:

1. It displays different color and adequate animation to show the activation of speech listening.
2. It displays different color and adequate animation to show enable/disable of speech icon.
3. When user click the speech icon, a tool-tip appears to show that the voice commands gets converted to text.

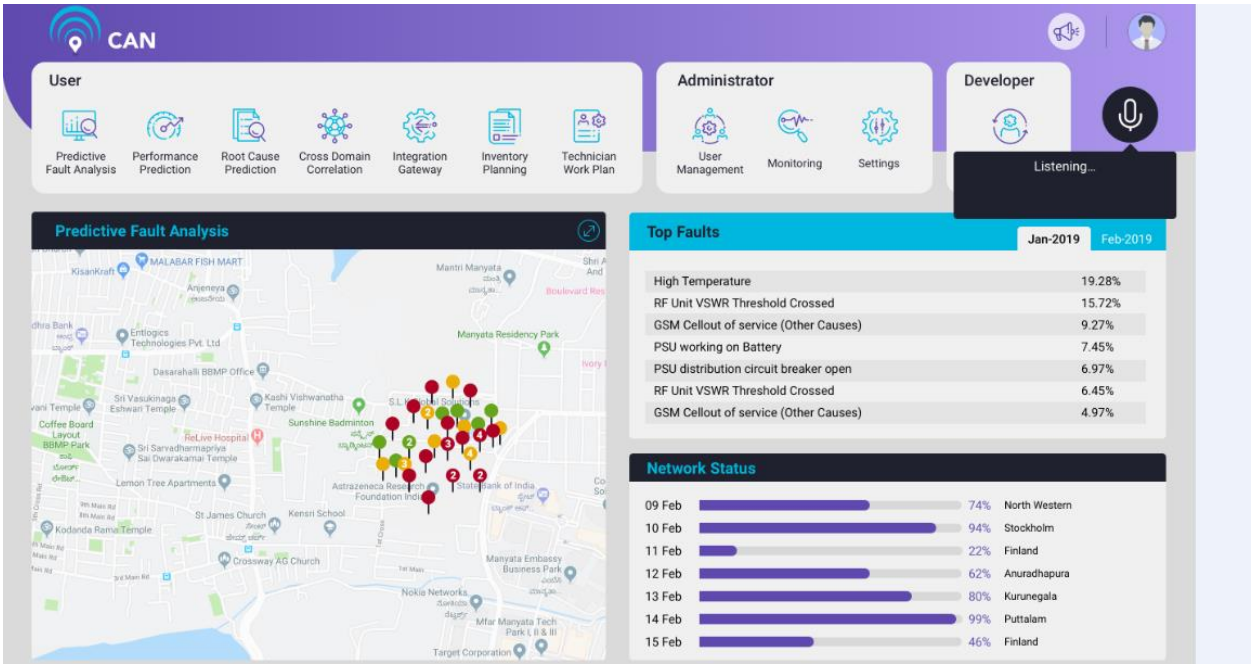


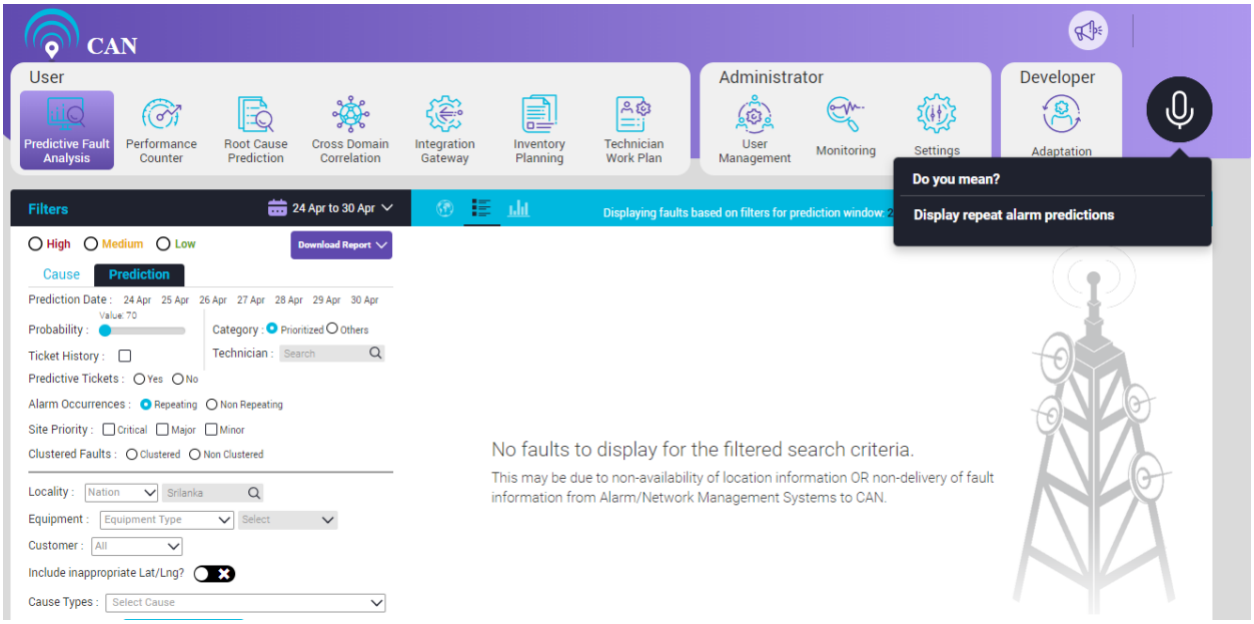
Figure 15.2 - Voice Commands conversion to text

4. The appropriate voice commands or the query navigates the user to appropriate CAN page and closes the voice command window on successful/correct query.
5. Tooltip auto closes the query on click of speech icon or appropriate query.

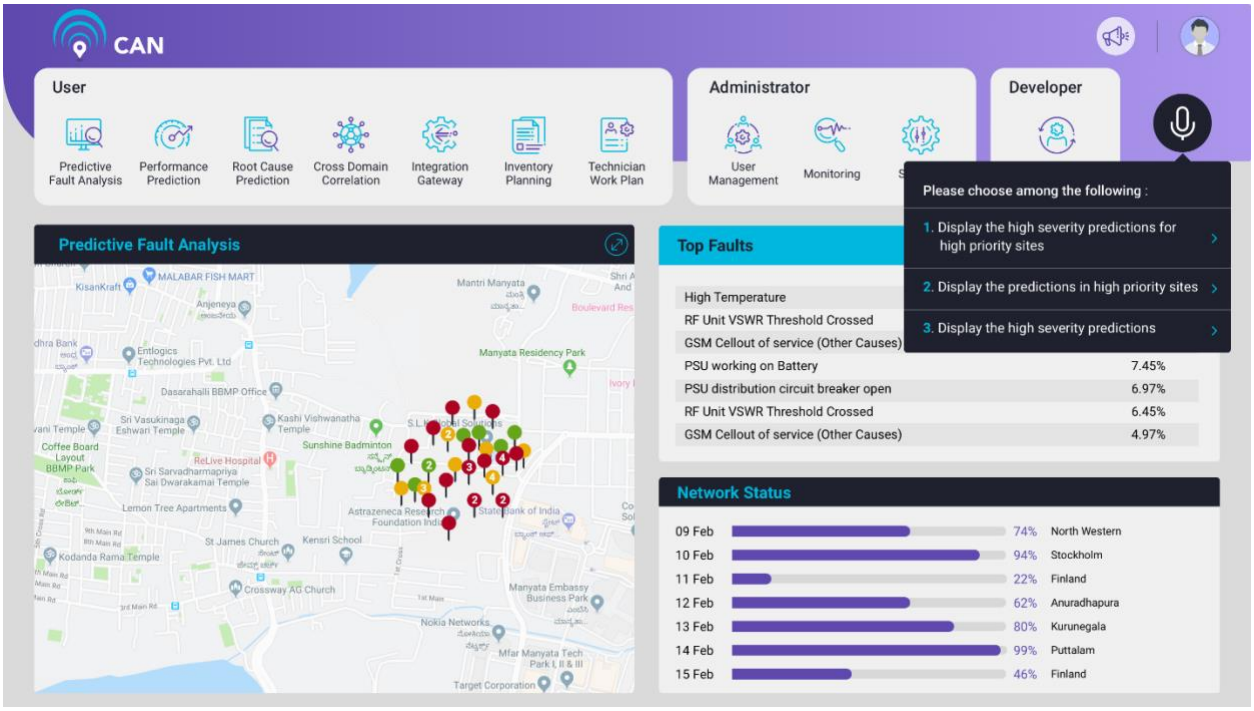
Points to note when accessing VBI

- For a few seconds after clicking the speech icon, if user will not speak anything then the tooltip will display “no speech is detected” with adequate animation.
- If the query is not clear to the system but the system understands the possibilities of the queries the user wants to know, then the system will give different options for different scenarios. There are two scenarios - Single suggestion or multiple suggestions.

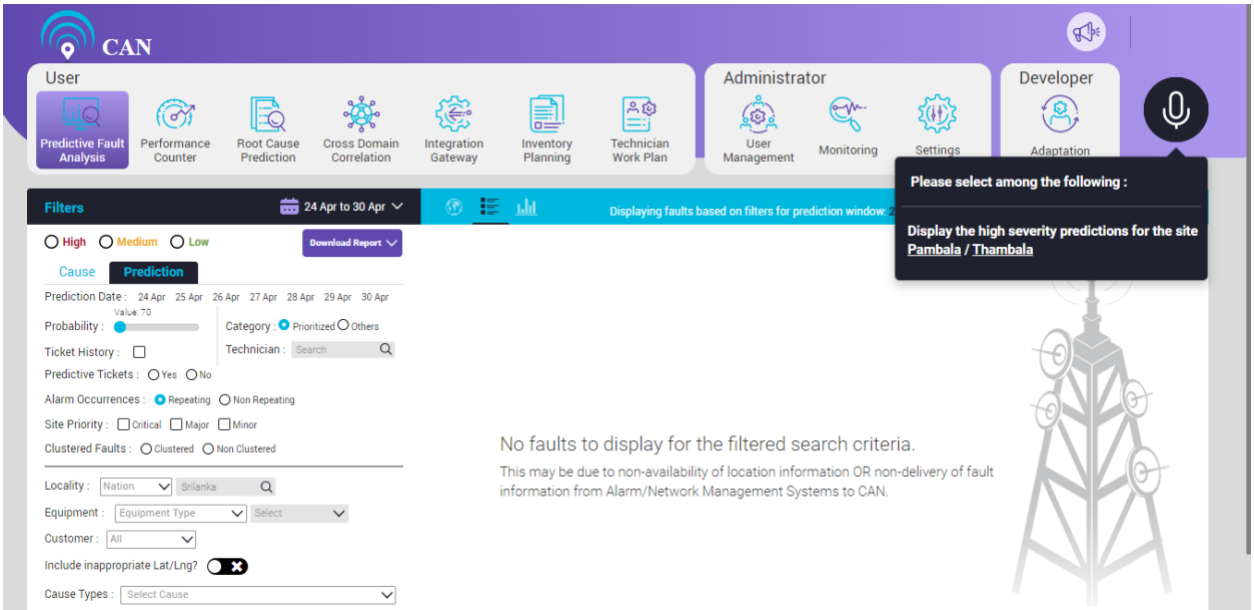
In case of single suggestion, the system will display “Do you mean”? with that suggestion.



If there are multiple suggestions, then the system will ask “Please choose among the following”.

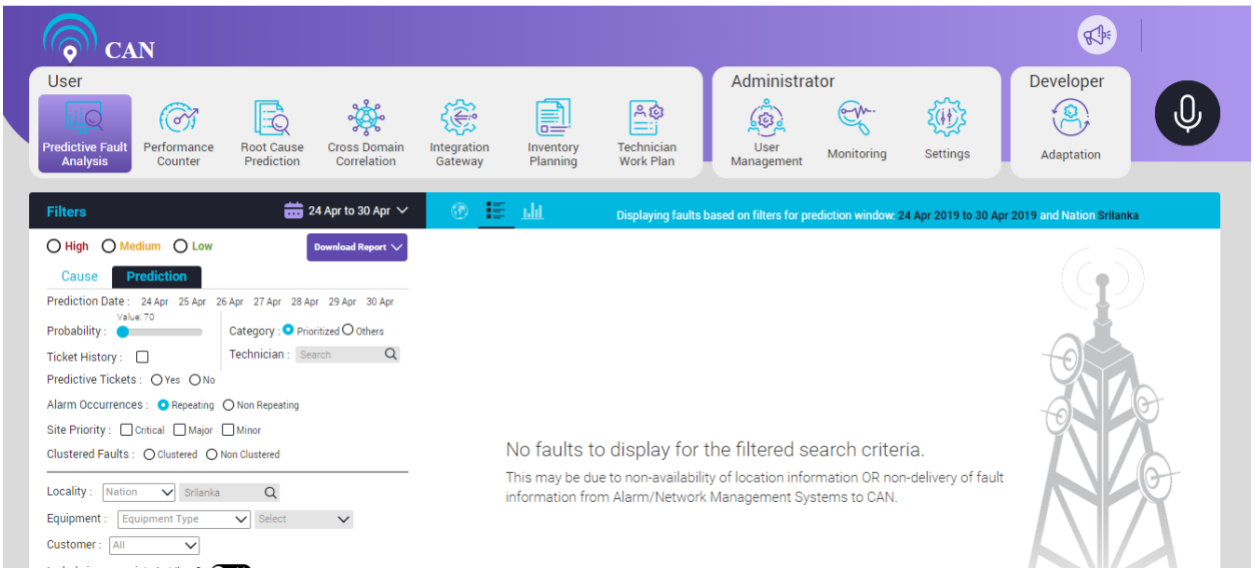


If site name or region name or network type (2G, 3G etc.) or customer name is ambiguous, the screen will display the closest word.



If the user asks invalid questions, the system will audibly inform “Sorry, no valid matches found, please speak again”.

If for a valid question, based on the particular filters applied, there are no faults predicted for the current prediction week, the system will audibly inform “Sorry, no valid records found”, please speak again. The screen will display that “No faults to display for the filtered search criteria”.



If the user asks a question which is currently not supported in the release, the system will audibly inform “The query is currently not supported, please speak again”.

Supported Queries

User can ask the 13 queries for which CAN will provide appropriate response with adequate semantics. The list of queries are as follows:

Query 1 - Display repeat alarm predictions.

When user asks the query, the screen navigates the user to Predictive Fault Analysis screen. The screen shows the selected Alarm Occurrences filter as “Repeating” radio button under the prediction tab. Alarm Occurrences filter have two radio buttons: Repeating and Non Repeating.

The system will inform “We are presenting you the predicted faults having closed or answered tickets for the latest prediction week”.

NOTE: Currently CAN VBI supports only Repeating radio button.

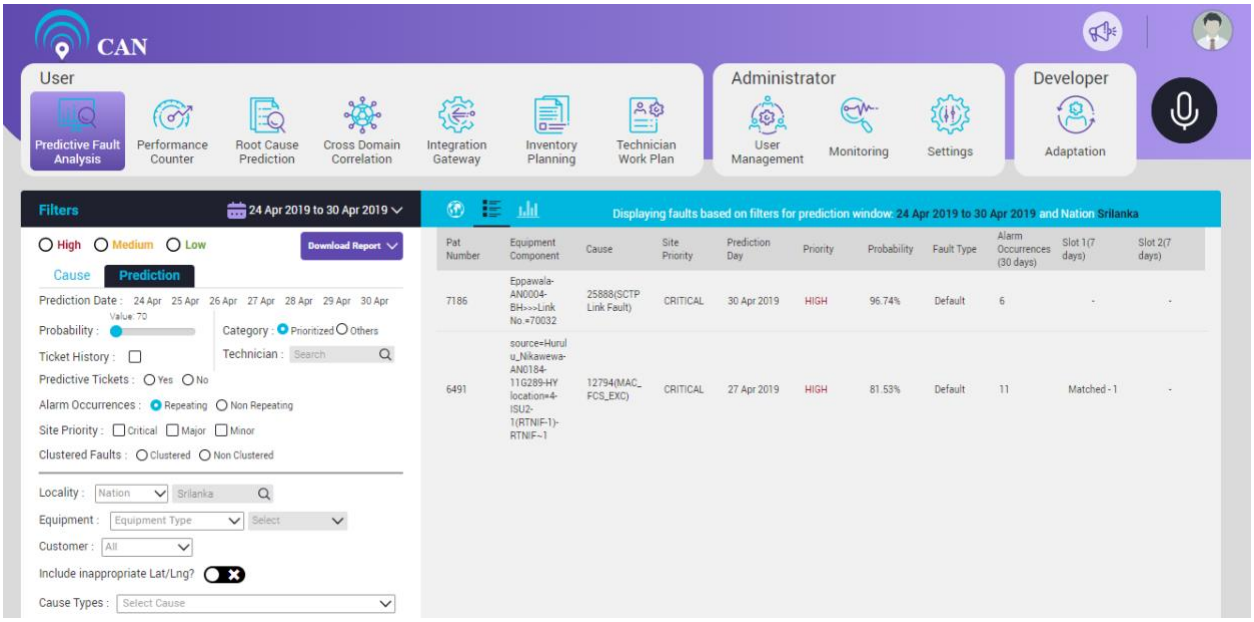


Figure 15.3 - Repeat Alarm Predictions

Query 2 - "Display high priority site fault predictions".

When user asks the query, the screen navigates the user to Predictive Fault Analysis screen. The screen shows the selected Site Priority filter as “Critical” checked in the check box under the prediction tab. The Site Priority have three check boxes: Critical, Major, Minor.

The system will inform “We are presenting you the predicted faults in high priority sites for the latest prediction week”.

Query 3 - "Display the predictions of high severity faults".

When user asks the query, the screen navigates the user to Predictive Fault Analysis screen. The screen shows the selected filter as High severity.

The system will inform “We are presenting you the high severity faults predicted for the latest prediction week”.

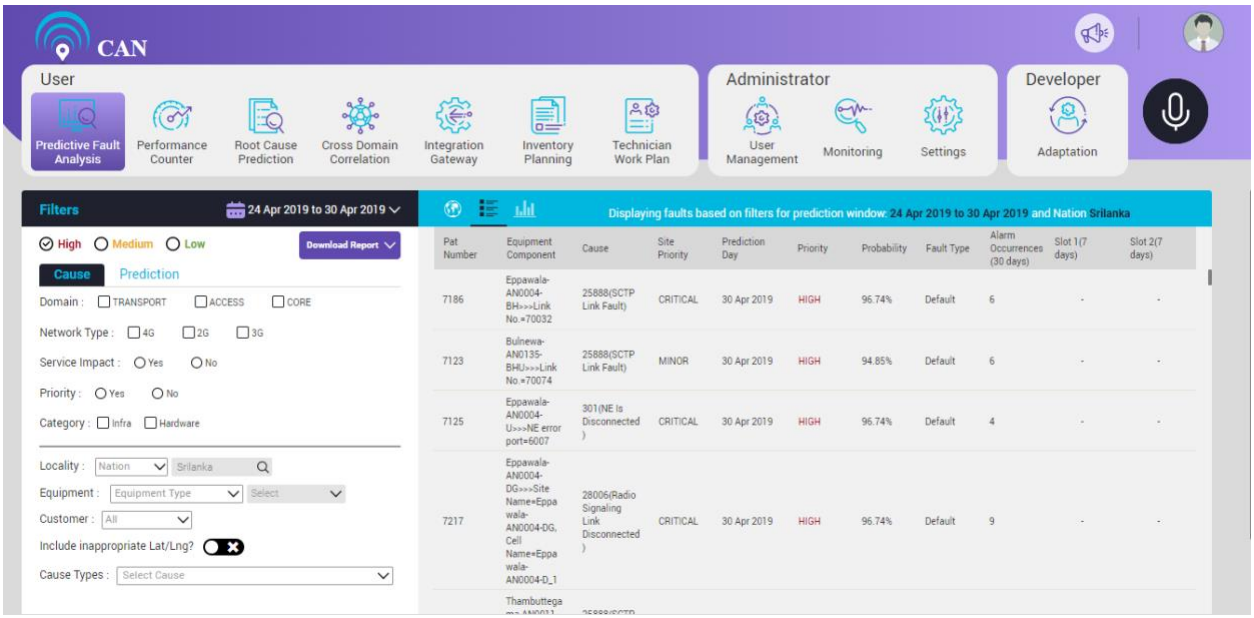


Figure 15.4 - High Severity Faults Predictions

Query 4 - "Display the predictions of clustered faults".

When user asks the query, the screen navigates the user to Predictive Fault Analysis screen. The screen shows the selected Clustered Faults filter as “Clustered” radio button under the prediction tab.

The system will inform “We are presenting you the clustered faults predicted for the latest prediction week”.

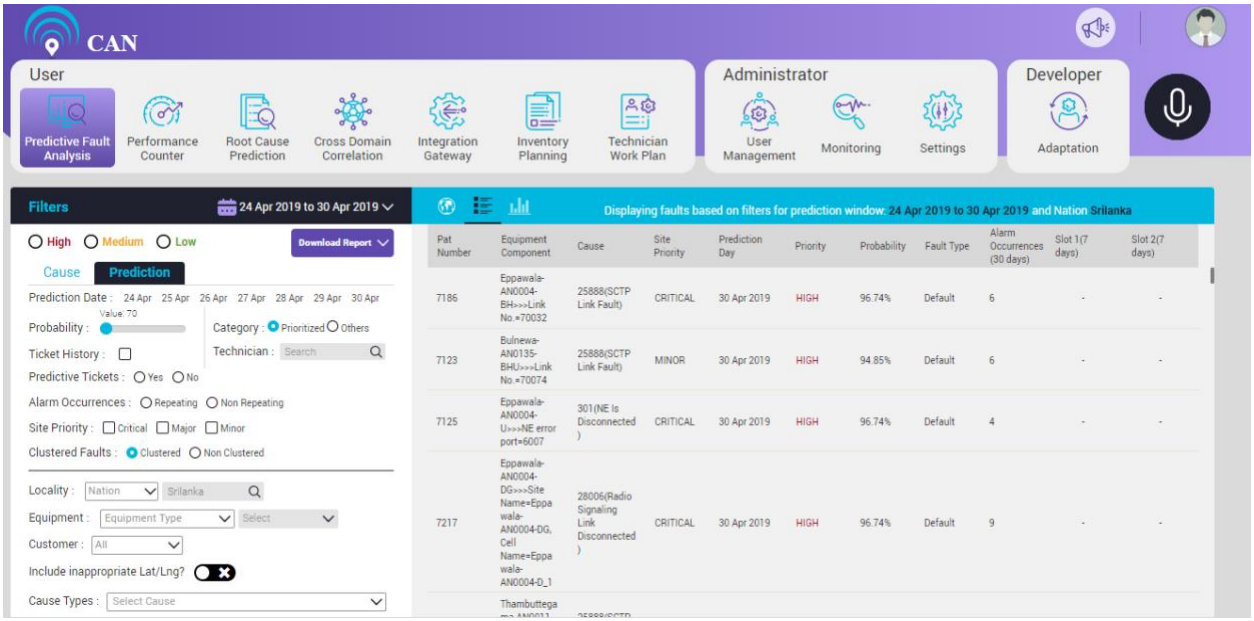


Figure 15.5 - Clustered Faults Predictions

Query 5 - "Display the prediction of hardware fault"

When user asks the query, the screen navigates the user to Predictive Fault Analysis screen. The screen shows the selected Category filter as “Hardware” checked in the check box under the Cause tab.

The system will inform "We are presenting you the hardware faults predicted for the latest prediction week".

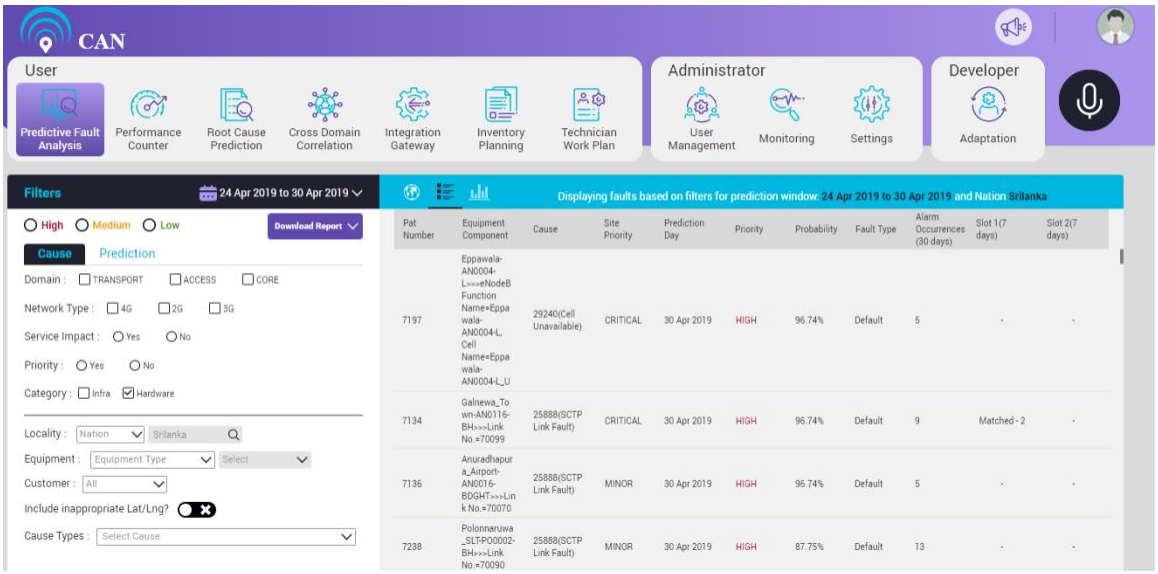


Figure 15.6 - Hardware Faults Predictions

Query 6 - "Display high severity predictions for the site <site_name>".

When user asks the query, the screen navigates the user to Predictive Fault Analysis screen. The screen shows the selected filter Alarm Severity as “High” and name of the specific office code name in the search box.

The system will inform "We are presenting you the high severity faults for the site <site_name> predicted for the latest prediction week.".

If for a specific user, region & zone are specified, then the site name for the query “display high severity predictions for the site name <site_name>” or the region name for the query “display high severity predictions for the region <region_name>” will be considered as valid it is in the specified regions & zones.

Query 7 - "Display high severity predictions for the region <region_name>".

When user asks the query, the screen navigates the user to Predictive Fault Analysis screen. The screen shows the selected filter Alarm Severity as “High” and name of the specific region in the search box.

The system will inform "We are presenting you the high severity faults for the region <region_name> predicted for the latest prediction week".

If for a specific user, region & zone are specified, then the site name for the query “display high severity predictions for the site name <site_name>” or the region name for the query “display high severity predictions for the region <region_name>” will be considered as valid it is in the specified regions & zones.

Query 8 - "Display high severity predictions in <networkType_name> site (2G/3G etc)".

When user asks the query, the screen navigates the user to Predictive Fault Analysis screen. The screen shows the selected filter Alarm Severity as “High” and name of the Network type with the appropriate value like (2G/3G/4G).

The system will inform "We are presenting you the high severity faults for the <networkType_name> sites predicted for the latest prediction week".

Query 9 - "Display high severity predictions for high priority sites".

When user asks the query, the screen navigates the user to Predictive Fault Analysis screen. The screen shows the selected filter Alarm Severity as “High” and Site Priority as “Critical” under prediction tab.

The system will inform "We are presenting you the high severity predicted faults in high priority sites for the latest prediction week".

Query 10 - "Display predictions with ticket history".

When user asks the query, the screen navigates the user to Predictive Fault Analysis screen. The screen shows the selected filter Ticket History check box checked under the prediction tab.

The system will inform "We are presenting you the predicted faults having ticket history for the latest prediction week. Click on the faults for details".

Query 11 - "Display the latest predictions with predictive tickets".

When user asks the query, the screen navigates the user to Predictive Fault Analysis screen. The screen shows the selected filter Predictive Tickets as “Yes” radio button under the prediction tab.

The system will inform "We are presenting you the predicted faults having necessary ticket information’s for the latest prediction week. Click on the faults to find relevant ticket details."

Query 12 - "Display high severity predictions for the customer <customer_name>".

When user asks the query, the screen navigates the user to Predictive Fault Analysis screen. The screen shows the selected filter Alarm Severity as “High” and name of the specific Customer Name in the search box.

The system will inform "We are presenting you the high severity predicted faults for the customer <customer_name> for the latest prediction week".

If the customer is present, then only the query will be valid otherwise the system will inform "Sorry, no such customer found".

Query 13 - "How is network doing"?

When user asks the query, the screen navigates the user to Predictive Fault Analysis screen.

The screen shows the most critical faults (by default top 50) based on Region & Zone for the latest prediction week.

Based on Cause name, the faults will be filtered. If Regions have not been created, Region tab will not appear. The tabular or list view will show the below components:

- Equipment Component
- Pat-Number
- Cluster Id
- Site Priority
- Cause
- Prediction Day
- Priority
- Probability
- Fault Type,
- Alarm Occurrences
- Repeating Alarms

If only one region name/zone name is there under the corresponding tab, then by default that will be clicked.

The system will inform "We are presenting you the most critical faults predicted for the latest prediction week. Click on the faults for necessary details".

The screen will display “No critical faults to display” if there are no critical faults for the current prediction week.

Click each fault for detailed view (Predicted Fault Details without Prediction Action Tracking).

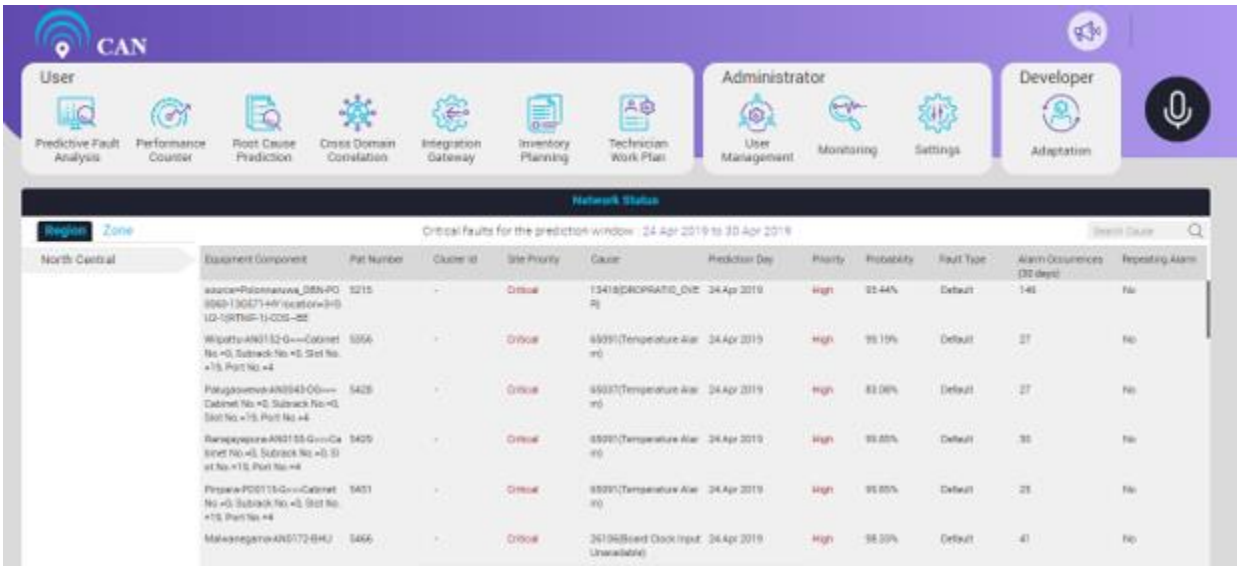


Figure 15.7 - Network Status