CAN - COGNITIVE ASSISTANT FOR NETWORKS

User Manual for Desktop Application Version 6.0

MARCH 1, 2023

AVANSEUS TECHNOLOGIES PVT. 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 6.0 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 6.0. 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:

AVANSEUS TECHNOLOGIES PVT LTD, 5-107, 5th Floor, Manyata Nxt, Tower-1, Embassy Manyata Business Park, Nagavara, Bengaluru - 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	August, 2021	Updates	Sandeep Singh	Sandeep Singh	Chiranjib
V 5.5	January, 2022	Updates	Raksha	Raksha	Chiranjib
V 6.0	March, 2023	Updates	Raksha	Raksha	Chiranjib

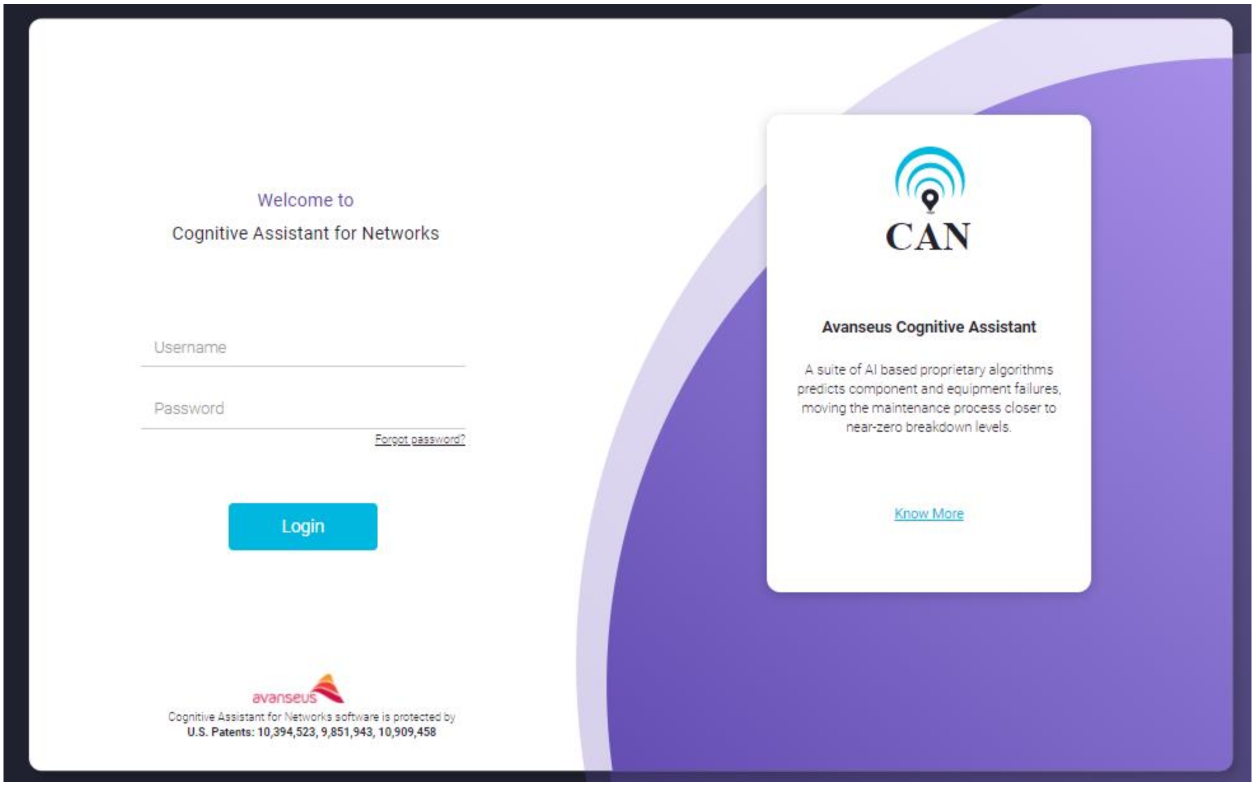
Table of Contents

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.



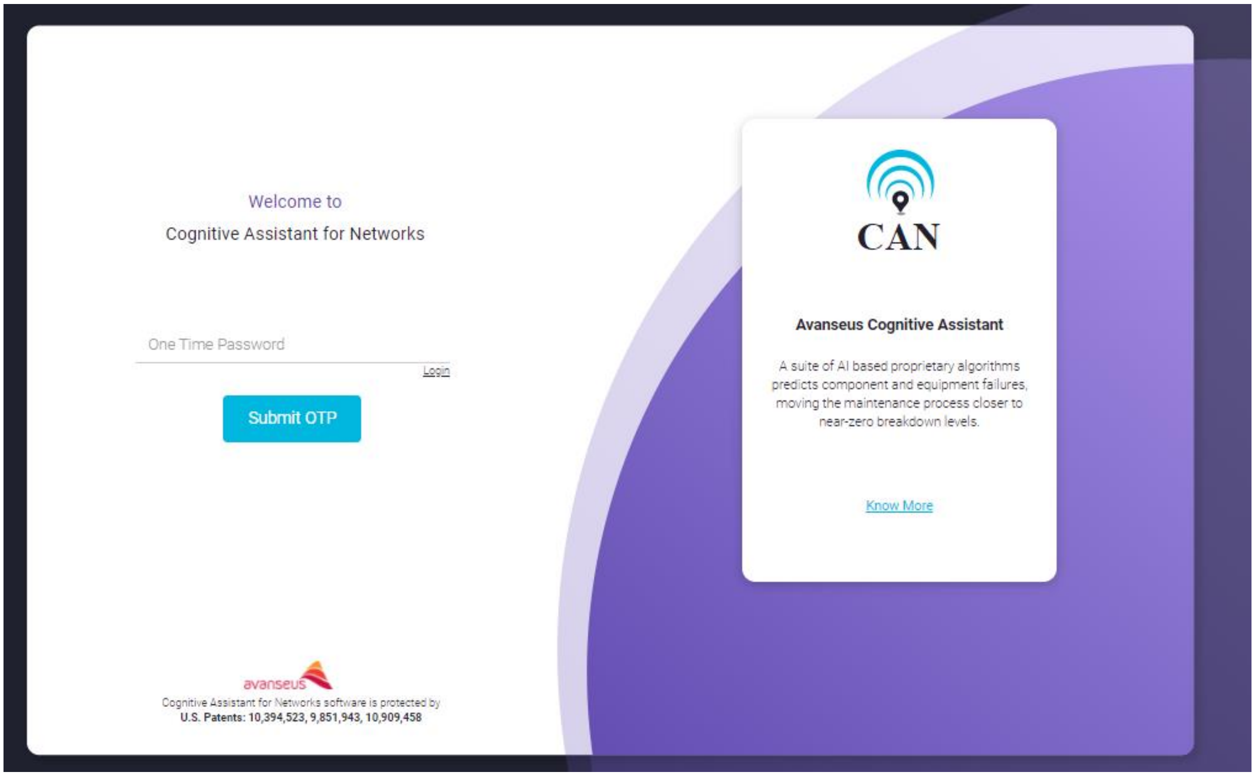
Avanseus Cognitive Assistant

A suite of AI based proprietary algorithms predicts component and equipment failures, moving the maintenance process closer to near-zero breakdown levels.

Cognitive Assistant for Networks software is protected by U.S. Patents: 10,394,523, 9,851,943, 10,909,458

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.



Welcome to
Cognitive Assistant for Networks

A suite of AI based proprietary algorithms predicts component and equipment failures, moving the maintenance process closer to near-zero breakdown levels.

Cognitive Assistant for Networks software is protected by U.S. Patents: 10,394,523, 9,851,943, 10,909,458

Figure 1.2 - Submit OTP Screen to Login

You can access the dashboard application.

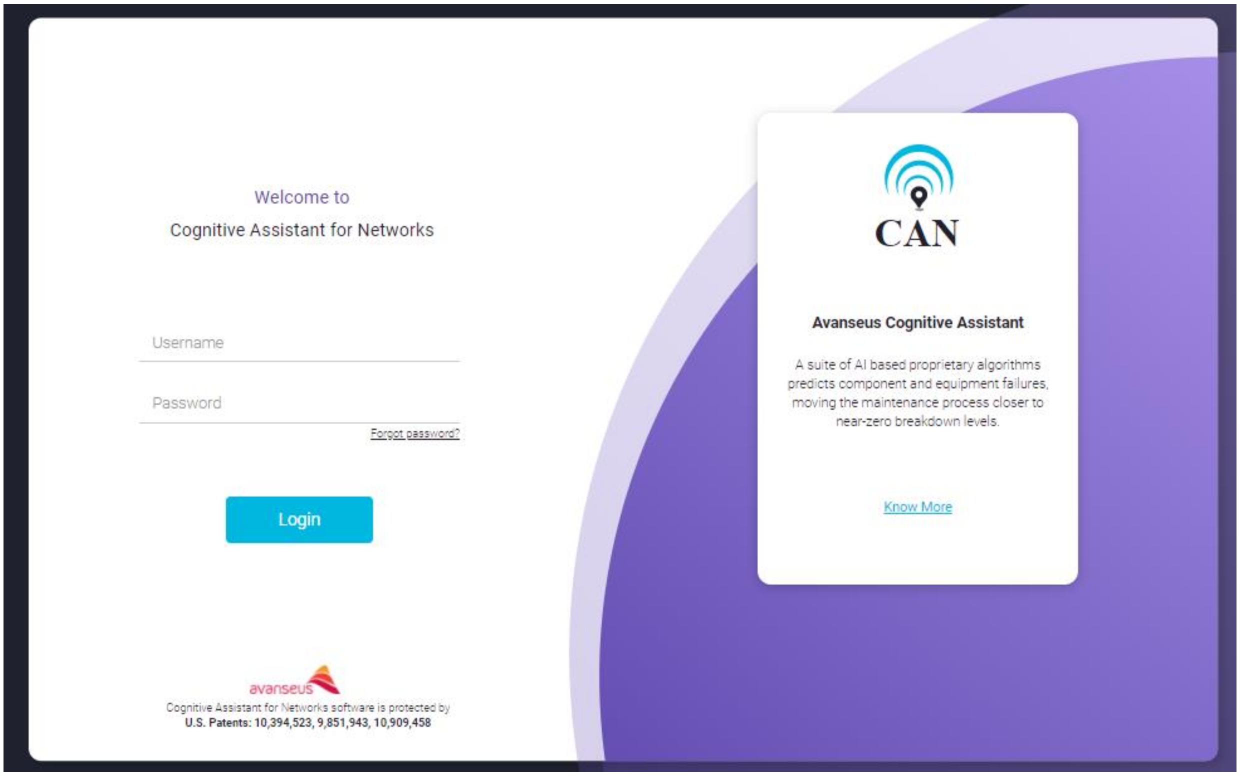
To know more about CAN (Cognitive Assistant Network), click Know More.

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.

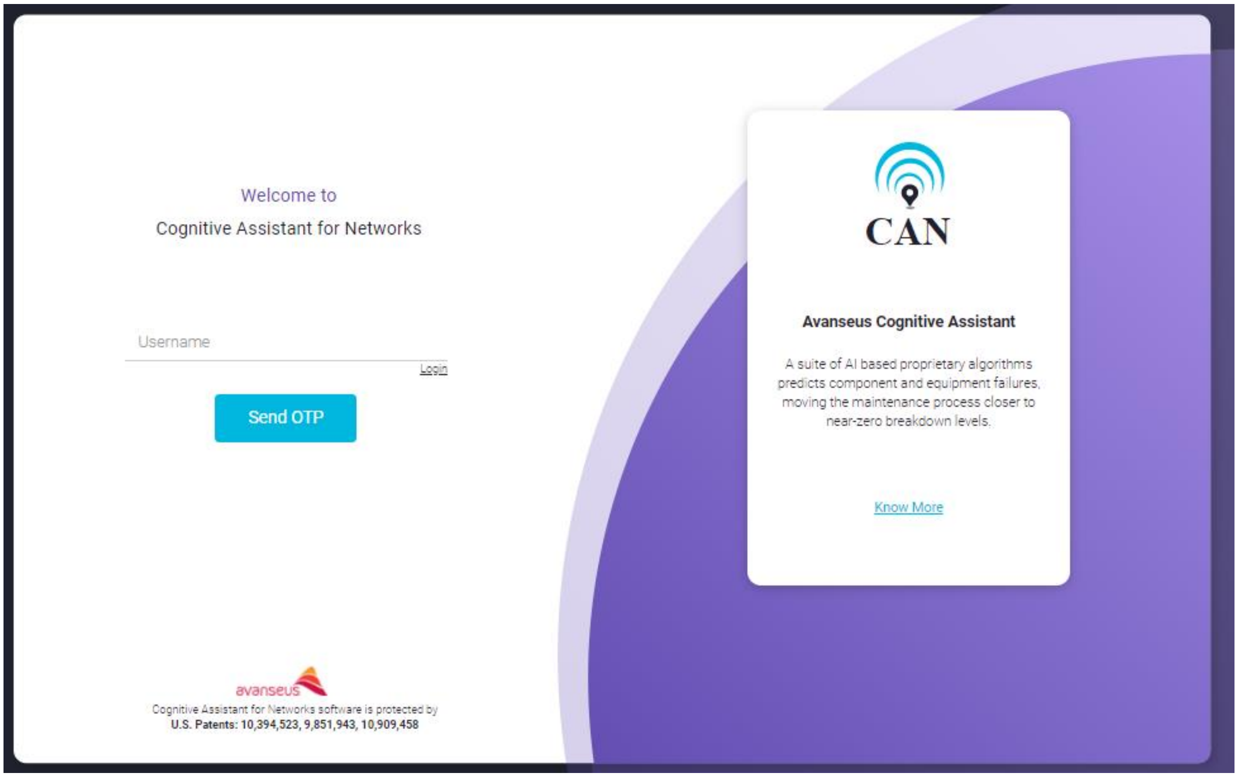


A suite of AI based proprietary algorithms predicts component and equipment failures, moving the maintenance process closer to near-zero breakdown levels.

Cognitive Assistant for Networks software is protected by **U.S. Patents: 10,394,523, 9,851,943, 10,909,458**

Figure 1.3 - Forgot Password Screen

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



Welcome to

Cognitive Assistant for Networks

Avanseus Cognitive Assistant

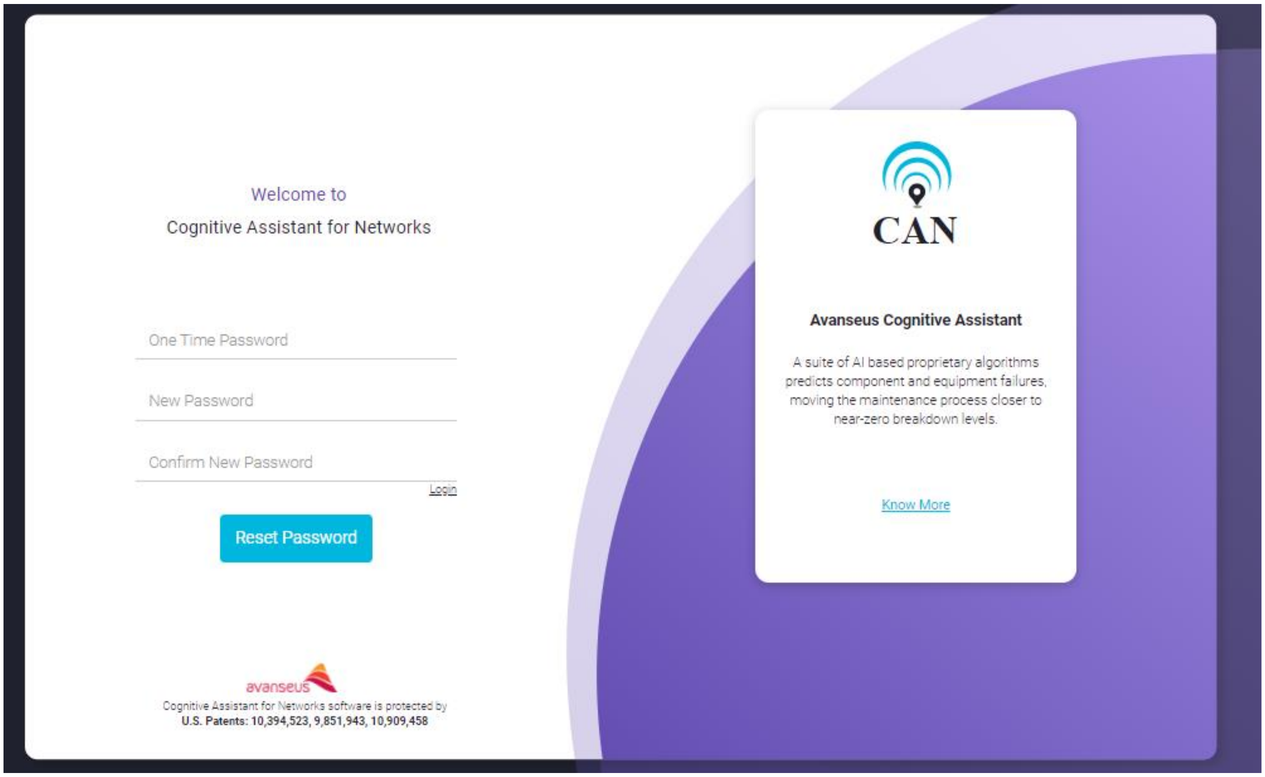
A suite of AI based proprietary algorithms predicts component and equipment failures, moving the maintenance process closer to near-zero breakdown levels.

Cognitive Assistant for Networks software is protected by U.S. Patents: 10,394,523, 9,851,943, 10,909,458

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**.



Cognitive Assistant for Networks software is protected by
U.S. Patents: 10,394,523, 9,851,943, 10,909,458

Avanseus Cognitive Assistant

A suite of AI based proprietary algorithms predicts component and equipment failures, moving the maintenance process closer to near-zero breakdown levels.

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 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.

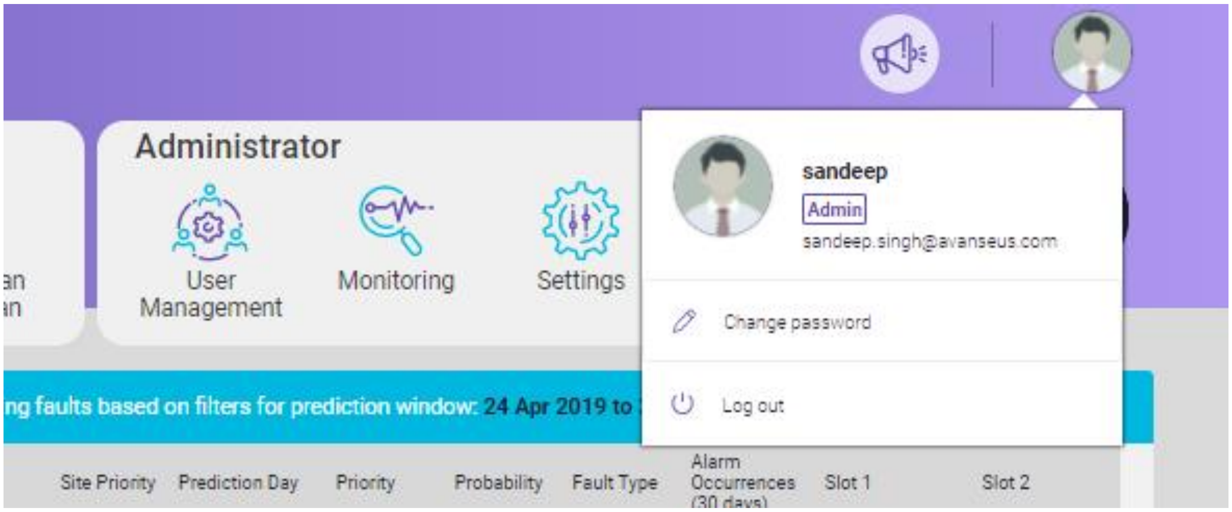


Figure 1.6 - User Profile

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.

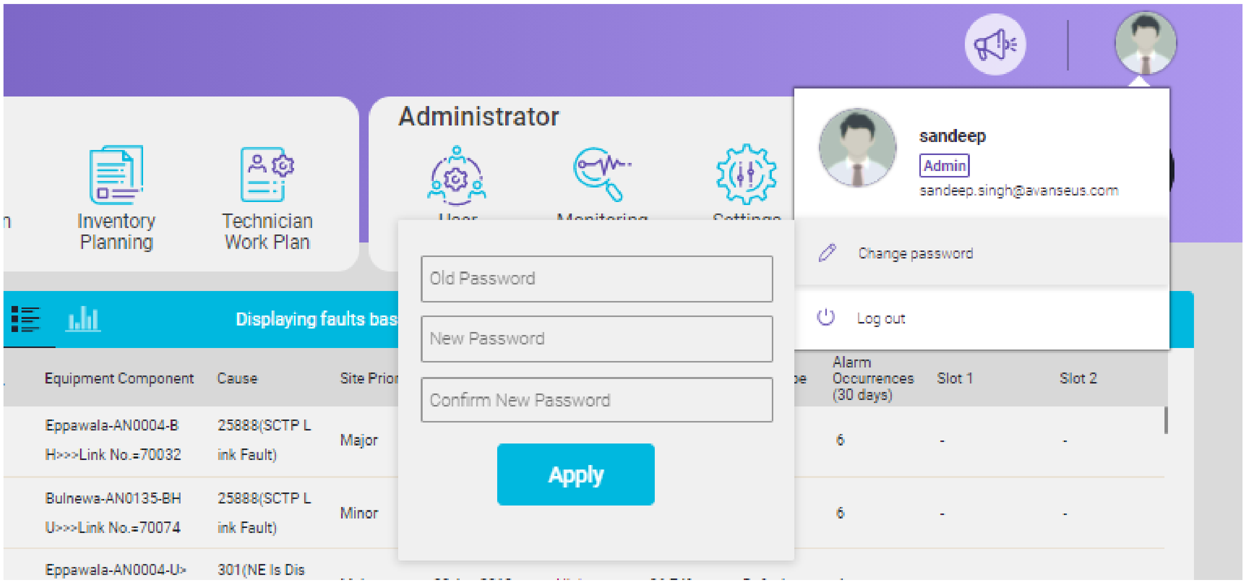


Figure 1.7 - Update Password Screen

Log Out

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

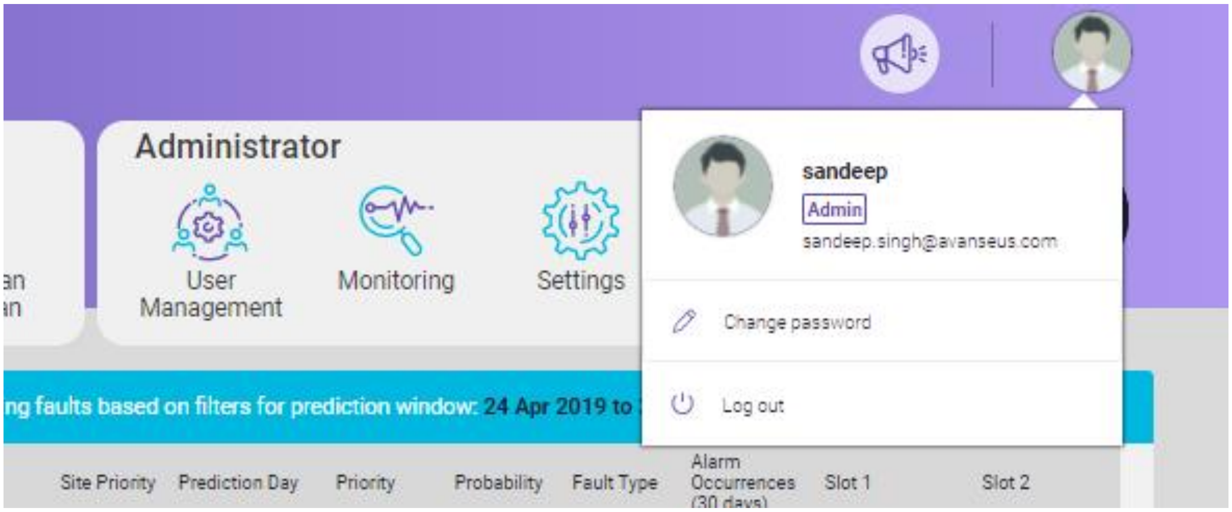


Figure 1.8 - Log Out Button

Page Intentionally Left Blank

2. EXECUTIVE DASHBOARD HOME

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

The executive dashboard has three sections:

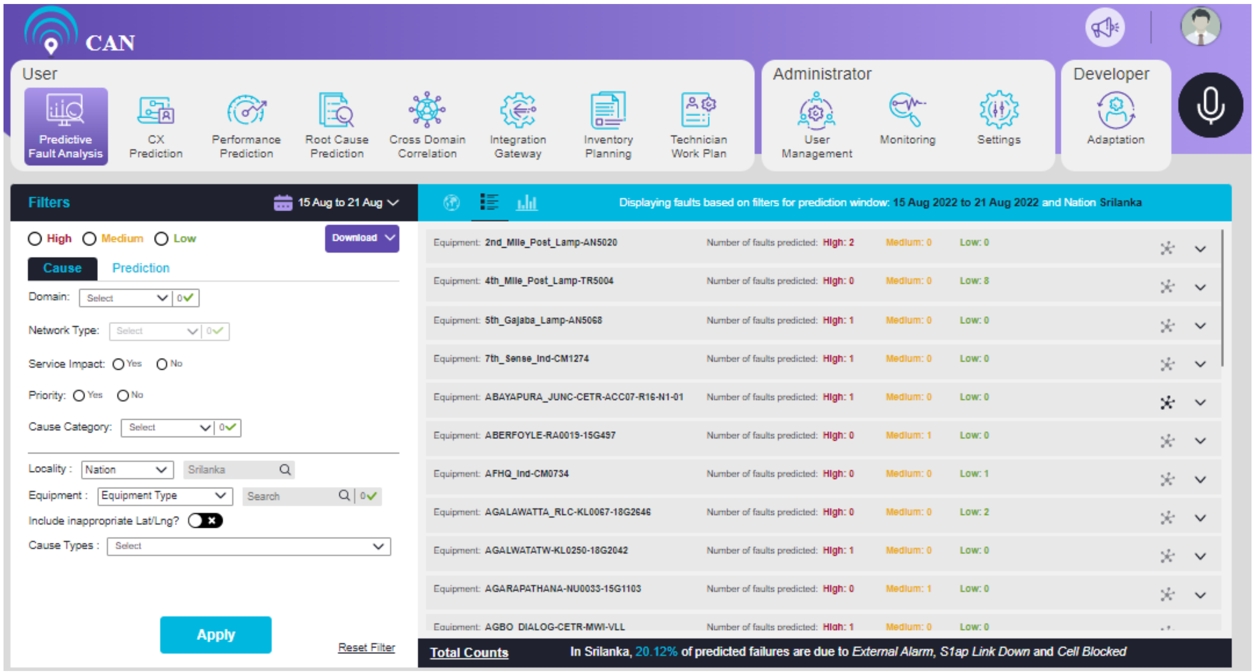
1. User
2. Administrator
3. Developer
4. VBI

The **User** section provides access to **Predictive Fault Analysis**, **CX Prediction**, **Anomaly 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**.

VBI (Voice Based Interaction) interface to fetch relevant (supported) set of queries on fault predictions.



15 Aug to 21 Aug

○ High ○ Medium ○ Low

Domain: Select 0✓

Network Type: Select 0✓

Service Impact: ○ Yes ○ No

Priority: ○ Yes ○ No

Cause Category: Select 0✓

Locality : Nation Srilanka

Equipment : Equipment Type Search 0✓

Include inappropriate Lat/Lng? ✕

Cause Types : Select

Displaying faults based on filters for prediction window: 15 Aug 2022 to 21 Aug 2022 and Nation Srilanka

Equipment: 2nd_Mile_Post_Lamp-AN5020 Number of faults predicted: High: 2 Medium: 0 Low: 0

Equipment: 4th_Mile_Post_Lamp-TR5004 Number of faults predicted: High: 0 Medium: 0 Low: 8

Equipment: 5th_Gajaba_Lamp-AN5068 Number of faults predicted: High: 1 Medium: 0 Low: 0

Equipment: 7th_Sense_Ind-CM1274 Number of faults predicted: High: 1 Medium: 0 Low: 0

Equipment: ABAYAPURA_JUNC-CETR-ACC07-R16-N1-01 Number of faults predicted: High: 1 Medium: 0 Low: 0

Equipment: ABERFOYLE-RA0019-15G457 Number of faults predicted: High: 0 Medium: 1 Low: 0

Equipment: AFHQ_Ind-CM0734 Number of faults predicted: High: 0 Medium: 0 Low: 1

Equipment: AGALAWATTA_RLC-KL0067-18G2646 Number of faults predicted: High: 0 Medium: 0 Low: 2

Equipment: AGALWATATW-KL0250-18G2042 Number of faults predicted: High: 1 Medium: 0 Low: 0

Equipment: AGARAPATHANA-NU0033-15G1103 Number of faults predicted: High: 0 Medium: 1 Low: 0

Equipment: AGBO_DIALOG-CETR-MWI-VLL Number of faults predicted: High: 1 Medium: 0 Low: 0

In Srilanka, 20.12% of predicted failures are due to *External Alarm*, *S1ap Link Down* and *Cell Blocked*

Figure 2.1 - Executive Dashboard Home

Page Intentionally Left Blank

3. PREDICTIVE FAULT ANALYSIS

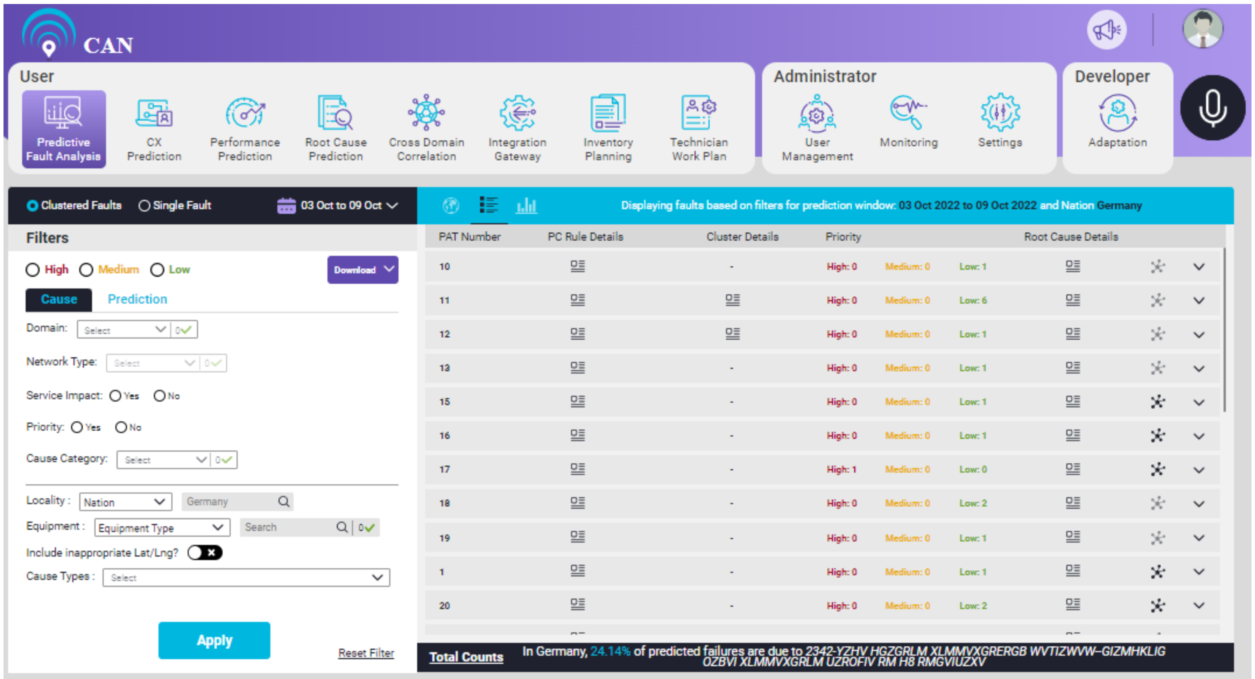
Predictive Fault Analysis screen navigates to the fault predictions made by CAN for the available data. By default, Predictive Fault Analysis screen displays the predictions related to the latest prediction window in the tabular form.

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

Based on the Parent-child rules, clusters are generated. Once predictions are complete, Predictive Fault Analysis screen categorizes the data as **Clustered Faults** and **Single Fault**. By default, Clustered Faults are displayed.

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).



● Clustered Faults ○ Single Fault

03 Oct to 09 Oct

○ High ○ Medium ○ Low

Cause | Prediction

Domain: Select | 0✓

Network Type: Select | 0✓

Service Impact: ○ Yes ○ No

Priority: ○ Yes ○ No

Cause Category: Select | 0✓

Locality : Nation | Germany

Equipment : Equipment Type | Search | 0✓

Include inappropriate Lat/Lng? ✕

Cause Types : Select

Displaying faults based on filters for prediction window: 03 Oct 2022 to 09 Oct 2022 and Nation Germany

PAT Number	PC Rule Details	Cluster Details	Priority			Root Cause Details		
10	▤	-	High: 0	Medium: 0	Low: 1	▤	✱	⌄
11	▤	▤	High: 0	Medium: 0	Low: 6	▤	✱	⌄
12	▤	▤	High: 0	Medium: 0	Low: 1	▤	✱	⌄
13	▤	-	High: 0	Medium: 0	Low: 1	▤	✱	⌄
15	▤	-	High: 0	Medium: 0	Low: 1	▤	✱	⌄
16	▤	-	High: 0	Medium: 0	Low: 1	▤	✱	⌄
17	▤	-	High: 1	Medium: 0	Low: 0	▤	✱	⌄
18	▤	-	High: 0	Medium: 0	Low: 2	▤	✱	⌄
19	▤	-	High: 0	Medium: 0	Low: 1	▤	✱	⌄
1	▤	-	High: 0	Medium: 0	Low: 1	▤	✱	⌄
20	▤	-	High: 0	Medium: 0	Low: 2	▤	✱	⌄

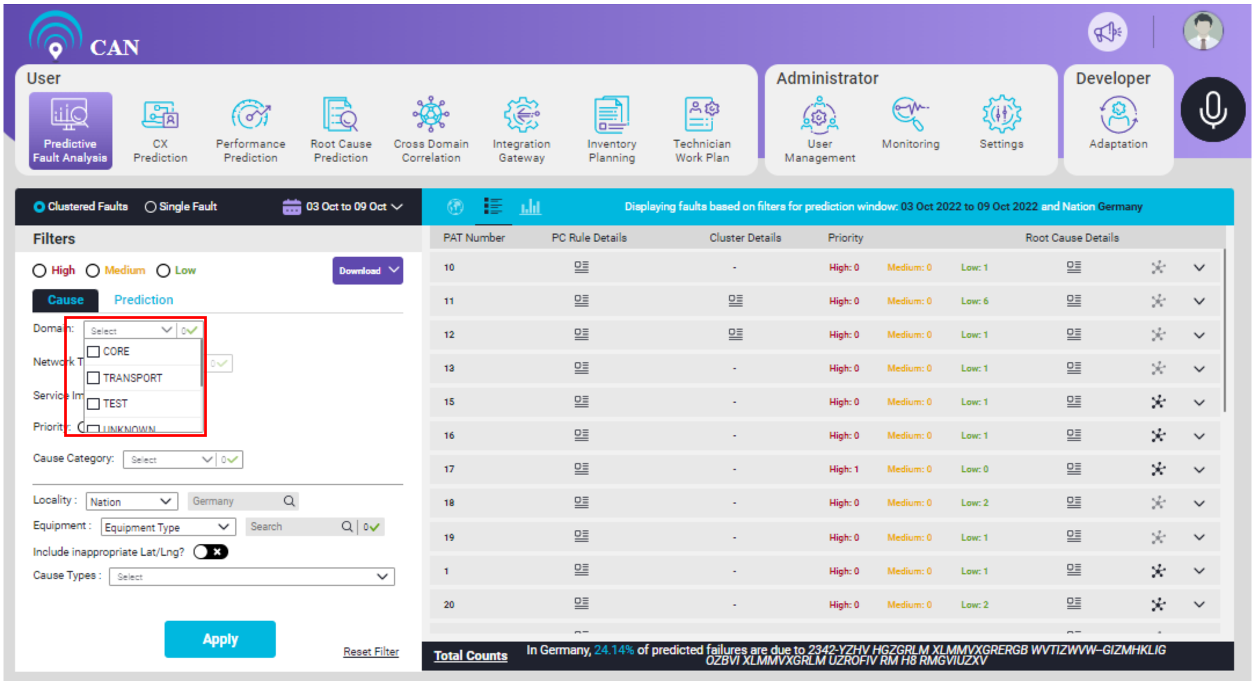
Total Counts — In Germany, 24.14% of predicted failures are due to 2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW–GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV

Figure 3.1 - Predictive Fault Analysis Screen

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. There are three **priority** check boxes. **High** (written in red color), **Medium** (written in yellow color) and **Low** (written in green color). User can select any or all of the priorities check boxes at a time.
2. **Domain**: There can be multiple domains (Currently, the screen displays three domains i.e. **Core**, **Transport** and **Access**. Each **Domain** will have their dependent **Network Type**).



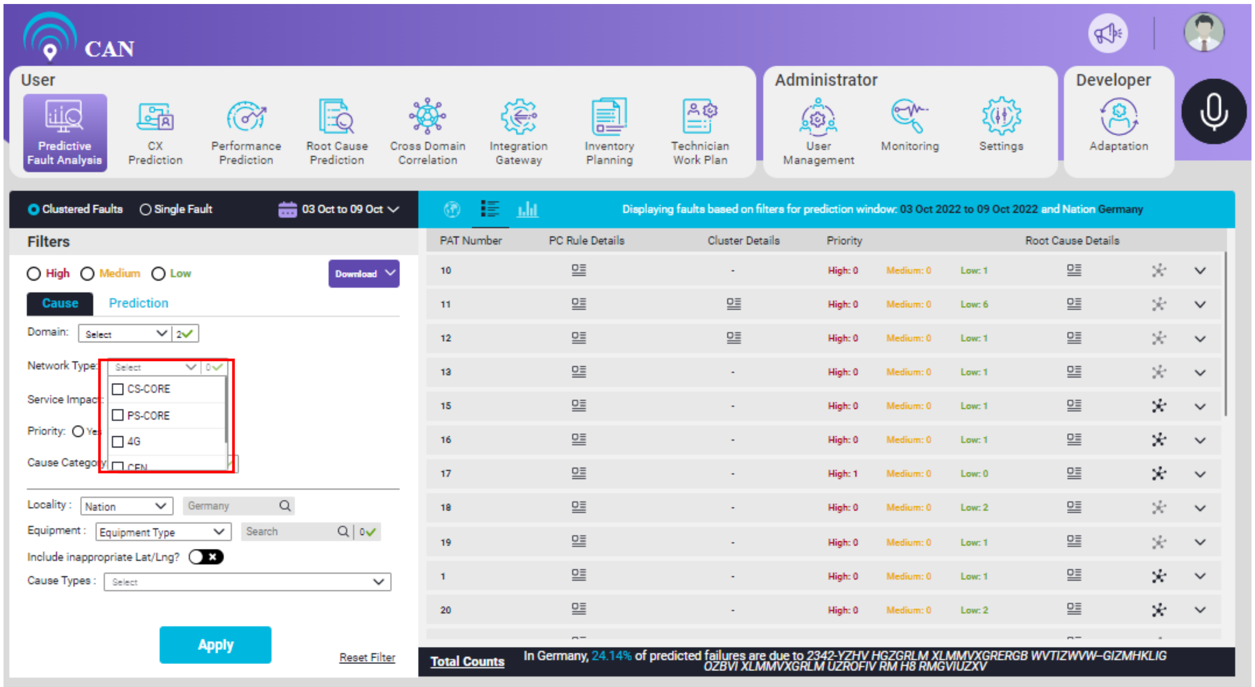
Displaying faults based on filters for prediction window: 03 Oct 2022 to 09 Oct 2022 and Nation Germany

PAT Number	PC Rule Details	Cluster Details	Priority			Root Cause Details
10		-	High: 0	Medium: 0	Low: 1	
11			High: 0	Medium: 0	Low: 6	
12			High: 0	Medium: 0	Low: 1	
13		-	High: 0	Medium: 0	Low: 1	
15		-	High: 0	Medium: 0	Low: 1	
16		-	High: 0	Medium: 0	Low: 1	
17		-	High: 1	Medium: 0	Low: 0	
18		-	High: 0	Medium: 0	Low: 2	
19		-	High: 0	Medium: 0	Low: 1	
1		-	High: 0	Medium: 0	Low: 1	
20		-	High: 0	Medium: 0	Low: 2	

In Germany, 24.14% of predicted failures are due to 2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW–GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV

Figure 3.2 - Domain Dropdown

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



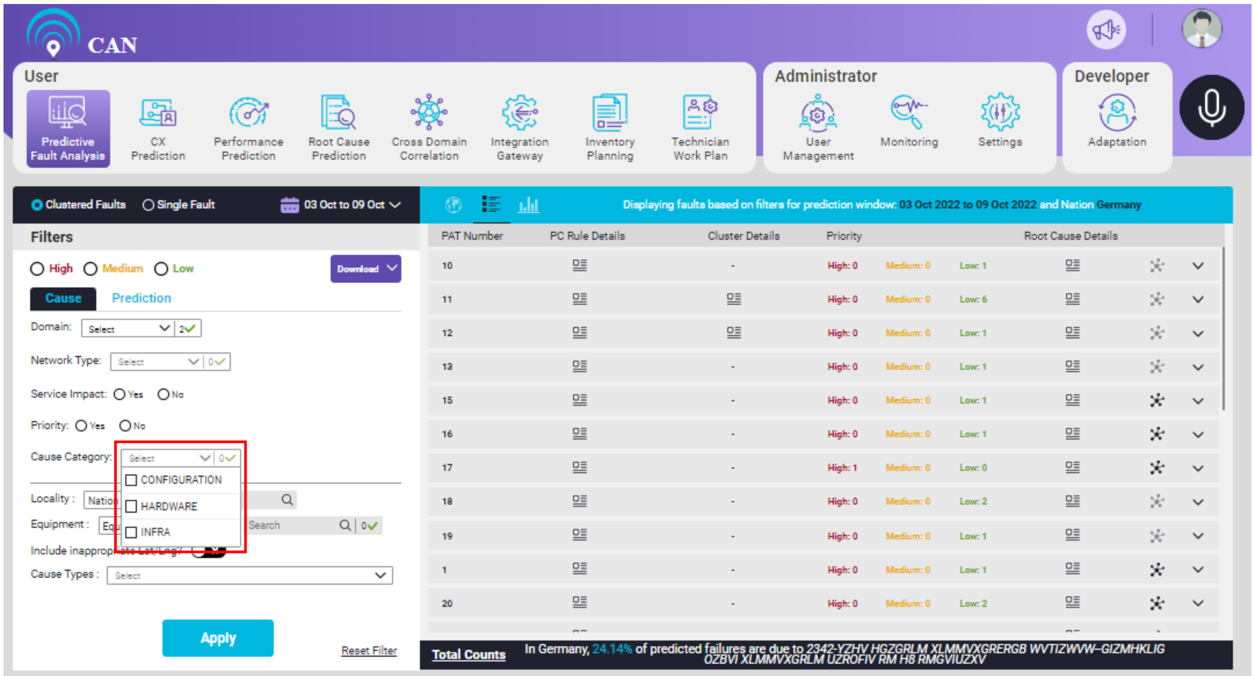
Displaying faults based on filters for prediction window: 03 Oct 2022 to 09 Oct 2022 and Nation Germany

PAT Number	PC Rule Details	Cluster Details	Priority			Root Cause Details
10		-	High: 0	Medium: 0	Low: 1	
11			High: 0	Medium: 0	Low: 6	
12			High: 0	Medium: 0	Low: 1	
13		-	High: 0	Medium: 0	Low: 1	
15		-	High: 0	Medium: 0	Low: 1	
16		-	High: 0	Medium: 0	Low: 1	
17		-	High: 1	Medium: 0	Low: 0	
18		-	High: 0	Medium: 0	Low: 2	
19		-	High: 0	Medium: 0	Low: 1	
1		-	High: 0	Medium: 0	Low: 1	
20		-	High: 0	Medium: 0	Low: 2	

In Germany, 24.14% of predicted failures are due to 2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW–GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV

Figure 3.3 - Network Type Dropdown

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



● Clustered Faults ○ Single Fault 03 Oct to 09 Oct

Filters

○ High ○ Medium ○ Low

Cause | Prediction

Domain: Select 2✓

Network Type: Select 0✓

Service Impact: ○ Yes ○ No

Priority: ○ Yes ○ No

Cause Category: Select 0✓
- □ CONFIGURATION
- □ HARDWARE
- □ INFRA

Locality : Natio

Equipment : Equ Search 0✓

Include inappropriate Lat/Lng?

Cause Types : Select

Displaying faults based on filters for prediction window: 03 Oct 2022 to 09 Oct 2022 and Nation Germany

PAT Number	PC Rule Details	Cluster Details	Priority			Root Cause Details
10		-	High: 0	Medium: 0	Low: 1	
11			High: 0	Medium: 0	Low: 6	
12			High: 0	Medium: 0	Low: 1	
13		-	High: 0	Medium: 0	Low: 1	
15		-	High: 0	Medium: 0	Low: 1	
16		-	High: 0	Medium: 0	Low: 1	
17		-	High: 1	Medium: 0	Low: 0	
18		-	High: 0	Medium: 0	Low: 2	
19		-	High: 0	Medium: 0	Low: 1	
1		-	High: 0	Medium: 0	Low: 1	
20		-	High: 0	Medium: 0	Low: 2	

In Germany, 24.14% of predicted failures are due to 2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW–GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV

Figure 3.4 - Cause Category Dropdown

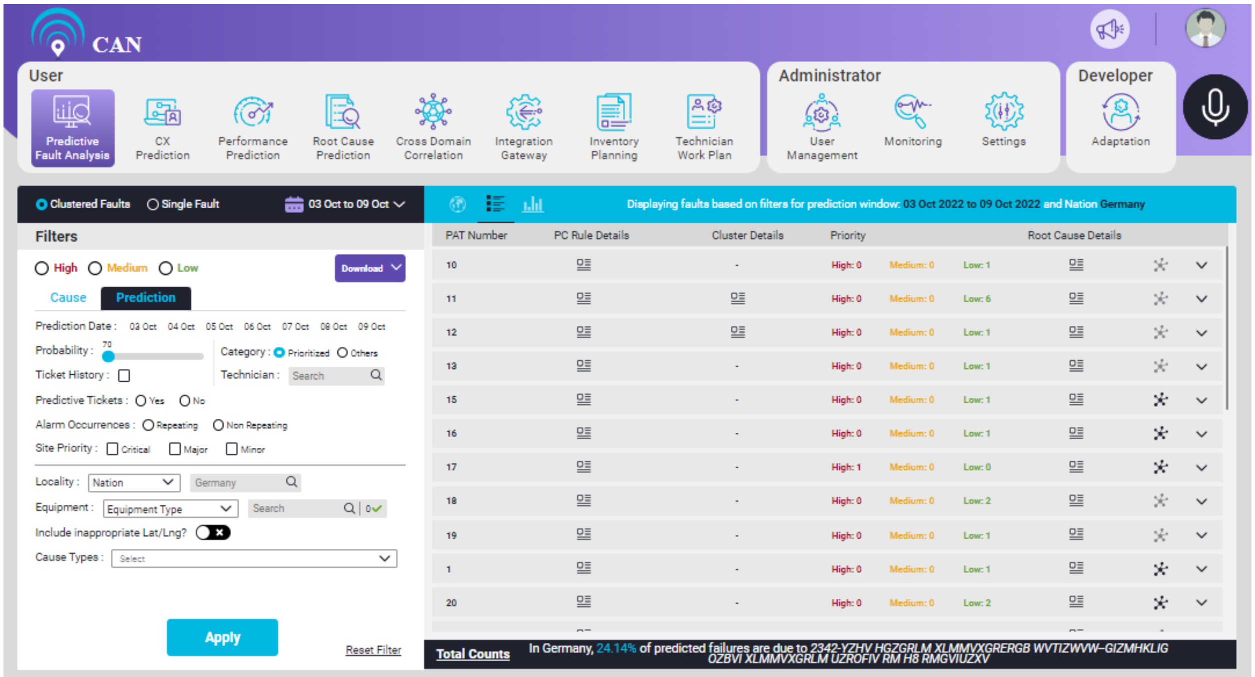
User can select the appropriate **Cause** attributes as per the requirement.

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 has 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.

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, and 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/Long**: A toggle button to include or exclude the inappropriate Lat/Long.
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.



● Clustered Faults ○ Single Fault 03 Oct to 09 Oct

Filters

○ High ○ Medium ○ Low Download

Cause **Prediction**

Prediction Date : 03 Oct 04 Oct 05 Oct 06 Oct 07 Oct 08 Oct 09 Oct

Probability : 70

Category : ● Prioritized ○ Others

Ticket History : □

Technician : Search

Predictive Tickets : ○ Yes ○ No

Alarm Occurrences : ○ Repeating ○ Non Repeating

Site Priority : □ Critical □ Major □ Minor

Locality : Nation Germany

Equipment : Equipment Type Search 0✓

Include inappropriate Lat/Lng? ☒

Cause Types : Select

Apply

Reset Filter

Displaying faults based on filters for prediction window: 03 Oct 2022 to 09 Oct 2022 and Nation Germany

PAT Number	PC Rule Details	Cluster Details	Priority			Root Cause Details		
10	☰	-	High: 0	Medium: 0	Low: 1	☰	✳	⌄
11	☰	☰	High: 0	Medium: 0	Low: 6	☰	✳	⌄
12	☰	☰	High: 0	Medium: 0	Low: 1	☰	✳	⌄
13	☰	-	High: 0	Medium: 0	Low: 1	☰	✳	⌄
15	☰	-	High: 0	Medium: 0	Low: 1	☰	✳	⌄
16	☰	-	High: 0	Medium: 0	Low: 1	☰	✳	⌄
17	☰	-	High: 1	Medium: 0	Low: 0	☰	✳	⌄
18	☰	-	High: 0	Medium: 0	Low: 2	☰	✳	⌄
19	☰	-	High: 0	Medium: 0	Low: 1	☰	✳	⌄
1	☰	-	High: 0	Medium: 0	Low: 1	☰	✳	⌄
20	☰	-	High: 0	Medium: 0	Low: 2	☰	✳	⌄

Total Counts In Germany, 24.14% of predicted failures are due to *2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW–GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV*

Figure 3.5 - Filters for Prediction Tab

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:

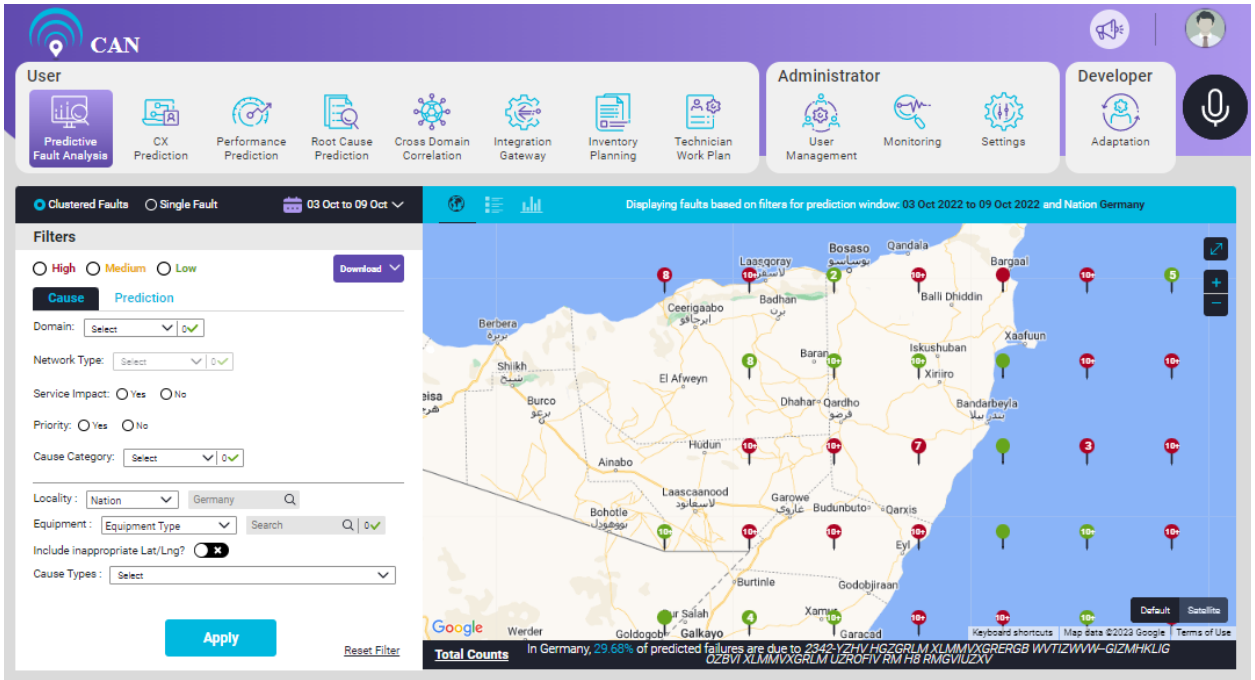
- Map View
- Tabular View
- Stats View

To select the Map view, click the map icon 🌐.

Map View

By default, Map view is displayed for **Clustered Faults**. To view the map for individual faults, click the **Single Fault** radio button and then click **Apply**.

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.



Displaying faults based on filters for prediction window: 03 Oct 2022 to 09 Oct 2022 and Nation Germany

In Germany, 29.68% of predicted failures are due to 2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWW–GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV

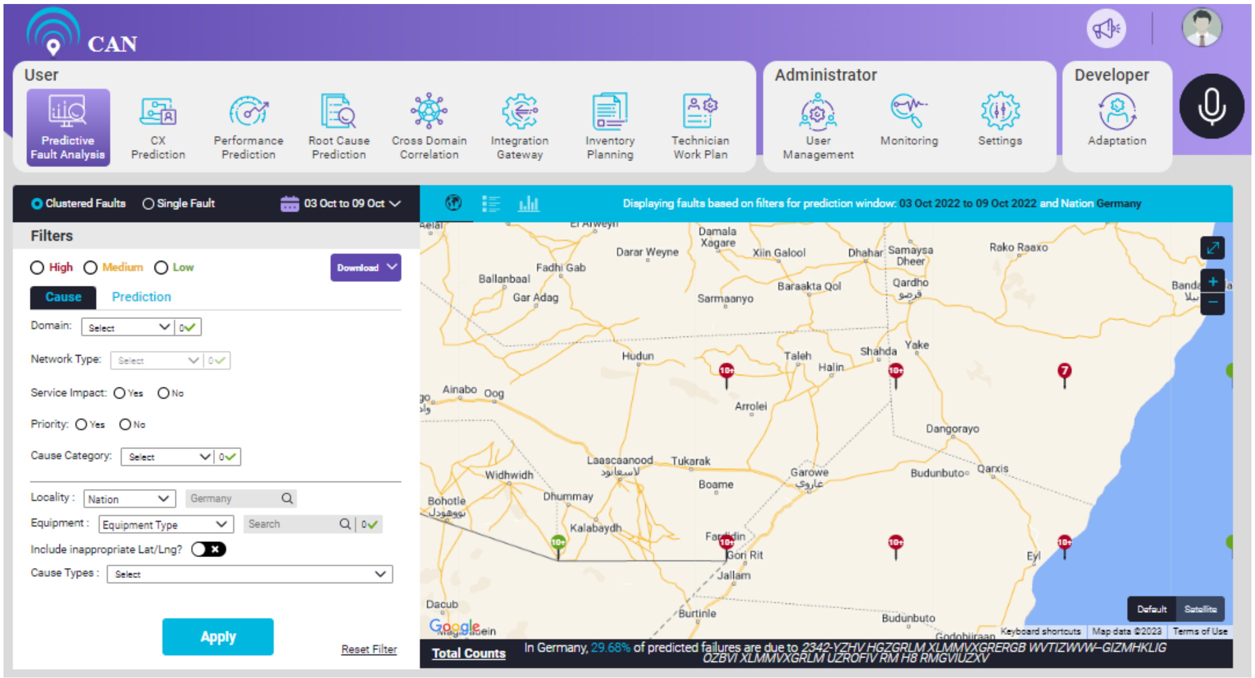
Figure 3.6 - Location Based Filtering

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



● Clustered Faults ○ Single Fault 03 Oct to 09 Oct

Displaying faults based on filters for prediction window: 03 Oct 2022 to 09 Oct 2022 and Nation Germany

○ High ○ Medium ○ Low

Domain: Select 0✓

Network Type: Select 0✓

Service Impact: ○ Yes ○ No

Priority: ○ Yes ○ No

Cause Category: Select 0✓

Locality : Nation Germany

Equipment : Equipment Type Search 0✓

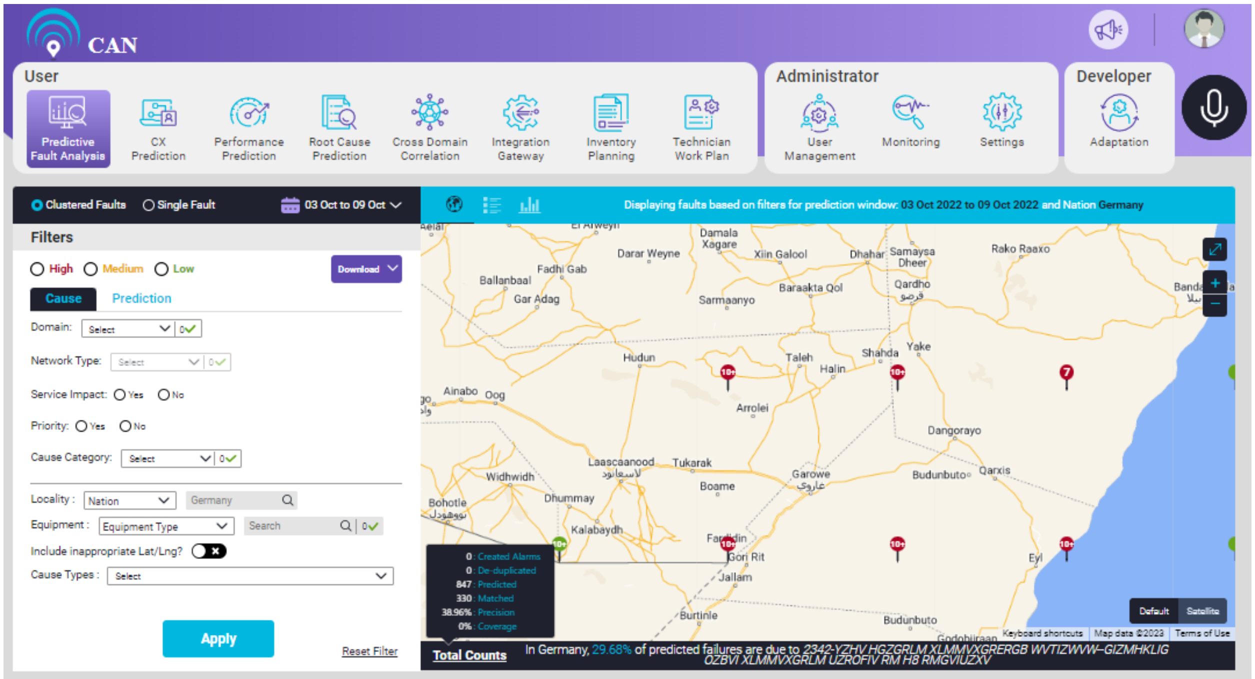
Include inappropriate Lat/Lng?

Cause Types : Select

Total Counts In Germany, 29.68% of predicted failures are due to 2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW–GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV

Figure 3.7 - Faults Based on Priority

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



● Clustered Faults ○ Single Fault 03 Oct to 09 Oct

Displaying faults based on filters for prediction window: 03 Oct 2022 to 09 Oct 2022 and Nation Germany

○ High ○ Medium ○ Low

Domain: Select 0✓

Network Type: Select 0✓

Service Impact: ○ Yes ○ No

Priority: ○ Yes ○ No

Cause Category: Select 0✓

Locality : Nation Germany

Equipment : Equipment Type Search 0✓

Include inappropriate Lat/Lng?

Cause Types : Select

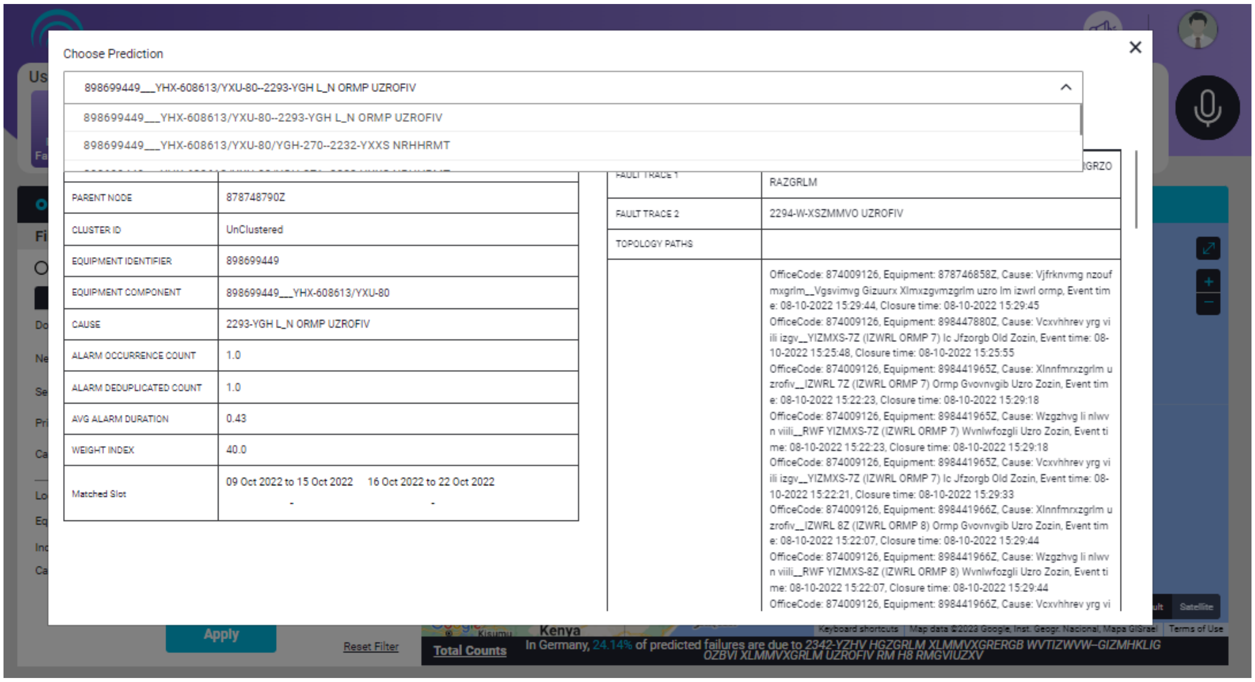
0 : Created Alarms
0 : De-duplicated
847 : Predicted
330 : Matched
38.96% : Precision
0% : Coverage

Total Counts In Germany, 29.68% of predicted failures are due to 2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW–GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV

Figure 3.8 - 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.


Choose Prediction
Apply
Reset Filter
Total Counts
Kenya
Kisumu
Keyboard shortcuts | Map data ©2023 Google, Inst. Geogr. Nacional, Mapa GISrael | Terms of Use
Satellite

898699449___YHX-608613/YXU-80--2293-YGH L_N ORMP UZROFIV

- 898699449___YHX-608613/YXU-80--2293-YGH L_N ORMP UZROFIV
- 898699449___YHX-608613/YXU-80/YGH-270--2232-YXXS NRHHRMT

PARENT NODE	878748790Z
CLUSTER ID	UnClustered
EQUIPMENT IDENTIFIER	898699449
EQUIPMENT COMPONENT	898699449___YHX-608613/YXU-80
CAUSE	2293-YGH L_N ORMP UZROFIV
ALARM OCCURRENCE COUNT	1.0
ALARM DEDUPLICATED COUNT	1.0
AVG ALARM DURATION	0.43
WEIGHT INDEX	40.0
Matched Slot	09 Oct 2022 to 15 Oct 2022 - 16 Oct 2022 to 22 Oct 2022 -

FAULT TRACE 1	IGRZO RAZGRLM
FAULT TRACE 2	2294-W-XSZMMVO UZROFIV
TOPOLOGY PATHS	
	OfficeCode: 874009126, Equipment: 878746858Z, Cause: Vjfrknvmg nzouf mxgrlm__Vgsvimvg Gizuurx Xlmxzgvmzgrlm uzro lm izwrl ormp, Event time: 08-10-2022 15:29:44, Closure time: 08-10-2022 15:29:45 OfficeCode: 874009126, Equipment: 898447880Z, Cause: Vcxvhhrev yrg vi ili izgv__YIZMXS-7Z (IZWRL ORMP 7) Ic Jfzorgb Old Zozin, Event time: 08-10-2022 15:25:48, Closure time: 08-10-2022 15:25:55 OfficeCode: 874009126, Equipment: 898441965Z, Cause: Xlnnfmrxzgrlm uzrofiv__IZWRL 7Z (IZWRL ORMP 7) Ormp Gvovnvgib Uzro Zozin, Event time: 08-10-2022 15:22:23, Closure time: 08-10-2022 15:29:18 OfficeCode: 874009126, Equipment: 898441965Z, Cause: Wzgzhvg li nlwvn viili__RWF YIZMXS-7Z (IZWRL ORMP 7) Wvnlwfozgli Uzro Zozin, Event time: 08-10-2022 15:22:23, Closure time: 08-10-2022 15:29:18 OfficeCode: 874009126, Equipment: 898441965Z, Cause: Vcxvhhrev yrg vi ili izgv__YIZMXS-7Z (IZWRL ORMP 7) Ic Jfzorgb Old Zozin, Event time: 08-10-2022 15:22:21, Closure time: 08-10-2022 15:29:33 OfficeCode: 874009126, Equipment: 898441966Z, Cause: Xlnnfmrxzgrlm uzrofiv__IZWRL 8Z (IZWRL ORMP 8) Ormp Gvovnvgib Uzro Zozin, Event time: 08-10-2022 15:22:07, Closure time: 08-10-2022 15:29:44 OfficeCode: 874009126, Equipment: 898441966Z, Cause: Wzgzhvg li nlwvn viili__RWF YIZMXS-8Z (IZWRL ORMP 8) Wvnlwfozgli Uzro Zozin, Event time: 08-10-2022 15:22:07, Closure time: 08-10-2022 15:29:44 OfficeCode: 874009126, Equipment: 898441966Z, Cause: Vcxvhhrev yrg vi

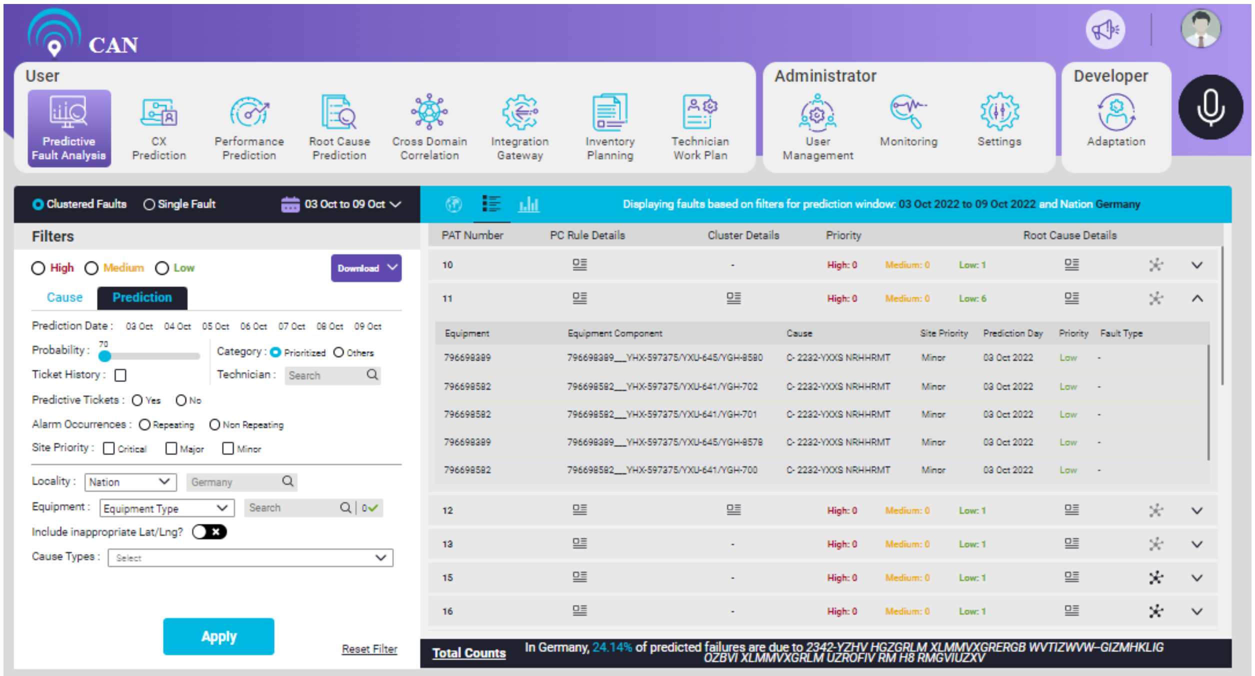
In Germany, 24.14% of predicted failures are due to 2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW–GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV

Figure 3.9 - Clustered Equipment

Tabular View

Clustered Faults

1. To view the tabular view, click the tabular icon.
2. By default, **Clustered Faults** is selected.
3. The tabular view has the following attributes:
   - Pat Number
   - PC Rule Details
   - Cluster Details
   - Priority
   - Root Cause Details
4. To view the Predicted Fault Details, click the ⌄ icon. The attributes are:
   - Equipment
   - Equipment Component
   - Cause
   - Site Priority
   - Prediction Day
   - Priority
   - Fault Type



● Clustered Faults ○ Single Fault 03 Oct to 09 Oct

Displaying faults based on filters for prediction window: 03 Oct 2022 to 09 Oct 2022 and Nation Germany

○ High ○ Medium ○ Low

Cause | Prediction

Prediction Date : 03 Oct 04 Oct 05 Oct 06 Oct 07 Oct 08 Oct 09 Oct

Probability : 70

Category : ● Prioritized ○ Others

Ticket History : □

Technician : Search

Predictive Tickets : ○ Yes ○ No

Alarm Occurrences : ○ Repeating ○ Non Repeating

Site Priority : □ Critical □ Major □ Minor

Locality : Nation Germany

Equipment : Equipment Type Search 0✓

Include inappropriate Lat/Lng?

Cause Types : Select

PAT Number	PC Rule Details	Cluster Details	Priority			Root Cause Details
10	☰	-	High: 0	Medium: 0	Low: 1	☰
11	☰	☰	High: 0	Medium: 0	Low: 6	☰

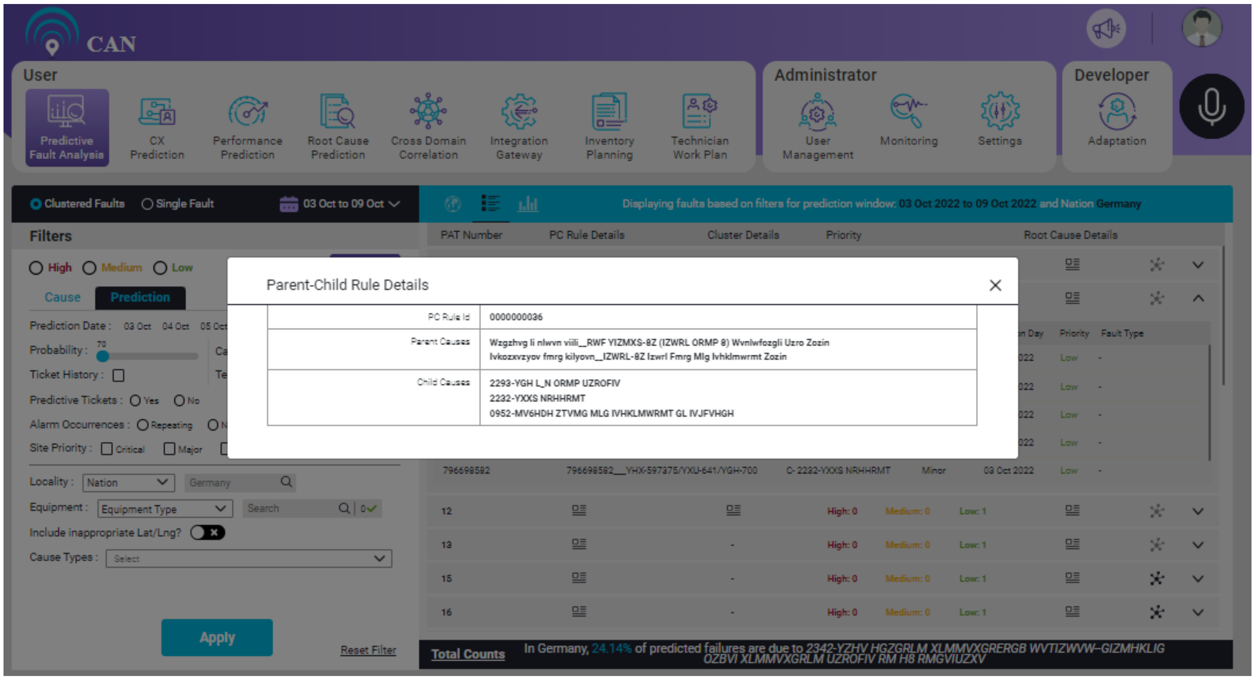
Equipment	Equipment Component	Cause	Site Priority	Prediction Day	Priority	Fault Type
796698389	796698389___YHX-597375/YXU-645/YGH-8580	C- 2232-YXXS NRHHRMT	Minor	03 Oct 2022	Low	-
796698582	796698582___YHX-597375/YXU-641/YGH-702	C- 2232-YXXS NRHHRMT	Minor	03 Oct 2022	Low	-
796698582	796698582___YHX-597375/YXU-641/YGH-701	C- 2232-YXXS NRHHRMT	Minor	03 Oct 2022	Low	-
796698389	796698389___YHX-597375/YXU-645/YGH-8578	C- 2232-YXXS NRHHRMT	Minor	03 Oct 2022	Low	-
796698582	796698582___YHX-597375/YXU-641/YGH-700	C- 2232-YXXS NRHHRMT	Minor	03 Oct 2022	Low	-

PAT Number	PC Rule Details	Cluster Details	Priority			Root Cause Details
12	☰	☰	High: 0	Medium: 0	Low: 1	☰
13	☰	-	High: 0	Medium: 0	Low: 1	☰
15	☰	-	High: 0	Medium: 0	Low: 1	☰
16	☰	-	High: 0	Medium: 0	Low: 1	☰

In Germany, 24.14% of predicted failures are due to 2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW–GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV

Figure 3.10 - Predictive Failure Analysis (Tabular View)

5. To view the PC Rule Details, click the icon ☰.

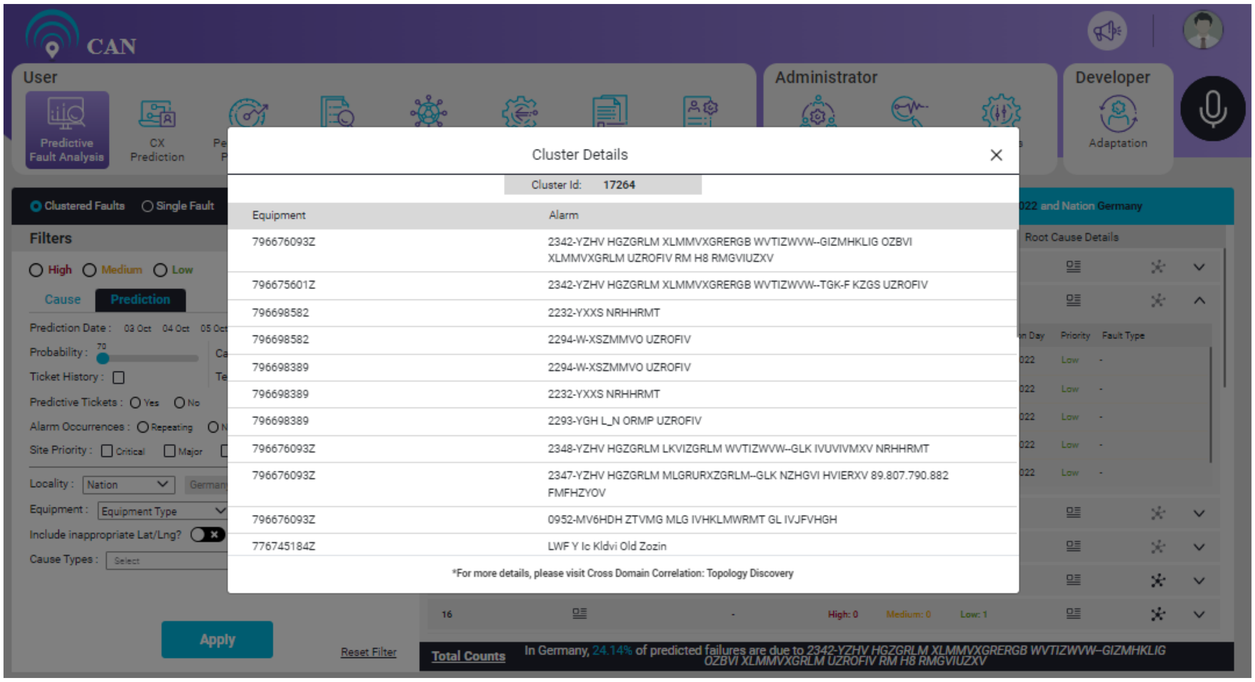


Parent-Child Rule Details

PC Rule Id	0000000036
Parent Causes	Wzgzhvg li nlwvn viili__RWF YIZMXS-8Z (IZWRL ORMP 8) Wvnlwfozgli Uzro Zozin Ivkozxvzyov fmrg kilyovn__IZWRL-8Z Izwrl Fmrg Mlg Ivhklmwrmt Zozin
Child Causes	2293-YGH L_N ORMP UZROFIV 2232-YXXS NRHHRMT 0952-MV6HDH ZTVMG MLG IVHKLMWRMT GL IVJFVHGH

Figure 3.11 - PC Rule Details

6. To view the Cluster Details, click the icon ☰.



Cluster Details

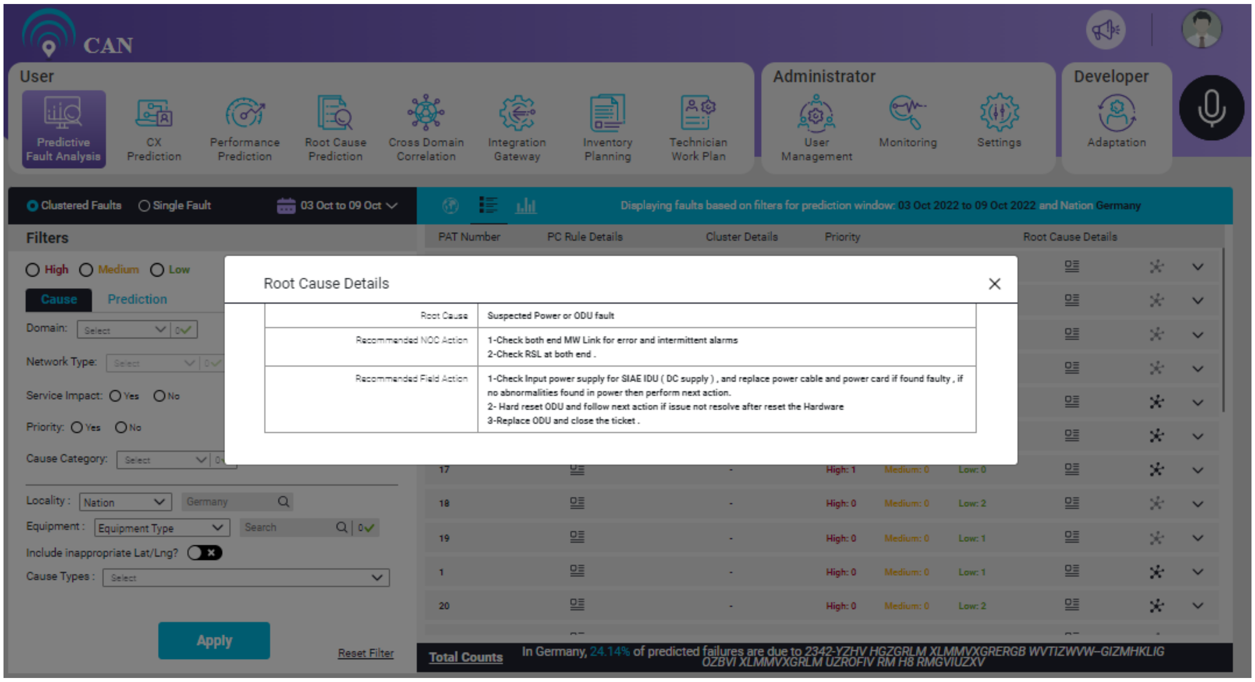
Cluster Id: 17264

Equipment	Alarm
796676093Z	2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW--GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV
796675601Z	2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW--TGK-F KZGS UZROFIV
796698582	2232-YXXS NRHHRMT
796698582	2294-W-XSZMMVO UZROFIV
796698389	2294-W-XSZMMVO UZROFIV
796698389	2232-YXXS NRHHRMT
796698389	2293-YGH L_N ORMP UZROFIV
796676093Z	2348-YZHV HGZGRLM LKVIZGRLM WVTIZWVW--GLK IVUVIVMXV NRHHRMT
796676093Z	2347-YZHV HGZGRLM MLGRURXZGRLM--GLK NZHGVI HVIERXV 89.807.790.882 FMFHZYOV
796676093Z	0952-MV6HDH ZTVMG MLG IVHKLMWRMT GL IVJFVHGH
776745184Z	LWF Y Ic Kldvi Old Zozin

*For more details, please visit Cross Domain Correlation: Topology Discovery

In Germany, 24.14% of predicted failures are due to 2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW--GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV

7. To view the **Root Cause Details**, click the icon ☰.



Displaying faults based on filters for prediction window: 03 Oct 2022 to 09 Oct 2022 and Nation Germany

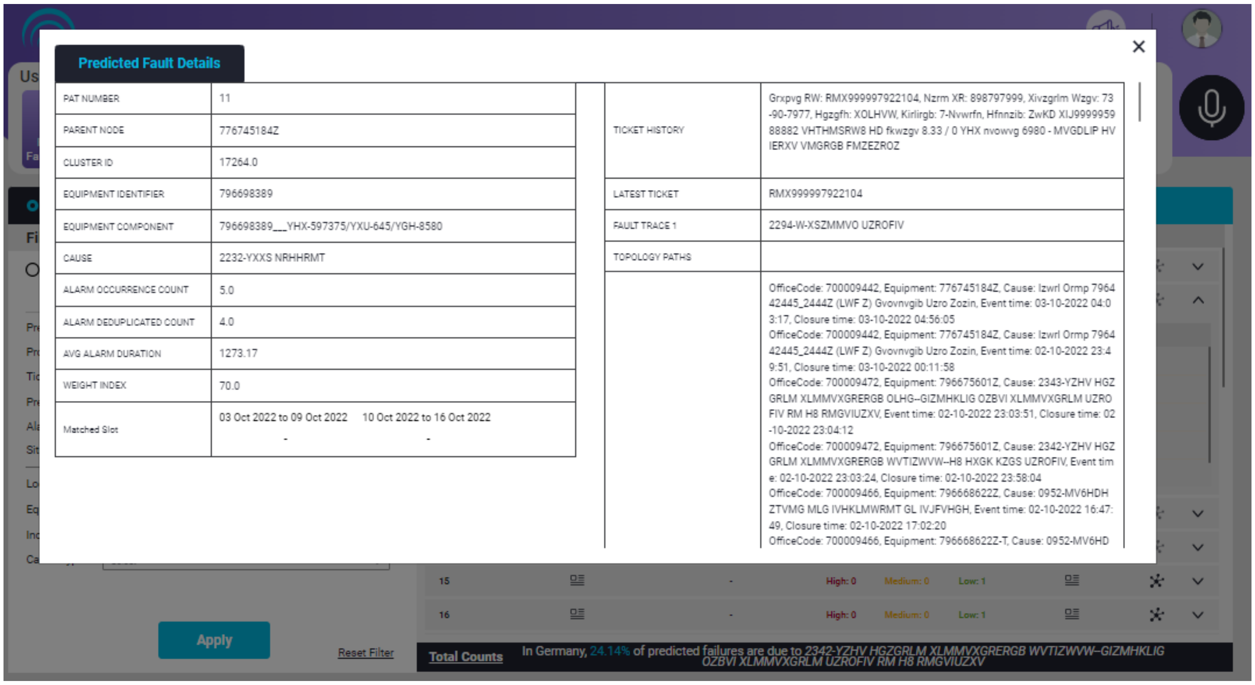
Root Cause Details

Root Cause	Suspected Power or ODU fault
Recommended NOC Action	1-Check both end MW Link for error and intermittent alarms 2-Check RSL at both end .
Recommanded Field Action	1-Check Input power supply for SIAE IDU (DC supply) , and replace power cable and power card if found faulty , if no abnormalities found in power then perform next action. 2- Hard reset ODU and follow next action if issue not resolve after reset the Hardware 3-Replace ODU and close the ticket .

In Germany, 24.14% of predicted failures are due to 2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW--GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV

Figure 3.12 - Clustered Faults Root Cause Details

8. User can click anywhere on the row to view the **Predicted Fault Details** on the screen.



Predicted Fault Details

PAT NUMBER	11
PARENT NODE	776745184Z
CLUSTER ID	17264.0
EQUIPMENT IDENTIFIER	796698389
EQUIPMENT COMPONENT	796698389___YHX-597375/YXU-645/YGH-8580
CAUSE	2232-YXXS NRHHRMT
ALARM OCCURRENCE COUNT	5.0
ALARM DEDUPLICATED COUNT	4.0
AVG ALARM DURATION	1273.17
WEIGHT INDEX	70.0
Matched Slot	03 Oct 2022 to 09 Oct 2022 - 10 Oct 2022 to 16 Oct 2022 -

TICKET HISTORY	Grxpvg RW: RMX999997922104, Nzrm XR: 898797999, Xivzgrlm Wzgv: 73-90-7977, Hgzgfh: XOLHVW, Kirlirgb: 7-Nvwrfn, Hfnnzib: ZwKD XIJ999995988882 VHTHMSRW8 HD fkwzgv 8.33 / 0 YHX nvowvg 6980 - MVGDLIP HV IERXV VMGRGB FMZEZROZ
LATEST TICKET	RMX999997922104
FAULT TRACE 1	2294-W-XSZMMVO UZROFIV
TOPOLOGY PATHS	
	OfficeCode: 700009442, Equipment: 776745184Z, Cause: Izwrl Ormp 796442445_2444Z (LWF Z) Gvovnvgib Uzro Zozin, Event time: 03-10-2022 04:03:17, Closure time: 03-10-2022 04:56:05 OfficeCode: 700009442, Equipment: 776745184Z, Cause: Izwrl Ormp 796442445_2444Z (LWF Z) Gvovnvgib Uzro Zozin, Event time: 02-10-2022 23:49:51, Closure time: 03-10-2022 00:11:58 OfficeCode: 700009472, Equipment: 796675601Z, Cause: 2343-YZHV HGZGRLM XLMMVXGRERGB OLHG--GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV, Event time: 02-10-2022 23:03:51, Closure time: 02-10-2022 23:04:12 OfficeCode: 700009472, Equipment: 796675601Z, Cause: 2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW--H8 HXGK KZGS UZROFIV, Event time: 02-10-2022 23:03:24, Closure time: 02-10-2022 23:58:04 OfficeCode: 700009466, Equipment: 796668622Z, Cause: 0952-MV6HDH ZTVMG MLG IVHKLMWRMT GL IVJFVHGH, Event time: 02-10-2022 16:47:49, Closure time: 02-10-2022 17:02:20 OfficeCode: 700009466, Equipment: 796668622Z-T, Cause: 0952-MV6HD

15	-	High: 0	Medium: 0	Low: 1	
16	-	High: 0	Medium: 0	Low: 1	

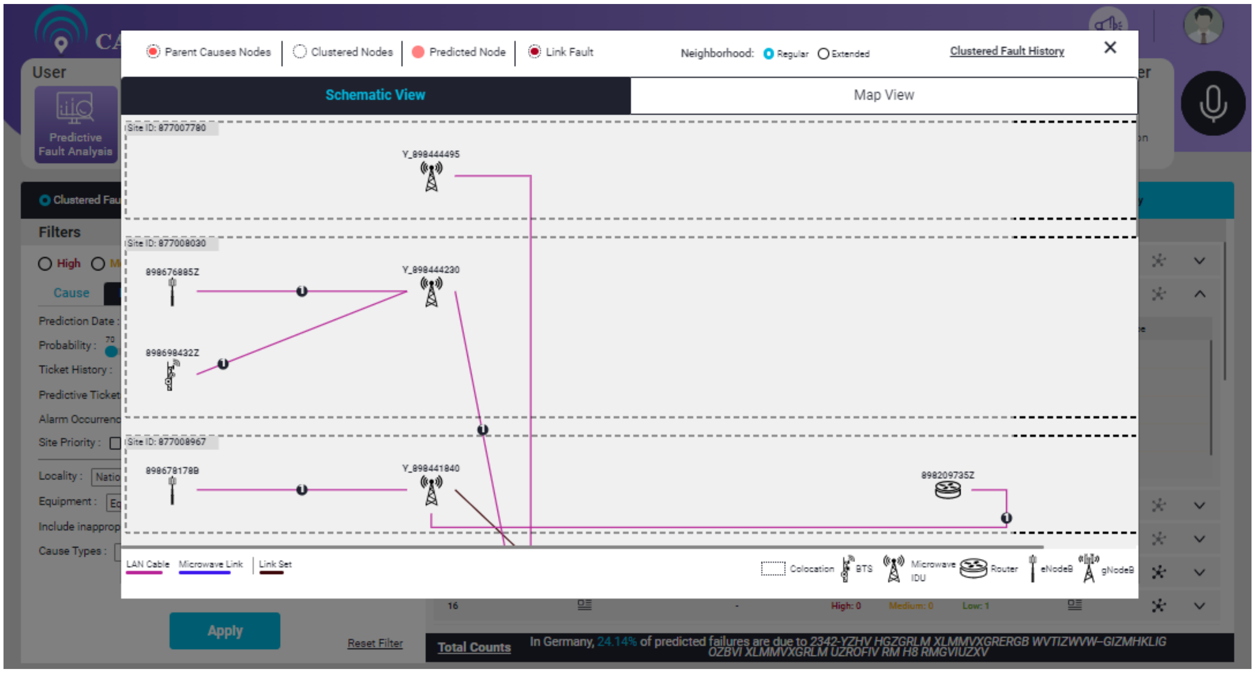
Apply

Reset Filter

Total Counts In Germany, 24.14% of predicted failures are due to *2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW–GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV*

Figure 3.13 - Predicted Fault Details

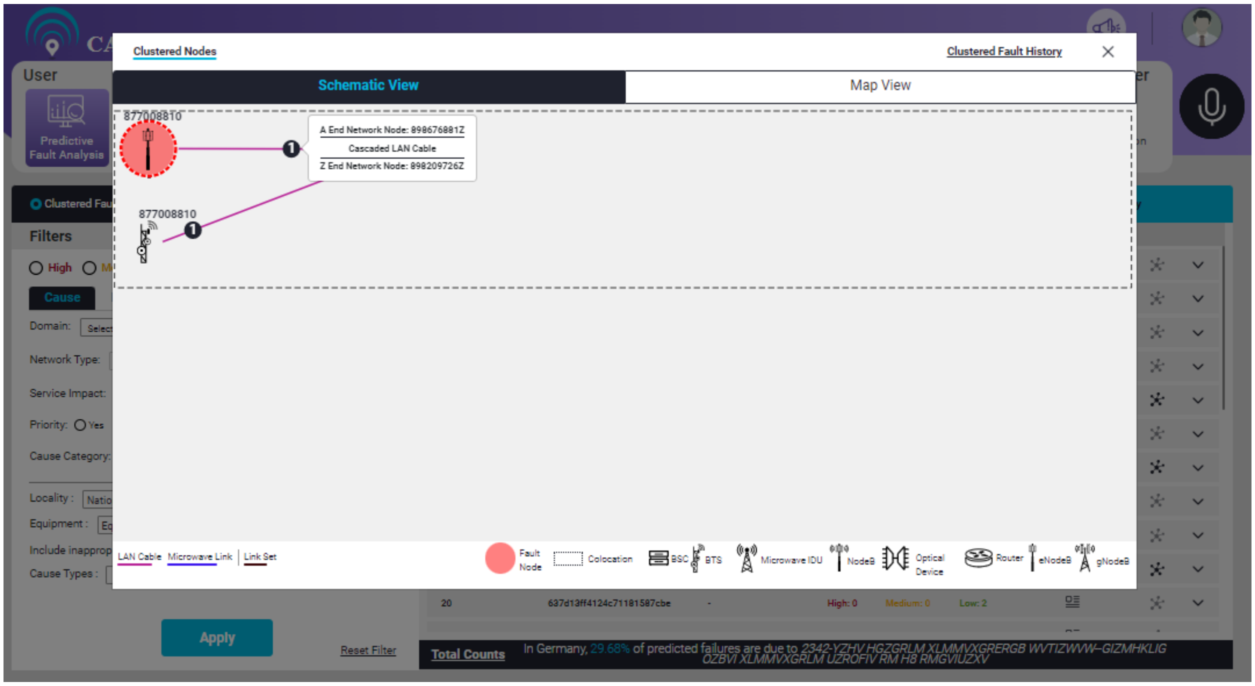
9. Click the **Network Topology View** icon ✱ to view the Schematic View and Map View topology for a particular equipment. The popup lands on **Schematic View**.



In Germany, 24.14% of predicted failures are due to *2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW–GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV*

Figure 3.14 – Clustered Faults Schematic View

10. Blinking nodes represent the Clustered Nodes. Click on a Link Set to view the Active Connection Details with Link Faults and Router to view Node Details.



A End Network Node: 898676881Z

Cascaded LAN Cable

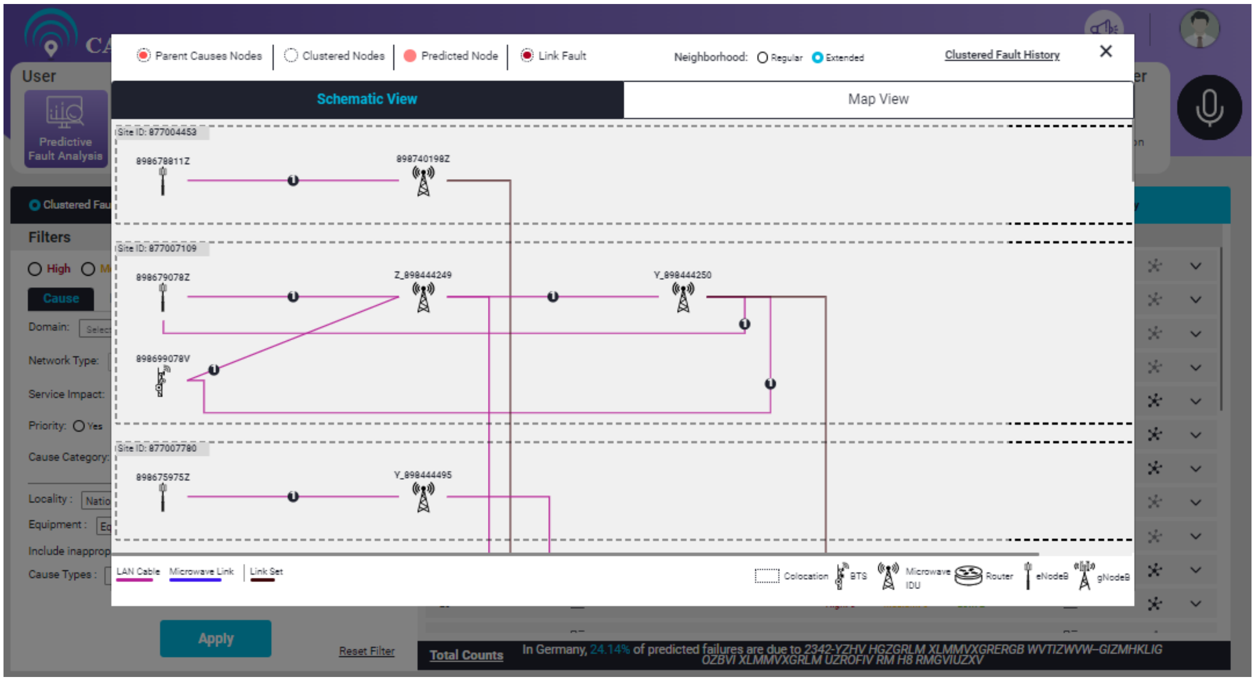
Z End Network Node: 898209726Z

20 637d13ff4124c71181587cbe - High: 0 Medium: 0 Low: 2

In Germany, 29.68% of predicted failures are due to *2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW–GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV*

Figure 3.15 - Schematic View Information

11. The faults as per the group are available in the expansion mode. Network topology view (consisting of Regular and Extended Neighbourhoods) is associated for each group. **Regular** neighbourhood indicates the topological connections available for the predicted node(s). **Extended** neighbourhood indicates the topological connections at office code level.

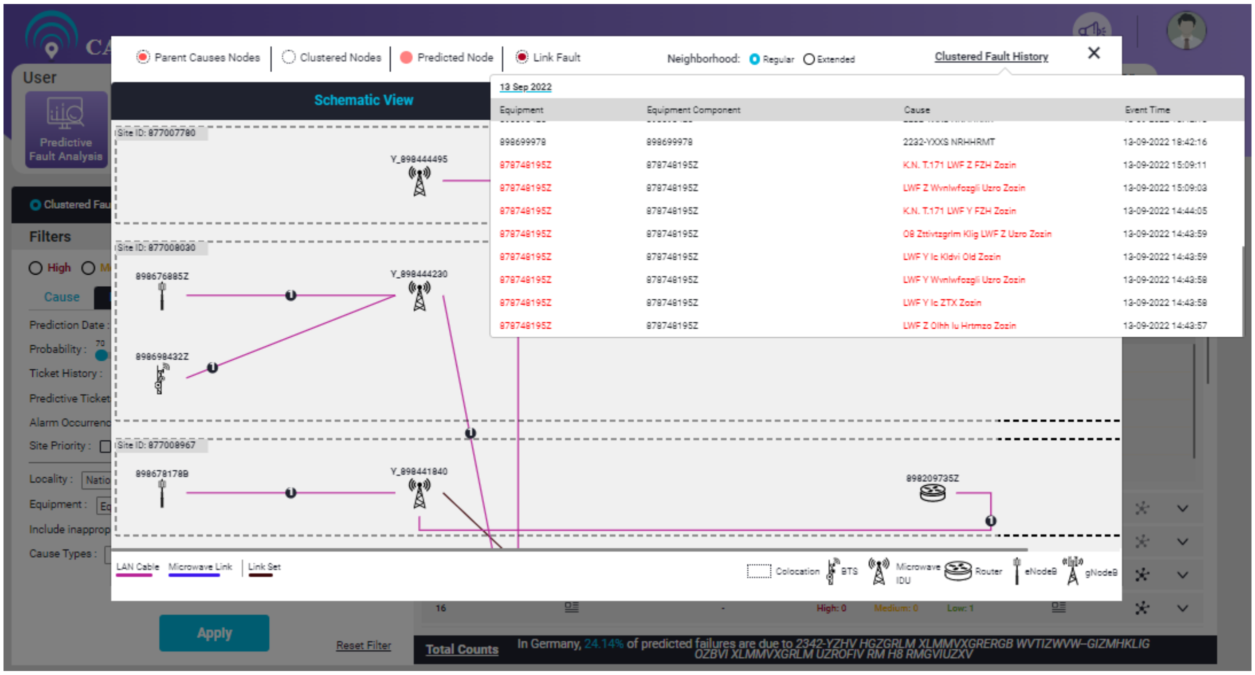


Neighborhood: ○ Regular ● Extended

In Germany, 24.14% of predicted failures are due to 2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW–GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV

Figure 3.16 - Extended Neighborhood

12. User can view the fault history for an equipment-cause by clicking the **Clustered Fault History**. **Parent Cause Nodes** and **Parent Causes** are highlighted in red.



13 Sep 2022

Equipment	Equipment Component	Cause	Event Time
898699978	898699978	2232-YXXS NRHHRMT	13-09-2022 18:42:16
878748195Z	878748195Z	K.N. T.171 LWF Z FZH Zozin	13-09-2022 15:09:11
878748195Z	878748195Z	LWF Z Wvnlwfozgli Uzro Zozin	13-09-2022 15:09:03
878748195Z	878748195Z	K.N. T.171 LWF Y FZH Zozin	13-09-2022 14:44:05
878748195Z	878748195Z	08 Zttivtzgrlm Klig LWF Z Uzro Zozin	13-09-2022 14:43:59
878748195Z	878748195Z	LWF Y Ic Kldvi Old Zozin	13-09-2022 14:43:59
878748195Z	878748195Z	LWF Y Wvnlwfozgli Uzro Zozin	13-09-2022 14:43:58
878748195Z	878748195Z	LWF Y Ic ZTX Zozin	13-09-2022 14:43:58
878748195Z	878748195Z	LWF Z Olhh lu Hrtmzo Zozin	13-09-2022 14:43:57

Figure 3.17 - Clustered Fault History

13. User can also view the equipment topology as a Map View.

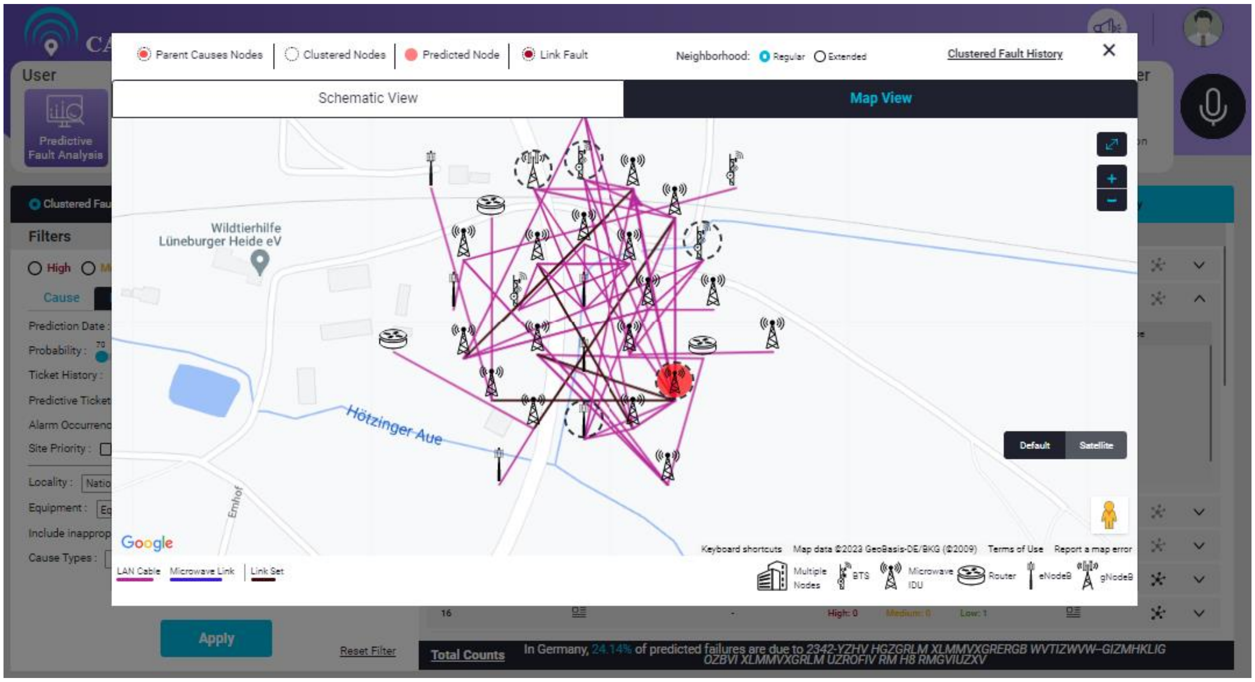
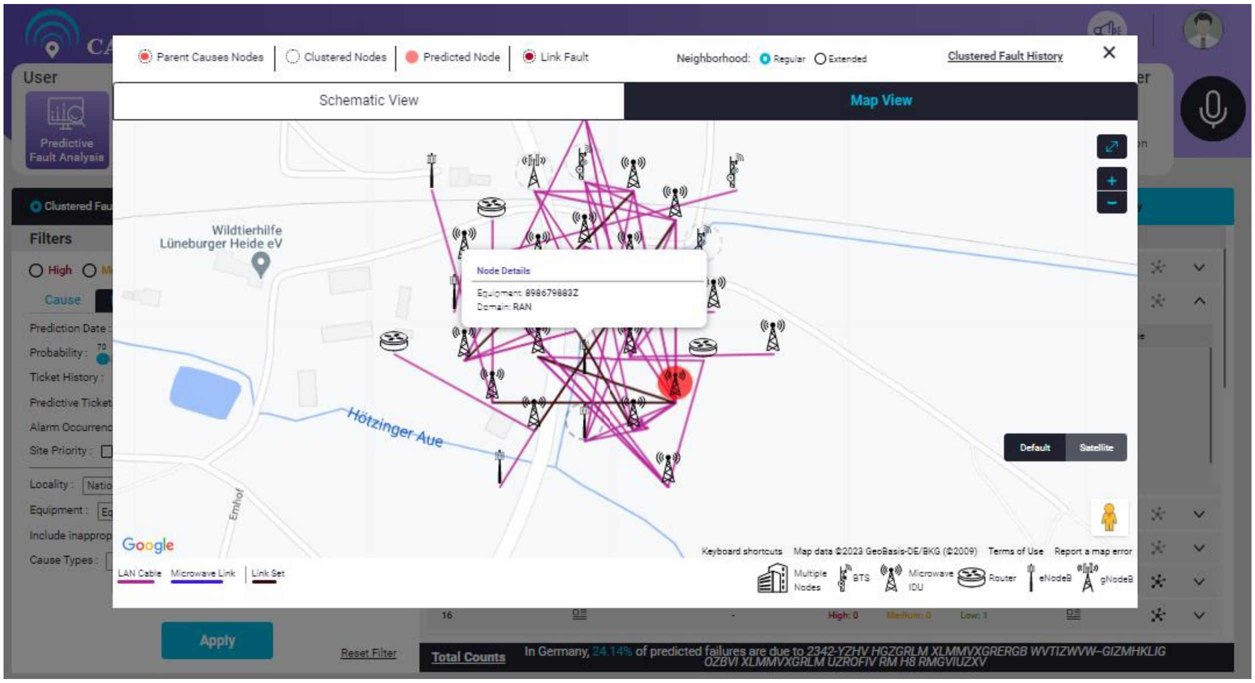


Figure 3.18 – Clustered Faults Map View

14. Click on Multiple Nodes to view the Active Node Information, Link Set to view the Active Connection Details with Link Faults and Router to view Node Details.



Node Details

Equipment: 8986798832

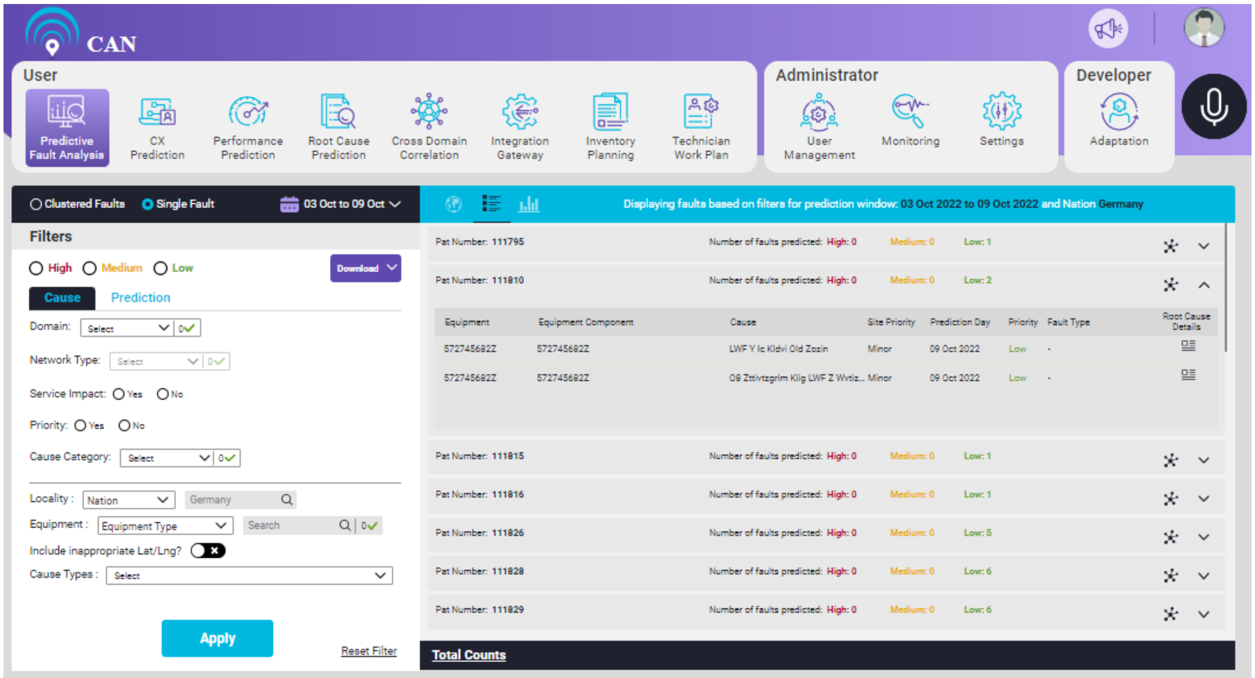
Domain: RAN

Total Counts In Germany, 24.14% of predicted failures are due to 2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW–GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV

Figure 3.19 - Map View Information

Single Fault

- To view the tabular view of individual faults, click the radio button **Single Fault**.
- Click **Apply** to filter individual faults.
- The tabular view for Single Fault has the following attributes:
  - PAT number
  - Priority
- User can click the ⌄ icon to view the Predicted Fault Details on the screen. The Predicted Fault Details tab includes the following fields:
  - Equipment
  - Equipment Component
  - Cause
  - Site Priority
  - Prediction Day
  - Priority
  - Fault Type
  - Root Cause Details



Displaying faults based on filters for prediction window: 03 Oct 2022 to 09 Oct 2022 and Nation Germany

Pat Number: 111795 Number of faults predicted: High: 0 Medium: 0 Low: 1

Pat Number: 111810 Number of faults predicted: High: 0 Medium: 0 Low: 2

Equipment	Equipment Component	Cause	Site Priority	Prediction Day	Priority	Fault Type	Root Cause Details
5727456822	5727456822	LWF Y Ic Kldvi Old Zozin	Minor	09 Oct 2022	Low	-	☰
5727456822	5727456822	08 Zttivtzgrlm Klig LWF Z Wvtiz...	Minor	09 Oct 2022	Low	-	☰

Pat Number: 111815 Number of faults predicted: High: 0 Medium: 0 Low: 1

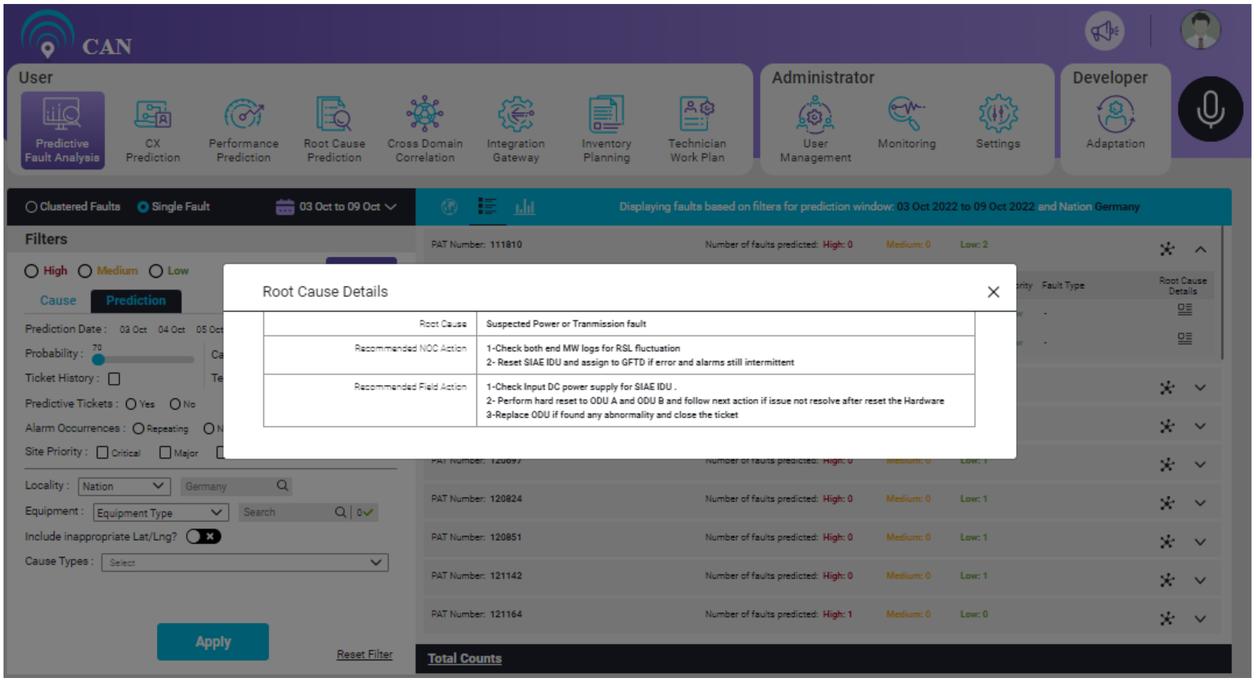
Pat Number: 111816 Number of faults predicted: High: 0 Medium: 0 Low: 1

Pat Number: 111826 Number of faults predicted: High: 0 Medium: 0 Low: 5

Pat Number: 111828 Number of faults predicted: High: 0 Medium: 0 Low: 6

Pat Number: 111829 Number of faults predicted: High: 0 Medium: 0 Low: 6

Figure 3.20 - Single Fault Details



Displaying faults based on filters for prediction window: 03 Oct 2022 to 09 Oct 2022 and Nation Germany

PAT Number: 111810 Number of faults predicted: High: 0 Medium: 0 Low: 2

Root Cause Details

Root Cause	Suspected Power or Tranmission fault
Recommanded NOC Action	1-Check both end MW logs for RSL fluctuation 2- Reset SIAE IDU and assign to GFTD if error and alarms still intermittent
Recommanded Field Action	1-Check Input DC power supply for SIAE IDU . 2- Perform hard reset to ODU A and ODU B and follow next action if issue not resolve after reset the Hardware 3-Replace ODU if found any abnormality and close the ticket

PAT Number: 120697 Number of faults predicted: High: 0 Medium: 0 Low: 1

PAT Number: 120824 Number of faults predicted: High: 0 Medium: 0 Low: 1

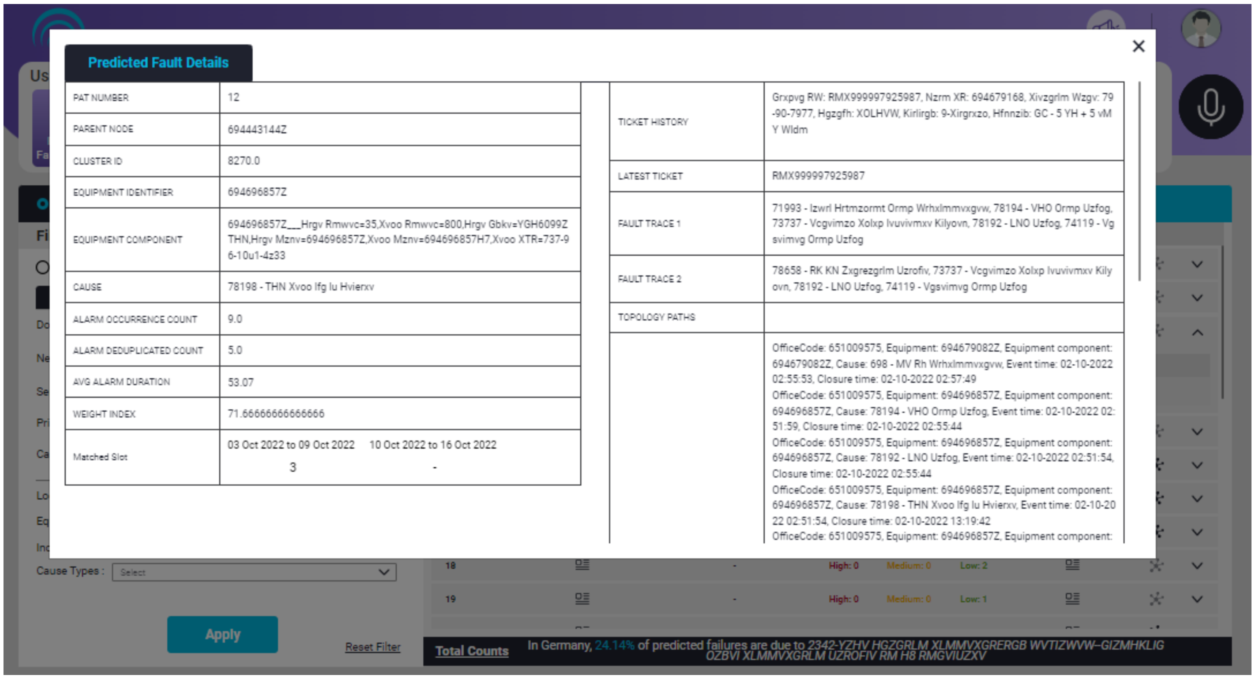
PAT Number: 120851 Number of faults predicted: High: 0 Medium: 0 Low: 1

PAT Number: 121142 Number of faults predicted: High: 0 Medium: 0 Low: 1

PAT Number: 121164 Number of faults predicted: High: 1 Medium: 0 Low: 0

Figure 3.21 – Single Fault Root Cause Details

- User can click anywhere on the row to view the **Predicted Fault Details** on the screen.



Predicted Fault Details

PAT NUMBER	12
PARENT NODE	694443144Z
CLUSTER ID	8270.0
EQUIPMENT IDENTIFIER	694696857Z
EQUIPMENT COMPONENT	694696857Z___Hrgv Rmwvc=35,Xvoo Rmwvc=800,Hrgv Gbkv=YGH6099Z THN,Hrgv Mznv=694696857Z,Xvoo Mznv=694696857H7,Xvoo XTR=737-96-10u1-4z33
CAUSE	78198 - THN Xvoo Ifg lu Hvierxv
ALARM OCCURRENCE COUNT	9.0
ALARM DEDUPLICATED COUNT	5.0
AVG ALARM DURATION	53.07
WEIGHT INDEX	71.66666666666666
Matched Slot	03 Oct 2022 to 09 Oct 2022 10 Oct 2022 to 16 Oct 2022 3 -

TICKET HISTORY	Grxpvg RW: RMX999997925987, Nzrm XR: 694679168, Xivzgrlm Wzgv: 79-90-7977, Hgzgfh: XOLHVW, Kirlirgb: 9-Xirgrxzo, Hfnnzib: GC - 5 YH + 5 vMY Wldm
LATEST TICKET	RMX999997925987
FAULT TRACE 1	71993 - Izwrl Hrtmzormt Ormp Wrhxlmmvxgvw, 78194 - VHO Ormp Uzfog, 73737 - Vcgvimzo Xolxp Ivuvivmxv Kilyovn, 78192 - LNO Uzfog, 74119 - Vgsvimvg Ormp Uzfog
FAULT TRACE 2	78658 - RK KN Zxgrezgrlm Uzrofiv, 73737 - Vcgvimzo Xolxp Ivuvivmxv Kilyovn, 78192 - LNO Uzfog, 74119 - Vgsvimvg Ormp Uzfog
TOPOLOGY PATHS	
	OfficeCode: 651009575, Equipment: 694679082Z, Equipment component: 694679082Z, Cause: 698 - MV Rh Wrhxlmmvxgvw, Event time: 02-10-2022 02:55:53, Closure time: 02-10-2022 02:57:49 OfficeCode: 651009575, Equipment: 694696857Z, Equipment component: 694696857Z, Cause: 78194 - VHO Ormp Uzfog, Event time: 02-10-2022 02:51:59, Closure time: 02-10-2022 02:55:44 OfficeCode: 651009575, Equipment: 694696857Z, Equipment component: 694696857Z, Cause: 78192 - LNO Uzfog, Event time: 02-10-2022 02:51:54, Closure time: 02-10-2022 02:55:44 OfficeCode: 651009575, Equipment: 694696857Z, Equipment component: 694696857Z, Cause: 78198 - THN Xvoo Ifg lu Hvierxv, Event time: 02-10-2022 02:51:54, Closure time: 02-10-2022 13:19:42 OfficeCode: 651009575, Equipment: 694696857Z, Equipment component:

In Germany, 24.14% of predicted failures are due to 2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW–GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV

Figure 3.22 - Predicted Fault Details

- Click the **Network Topology View** icon to view the Schematic View and Map View topology for a particular equipment. The popup lands on **Schematic View**. Dotted line represents the co-located nodes.

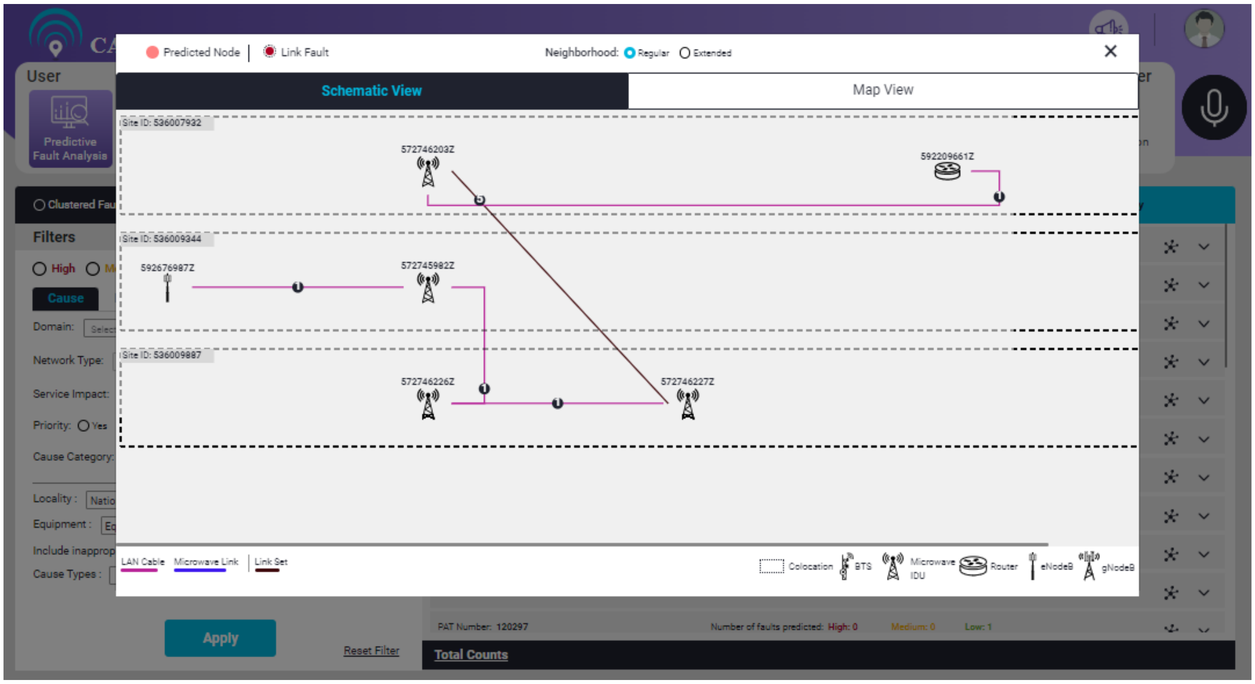
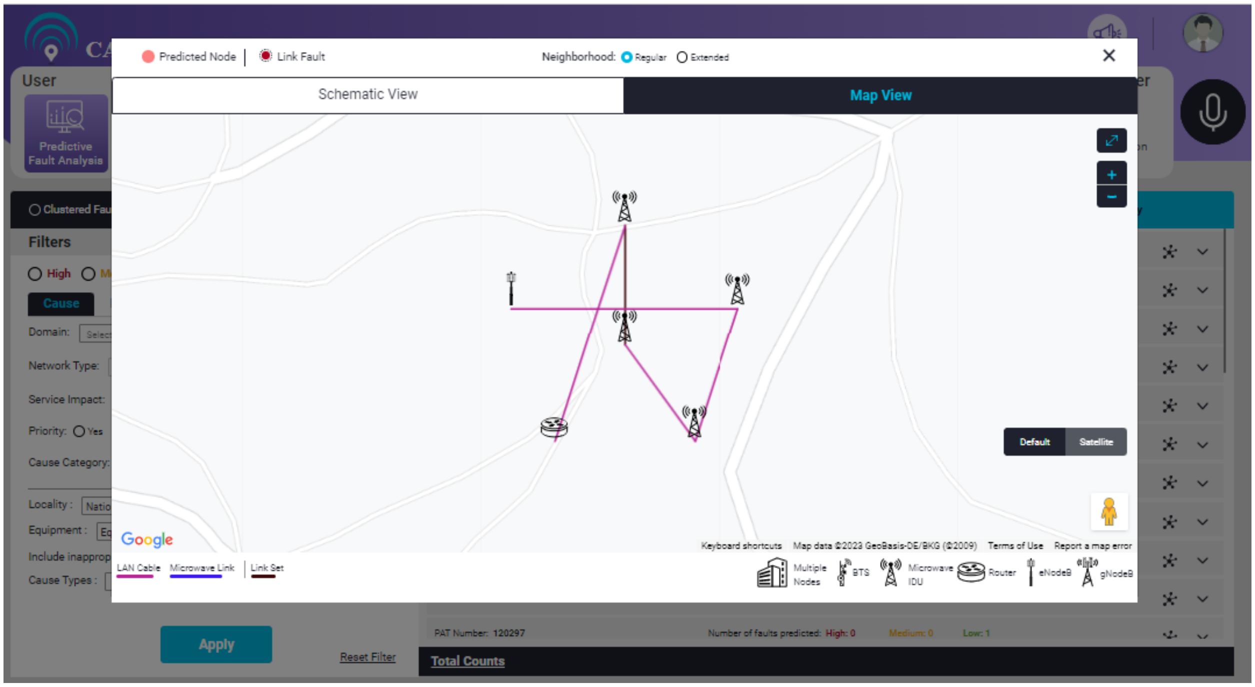


Figure 3.23 - Single Fault Schematic View

- User can also view the equipment topology as a **Map View**.

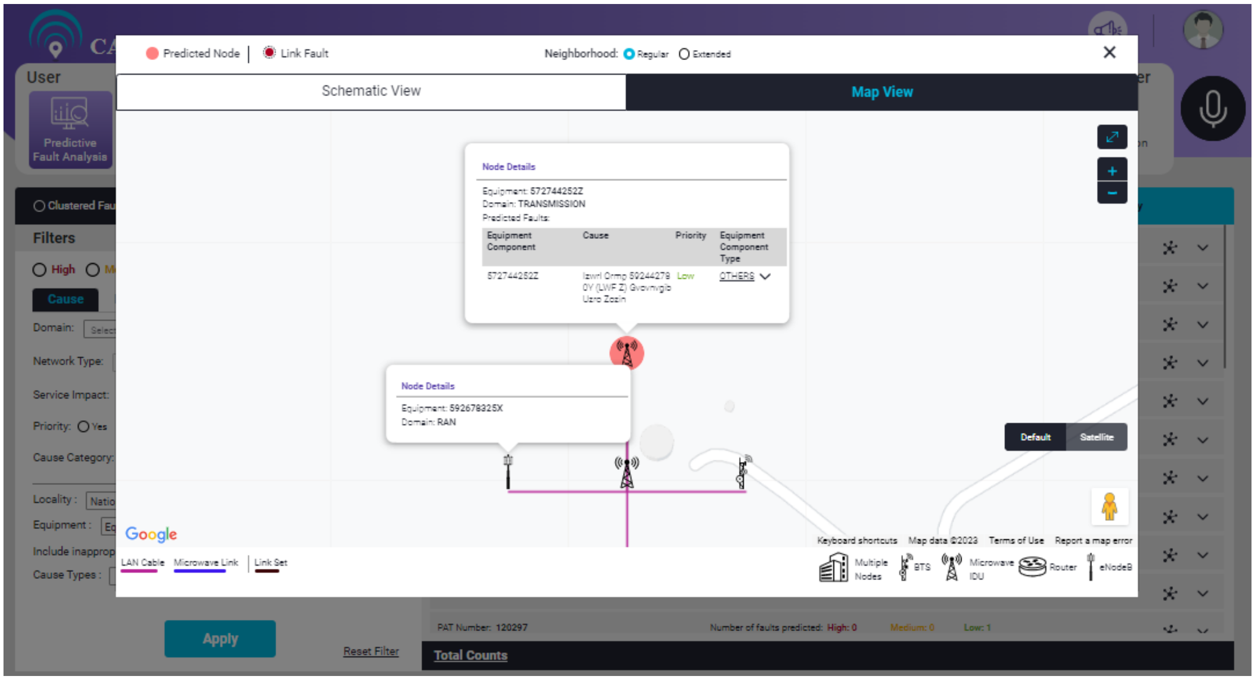


PAT Number: 120297

Number of faults predicted: High: 0 Medium: 0 Low: 1

Figure 3.24 - Single Fault Map View

- Click on Multiple Nodes to view the Active Node Information, Link Set to view the Active Connection Details with Link Faults and Router to view Node Details.



Node Details

Equipment: 572744252Z
Domain: TRANSMISSION
Predicted Faults:

Equipment Component	Cause	Priority	Equipment Component Type
572744252Z	Izwrl Ormp 59244278 0Y (LWF Z) Gvovnvgib Uzro Zozin	Low	OTHERS

Node Details

Equipment: 592678325X
Domain: RAN

PAT Number: 120297

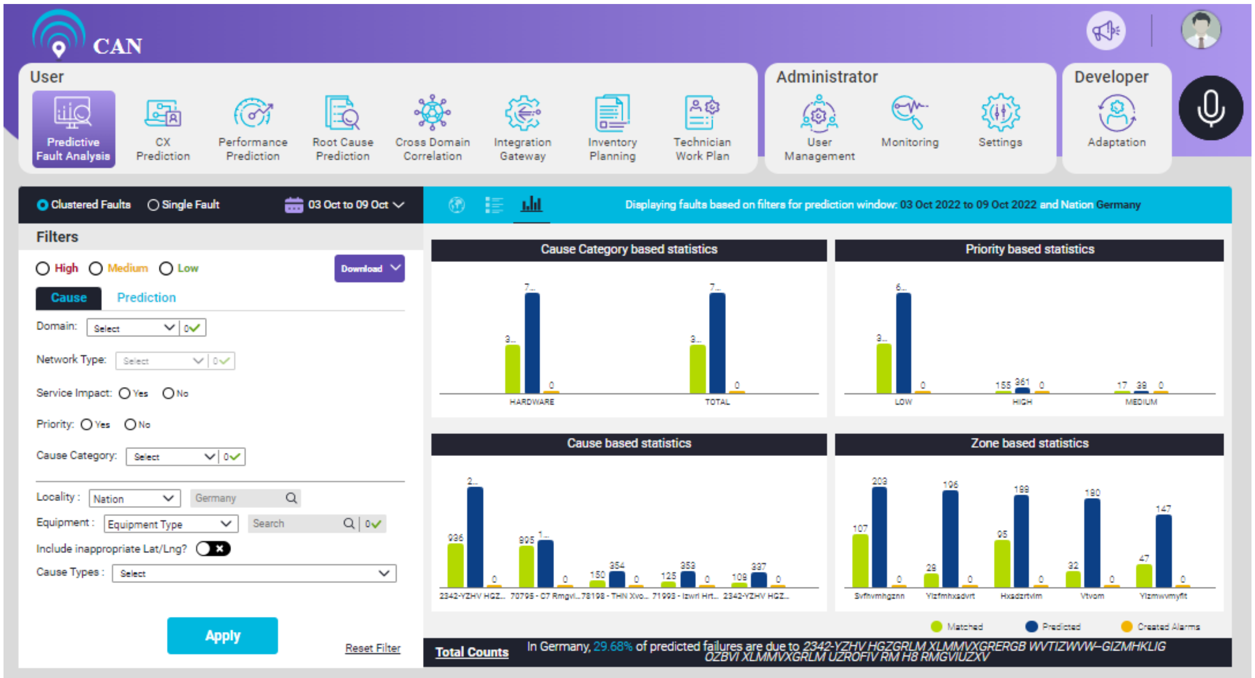
Number of faults predicted: High: 0 Medium: 0 Low: 1

Figure 3.25 - Node Details

Stats View

By default, Stats view is displayed for **Clustered Faults**. To view the graph of individual faults, click **Single Fault** radio button and then click **Apply**.

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**.



Displaying faults based on filters for prediction window: 03 Oct 2022 to 09 Oct 2022 and Nation Germany

In Germany, 29.68% of predicted failures are due to 2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW–GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV

Figure 3.26 - Predictive Failure Analysis (Stats View)

Download Faults Report

User can download four types of fault report:

1. Prediction
2. Daily Report
3. Filtered Report
4. Alarm Matching
5. Consolidated Report
6. Filtered Report
7. Ticket Matching
8. Consolidated Report
9. Inappropriate Lat/Long Report

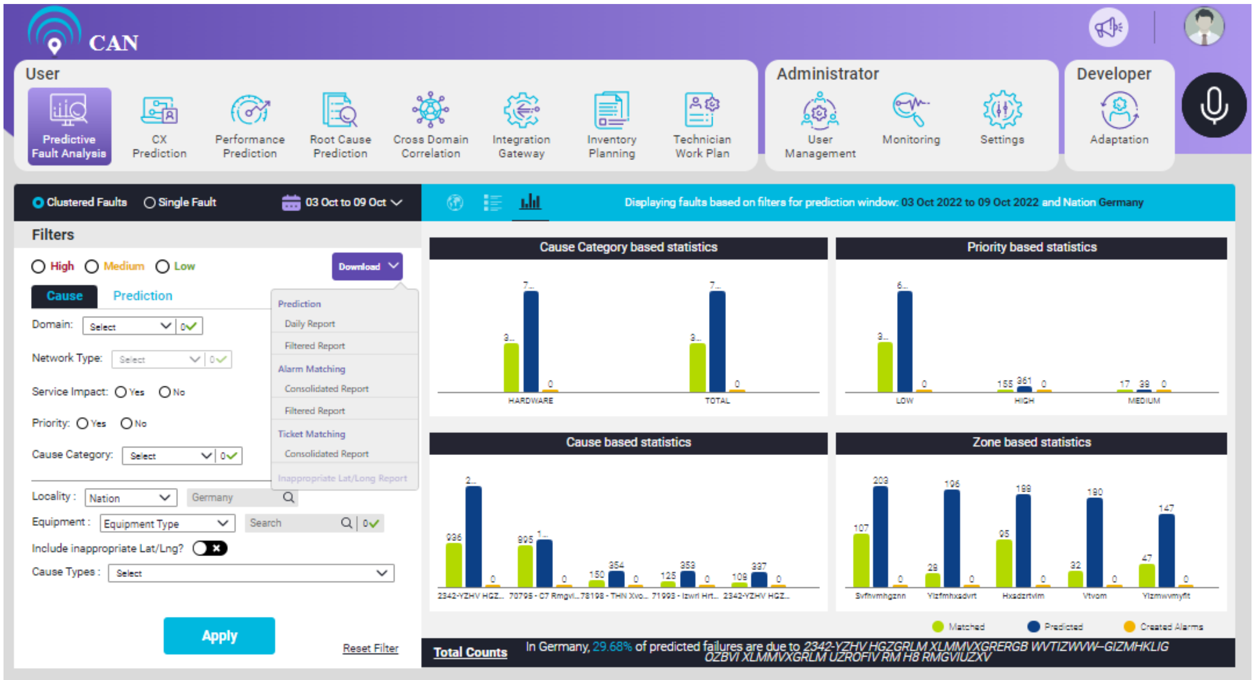
To download the **Prediction Fault Report**, select the option from the **Download Faults** drop down.

Prediction report is of two types: **Daily Report** and **Filtered Report**

Alarm Matching report is of two types: **Consolidated Report** and **Filtered Report**.

Ticket Matching report has only the **Consolidated Report**.

Inappropriate Lat/Long report contains Lat/Long information that are outside the specified locality.



03 Oct to 09 Oct

Displaying faults based on filters for prediction window: 03 Oct 2022 to 09 Oct 2022 and Nation Germany

Domain: Select 0✓

Network Type: Select 0✓

Service Impact: ○ Yes ○ No

Priority: ○ Yes ○ No

Cause Category: Select 0✓

Locality : Nation Germany

Equipment : Equipment Type Search 0✓

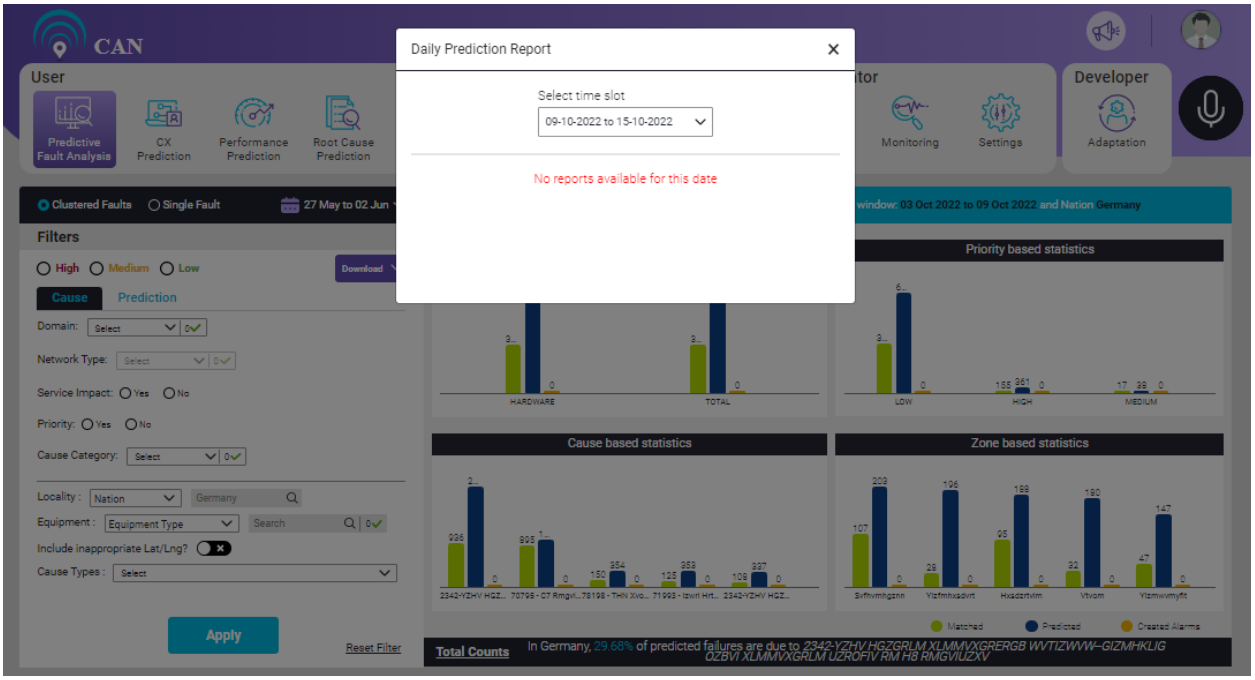
Include inappropriate Lat/Lng? ✗

Cause Types : Select

In Germany, 29.68% of predicted failures are due to 2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW–GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV

Figure 3.27 - Download Report

To view **Daily Report**, choose the period. 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 "**No reports available for this date**".



Daily Prediction Report ✕

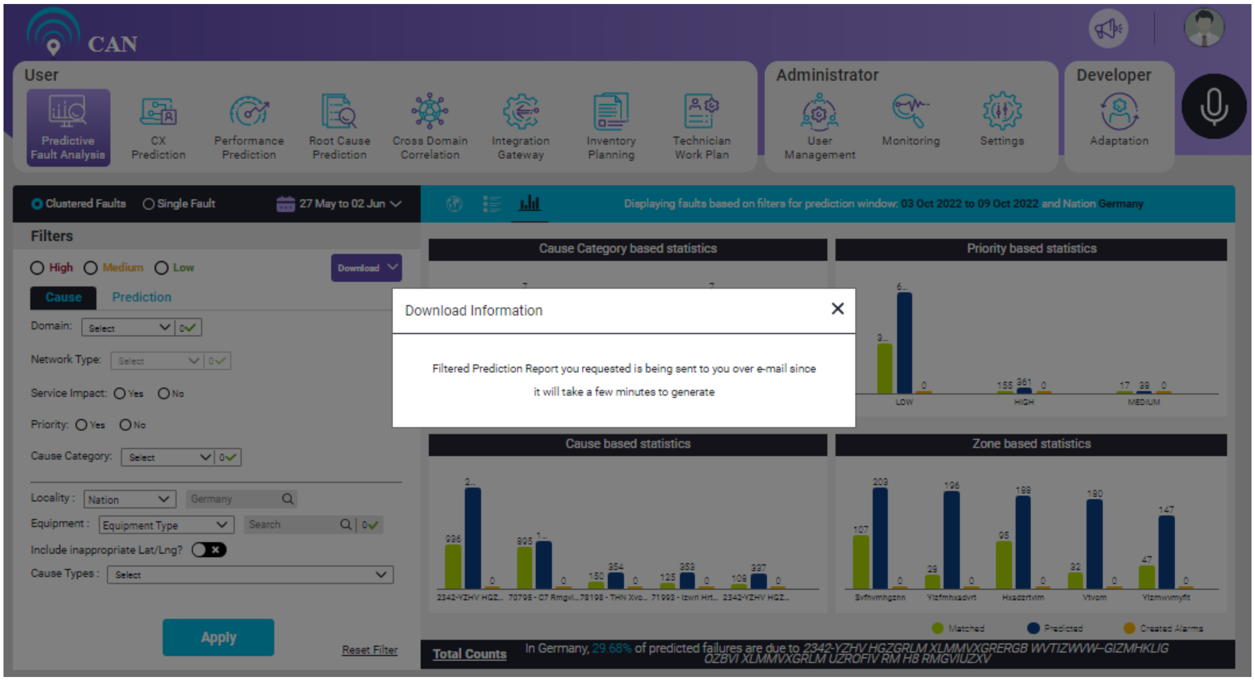
Select time slot

09-10-2022 to 15-10-2022

No reports available for this date

Figure 3.28 - Daily Report

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



Download Information ✕

Filtered Prediction Report you requested is being sent to you over e-mail since it will take a few minutes to generate

Figure 3.29 - Filtered Report

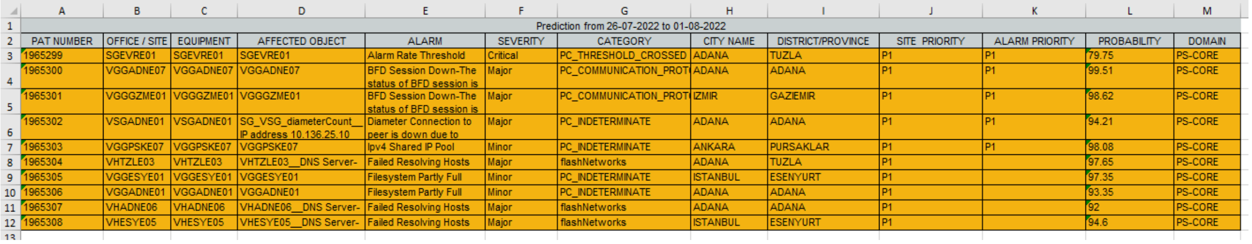
User can download the **Matching Report** for the selected predicted week.

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.

Inappropriate Lat/Long is not displayed on UI. Only a report is generated for the Inappropriate Lat/Long for validation.

See the below figure for sample prediction report.



Prediction from 26-07-2022 to 01-08-2022

PAT NUMBER	OFFICE / SITE	EQUIPMENT	AFFECTED OBJECT	ALARM	SEVERITY	CATEGORY	CITY NAME	DISTRICT/PROVINCE	SITE PRIORITY	ALARM PRIORITY	PROBABILITY	DOMAIN
1965299	SGEVRE01	SGEVRE01	SGEVRE01	Alarm Rate Threshold	Critical	PC_THRESHOLD_CROSSED	ADANA	TUZLA	P1	P1	79.75	PS-CORE
1965300	VGGADNE07	VGGADNE07	VGGADNE07	BFD Session Down-The status of BFD session is	Major	PC_COMMUNICATION_PROT	ADANA	ADANA	P1	P1	99.51	PS-CORE
1965301	VGGGZME01	VGGGZME01	VGGGZME01	BFD Session Down-The status of BFD session is	Major	PC_COMMUNICATION_PROT	IZMIR	GAZIEMIR	P1	P1	98.62	PS-CORE
1965302	VSGADNE01	VSGADNE01	SG_VSG_diameterCount__ IP address 10.136.25.10	Diameter Connection to peer is down due to	Major	PC_INDETERMINATE	ADANA	ADANA	P1	P1	94.21	PS-CORE
1965303	VGGPSKE07	VGGPSKE07	VGGPSKE07	Ipv4 Shared IP Pool	Minor	PC_INDETERMINATE	ANKARA	PURSAKLAR	P1	P1	98.08	PS-CORE
1965304	VHTZLE03	VHTZLE03	VHTZLE03__DNS Server-	Failed Resolving Hosts	Major	flashNetworks	ADANA	TUZLA	P1		97.65	PS-CORE
1965305	VGGESYE01	VGGESYE01	VGGESYE01	Filesystem Partly Full	Minor	PC_INDETERMINATE	ISTANBUL	ESENYURT	P1		97.35	PS-CORE
1965306	VGGADNE01	VGGADNE01	VGGADNE01	Filesystem Partly Full	Minor	PC_INDETERMINATE	ADANA	ADANA	P1		93.35	PS-CORE
1965307	VHADNE06	VHADNE06	VHADNE06__DNS Server-	Failed Resolving Hosts	Major	flashNetworks	ADANA	ADANA	P1		92	PS-CORE
1965308	VHESYE05	VHESYE05	VHESYE05__DNS Server-	Failed Resolving Hosts	Major	flashNetworks	ISTANBUL	ESENYURT	P1		94.6	PS-CORE

Figure 3.30 - Downloaded Report

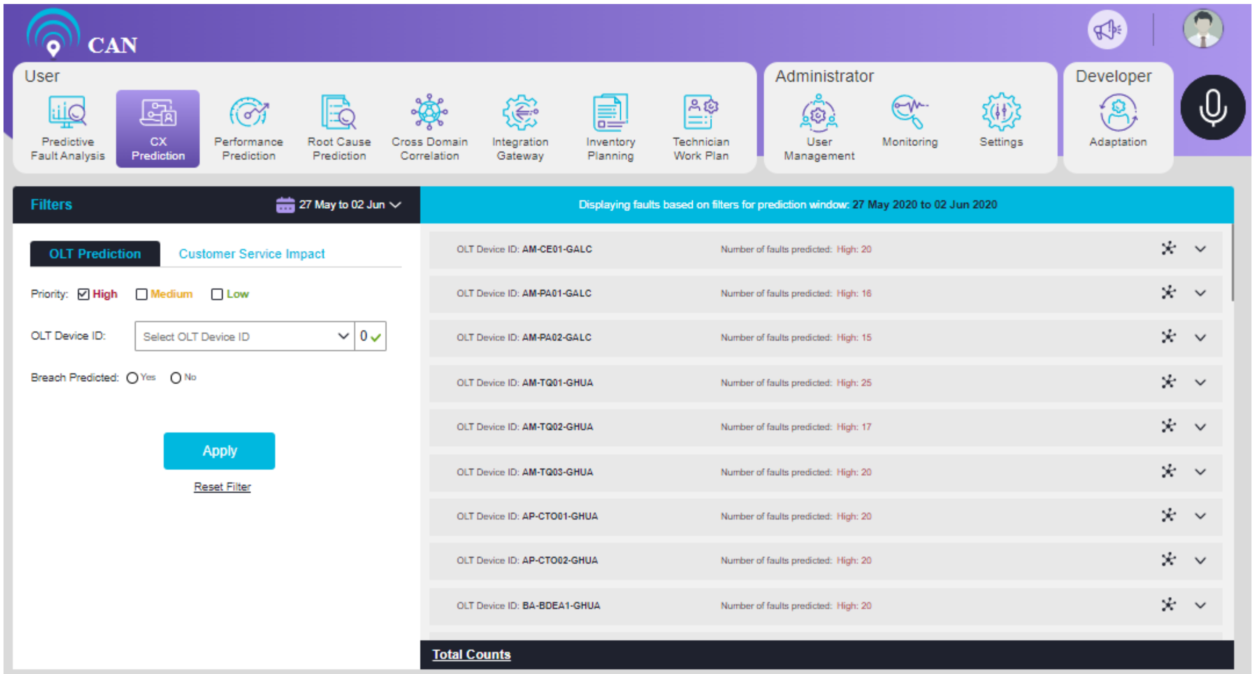
Page Intentionally Left Blank

4. CX PREDICTION

CX Prediction screen display faults based on filters for a prediction window. By default, CX Prediction screen display faults related to the latest prediction window in the tabular form.

CX Prediction allow users to view number of predicted faults based on priority for a particular OLT Device ID.

By default, the screen displays the result for a latest fault window for the selected week (High priority).



Displaying faults based on filters for prediction window: 27 May 2020 to 02 Jun 2020

Priority: ☑ High □ Medium □ Low

OLT Device ID: Select OLT Device ID 0 ✓

Breach Predicted: ○ Yes ○ No

OLT Device ID: AM-CE01-GALC Number of faults predicted: High: 20

OLT Device ID: AM-PA01-GALC Number of faults predicted: High: 16

OLT Device ID: AM-PA02-GALC Number of faults predicted: High: 15

OLT Device ID: AM-TQ01-GHUA Number of faults predicted: High: 25

OLT Device ID: AM-TQ02-GHUA Number of faults predicted: High: 17

OLT Device ID: AM-TQ03-GHUA Number of faults predicted: High: 20

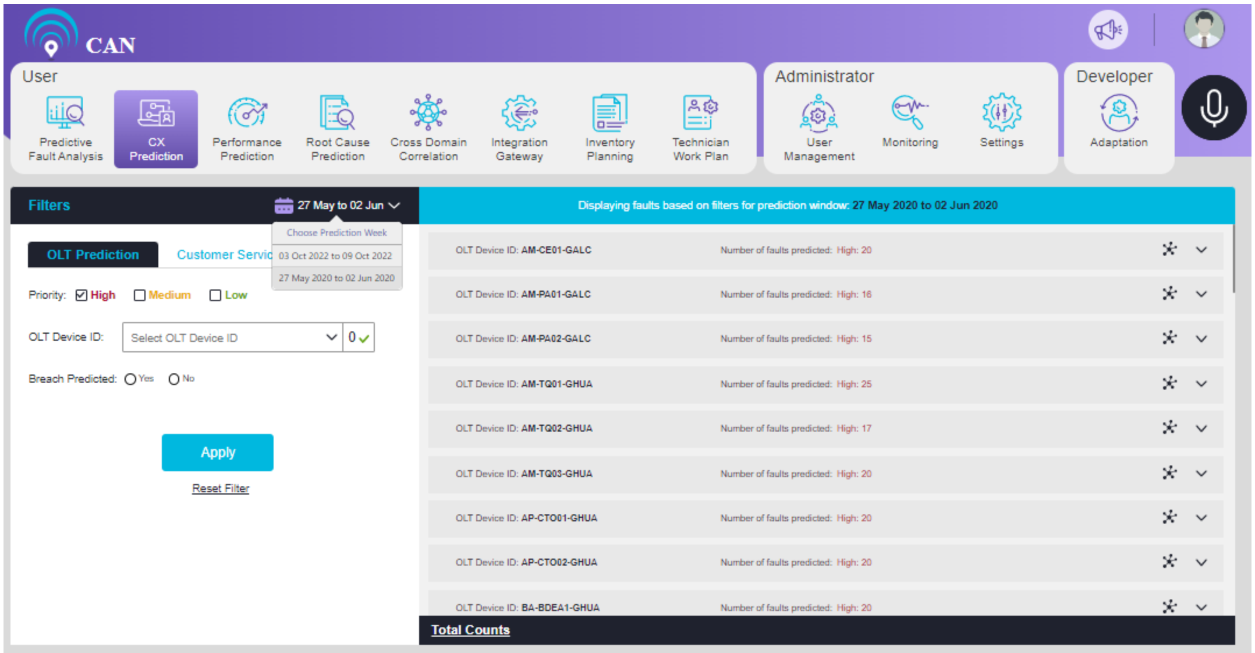
OLT Device ID: AP-CTO01-GHUA Number of faults predicted: High: 20

OLT Device ID: AP-CTO02-GHUA Number of faults predicted: High: 20

OLT Device ID: BA-BDEA1-GHUA Number of faults predicted: High: 20

Figure 4.1 - CX Prediction Screen

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



Displaying faults based on filters for prediction window: 27 May 2020 to 02 Jun 2020

Priority: ☑ High ☐ Medium ☐ Low

OLT Device ID: Select OLT Device ID | 0 ✓

Breach Predicted: ○ Yes ○ No

OLT Device ID: AM-CE01-GALC Number of faults predicted: High: 20

OLT Device ID: AM-PA01-GALC Number of faults predicted: High: 16

OLT Device ID: AM-PA02-GALC Number of faults predicted: High: 15

OLT Device ID: AM-TQ01-GHUA Number of faults predicted: High: 25

OLT Device ID: AM-TQ02-GHUA Number of faults predicted: High: 17

OLT Device ID: AM-TQ03-GHUA Number of faults predicted: High: 20

OLT Device ID: AP-CTO01-GHUA Number of faults predicted: High: 20

OLT Device ID: AP-CTO02-GHUA Number of faults predicted: High: 20

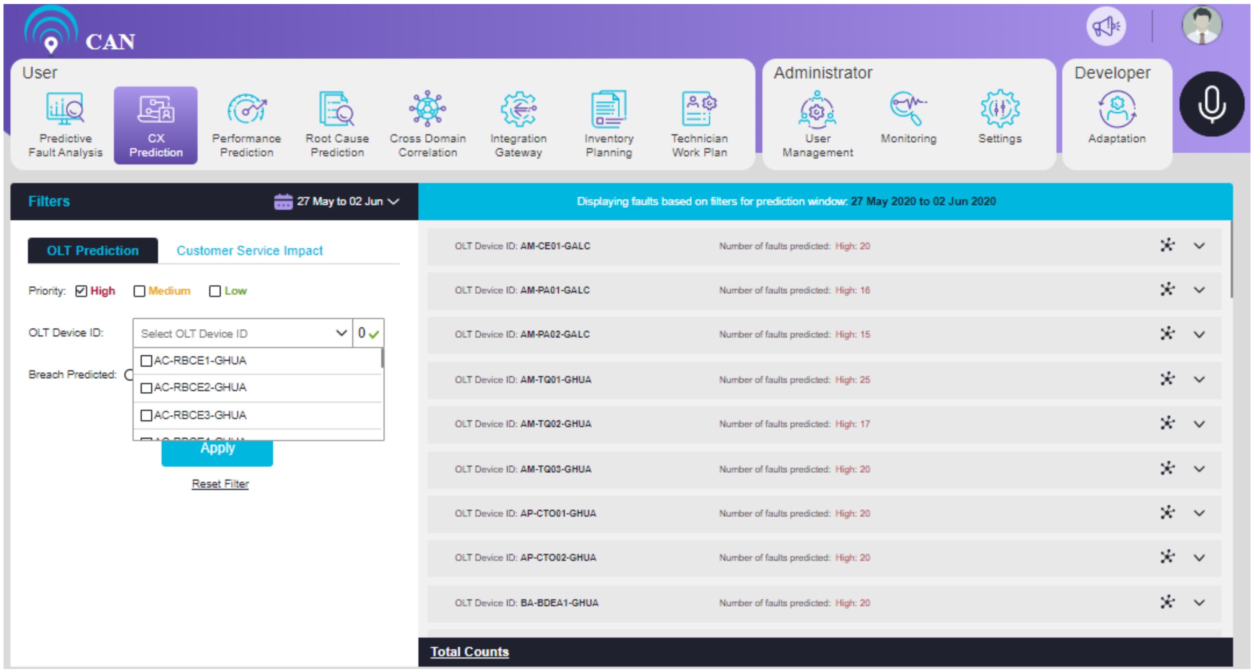
OLT Device ID: BA-BDEA1-GHUA Number of faults predicted: High: 20

Figure 4.2 - Week Selection

The filters have two tabs: **OLT Prediction** and **Customer Service Impact**.

By default, **OLT Prediction** tab is selected. **OLT Prediction** tab is designed for advanced filtering the faults based on various attributes that include:

1. **OLT Device ID**: There are many device IDs. User can select any or all of the IDs.



Displaying faults based on filters for prediction window: 27 May 2020 to 02 Jun 2020

Priority: ☑ High ☐ Medium ☐ Low

OLT Device ID: Select OLT Device ID | 0 ✓

☐ AC-RBCE1-GHUA

☐ AC-RBCE2-GHUA

☐ AC-RBCE3-GHUA

Breach Predicted:

OLT Device ID: AM-CE01-GALC Number of faults predicted: High: 20

OLT Device ID: AM-PA01-GALC Number of faults predicted: High: 16

OLT Device ID: AM-PA02-GALC Number of faults predicted: High: 15

OLT Device ID: AM-TQ01-GHUA Number of faults predicted: High: 25

OLT Device ID: AM-TQ02-GHUA Number of faults predicted: High: 17

OLT Device ID: AM-TQ03-GHUA Number of faults predicted: High: 20

OLT Device ID: AP-CTO01-GHUA Number of faults predicted: High: 20

OLT Device ID: AP-CTO02-GHUA Number of faults predicted: High: 20

OLT Device ID: BA-BDEA1-GHUA Number of faults predicted: High: 20

Figure 4.3 - OLT Device ID Dropdown

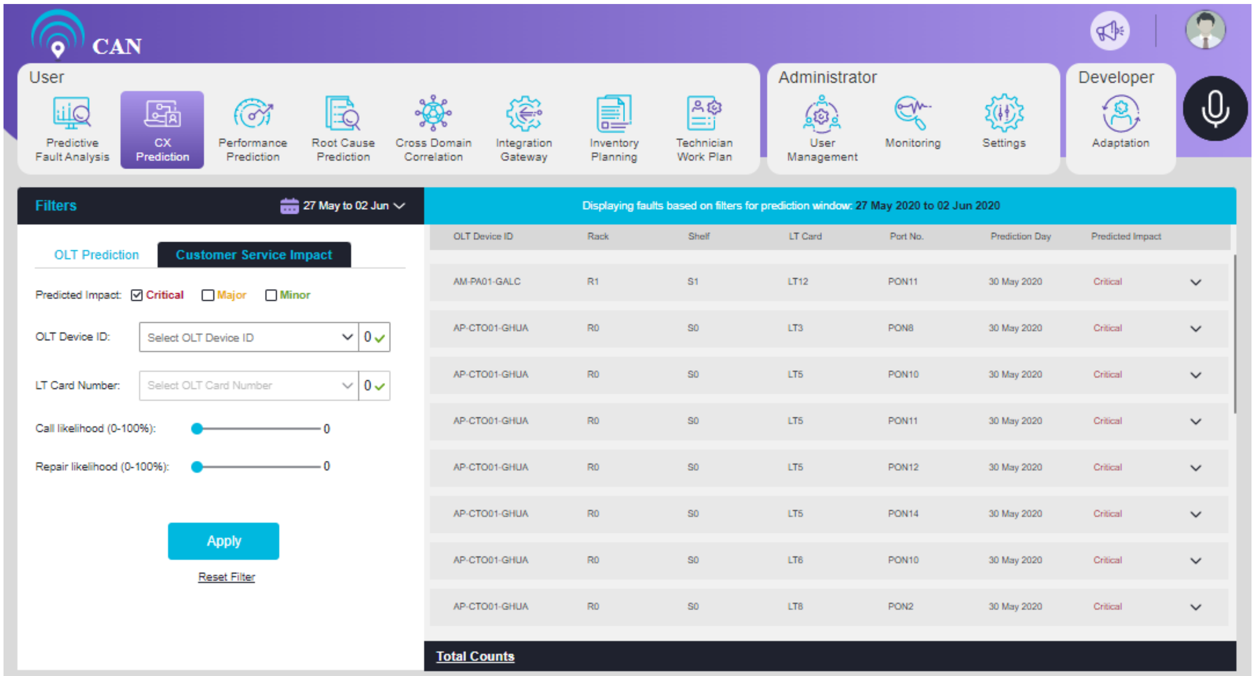
2. **Breach Predicted**: It has two radio buttons: Yes and No.

3. **Priority**: There are three priority check boxes:
4. High (written in red color)
5. Medium (written in yellow color)
6. Low (written in green color)

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

User can select the appropriate attributes as per the requirement.

In the **Customer Service Impact** tab, user can select the required filters. **Customer Service Impact** tab has the following attributes:



Predicted Impact: ☑ Critical ☐ Major ☐ Minor

OLT Device ID: Select OLT Device ID 0 ✓

LT Card Number: Select OLT Card Number 0 ✓

Call likelihood (0-100%): 0

Repair likelihood (0-100%): 0

Displaying faults based on filters for prediction window: 27 May 2020 to 02 Jun 2020

OLT Device ID	Rack	Shelf	LT Card	Port No.	Prediction Day	Predicted Impact
AM-PA01-GALC	R1	S1	LT12	PON11	30 May 2020	Critical
AP-CTO01-GHUA	R0	S0	LT3	PON8	30 May 2020	Critical
AP-CTO01-GHUA	R0	S0	LT5	PON10	30 May 2020	Critical
AP-CTO01-GHUA	R0	S0	LT5	PON11	30 May 2020	Critical
AP-CTO01-GHUA	R0	S0	LT5	PON12	30 May 2020	Critical
AP-CTO01-GHUA	R0	S0	LT5	PON14	30 May 2020	Critical
AP-CTO01-GHUA	R0	S0	LT6	PON10	30 May 2020	Critical
AP-CTO01-GHUA	R0	S0	LT8	PON2	30 May 2020	Critical

Figure 4.4 - Customer Service Impact Tab

1. **Predicted Impact**: It has three checkboxes. **Critical** (written in red color), **Major** (written in yellow color) and **Minor** (written in green color).
2. **OLT Device ID**: User can select the device ID from the drop down.
3. **LT Card Number**: User can select the OLT card number from the drop down.
4. **Call likelihood (0-100%)**: User can set the call probability percentage using the slide bar.
5. **Repair likelihood (0-100%)**: User can set the repair probability percentage using the slide bar.

To see the Predicted Faults:

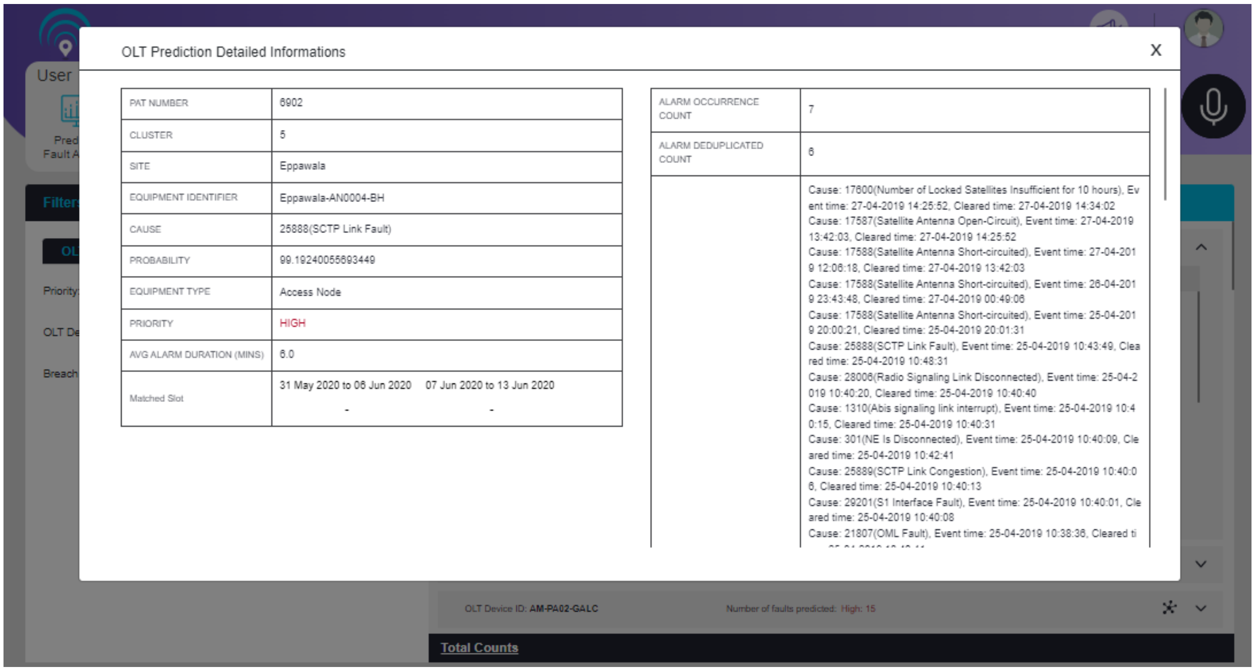
1. Select the appropriate filters as per the requirement.
2. Click the **Apply** button to see the results.

OLT Prediction has two representations:

- Tabular View
- Network View

Tabular View

1. By default, OLT Prediction screen displays the tabular view.
2. To view the **first level** of predicted fault details, click anywhere on the particular row.
3. First level has the following attributes:
   - Rack
   - Shelf
   - LT Card
   - Port No.
   - Priority
   - Cause
   - Prediction Day
   - Prediction Details



OLT Prediction Detailed Informations

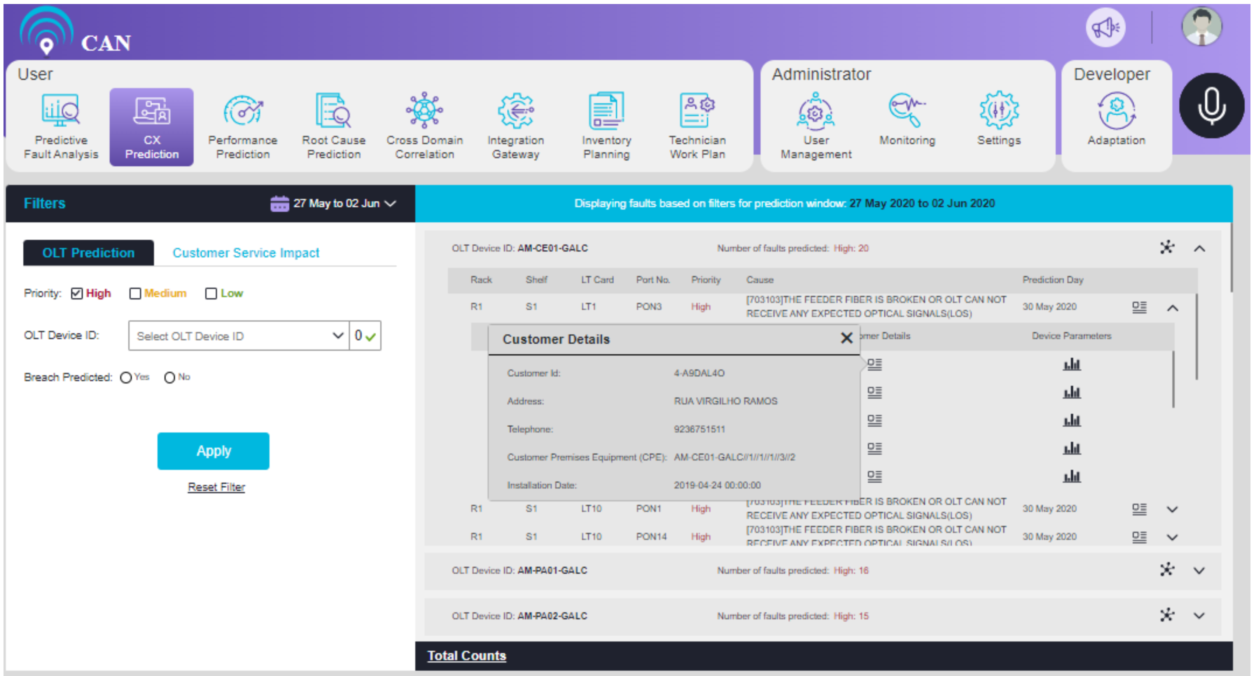
PAT NUMBER	6902
CLUSTER	5
SITE	Eppawala
EQUIPMENT IDENTIFIER	Eppawala-AN0004-BH
CAUSE	25888(SCTP Link Fault)
PROBABILITY	99.19240055693449
EQUIPMENT TYPE	Access Node
PRIORITY	HIGH
AVG ALARM DURATION (MINS)	6.0
Matched Slot	31 May 2020 to 06 Jun 2020 - 07 Jun 2020 to 13 Jun 2020 -

ALARM OCCURRENCE COUNT	7
ALARM DEDUPLICATED COUNT	6
	Cause: 17600(Number of Locked Satellites Insufficient for 10 hours), Event time: 27-04-2019 14:25:52, Cleared time: 27-04-2019 14:34:02 Cause: 17587(Satellite Antenna Open-Circuit), Event time: 27-04-2019 13:42:03, Cleared time: 27-04-2019 14:25:52 Cause: 17588(Satellite Antenna Short-circuited), Event time: 27-04-2019 12:06:18, Cleared time: 27-04-2019 13:42:03 Cause: 17588(Satellite Antenna Short-circuited), Event time: 26-04-2019 23:43:48, Cleared time: 27-04-2019 00:49:06 Cause: 17588(Satellite Antenna Short-circuited), Event time: 25-04-2019 20:00:21, Cleared time: 25-04-2019 20:01:31 Cause: 25888(SCTP Link Fault), Event time: 25-04-2019 10:43:49, Cleared time: 25-04-2019 10:48:31 Cause: 28006(Radio Signaling Link Disconnected), Event time: 25-04-2019 10:40:20, Cleared time: 25-04-2019 10:40:40 Cause: 1310(Abis signaling link interrupt), Event time: 25-04-2019 10:40:15, Cleared time: 25-04-2019 10:40:31 Cause: 301(NE Is Disconnected), Event time: 25-04-2019 10:40:09, Cleared time: 25-04-2019 10:42:41 Cause: 25889(SCTP Link Congestion), Event time: 25-04-2019 10:40:06, Cleared time: 25-04-2019 10:40:13 Cause: 29201(S1 Interface Fault), Event time: 25-04-2019 10:40:01, Cleared time: 25-04-2019 10:40:08 Cause: 21807(OML Fault), Event time: 25-04-2019 10:38:36, Cleared ti

X
User
Pred
Fault A
Filters
OL
Priority
OLT De
Breach
OLT Device ID: AM-PA02-GALC
Number of faults predicted: High: 15
Total Counts

Figure 4.5 - OLT Prediction Detailed Information

4. To view the **second level** of predicted fault details, click anywhere on the first level.
5. Second level has the following attributes:
   - ONU ID
   - Breach Predicted
   - Customer Details



27 May to 02 Jun

Displaying faults based on filters for prediction window: **27 May 2020 to 02 Jun 2020**

Priority: ☑ High □ Medium □ Low

OLT Device ID: Select OLT Device ID 0 ✓

Breach Predicted: ○ Yes ○ No

OLT Device ID: **AM-CE01-GALC** Number of faults predicted: High: 20

Rack	Shelf	LT Card	Port No.	Priority	Cause	Prediction Day
R1	S1	LT1	PON3	High	[703103]THE FEEDER FIBER IS BROKEN OR OLT CAN NOT RECEIVE ANY EXPECTED OPTICAL SIGNALS(LOS)	30 May 2020
R1	S1	LT10	PON1	High	[703103]THE FEEDER FIBER IS BROKEN OR OLT CAN NOT RECEIVE ANY EXPECTED OPTICAL SIGNALS(LOS)	30 May 2020
R1	S1	LT10	PON14	High	[703103]THE FEEDER FIBER IS BROKEN OR OLT CAN NOT RECEIVE ANY EXPECTED OPTICAL SIGNALS(LOS)	30 May 2020

Customer Details

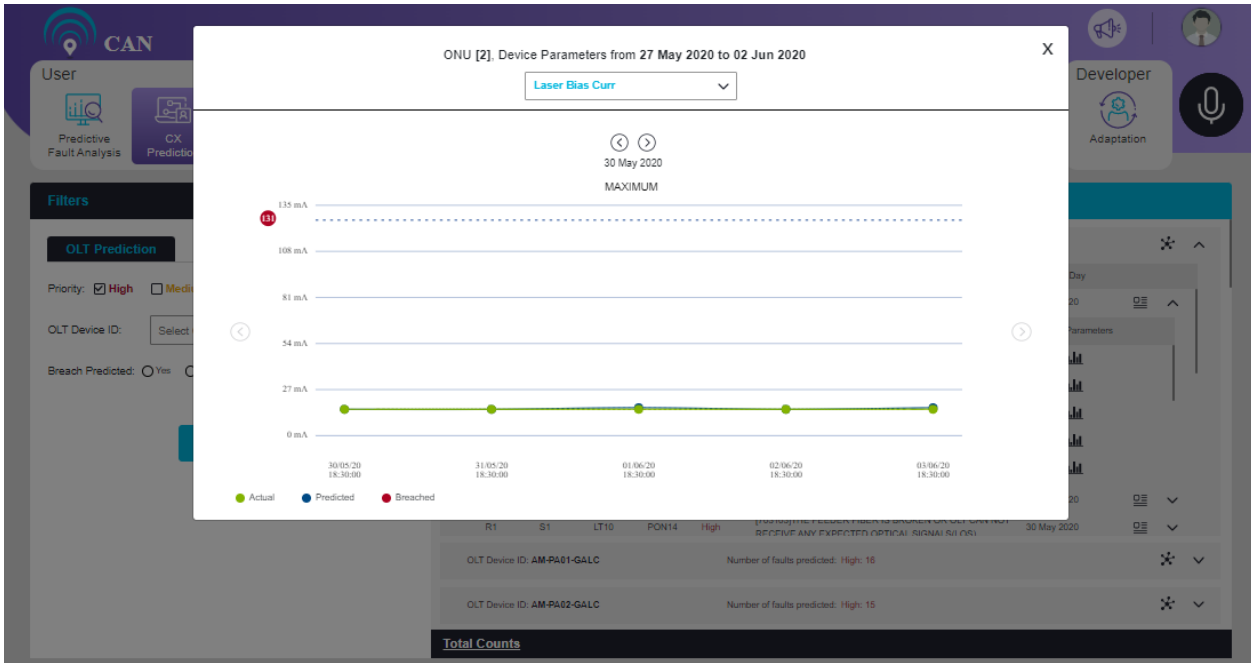
Customer Id:	4-A9DAL4O
Address:	RUA VIRGILHO RAMOS
Telephone:	9236751511
Customer Premises Equipment (CPE):	AM-CE01-GALC//1//1//1//3//2
Installation Date:	2019-04-24 00:00:00

OLT Device ID: **AM-PA01-GALC** Number of faults predicted: High: 16

OLT Device ID: **AM-PA02-GALC** Number of faults predicted: High: 15

Figure 4.6 - Customer Details

- Device Parameters ılıl



ONU [2], Device Parameters from **27 May 2020 to 02 Jun 2020**

Laser Bias Curr

Figure 4.7 - Device Parameters

6. To select Network view, click the network icon ✲.

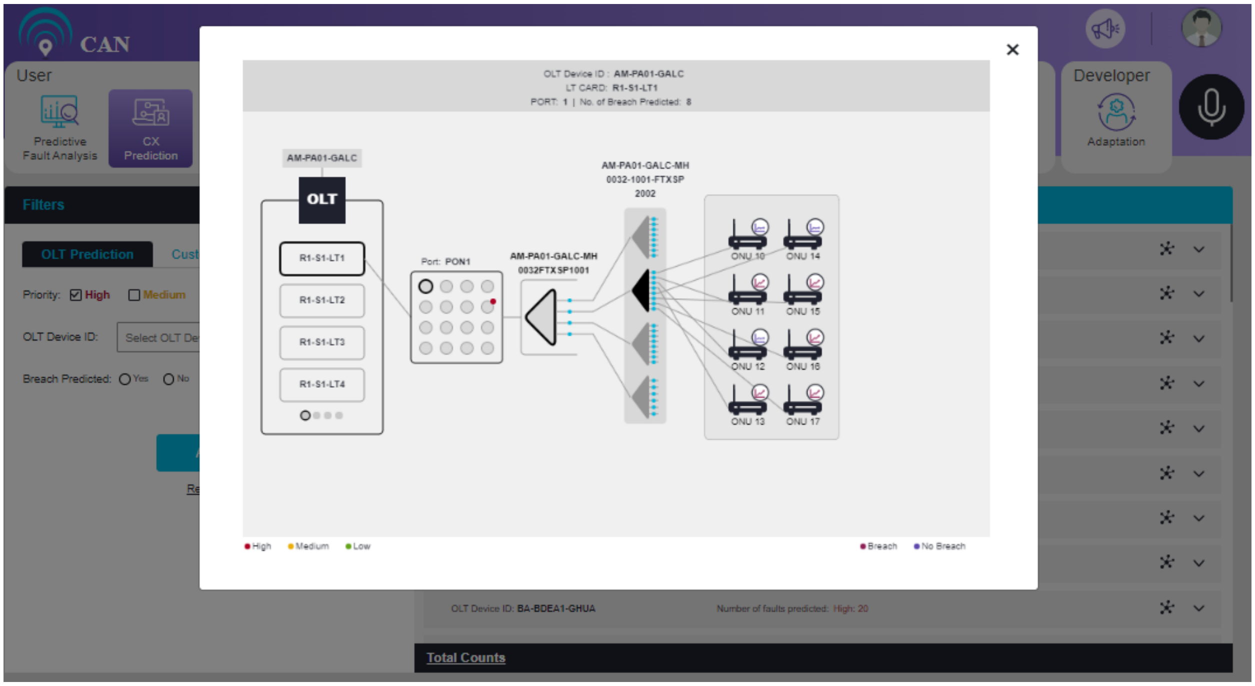
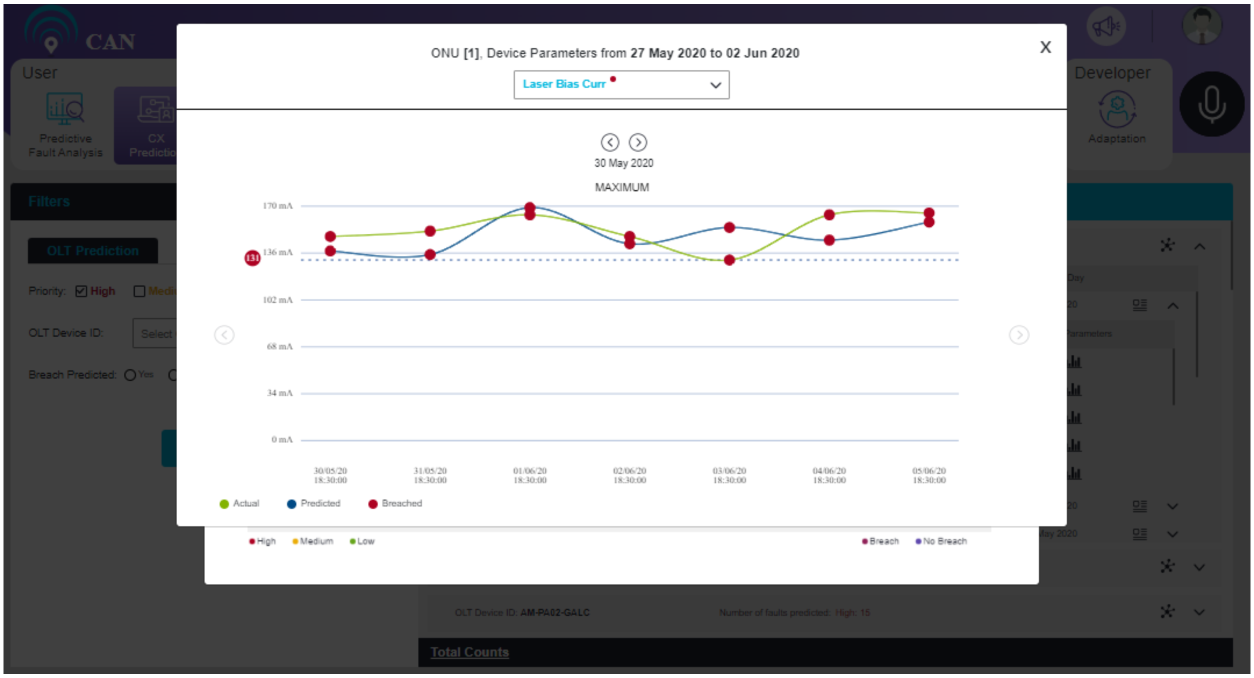

OLT Device ID : AM-PA01-GALC
LT CARD: R1-S1-LT1
PORT: 1 | No. of Breach Predicted: 8

Figure 4.8 - OLT Prediction Network View

7. To view the connected ports and ONUs, click on a particular LT-Card.
8. Click on any port/splitter to view the ONUs connected to that particular port/splitter.
9. Click the graph icon on the ONU to view the graph of KPI prediction data.


ONU [1], Device Parameters from 27 May 2020 to 02 Jun 2020

Laser Bias Curr

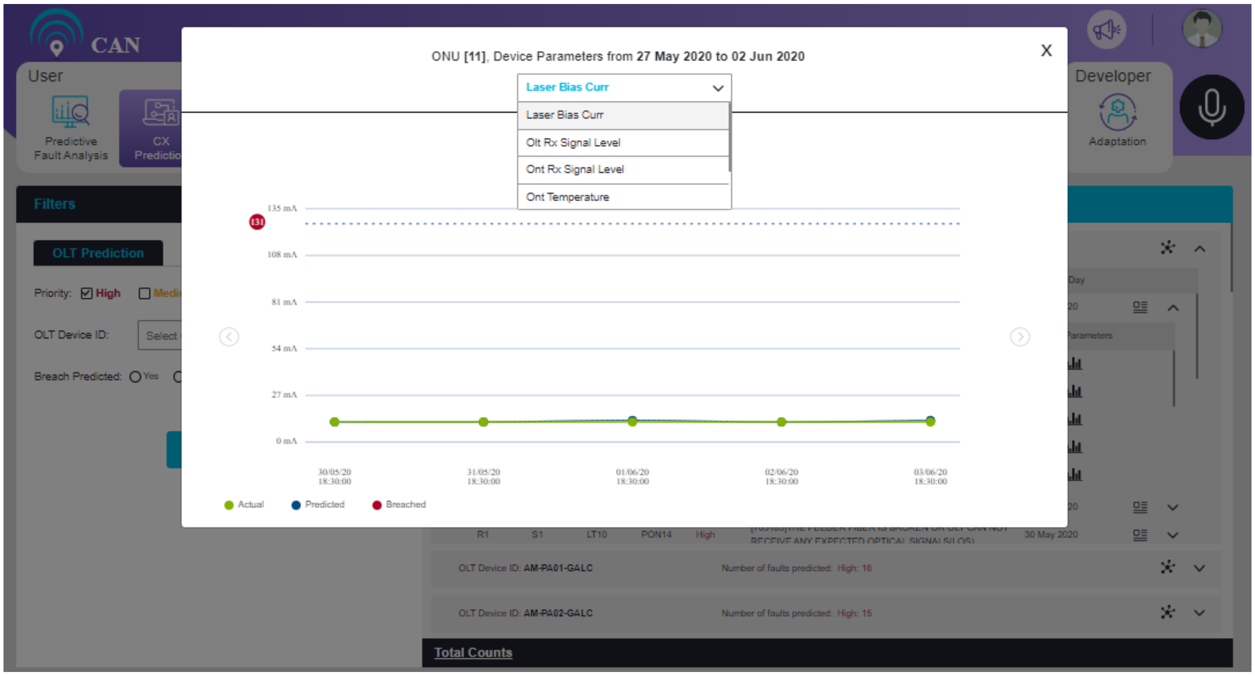
30 May 2020

MAXIMUM

Figure 4.9 - Breach Prediction Graph

10. By default, the breached KPI on the day within given window is displayed.

11. Navigate through all 7 days of window ⓘ ⓘ .
12. User can view the desired data from the drop down.



ONU [11], Device Parameters from 27 May 2020 to 02 Jun 2020

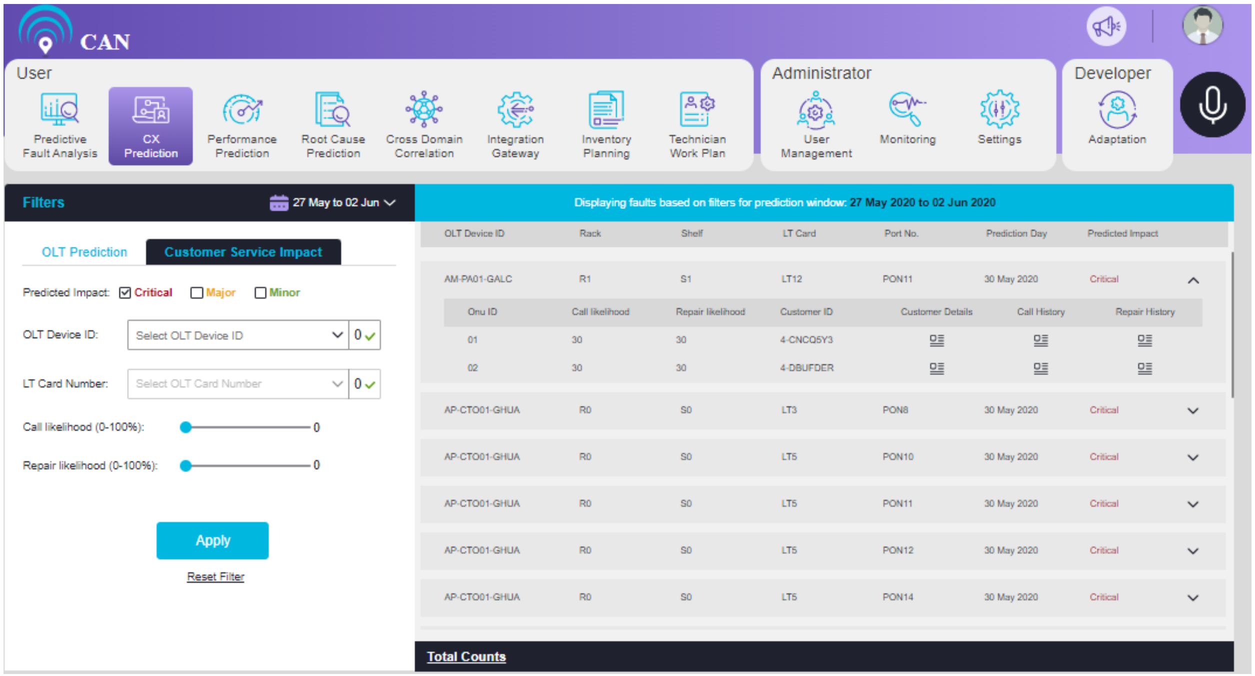
Laser Bias Curr

- Laser Bias Curr
- Olt Rx Signal Level
- Ont Rx Signal Level
- Ont Temperature

Figure 4.10 - Device Parameters Dropdown

Customer Service Impact has only tabular representation.

1. To view the ports that are predicted as faults and predicted impact on port, click anywhere on the particular row.



Predicted Impact: ☑ Critical ☐ Major ☐ Minor

OLT Device ID: Select OLT Device ID 0 ✓

LT Card Number: Select OLT Card Number 0 ✓

Call likelihood (0-100%): 0

Repair likelihood (0-100%): 0

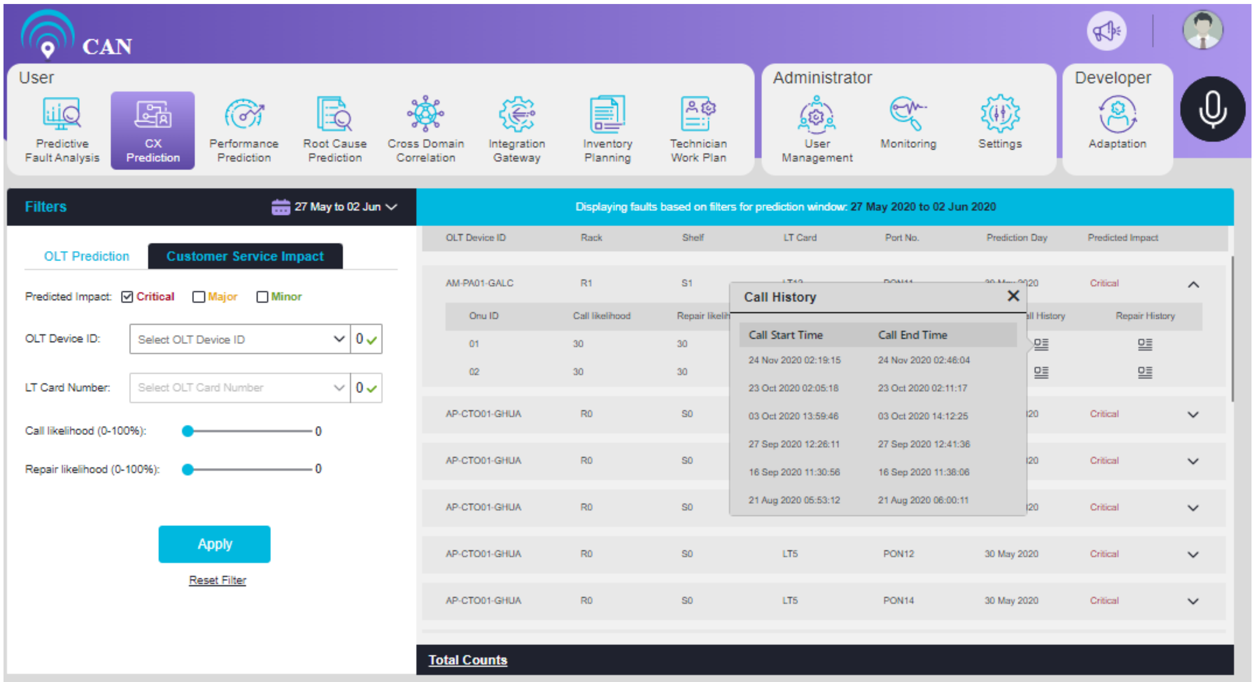
Displaying faults based on filters for prediction window: 27 May 2020 to 02 Jun 2020

OLT Device ID	Rack	Shelf	LT Card	Port No.	Prediction Day	Predicted Impact
AM-PA01-GALC	R1	S1	LT12	PON11	30 May 2020	Critical
AP-CTO01-GHUA	R0	S0	LT3	PON8	30 May 2020	Critical
AP-CTO01-GHUA	R0	S0	LT5	PON10	30 May 2020	Critical
AP-CTO01-GHUA	R0	S0	LT5	PON11	30 May 2020	Critical
AP-CTO01-GHUA	R0	S0	LT5	PON12	30 May 2020	Critical
AP-CTO01-GHUA	R0	S0	LT5	PON14	30 May 2020	Critical

Onu ID	Call likelihood	Repair likelihood	Customer ID	Customer Details	Call History	Repair History
01	30	30	4-CNCQ5Y3	▤	▤	▤
02	30	30	4-DBUFDER	▤	▤	▤

Figure 4.11 - Customer Service Impact Attributes

2. First level has the following attributes:
   - OLT Device ID
   - Rack
   - Shelf
   - LT Card
   - Port No.
   - Prediction Day
   - Predicted Impact (Critical / Major / Minor)
3. Second level displays the call and repair values for each ONU and Call & Repair History.
4. Second level has the following attributes:
   - ONU ID
   - Call likelihood
   - Repair likelihood
   - Customer ID
   - Customer Details ▤
   - Call History ▤

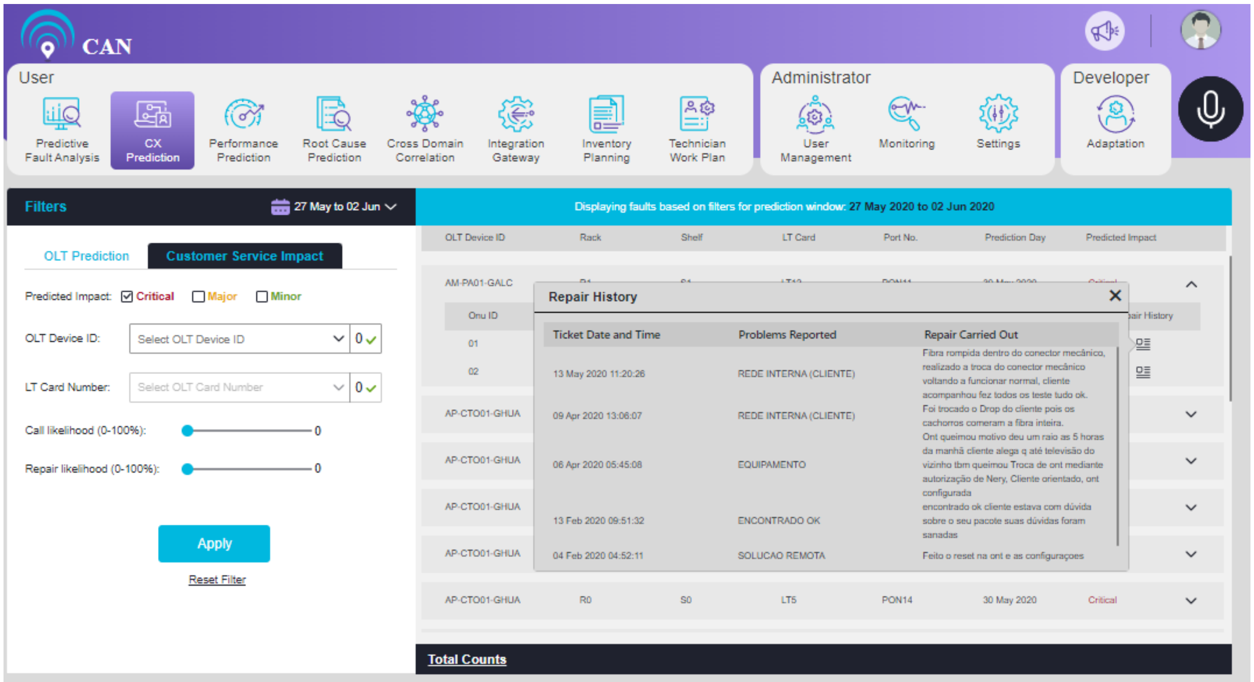


Call History

Call Start Time	Call End Time
24 Nov 2020 02:19:15	24 Nov 2020 02:46:04
23 Oct 2020 02:05:18	23 Oct 2020 02:11:17
03 Oct 2020 13:59:46	03 Oct 2020 14:12:25
27 Sep 2020 12:26:11	27 Sep 2020 12:41:36
16 Sep 2020 11:30:56	16 Sep 2020 11:38:06
21 Aug 2020 05:53:12	21 Aug 2020 06:00:11

Figure 4.12 - Call History

- Repair History ☰



Repair History

Ticket Date and Time	Problems Reported	Repair Carried Out
13 May 2020 11:20:26	REDE INTERNA (CLIENTE)	Fibra rompida dentro do conector mecânico, realizado a troca do conector mecânico voltando a funcionar normal, cliente acompanhou fez todos os teste tudo ok.
09 Apr 2020 13:06:07	REDE INTERNA (CLIENTE)	Foi trocado o Drop do cliente pois os cachorros comeram a fibra inteira.
06 Apr 2020 05:45:08	EQUIPAMENTO	Ont queimou motivo deu um raio as 5 horas da manhã cliente alega q até televisão do vizinho tbm queimou Troca de ont mediante autorização de Nery, Cliente orientado, ont configurada
13 Feb 2020 09:51:32	ENCONTRADO OK	encontrado ok cliente estava com dúvida sobre o seu pacote suas dúvidas foram sanadas
04 Feb 2020 04:52:11	SOLUCAO REMOTA	Feito o reset na ont e as configuraçoes

Figure 4.13 - Repair History

Page Intentionally Left Blank

5. PERFORMANCE PREDICTION

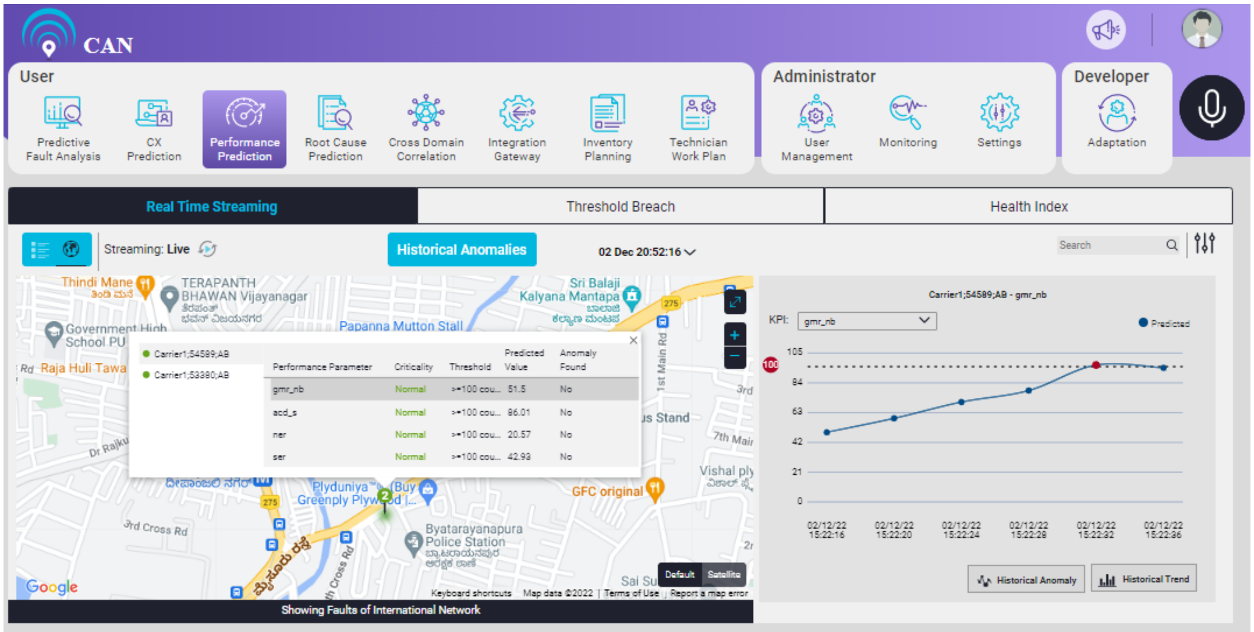
The Performance Prediction module enables CAN users to monitor the health status of every equipment along with its KPI behavior. In the event of threshold breach or health degradation corresponding devices are highlighted so that users can take appropriate action.

The Performance Prediction has three tabs:

1. Real Time Streaming
2. Threshold Breach
3. Health Index

Real Time Streaming

Performance Prediction screen screen navigates to the anomalies made by CAN for the available data. By default, Performance Prediction screen displays real time streaming to the latest prediction window as **Map view**.



Carrier1;54589;AB
Carrier1;53380;AB

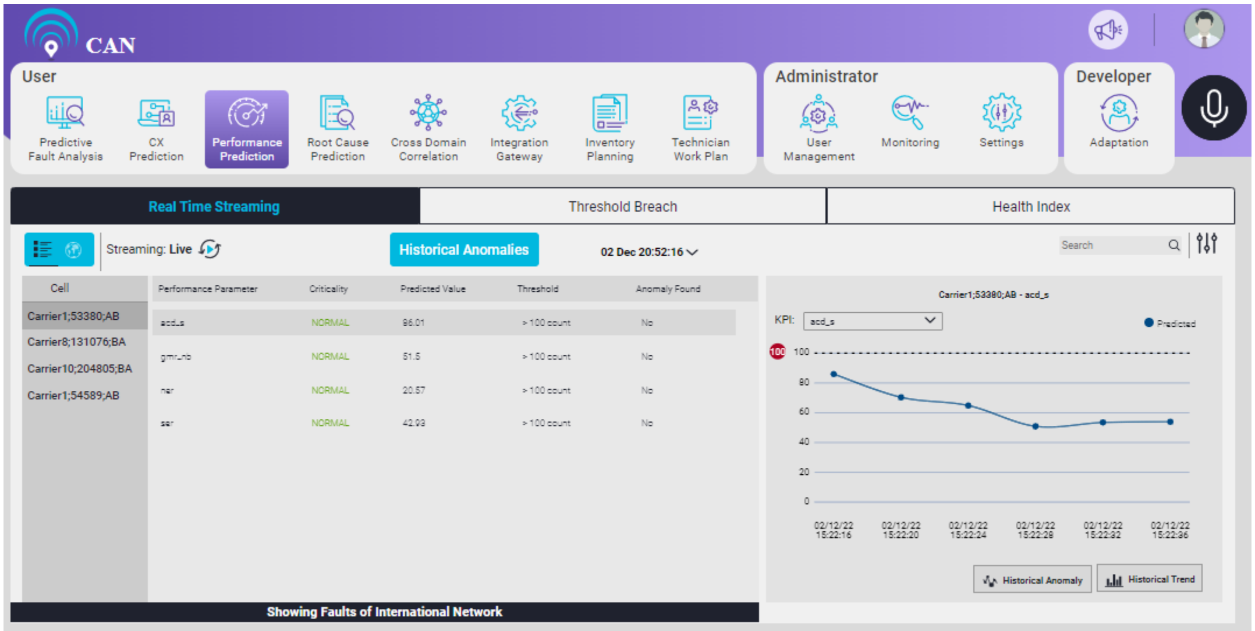
Performance Parameter	Criticality	Threshold	Predicted Value	Anomaly Found
gmr_nb	Normal	>=100 cou...	51.5	No
acd_s	Normal	>=100 cou...	86.01	No
ner	Normal	>=100 cou...	20.57	No
ser	Normal	>=100 cou...	42.93	No

Figure 5.1 - Performance Prediction Screen

Live status represents the real time streaming . The data is refreshed every 4 seconds. The screen is refreshed and displays the result for a latest prediction window for the selected date (Nation wise).

Performance Prediction allows the users to view the predictions Nation wise, Region wise, Zone wise and so on.

User can select **Tabular view**. For every prediction, there are data as well as graphical representation of the data. The graphical representation shows the predicted value.

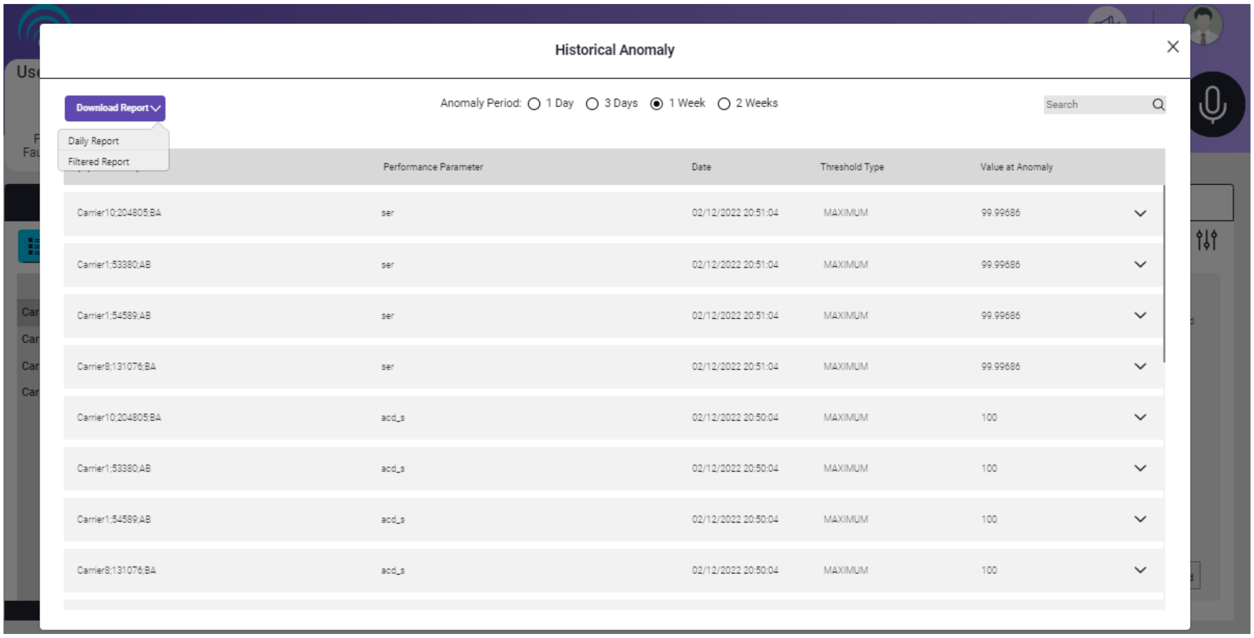


Cell
Carrier1;53380;AB
Carrier8;131076;BA
Carrier10;204805;BA
Carrier1;54589;AB

Performance Parameter	Criticality	Predicted Value	Threshold	Anomaly Found
acd_s	NORMAL	96.01	> 100 count	No
gmr_nb	NORMAL	51.5	> 100 count	No
ner	NORMAL	20.57	> 100 count	No
ser	NORMAL	42.93	> 100 count	No

Figure 5.2 - Real Time Streaming Tabular View

If the user click the **Historical Anomalies** button, the Historical Anomaly screen for all the equipment components pops up. Click anywhere on the row to display Historical Anomaly graph. User can select the **Anomaly Period** (1 Day, 3 Days, 1 Week and 2 Weeks), **Search** an equipment component and **Download Report** (Daily and Filtered).



Anomaly Period: ○ 1 Day ○ 3 Days ● 1 Week ○ 2 Weeks

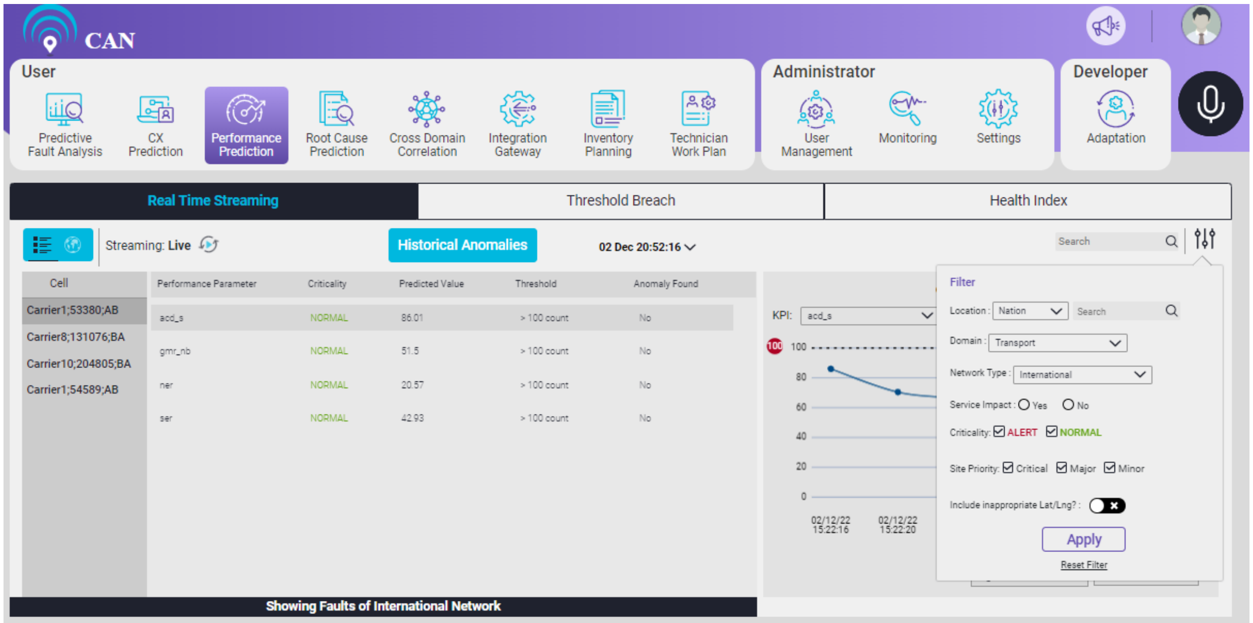
	Performance Parameter	Date	Threshold Type	Value at Anomaly
Carrier10;204805;BA	ser	02/12/2022 20:51:04	MAXIMUM	99.99686
Carrier1;53380;AB	ser	02/12/2022 20:51:04	MAXIMUM	99.99686
Carrier1;54589;AB	ser	02/12/2022 20:51:04	MAXIMUM	99.99686
Carrier8;131076;BA	ser	02/12/2022 20:51:04	MAXIMUM	99.99686
Carrier10;204805;BA	acd_s	02/12/2022 20:50:04	MAXIMUM	100
Carrier1;53380;AB	acd_s	02/12/2022 20:50:04	MAXIMUM	100
Carrier1;54589;AB	acd_s	02/12/2022 20:50:04	MAXIMUM	100
Carrier8;131076;BA	acd_s	02/12/2022 20:50:04	MAXIMUM	100

Figure 5.3 - Historical Anomalies

User has the option to **Filter** Performance Prediction Analysis based on the following parameters:

1. **Location**: There are multiple location options. (Currently, screen displays 2 locations i.e. **Nation** and **Region**).

2. **Domain**: There are multiple domains (Currently, screen displays 3 domains i.e. **Core**, **Transport** and **Access**).
3. **Network Type**: User can select the **Network Type** based on the selected **Domain**.
4. **Service Impact**: It has two radio buttons: Yes and No
5. **Criticality**: It has two check boxes - ALERT and NORMAL.
6. **Site Priority**: It has three check boxes - Critical, Major and Minor to filter out respective priority sites.
7. **Include Inappropriate Lat/Long**: A toggle button to include or exclude the inappropriate Lat/Long.



Cell
Carrier1;53380;AB
Carrier8;131076;BA
Carrier10;204805;BA
Carrier1;54589;AB

Performance Parameter	Criticality	Predicted Value	Threshold	Anomaly Found
acd_s	NORMAL	86.01	> 100 count	No
gmr_nb	NORMAL	51.5	> 100 count	No
ner	NORMAL	20.57	> 100 count	No
ser	NORMAL	42.93	> 100 count	No

Filter

Location : Nation Search

Domain : Transport

Network Type : International

Service Impact : ○ Yes ○ No

Criticality: ☑ ALERT ☑ NORMAL

Site Priority: ☑ Critical ☑ Major ☑ Minor

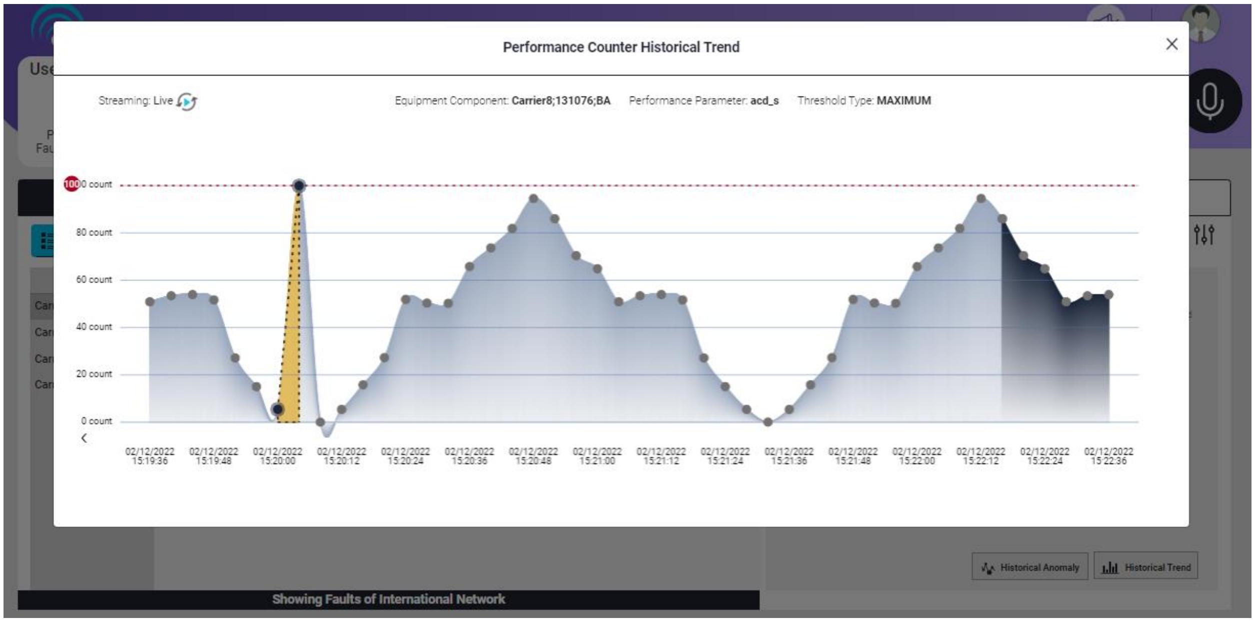
Include inappropriate Lat/Lng? : ☒

Apply

Reset Filter

Figure 5.4 - Performance Prediction Filter

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



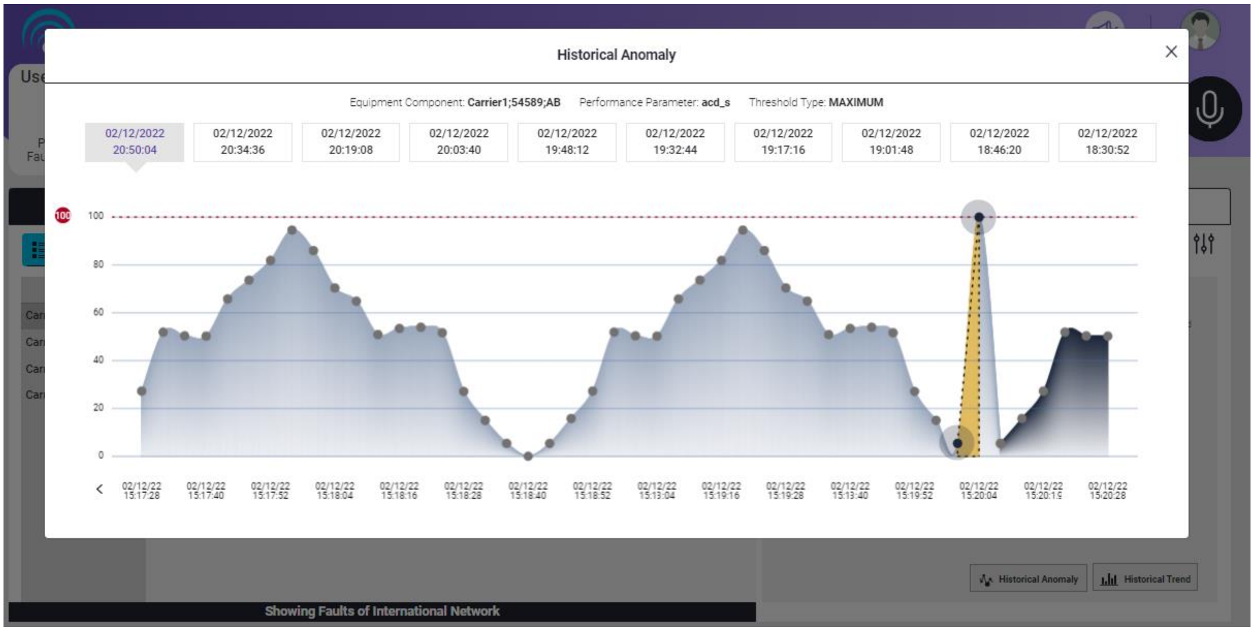
Performance Counter Historical Trend

Streaming: Live

Equipment Component: **Carrier8;131076;BA** Performance Parameter: **acd_s** Threshold Type: **MAXIMUM**

Figure 5.5 - Performance Counter Historical Trend

If the user click the **Historical Anomaly** button for the particular graph, the **Historical Anomaly** screen pops up.



Historical Anomaly

Equipment Component: **Carrier1;54589;AB** Performance Parameter: **acd_s** Threshold Type: **MAXIMUM**

Figure 5.6 - Historical Anomaly Screen

Threshold Breach

Threshold breach screen shows the performance counter predictions.

By default, Threshold breach screen displays **Map view**. Markers represent the breached equipment. Map view has two options: Default and Satellite. To view the details of the breached equipment, click on the Marker.

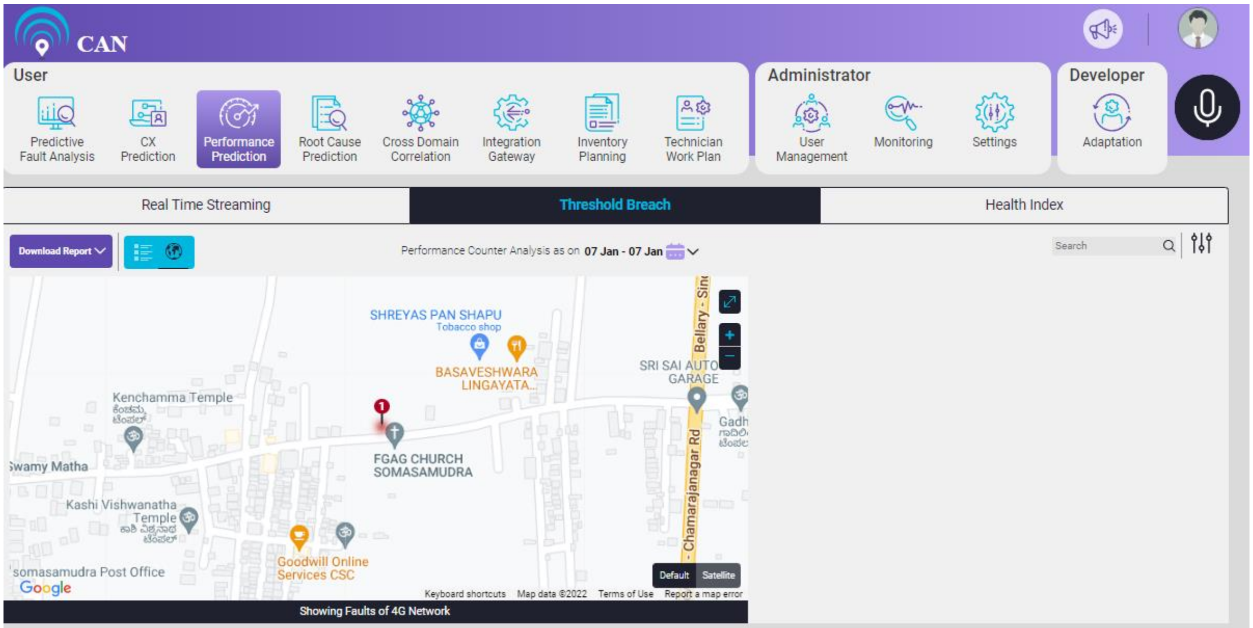
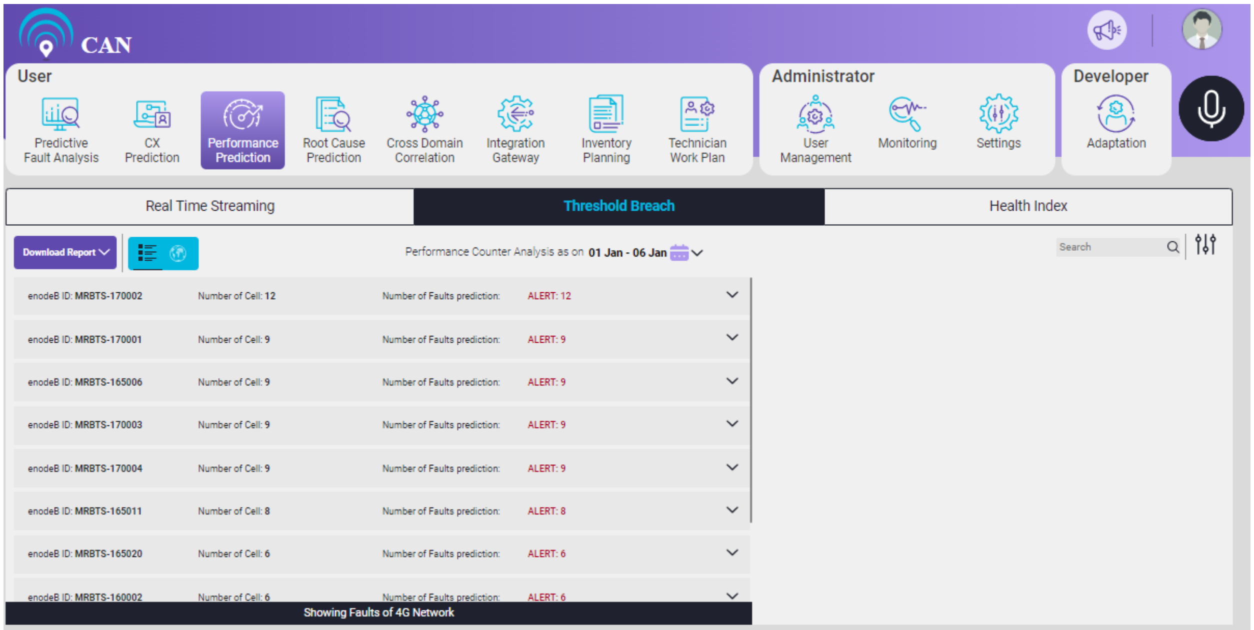


Figure 5.7 - Threshold Breach Screen

User can select **Tabular view**.



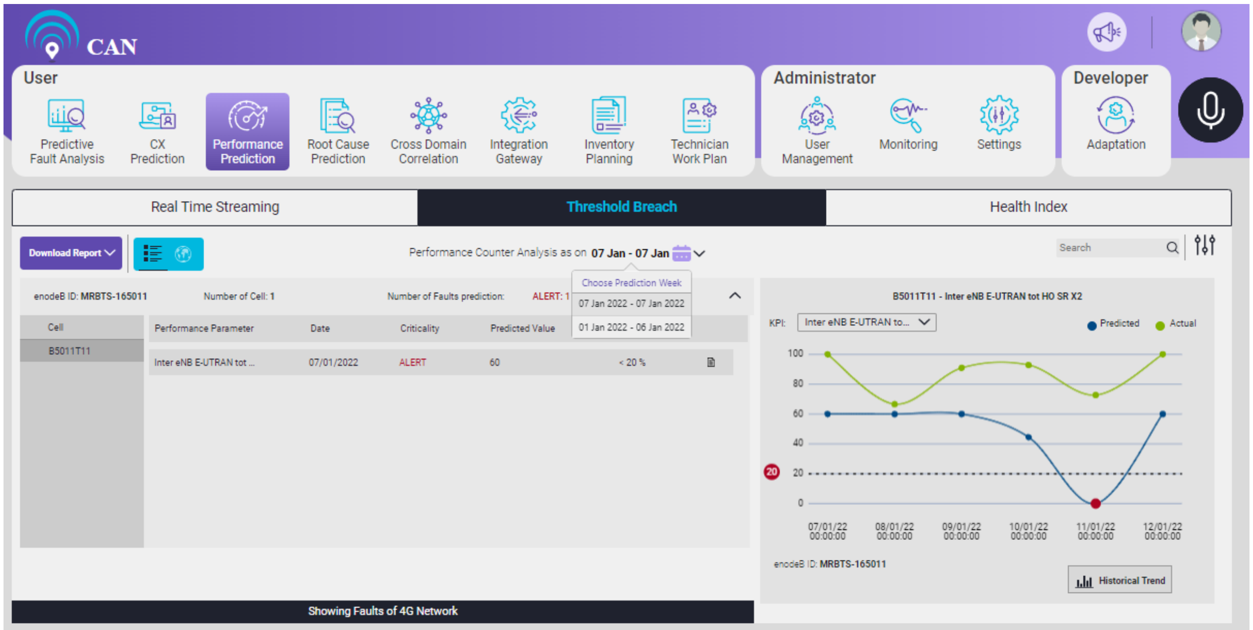
Performance Counter Analysis as on **01 Jan - 06 Jan**

enodeB ID: **MRBTS-170002**	Number of Cell: **12**	Number of Faults prediction:	ALERT: 12
enodeB ID: **MRBTS-170001**	Number of Cell: **9**	Number of Faults prediction:	ALERT: 9
enodeB ID: **MRBTS-165006**	Number of Cell: **9**	Number of Faults prediction:	ALERT: 9
enodeB ID: **MRBTS-170003**	Number of Cell: **9**	Number of Faults prediction:	ALERT: 9
enodeB ID: **MRBTS-170004**	Number of Cell: **9**	Number of Faults prediction:	ALERT: 9
enodeB ID: **MRBTS-165011**	Number of Cell: **8**	Number of Faults prediction:	ALERT: 8
enodeB ID: **MRBTS-165020**	Number of Cell: **6**	Number of Faults prediction:	ALERT: 6
enodeB ID: **MRBTS-160002**	Number of Cell: **6**	Number of Faults prediction:	ALERT: 6

Figure 5.8 - Threshold Breach Tabular View

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

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



Performance Counter Analysis as on **07 Jan - 07 Jan**

enodeB ID: **MRBTS-165011** Number of Cell: **1** Number of Faults prediction: ALERT: 1

Cell	Performance Parameter	Date	Criticality	Predicted Value		
B5011T11	Inter eNB E-UTRAN tot ...	07/01/2022	ALERT	60	< 20 %	🗎

enodeB ID: **MRBTS-165011**

Figure 5.9 - Week Selection

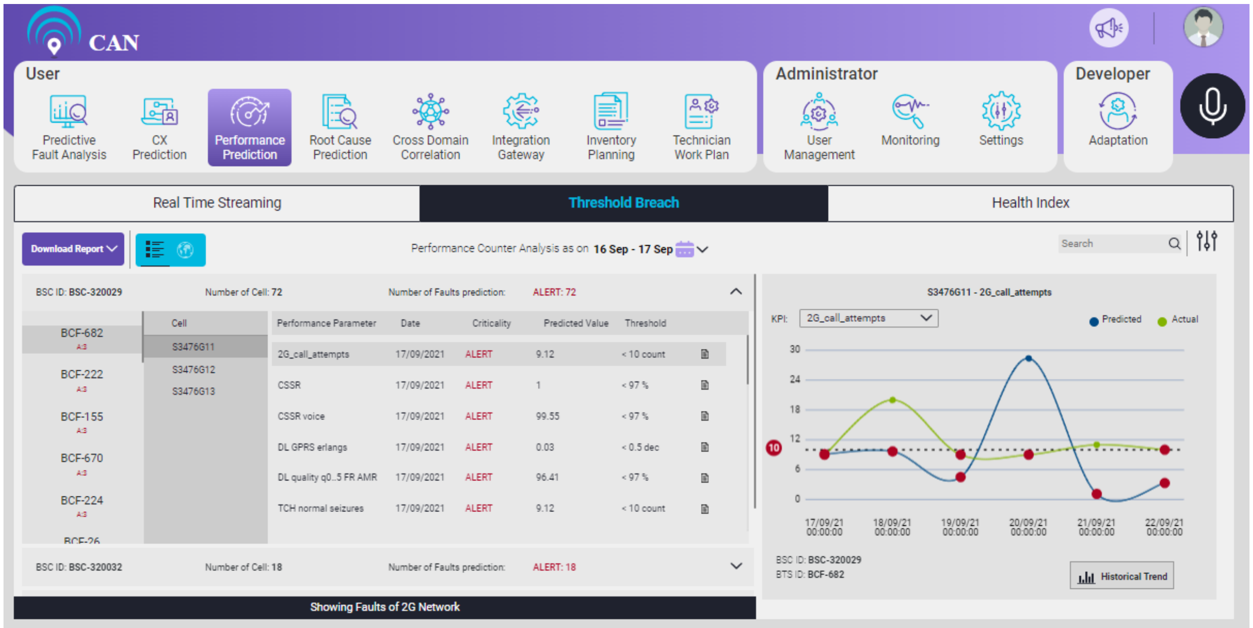
Threshold Breach screen contains the following details:

- Cell: It is also known as Equipment Component.
- Performance Parameter: There are multiple KPIs.
- Date: The day breach occurred in the selected week.
- Criticality: Criticality of the KPI will be categorized as either ALERT or NORMAL based on predicted value.
- Predicted Value: The value predicted by the CAN Prediction engine is Predicted Value.
- Threshold: The value above which the device can fail.
- Matching Details 🗎: It indicates actual value vs predicted value.

When predictions happen 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.

User has the option to **Filter** Performance Prediction Analysis based on the following parameters:

1. **Location**: There are multiple location options. (Currently, screen displays two locations i.e. **Nation** and **Region**).
2. **Domain**: There are multiple domains (Currently, screen displays three domains i.e. **Core**, **Transport** and **Access**).
3. **Network Type**: User can select the **Network Type** based on the selected **Domain**.
4. The hierarchy varies for **2G**, **3G** and **4G** network type.



Performance Counter Analysis as on **16 Sep - 17 Sep**

BSC ID: **BSC-320029** Number of Cell: **72** Number of Faults prediction: ALERT: 72

BCF-682 A:3
BCF-222 A:3
BCF-155 A:3
BCF-670 A:3
BCF-224 A:3
BCF-26

Cell
S3476G11
S3476G12
S3476G13

Performance Parameter	Date	Criticality	Predicted Value	Threshold
2G_call_attempts	17/09/2021	ALERT	9.12	< 10 count
CSSR	17/09/2021	ALERT	1	< 97 %
CSSR voice	17/09/2021	ALERT	99.55	< 97 %
DL GPRS erlangs	17/09/2021	ALERT	0.03	< 0.5 dec
DL quality q0..5 FR AMR	17/09/2021	ALERT	96.41	< 97 %
TCH normal seizures	17/09/2021	ALERT	9.12	< 10 count

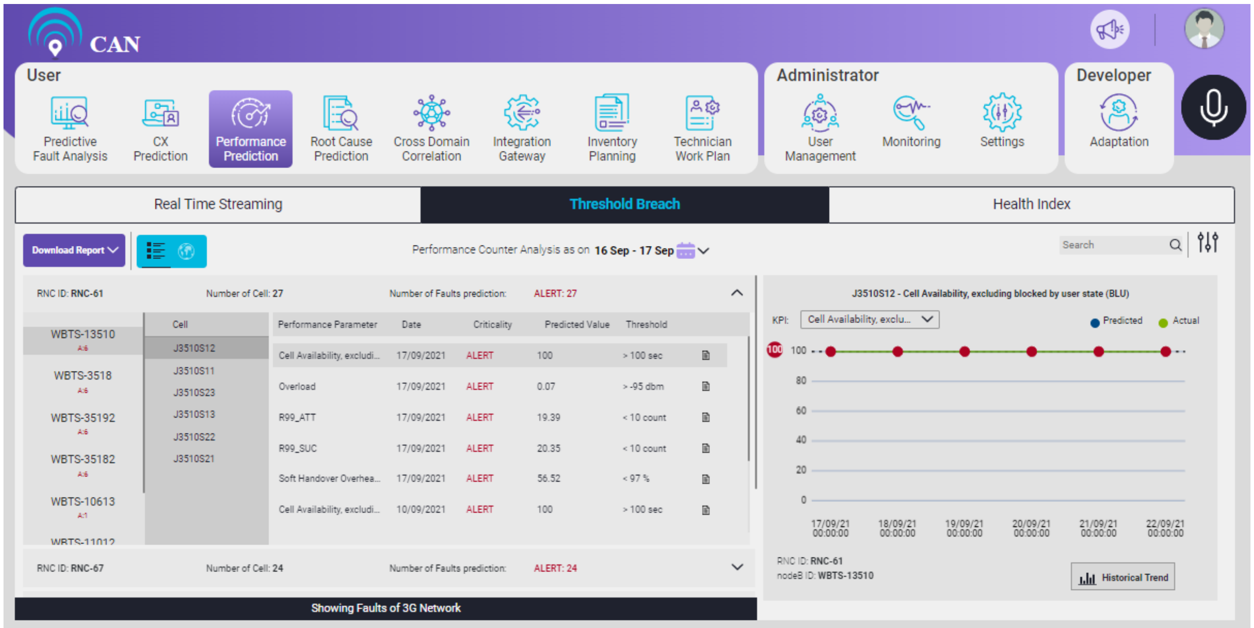
BSC ID: **BSC-320032** Number of Cell: **18** Number of Faults prediction: ALERT: 18

S3476G11 - 2G_call_attempts

KPI: 2G_call_attempts

BSC ID: **BSC-320029**
BTS ID: **BCF-682**

Figure 5.10 - 2G Network Type



Performance Counter Analysis as on **16 Sep - 17 Sep**

RNC ID: **RNC-61** Number of Cell: **27** Number of Faults prediction: ALERT: 27

WBTS-13510 A:6
WBTS-3518 A:6
WBTS-35192 A:6
WBTS-35182 A:6
WBTS-10613 A:1
WBTS-11012

Cell
J3510S12
J3510S11
J3510S23
J3510S13
J3510S22
J3510S21

Performance Parameter	Date	Criticality	Predicted Value	Threshold
Cell Availability, excludi...	17/09/2021	ALERT	100	> 100 sec
Overload	17/09/2021	ALERT	0.07	> -95 dbm
R99_ATT	17/09/2021	ALERT	19.39	< 10 count
R99_SUC	17/09/2021	ALERT	20.35	< 10 count
Soft Handover Overhea...	17/09/2021	ALERT	56.52	< 97 %
Cell Availability, excludi...	10/09/2021	ALERT	100	> 100 sec

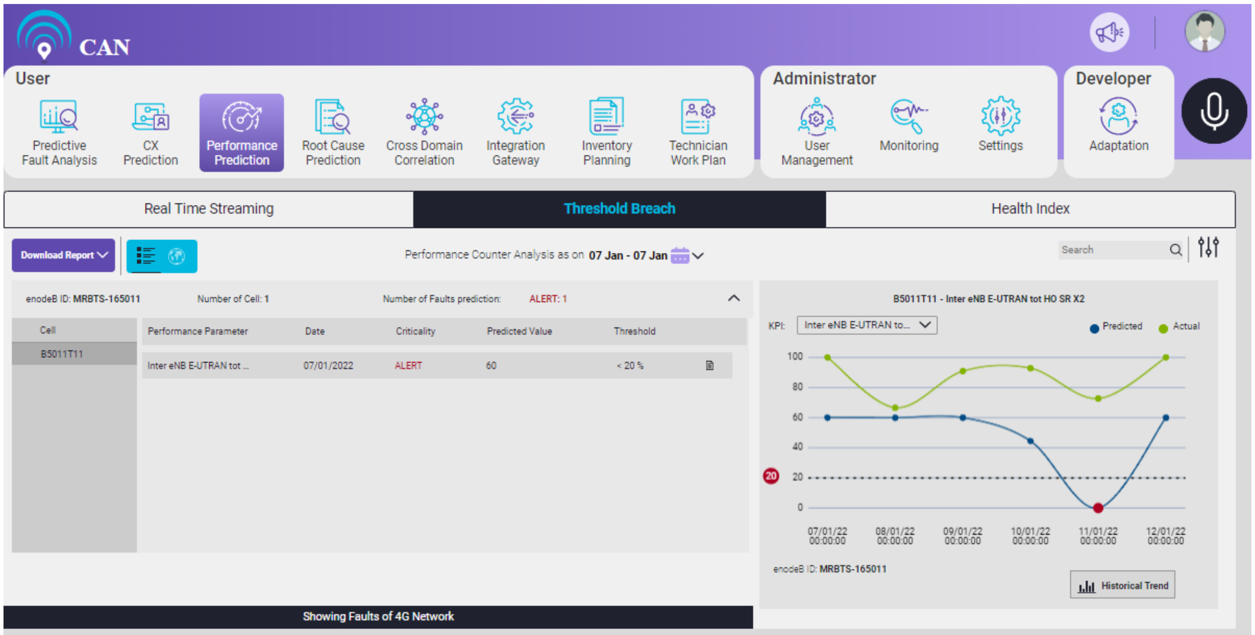
RNC ID: **RNC-67** Number of Cell: **24** Number of Faults prediction: ALERT: 24

J3510S12 - Cell Availability, excluding blocked by user state (BLU)

KPI: Cell Availability, exclu...

RNC ID: **RNC-61**
nodeB ID: **WBTS-13510**

Figure 5.11 - 3G Network Type



Performance Counter Analysis as on **07 Jan - 07 Jan**

enodeB ID: **MRBTS-165011** Number of Cell: **1** Number of Faults prediction: ALERT: 1

Cell	Performance Parameter	Date	Criticality	Predicted Value	Threshold
B5011T11	Inter eNB E-UTRAN tot ...	07/01/2022	ALERT	60	< 20 %

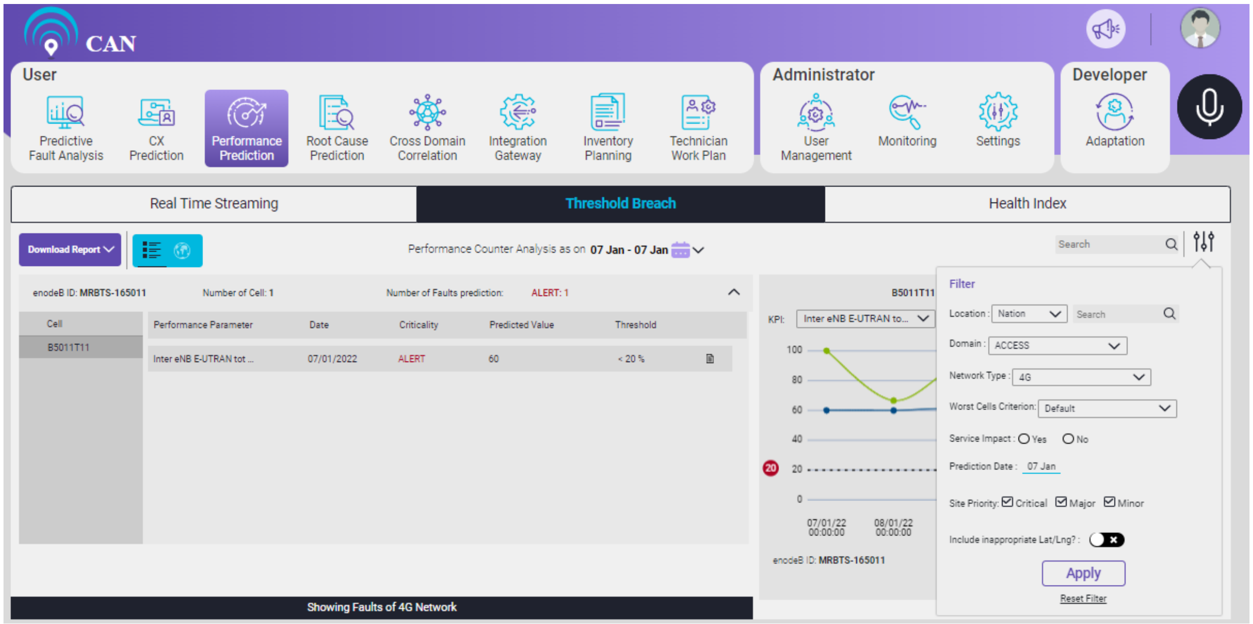
B5011T11 - Inter eNB E-UTRAN tot HO SR X2

enodeB ID: **MRBTS-165011**

Showing Faults of 4G Network

Figure 5.12 - 4G Network Type

5. **Worst Cells Criterion**: There are 4 criteria (Screen displays **Default** criteria)
6. **Service Impact**: It has two radio buttons: Yes and No
7. **Prediction Date**: List of dates in the selected week.
8. **Site Priority**: It has three check boxes: Critical, Major and Minor to filter out respective priority sites.
9. **Include Inappropriate Lat/Long**: A toggle button to include or exclude the inappropriate Lat/Long.



Performance Counter Analysis as on **07 Jan - 07 Jan**

enodeB ID: **MRBTS-165011** Number of Cell: **1** Number of Faults prediction: ALERT: 1

Cell	Performance Parameter	Date	Criticality	Predicted Value	Threshold
B5011T11	Inter eNB E-UTRAN tot ...	07/01/2022	ALERT	60	< 20 %

enodeB ID: **MRBTS-165011**

Filter

Location : Nation

Domain : ACCESS

Network Type : 4G

Worst Cells Criterion: Default

Service Impact : ○ Yes ○ No

Prediction Date : 07 Jan

Site Priority: ☑ Critical ☑ Major ☑ Minor

Include inappropriate Lat/Lng? :

Showing Faults of 4G Network

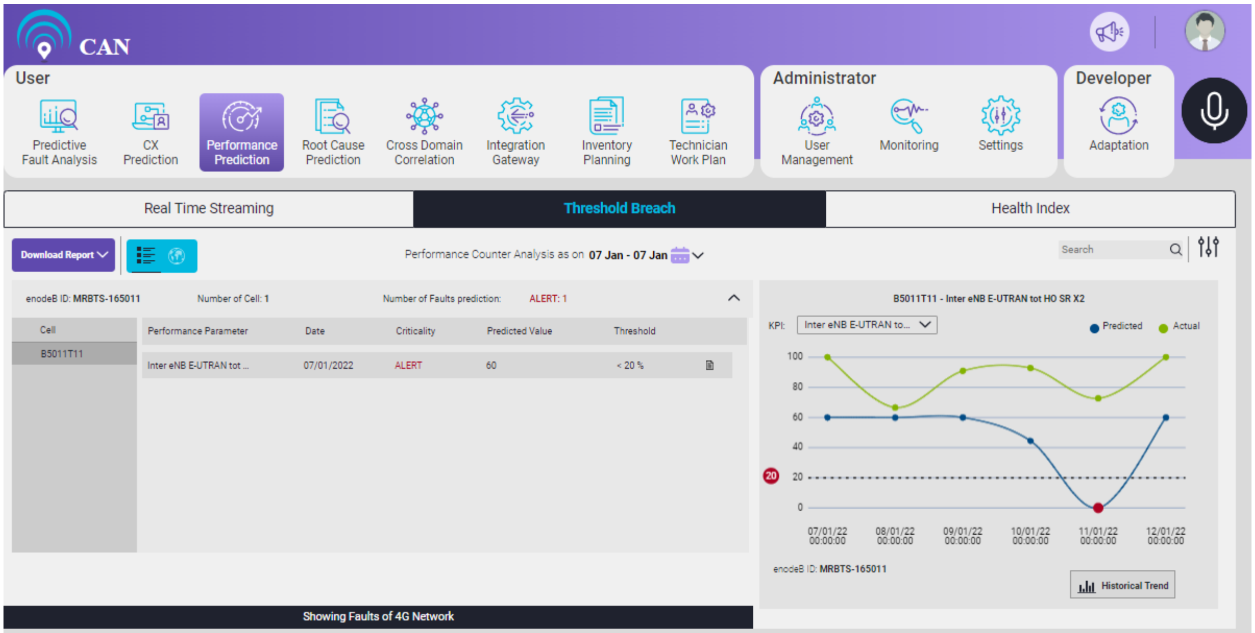
Figure 5.13 - Threshold Breach Filter

The **Threshold Breach** screen has the search box. User can use the search box to search for the particular field such as Cell, 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.



Performance Counter Analysis as on **07 Jan - 07 Jan**

enodeB ID: **MRBTS-165011** Number of Cell: **1** Number of Faults prediction: ALERT: 1

Cell	Performance Parameter	Date	Criticality	Predicted Value	Threshold
B5011T11	Inter eNB E-UTRAN tot ...	07/01/2022	ALERT	60	< 20 %

B5011T11 - Inter eNB E-UTRAN tot HO SR X2

enodeB ID: **MRBTS-165011**

Figure 5.14 – Threshold Breach 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:

1. Equipment Component
2. Performance Parameter
3. Threshold Type

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

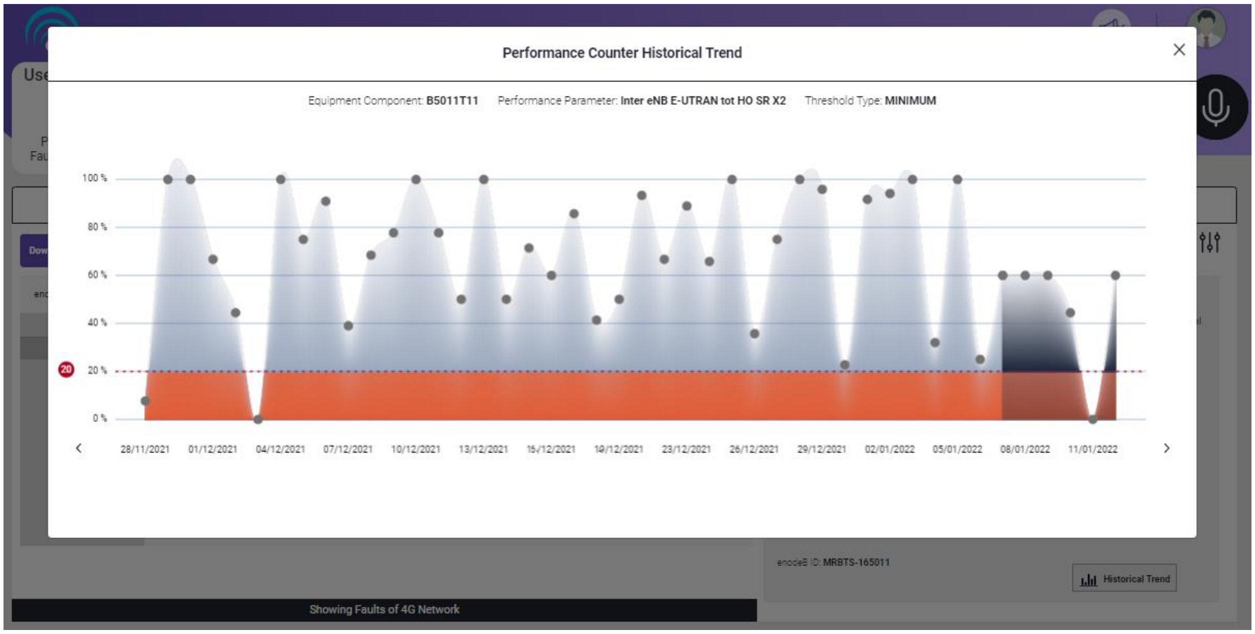


Figure 5.15 - Performance Counter Historical Trend

Health Index

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

By default, Health Index screen displays **Map view**. Markers represent the health degradation of an equipment. Map view has two options: Default and Satellite. To view the details of the equipment, click on the Marker.

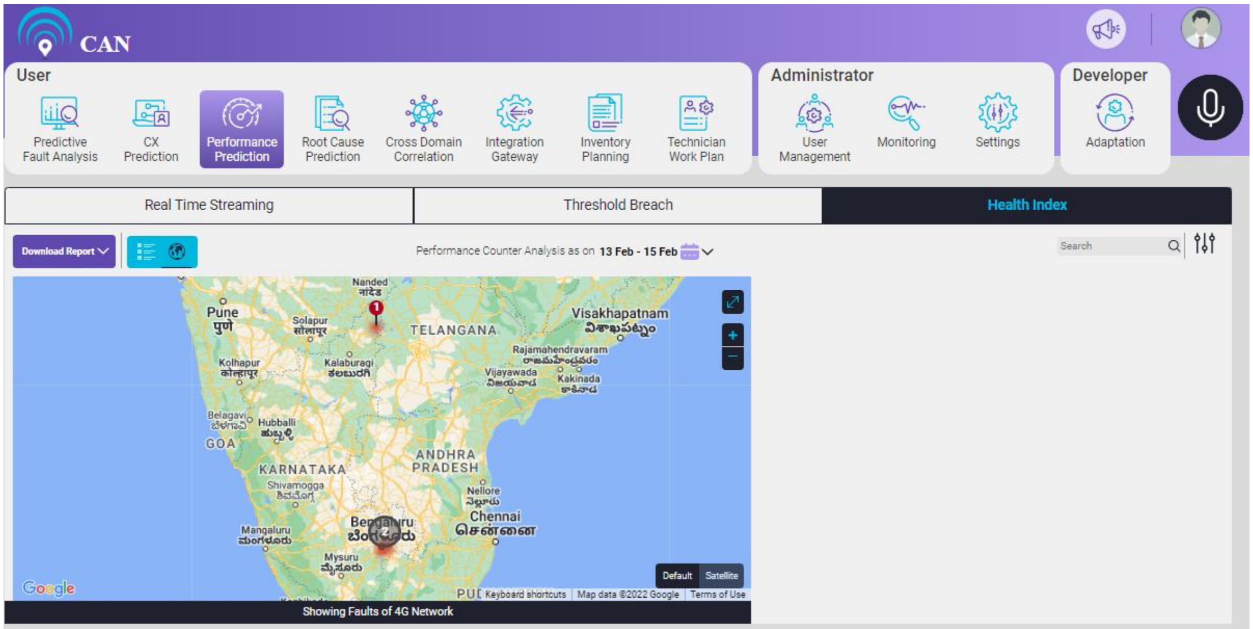
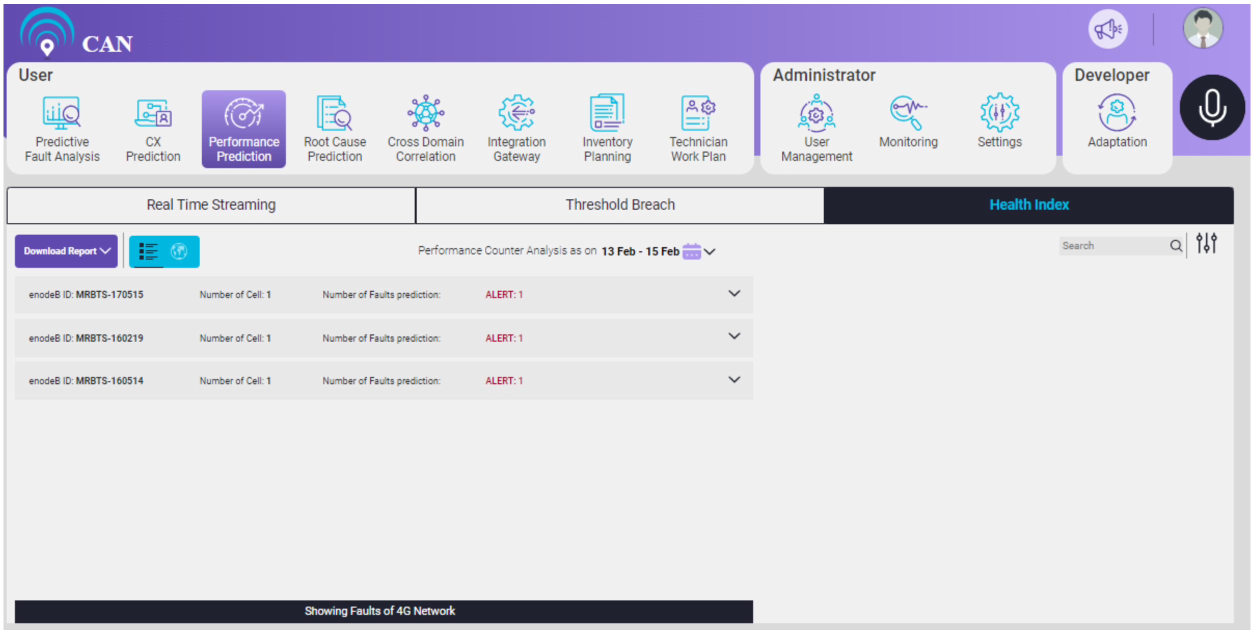


Figure 5.16 - Health Index Screen

User can select **Tabular view**.



Performance Counter Analysis as on **13 Feb - 15 Feb**

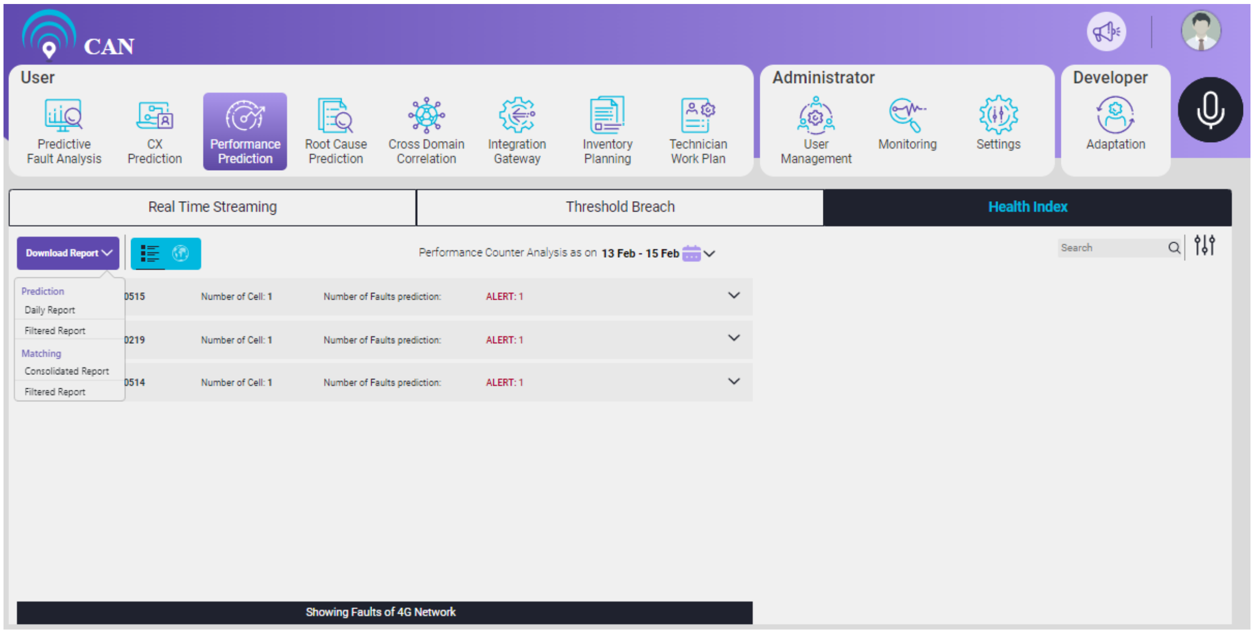
enodeB ID: **MRBTS-170515** Number of Cell: **1** Number of Faults prediction: ALERT: 1

enodeB ID: **MRBTS-160219** Number of Cell: **1** Number of Faults prediction: ALERT: 1

enodeB ID: **MRBTS-160514** Number of Cell: **1** Number of Faults prediction: ALERT: 1

Figure 5.17 - Health Index Tabular View

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



Performance Counter Analysis as on **13 Feb - 15 Feb**

0515 Number of Cell: **1** Number of Faults prediction: ALERT: 1

0219 Number of Cell: **1** Number of Faults prediction: ALERT: 1

0514 Number of Cell: **1** Number of Faults prediction: ALERT: 1

Figure 5.18 - Health Index Report Download

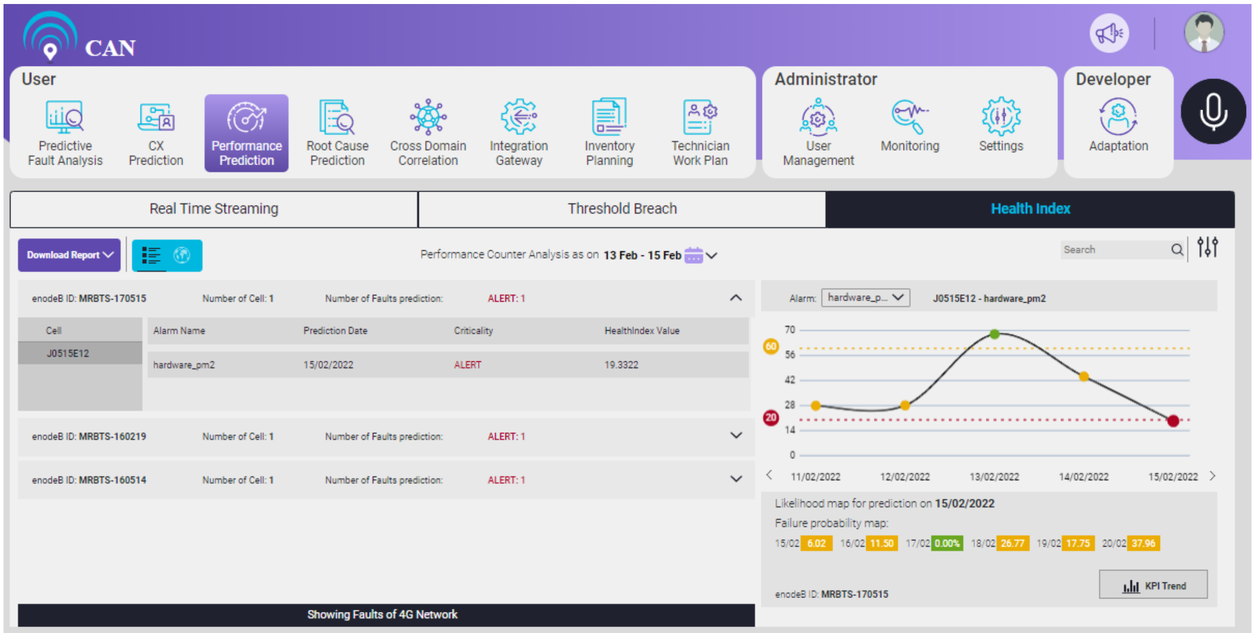
The screen has the search box. User can use the search box to search based on Equipment component or Criticality.

When the user clicks the **Equipment Component**, a graph appears on the right side of the screen that 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 go below 60, it is a warning zone and when it goes below 20, it is an alert zone.

The Alert and Normal criticality varies for the different predictions.



Performance Counter Analysis as on **13 Feb - 15 Feb**

enodeB ID: **MRBTS-170515** Number of Cell: **1** Number of Faults prediction: ALERT: 1

Cell	Alarm Name	Prediction Date	Criticality	HealthIndex Value
J0515E12	hardware_pm2	15/02/2022	ALERT	19.3322

enodeB ID: **MRBTS-160219** Number of Cell: **1** Number of Faults prediction: ALERT: 1

enodeB ID: **MRBTS-160514** Number of Cell: **1** Number of Faults prediction: ALERT: 1

Alarm: hardware_p... **J0515E12 - hardware_pm2**

Likelihood map for prediction on **15/02/2022**

Failure probability map:

15/02	16/02	17/02	18/02	19/02	20/02
6.02	11.50	0.00%	26.77	17.75	37.96

enodeB ID: **MRBTS-170515**

Figure 5.19 - Equipment Heath Prediction

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

User has the option to:

- View Shortlisted KPIs or All KPIs
- View KPI trend of Previous and Next dates ‹ ›
- Switch Thumbnail view and List view
- Zoom In and Zoom Out to accommodate data ⊕
- Select KPIs from Search box

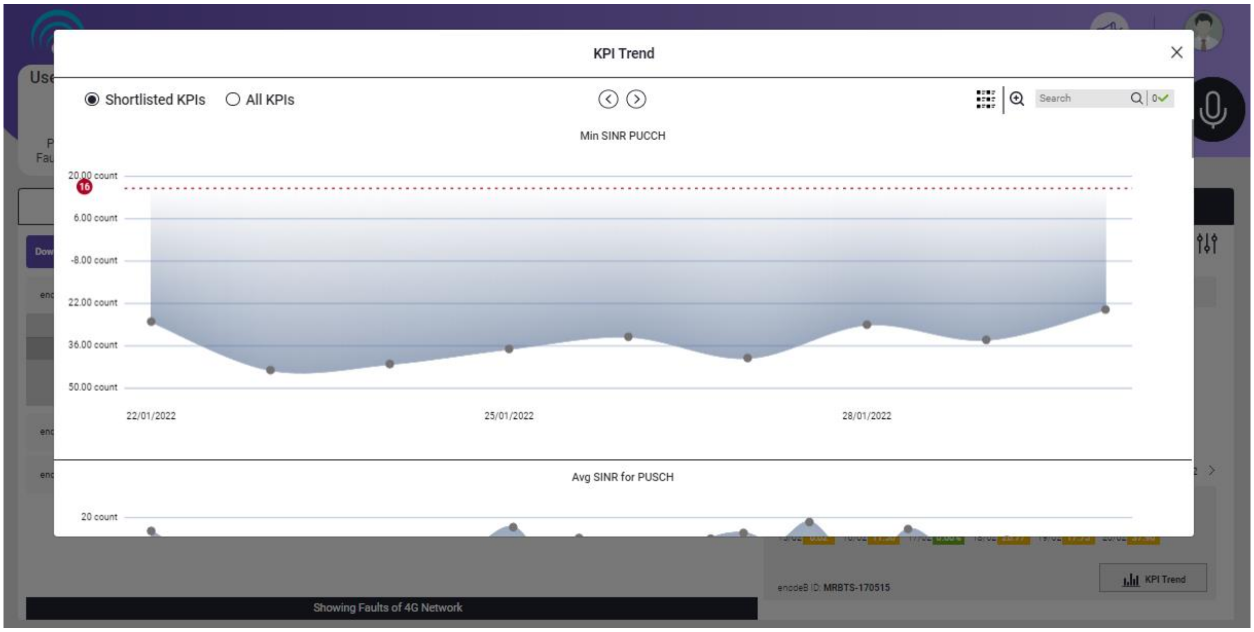
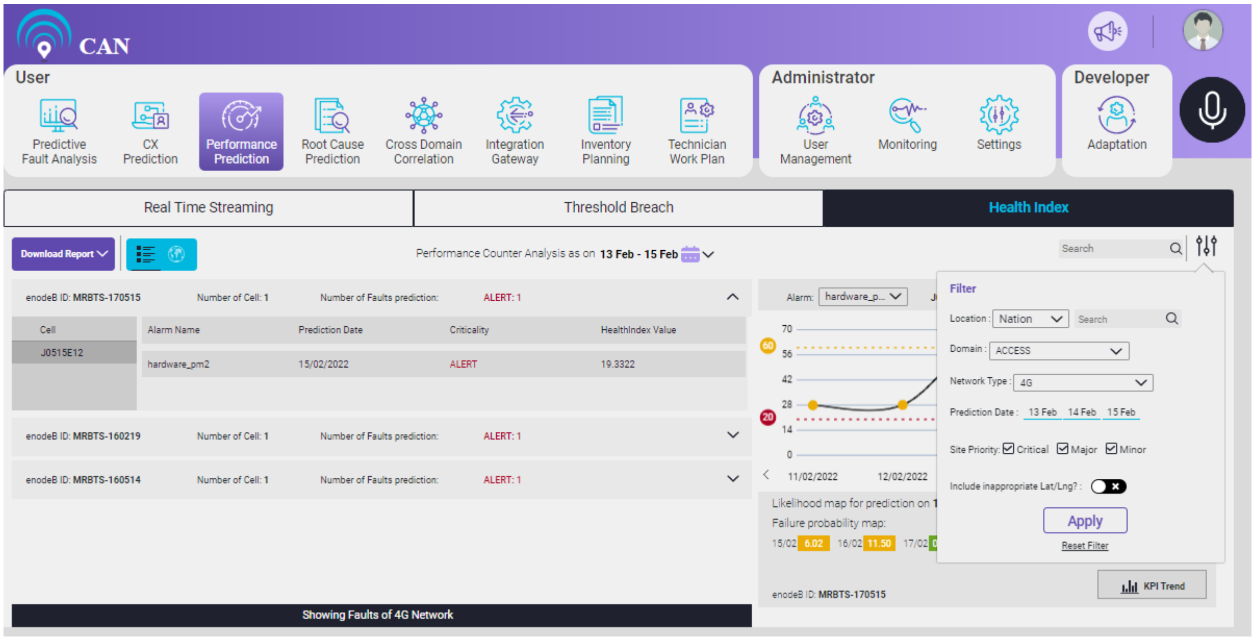


Figure 5.20 – KPI Trend

User has the option to filter Health Analysis based on the following parameters:

1. **Location**: There are multiple location options. (Currently, screen displays two locations i.e. **Nation** and **Region**).
2. **Domain**: There are multiple domains (Currently, screen displays three domains i.e. **Core**, **Transport** and **Access**).
3. **Network Type**: User can select the **Network Type** based on the selected **Domain**.
4. **Prediction Date**: List of dates in the selected week.
5. **Site Priority**: It has three check boxes: Critical, Major and Minor to filter out respective priority sites.
6. **Include Inappropriate Lat/Long**: A toggle button to include or exclude the inappropriate Lat/Long.



Performance Counter Analysis as on **13 Feb - 15 Feb**

enodeB ID: **MRBTS-170515** Number of Cell: **1** Number of Faults prediction: ALERT: 1

Cell	Alarm Name	Prediction Date	Criticality	HealthIndex Value
J0515E12	hardware_pm2	15/02/2022	ALERT	19.3322

enodeB ID: **MRBTS-160219** Number of Cell: **1** Number of Faults prediction: ALERT: 1

enodeB ID: **MRBTS-160514** Number of Cell: **1** Number of Faults prediction: ALERT: 1

Likelihood map for prediction on 1

Failure probability map:

15/02 6.02 16/02 11.50 17/02

enodeB ID: **MRBTS-170515**

Filter

Location : Nation

Domain : ACCESS

Network Type : 4G

Prediction Date : 13 Feb 14 Feb 15 Feb

Site Priority: ☑ Critical ☑ Major ☑ Minor

Include inappropriate Lat/Lng? : ✗

Figure 5.21 - Health Index Filter

Page Intentionally Left Blank

6. ROOT CAUSE PREDICTION

Root Cause Prediction module pinpoints the causes of predicted faults.

The “Operationalisation flow” displays the following information:

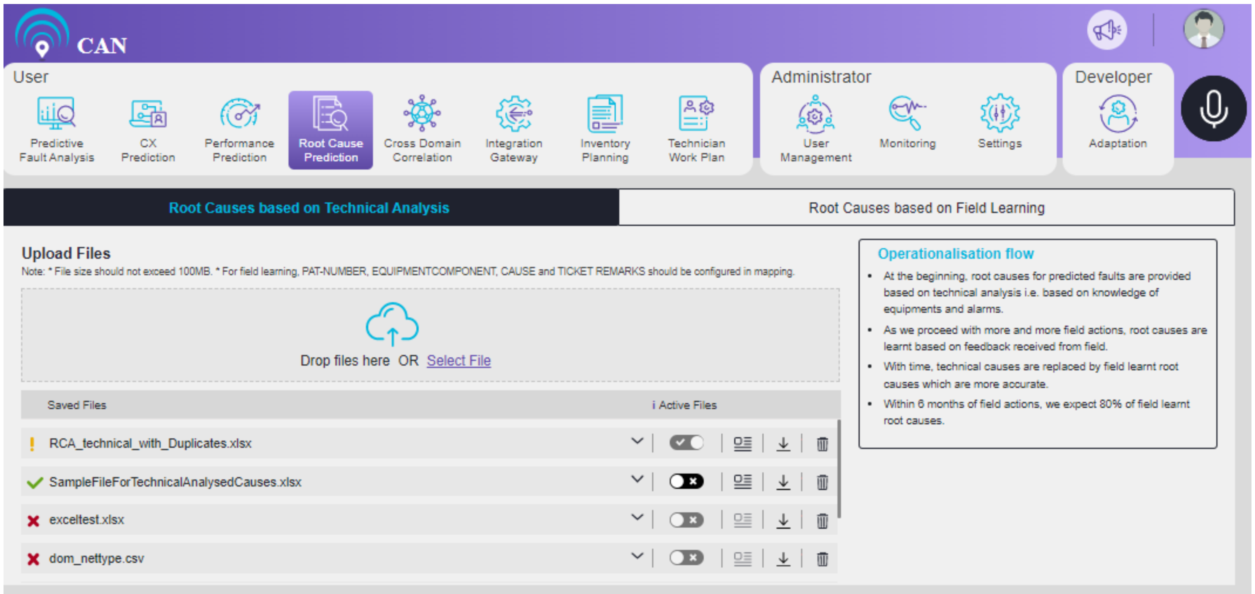
- At the beginning, root causes for predicted faults are provided based on technical analysis i.e. based on knowledge of the equipment and alarms.
- As we proceed with more and more field actions, root causes are learnt based on the feedback received from the field.
- With time, technical causes are 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.



Upload Files

Note: * File size should not exceed 100MB. * For field learning, PAT-NUMBER, EQUIPMENTCOMPONENT, CAUSE and TICKET REMARKS should be configured in mapping.

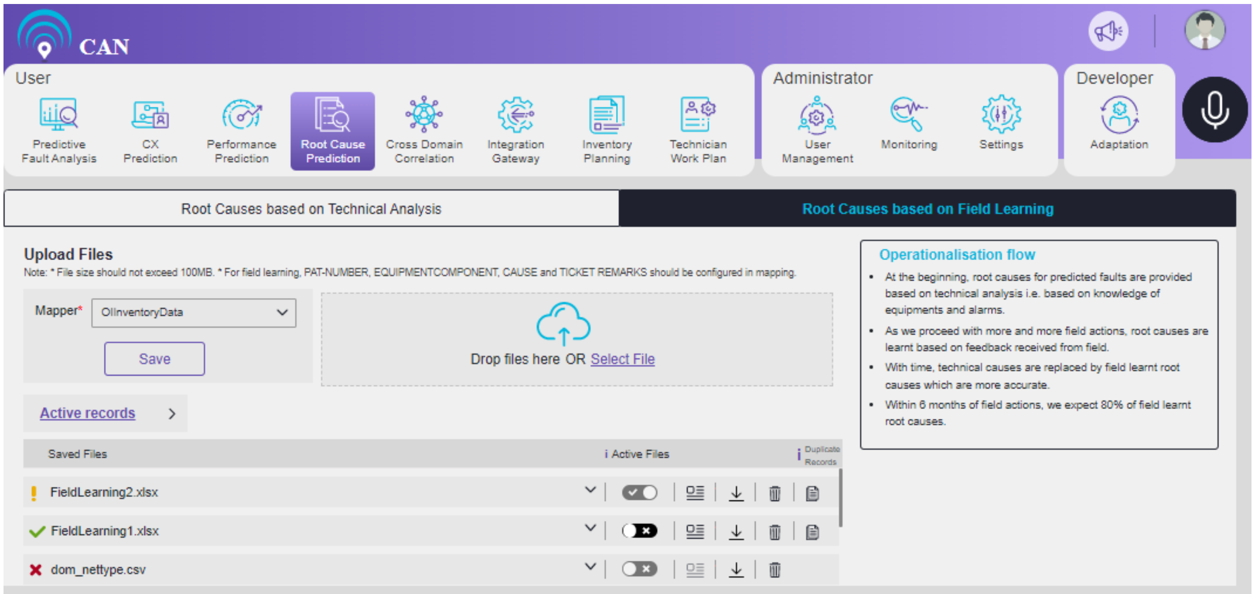
Drop files here OR Select File

Saved Files	i Active Files
! RCA_technical_with_Duplicates.xlsx	✓
✓ SampleFileForTechnicalAnalysedCauses.xlsx	✗
✗ exceltest.xlsx	✗
✗ dom_nettype.csv	✗

Operationalisation flow

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

Figure 6.1 - Root Causes Based on Technical Analysis Tab



Upload Files

Note: * File size should not exceed 100MB. * For field learning, PAT-NUMBER, EQUIPMENTCOMPONENT, CAUSE and TICKET REMARKS should be configured in mapping.

Mapper*: OIInventoryData

Saved Files	i Active Files	i Duplicate Records
! FieldLearning2.xlsx	✓	
✓ FieldLearning1.xlsx	✗	
✗ dom_nettype.csv	✗	

Operationalisation flow

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

Figure 6.2 - Root Causes Based on Field Learning Tab

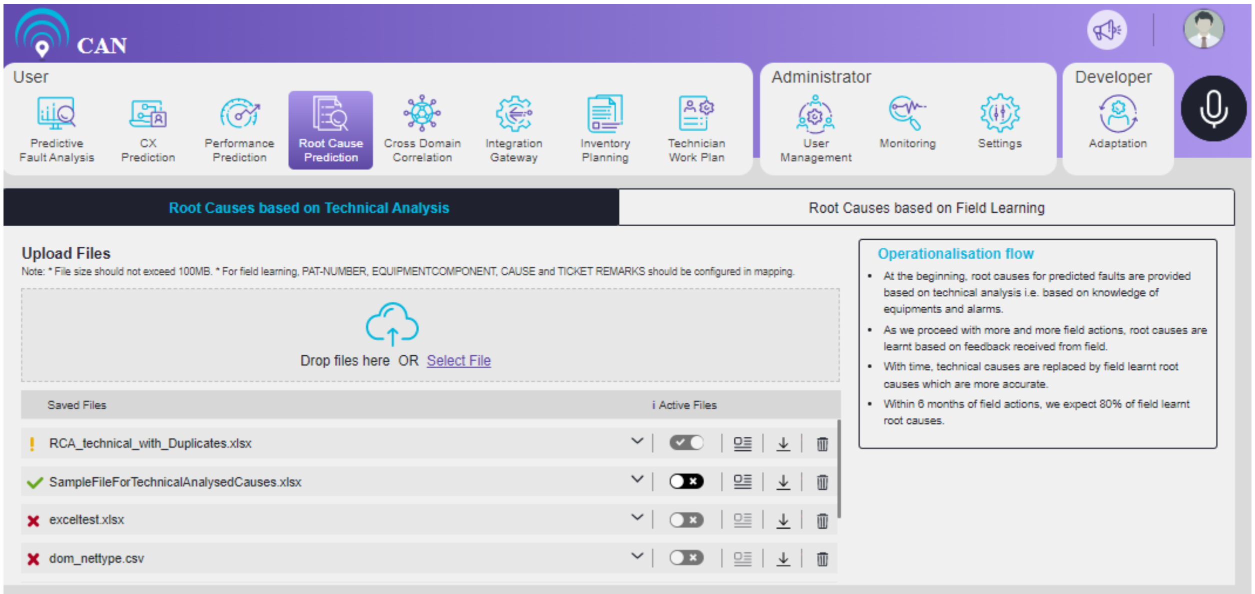
Root Causes Based on Technical Analysis

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.



Upload Files

Note: * File size should not exceed 100MB. * For field learning, PAT-NUMBER, EQUIPMENTCOMPONENT, CAUSE and TICKET REMARKS should be configured in mapping.

! RCA_technical_with_Duplicates.xlsx

✓ SampleFileForTechnicalAnalysedCauses.xlsx

✗ exceltest.xlsx

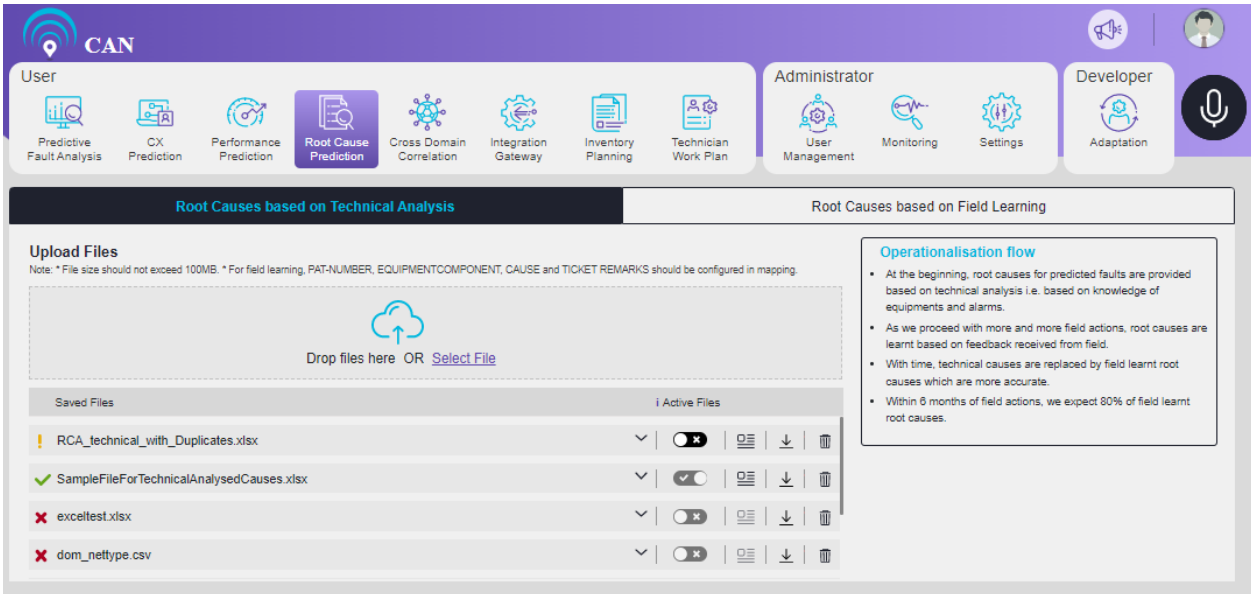
✗ dom_nettype.csv

Operationalisation flow

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

Figure 6.3 - 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.



Upload Files

Note: * File size should not exceed 100MB. * For field learning, PAT-NUMBER, EQUIPMENTCOMPONENT, CAUSE and TICKET REMARKS should be configured in mapping.

! RCA_technical_with_Duplicates.xlsx

✓ SampleFileForTechnicalAnalysedCauses.xlsx

✗ exceltest.xlsx

✗ dom_nettype.csv

Operationalisation flow

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

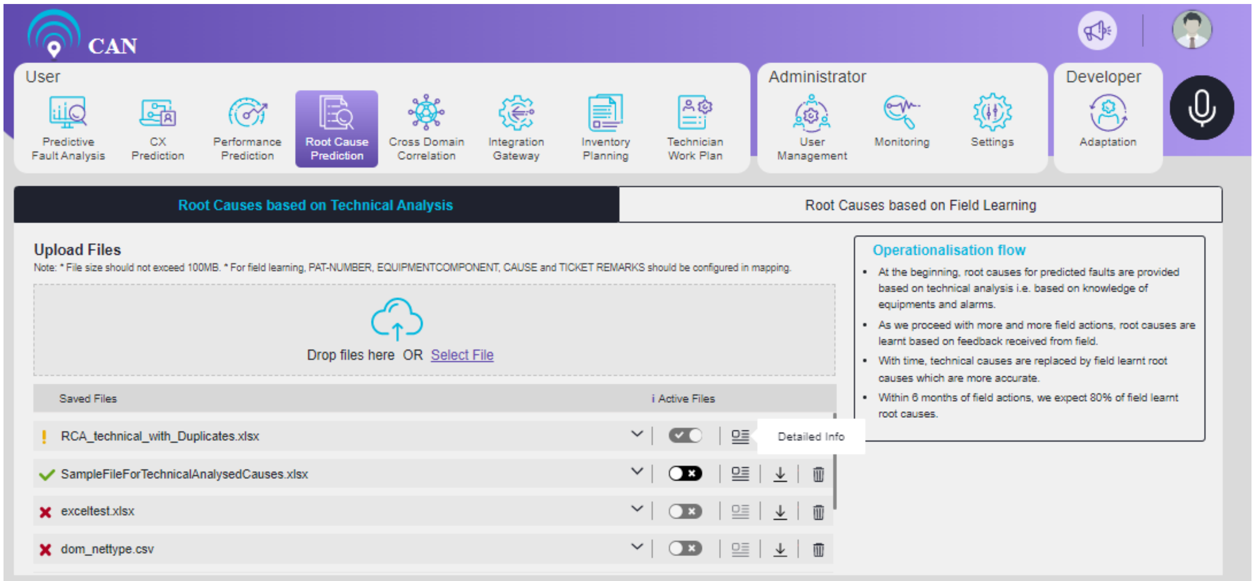
Figure 6.4 - Active against Multiple Files Scenario

- 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. NOC ACTION

5. FIELD ACTION
6. 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.



Root Causes based on Technical Analysis | Root Causes based on Field Learning

Upload Files

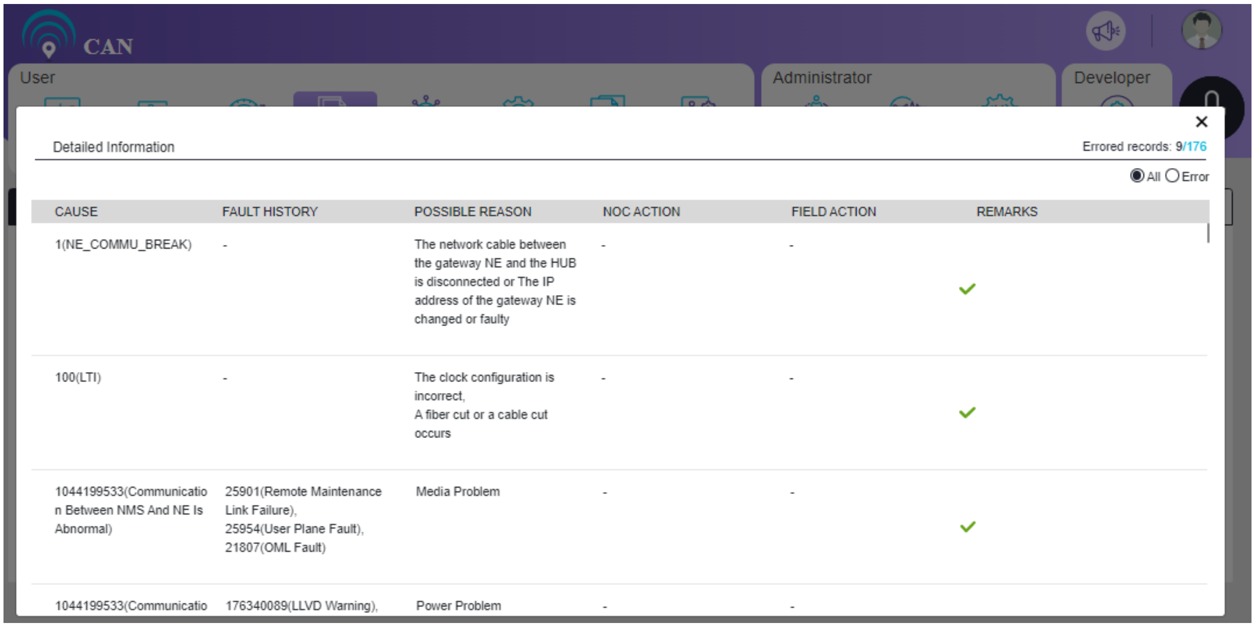
Note: * File size should not exceed 100MB. * For field learning, PAT-NUMBER, EQUIPMENTCOMPONENT, CAUSE and TICKET REMARKS should be configured in mapping.

Operationalisation flow

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

	Saved Files
!	RCA_technical_with_Duplicates.xlsx
✓	SampleFileForTechnicalAnalysedCauses.xlsx
✗	exceltest.xlsx
✗	dom_nettype.csv

Figure 6.5 - Detailed Info Button



Detailed Information

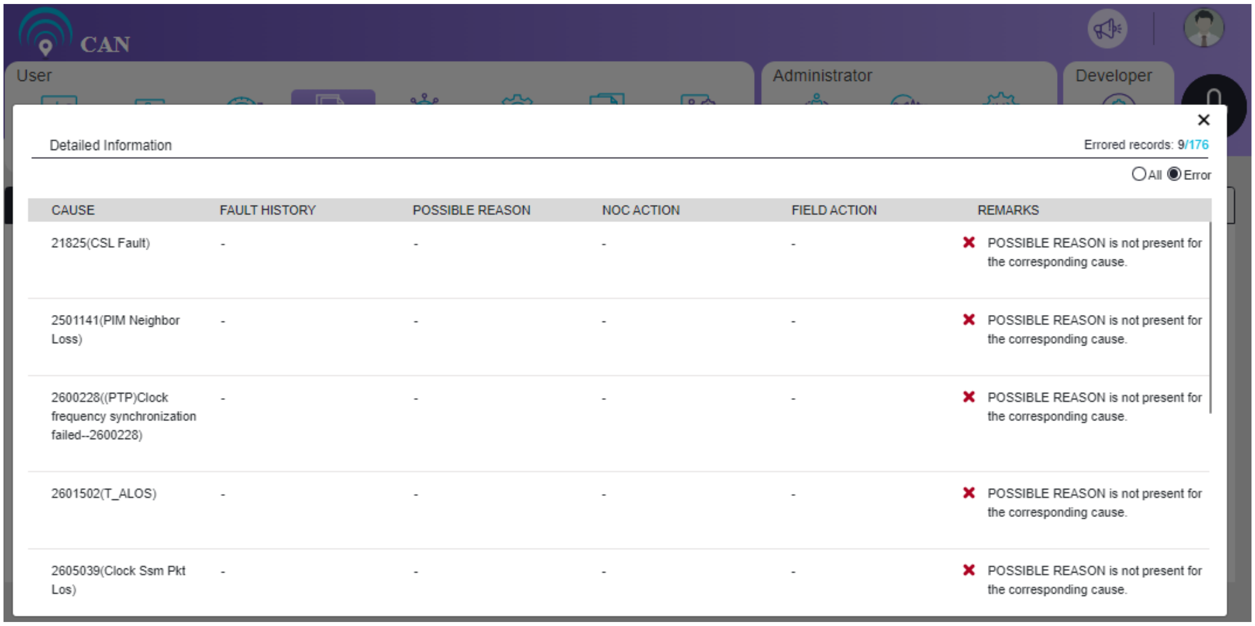
Errored records: 9/176

● All ○ Error

CAUSE	FAULT HISTORY	POSSIBLE REASON	NOC ACTION	FIELD ACTION	REMARKS
1(NE_COMMU_BREAK)	-	The network cable between the gateway NE and the HUB is disconnected or The IP address of the gateway NE is changed or faulty	-	-	✓
100(LTI)	-	The clock configuration is incorrect, A fiber cut or a cable cut occurs	-	-	✓
1044199533(Communication Between NMS And NE Is Abnormal)	25901(Remote Maintenance Link Failure), 25954(User Plane Fault), 21807(OML Fault)	Media Problem	-	-	✓
1044199533(Communicatio	176340089(LLVD Warning),	Power Problem	-	-	

Figure 6.6 - 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.



Detailed Information

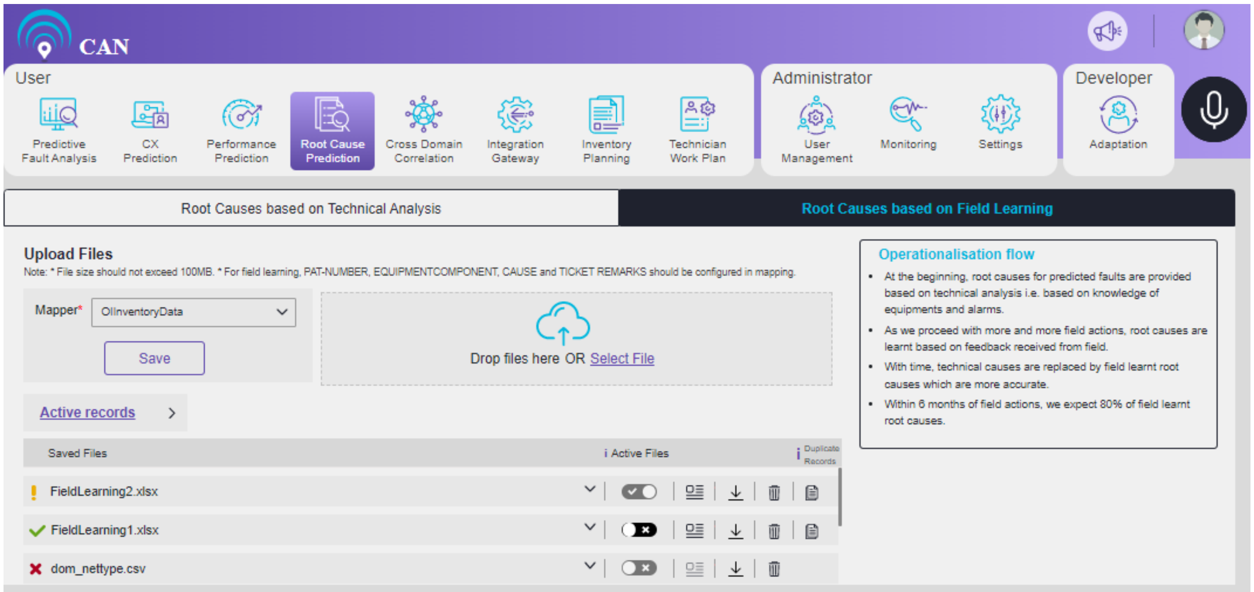
Errored records: 9/176

○All ●Error

CAUSE	FAULT HISTORY	POSSIBLE REASON	NOC ACTION	FIELD ACTION	REMARKS
21825(CSL Fault)	-	-	-	-	✖ POSSIBLE REASON is not present for the corresponding cause.
2501141(PIM Neighbor Loss)	-	-	-	-	✖ POSSIBLE REASON is not present for the corresponding cause.
2600228((PTP)Clock frequency synchronization failed--2600228)	-	-	-	-	✖ POSSIBLE REASON is not present for the corresponding cause.
2601502(T_ALOS)	-	-	-	-	✖ POSSIBLE REASON is not present for the corresponding cause.
2605039(Clock Ssm Pkt Los)	-	-	-	-	✖ POSSIBLE REASON is not present for the corresponding cause.

Figure 6.7 - Error Radio Button Selection and Error Record Sample

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



Upload Files

Note: * File size should not exceed 100MB. * For field learning, PAT-NUMBER, EQUIPMENTCOMPONENT, CAUSE and TICKET REMARKS should be configured in mapping.

Mapper* OIInventoryData

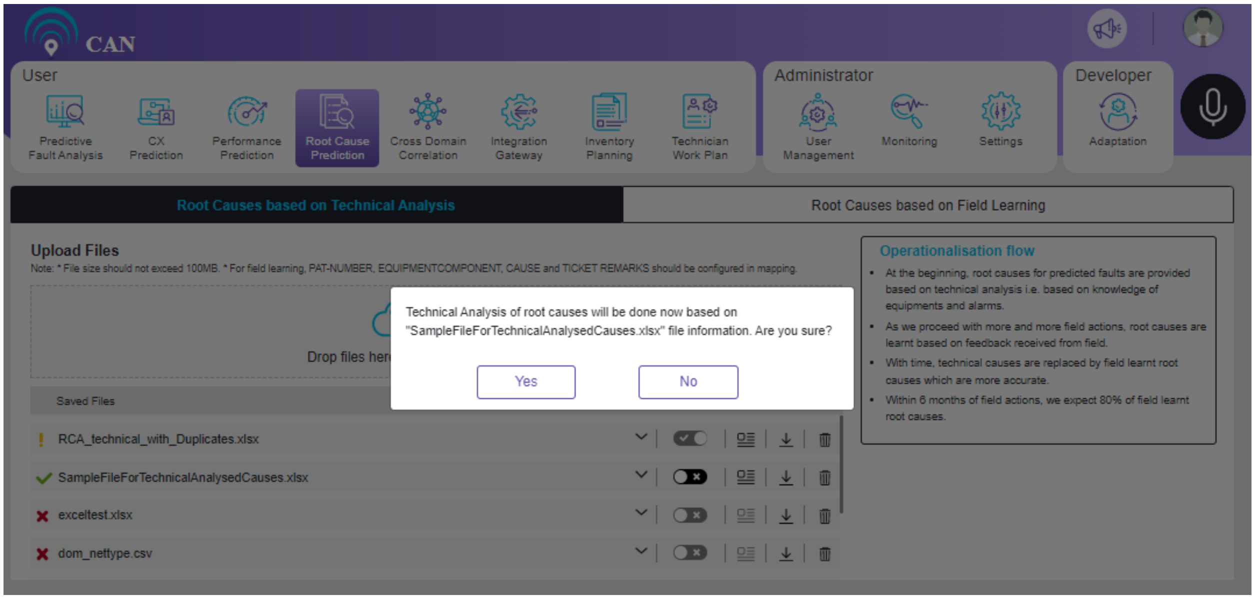
Saved Files	i Active Files	i Duplicate Records
! FieldLearning2.xlsx	✓	
✓ FieldLearning1.xlsx	✖	
✖ dom_nettype.csv	✖	

Operationalisation flow

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

Figure 6.8 - 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.



Root Causes based on Technical Analysis | Root Causes based on Field Learning

Upload Files

Note: * File size should not exceed 100MB. * For field learning, PAT-NUMBER, EQUIPMENTCOMPONENT, CAUSE and TICKET REMARKS should be configured in mapping.

Drop files her

Technical Analysis of root causes will be done now based on "SampleFileForTechnicalAnalysedCauses.xlsx" file information. Are you sure?

Yes No

Saved Files

- ! RCA_technical_with_Duplicates.xlsx
- ✓ SampleFileForTechnicalAnalysedCauses.xlsx
- ✗ exceltest.xlsx
- ✗ dom_nettype.csv

Operationalisation flow

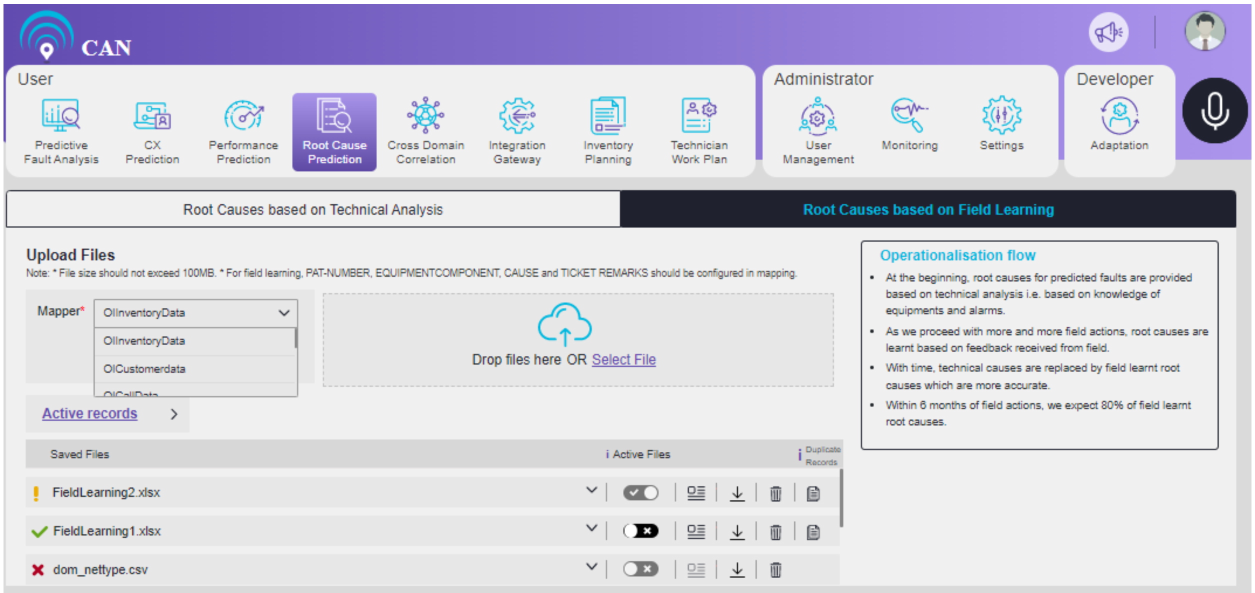
- At the beginning, root causes for predicted faults are provided based on technical analysis i.e. based on knowledge of equipments and alarms.
- As we proceed with more and more field actions, root causes are learnt based on feedback received from field.
- With time, technical causes are replaced by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

Figure 6.9 - 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.



Root Causes based on Technical Analysis | Root Causes based on Field Learning

Upload Files

Note: * File size should not exceed 100MB. * For field learning, PAT-NUMBER, EQUIPMENTCOMPONENT, CAUSE and TICKET REMARKS should be configured in mapping.

Mapper* OlInventoryData

- OlInventoryData
- OlCustomerdata
- OlCallData

Drop files here OR Select File

Active records >

Saved Files | Active Files | Duplicate Records

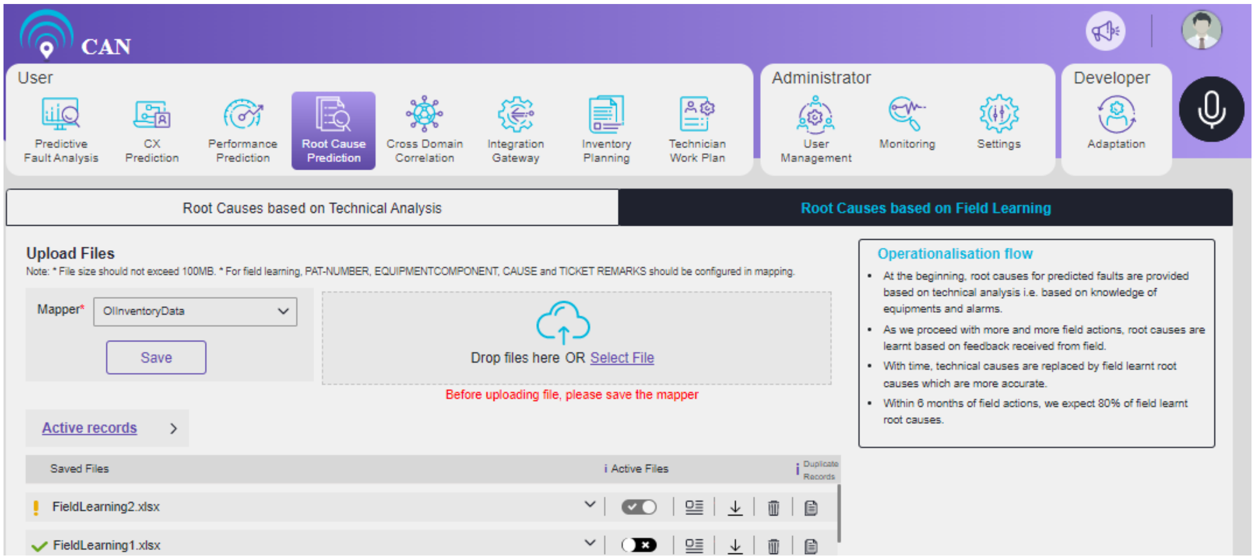
- ! FieldLearning2.xlsx
- ✓ FieldLearning1.xlsx
- ✗ dom_nettype.csv

Operationalisation flow

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

Figure 6.10 - 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.



Upload Files

Note: * File size should not exceed 100MB. * For field learning, PAT-NUMBER, EQUIPMENTCOMPONENT, CAUSE and TICKET REMARKS should be configured in mapping.

Mapper*: OlInventoryData

Before uploading file, please save the mapper

Operationalisation flow

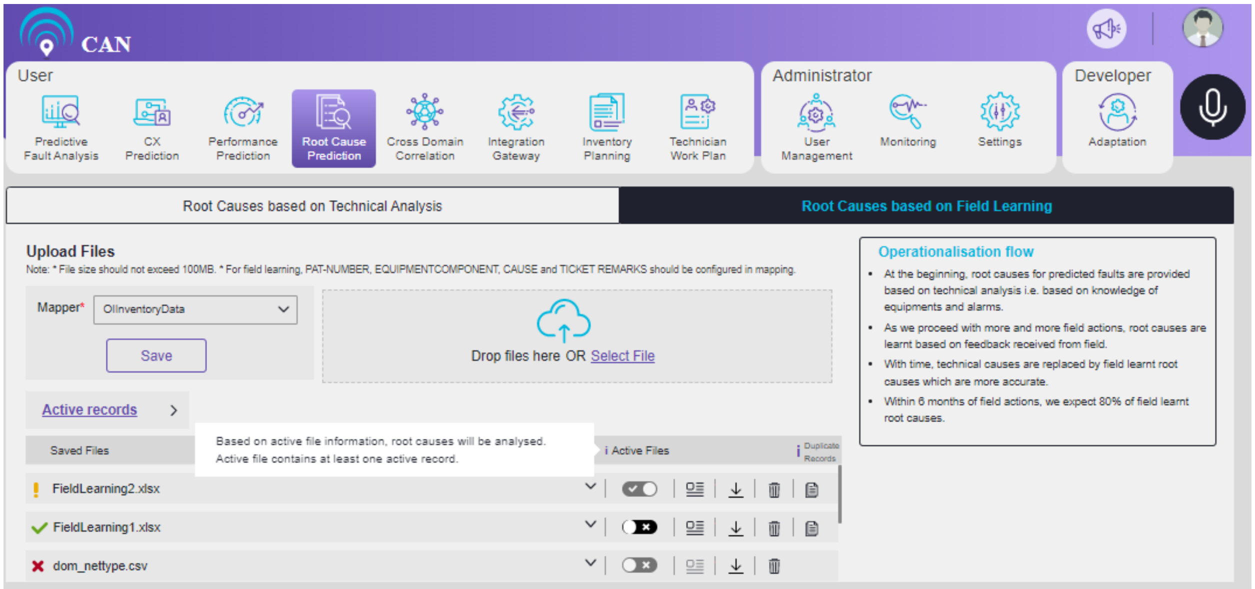
- At the beginning, root causes for predicted faults are provided based on technical analysis i.e. based on knowledge of equipments and alarms.
- As we proceed with more and more field actions, root causes are learnt based on feedback received from field.
- With time, technical causes are replaced by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

FieldLearning2.xlsx

FieldLearning1.xlsx

Figure 6.11 - 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.



Upload Files

Note: * File size should not exceed 100MB. * For field learning, PAT-NUMBER, EQUIPMENTCOMPONENT, CAUSE and TICKET REMARKS should be configured in mapping.

Mapper*: OlInventoryData

Based on active file information, root causes will be analysed.
Active file contains at least one active record.

Operationalisation flow

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

FieldLearning2.xlsx

FieldLearning1.xlsx

dom_nettype.csv

Figure 6.12 - 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

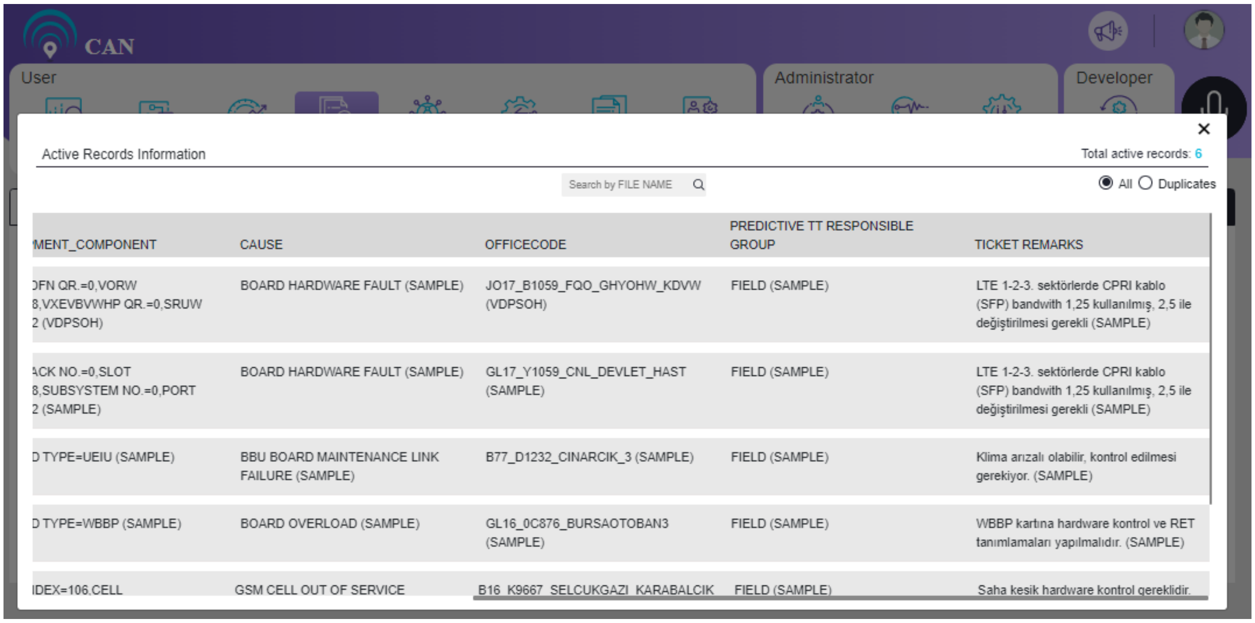
1. DUPLICATE RECORDS
2. FILENAME
3. PAT-NUMBER
4. EQUIPMENT_COMPONENT
5. CAUSE
6. REMARKS

Optional Information

7. OFFICECODE
8. PREDICTIVE TT RESPONSIBLE GROUP
9. TICKET REMARKS

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.



Active Records Information

Total active records: 6

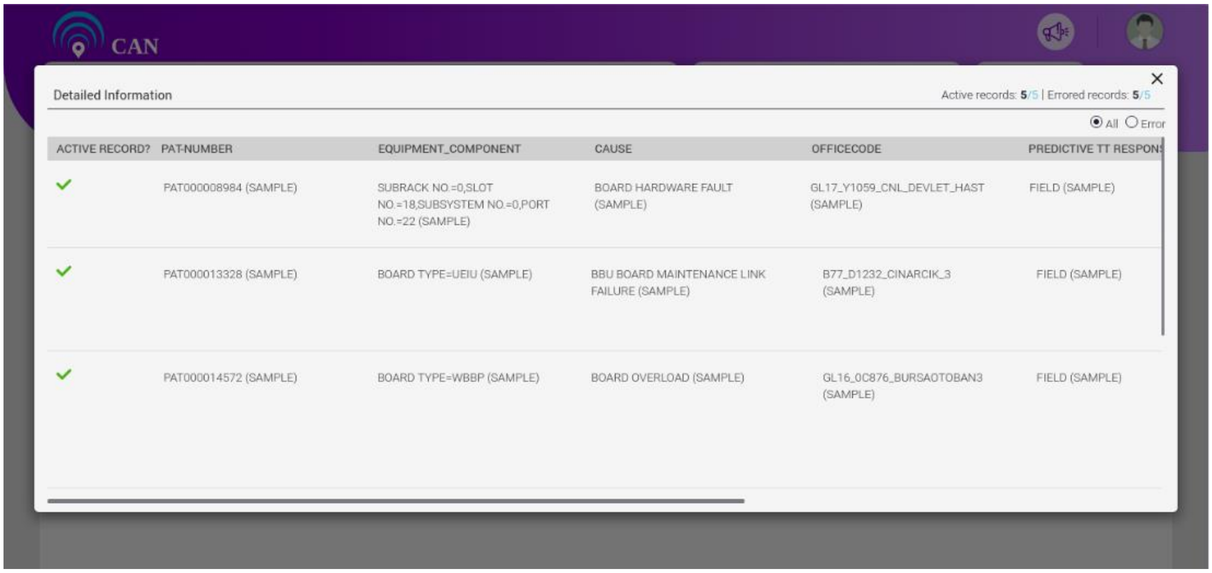
Search by FILE NAME

● All ○ Duplicates

'MENT_COMPONENT	CAUSE	OFFICECODE	PREDICTIVE TT RESPONSIBLE GROUP	TICKET REMARKS
ↄFN QR.=0,VORW 8,VXEVBVWHP QR.=0,SRUW 2 (VDPSOH)	BOARD HARDWARE FAULT (SAMPLE)	JO17_B1059_FQO_GHYOHW_KDVW (VDPSOH)	FIELD (SAMPLE)	LTE 1-2-3. sektörlerde CPRI kablo (SFP) bandwith 1,25 kullanılmış, 2,5 ile değiştirilmesi gerekli (SAMPLE)
ACK NO.=0,SLOT 8,SUBSYSTEM NO.=0,PORT 2 (SAMPLE)	BOARD HARDWARE FAULT (SAMPLE)	GL17_Y1059_CNL_DEVLET_HAST (SAMPLE)	FIELD (SAMPLE)	LTE 1-2-3. sektörlerde CPRI kablo (SFP) bandwith 1,25 kullanılmış, 2,5 ile değiştirilmesi gerekli (SAMPLE)
D TYPE=UEIU (SAMPLE)	BBU BOARD MAINTENANCE LINK FAILURE (SAMPLE)	B77_D1232_CINARCIK_3 (SAMPLE)	FIELD (SAMPLE)	Klima arızalı olabilir, kontrol edilmesi gerekiyor. (SAMPLE)
D TYPE=WBBP (SAMPLE)	BOARD OVERLOAD (SAMPLE)	GL16_0C876_BURSAOTOBAN3 (SAMPLE)	FIELD (SAMPLE)	WBBP kartına hardware kontrol ve RET tanımlamaları yapılmalıdır. (SAMPLE)
IDEX=106.CELL	GSM CELL OUT OF SERVICE	B16_K9667_SELCUKGAZI_KARABALCIK	FIELD (SAMPLE)	Saha kesik hardware kontrol gereklidir.

Figure 6.13 - 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.



Detailed Information

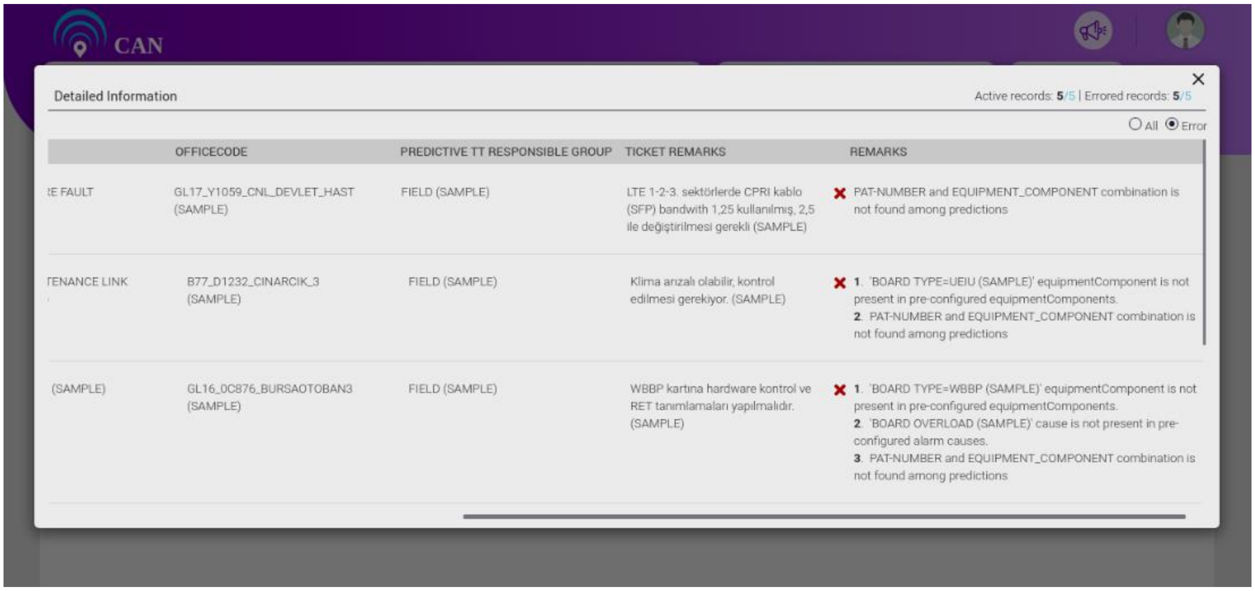
Active records: 5/5 | Errored records: 5/5

● All ○ Error

ACTIVE RECORD?	PAT-NUMBER	EQUIPMENT_COMPONENT	CAUSE	OFFICECODE	PREDICTIVE TT RESPON
✓	PAT000008984 (SAMPLE)	SUBRACK NO.=0,SLOT NO.=18,SUBSYSTEM NO.=0,PORT NO.=22 (SAMPLE)	BOARD HARDWARE FAULT (SAMPLE)	GL17_Y1059_CNL_DEVLET_HAST (SAMPLE)	FIELD (SAMPLE)
✓	PAT000013328 (SAMPLE)	BOARD TYPE=UEIU (SAMPLE)	BBU BOARD MAINTENANCE LINK FAILURE (SAMPLE)	B77_D1232_CINARCIK_3 (SAMPLE)	FIELD (SAMPLE)
✓	PAT000014572 (SAMPLE)	BOARD TYPE=WBBP (SAMPLE)	BOARD OVERLOAD (SAMPLE)	GL16_0C876_BURSAOTOBAN3 (SAMPLE)	FIELD (SAMPLE)

Figure 6.14 - 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.



Detailed Information

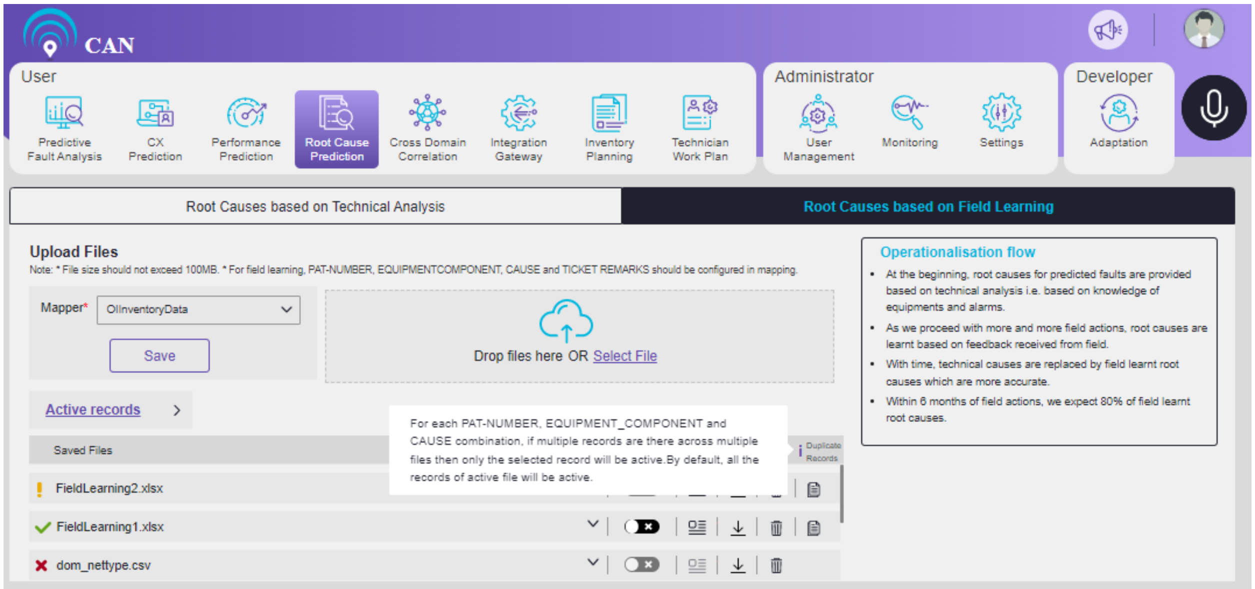
Active records: 5/5 | Errored records: 5/5

○ All ● Error

	OFFICECODE	PREDICTIVE TT RESPONSIBLE GROUP	TICKET REMARKS	REMARKS
E FAULT	GL17_Y1059_CNL_DEVLET_HAST (SAMPLE)	FIELD (SAMPLE)	LTE 1-2-3. sektörlerde CPRI kablo (SFP) bandwith 1,25 kullanılmış, 2,5 ile değiştirilmesi gerekli (SAMPLE)	✗ PAT-NUMBER and EQUIPMENT_COMPONENT combination is not found among predictions
TENANCE LINK	B77_D1232_CINARCIK_3 (SAMPLE)	FIELD (SAMPLE)	Klima arızalı olabilir, kontrol edilmesi gerekiyor. (SAMPLE)	✗ **1**. 'BOARD TYPE=UEIU (SAMPLE)' equipmentComponent is not present in pre-configured equipmentComponents. **2**. PAT-NUMBER and EQUIPMENT_COMPONENT combination is not found among predictions
(SAMPLE)	GL16_0C876_BURSAOTOBAN3 (SAMPLE)	FIELD (SAMPLE)	WBBP kartına hardware kontrol ve RET tanımlamaları yapılmalıdır. (SAMPLE)	✗ **1**. 'BOARD TYPE=WBBP (SAMPLE)' equipmentComponent is not present in pre-configured equipmentComponents. **2**. 'BOARD OVERLOAD (SAMPLE)' cause is not present in pre-configured alarm causes. **3**. PAT-NUMBER and EQUIPMENT_COMPONENT combination is not found among predictions

Figure 6.15 - 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.



Root Causes based on Technical Analysis | Root Causes based on Field Learning

Upload Files

Note: * File size should not exceed 100MB. * For field learning, PAT-NUMBER, EQUIPMENTCOMPONENT, CAUSE and TICKET REMARKS should be configured in mapping.

Mapper* OIInventoryData

Save

Drop files here OR Select File

Active records

Saved Files

For each PAT-NUMBER, EQUIPMENT_COMPONENT and CAUSE combination, if multiple records are there across multiple files then only the selected record will be active.By default, all the records of active file will be active.

Duplicate Records

FieldLearning2.xlsx

FieldLearning1.xlsx

dom_nettype.csv

Operationalisation flow

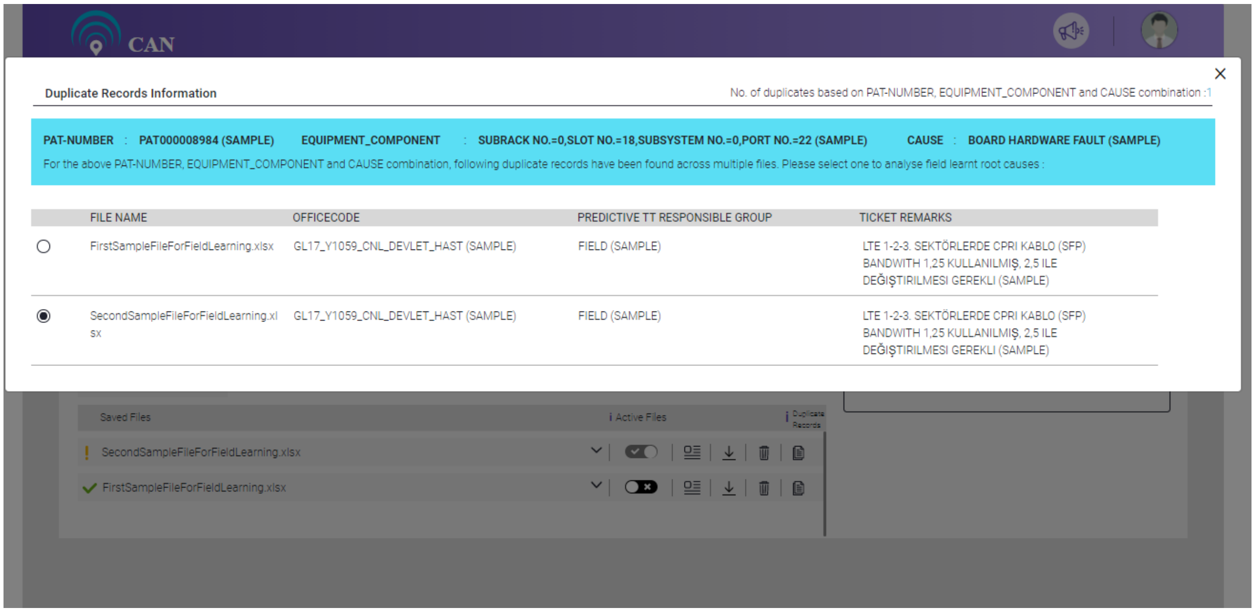
- At the beginning, root causes for predicted faults are provided based on technical analysis i.e. based on knowledge of equipments and alarms.
- As we proceed with more and more field actions, root causes are learnt based on feedback received from field.
- With time, technical causes are replaced by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

Figure 6.16 - 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.



Duplicate Records Information

No. of duplicates based on PAT-NUMBER, EQUIPMENT_COMPONENT and CAUSE combination :1

PAT-NUMBER : PAT000008984 (SAMPLE) EQUIPMENT_COMPONENT : SUBRACK NO.=0,SLOT NO.=18,SUBSYSTEM NO.=0,PORT NO.=22 (SAMPLE) CAUSE : BOARD HARDWARE FAULT (SAMPLE)

For the above PAT-NUMBER, EQUIPMENT_COMPONENT and CAUSE combination, following duplicate records have been found across multiple files. Please select one to analyse field learnt root causes :

	FILE NAME	OFFICECODE	PREDICTIVE TT RESPONSIBLE GROUP	TICKET REMARKS
○	FirstSampleFileForFieldLearning.xlsx	GL17_Y1059_CNL_DEVLET_HAST (SAMPLE)	FIELD (SAMPLE)	LTE 1-2-3. SEKTÖRLERDE CPRI KABLO (SFP) BANDWITH 1,25 KULLANILMIŞ, 2,5 ILE DEĞIŞTIRILMESI GEREKLI (SAMPLE)
●	SecondSampleFileForFieldLearning.xlsx	GL17_Y1059_CNL_DEVLET_HAST (SAMPLE)	FIELD (SAMPLE)	LTE 1-2-3. SEKTÖRLERDE CPRI KABLO (SFP) BANDWITH 1,25 KULLANILMIŞ, 2,5 ILE DEĞIŞTIRILMESI GEREKLI (SAMPLE)

Saved Files

Active Files

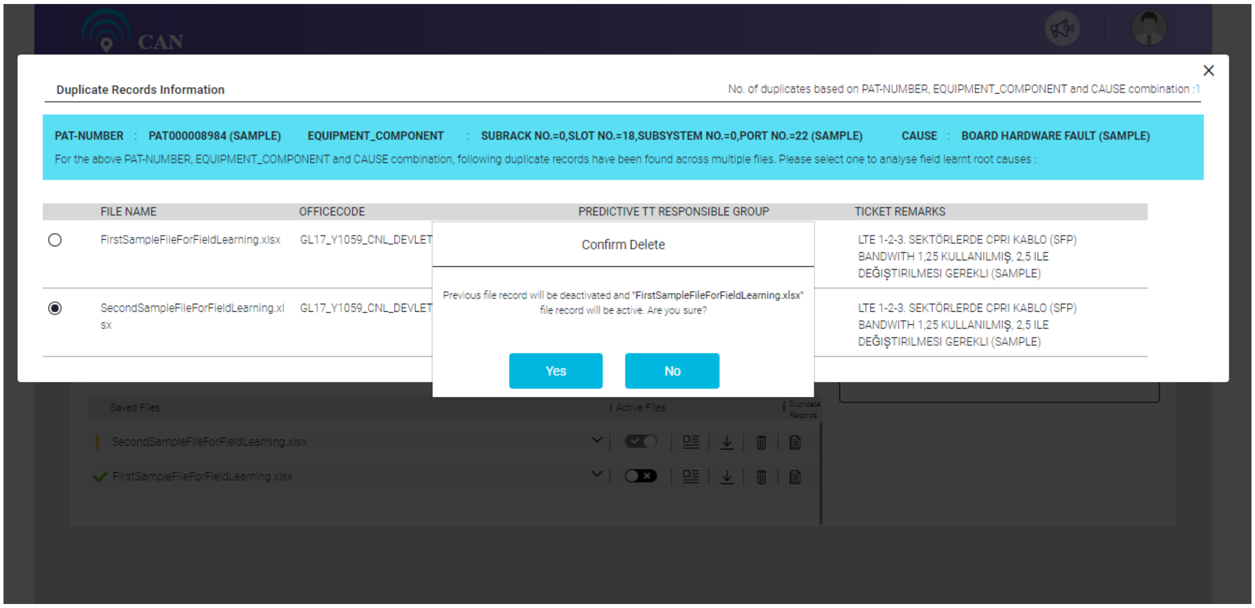
Duplicate Records

SecondSampleFileForFieldLearning.xlsx

FirstSampleFileForFieldLearning.xlsx

Figure 6.17 - 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.



Duplicate Records Information

No. of duplicates based on PAT-NUMBER, EQUIPMENT_COMPONENT and CAUSE combination :1

PAT-NUMBER : PAT000008984 (SAMPLE) EQUIPMENT_COMPONENT : SUBRACK NO.=0,SLOT NO.=18,SUBSYSTEM NO.=0,PORT NO.=22 (SAMPLE) CAUSE : BOARD HARDWARE FAULT (SAMPLE)

For the above PAT-NUMBER, EQUIPMENT_COMPONENT and CAUSE combination, following duplicate records have been found across multiple files. Please select one to analyse field learnt root causes :

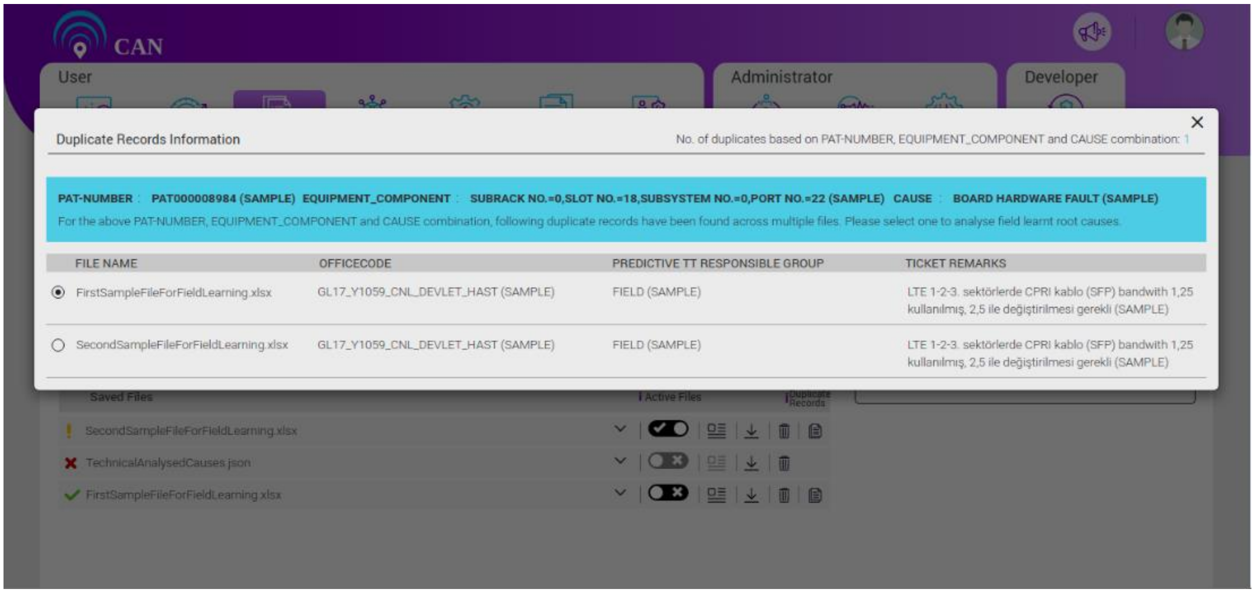
	FILE NAME	OFFICECODE	PREDICTIVE TT RESPONSIBLE GROUP	TICKET REMARKS
○	FirstSampleFileForFieldLearning.xlsx	GL17_Y1059_CNL_DEVLET		LTE 1-2-3. SEKTÖRLERDE CPRI KABLO (SFP) BANDWITH 1,25 KULLANILMIŞ, 2,5 ILE DEĞİŞTIRILMESI GEREKLI (SAMPLE)
●	SecondSampleFileForFieldLearning.xlsx	GL17_Y1059_CNL_DEVLET		LTE 1-2-3. SEKTÖRLERDE CPRI KABLO (SFP) BANDWITH 1,25 KULLANILMIŞ, 2,5 ILE DEĞİŞTIRILMESI GEREKLI (SAMPLE)

Confirm Delete

Previous file record will be deactivated and "FirstSampleFileForFieldLearning.xlsx" file record will be active. Are you sure?

CAN
Yes
No
Saved Files
Active Files
Duplicate Records
SecondSampleFileForFieldLearning.xlsx
FirstSampleFileForFieldLearning.xlsx

Figure 6.18 - Select the Other File Record



Duplicate Records Information

No. of duplicates based on PAT-NUMBER, EQUIPMENT_COMPONENT and CAUSE combination: 1

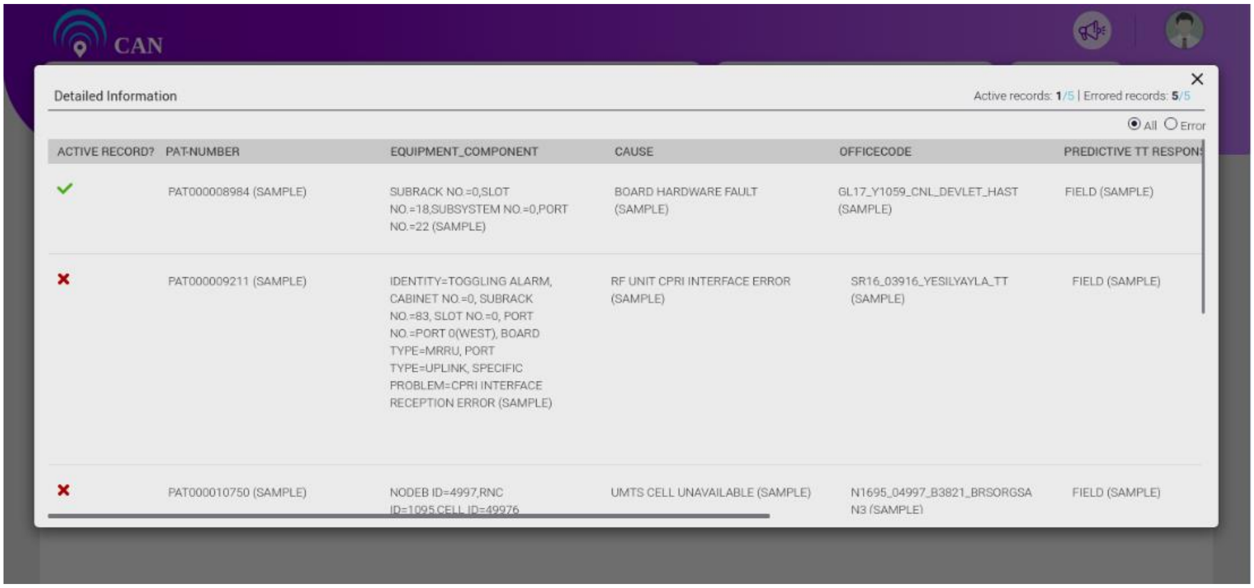
PAT-NUMBER : PAT000008984 (SAMPLE) EQUIPMENT_COMPONENT : SUBRACK NO.=0,SLOT NO.=18,SUBSYSTEM NO.=0,PORT NO.=22 (SAMPLE) CAUSE : BOARD HARDWARE FAULT (SAMPLE)

For the above PAT-NUMBER, EQUIPMENT_COMPONENT and CAUSE combination, following duplicate records have been found across multiple files. Please select one to analyse field learnt root causes.

	FILE NAME	OFFICECODE	PREDICTIVE TT RESPONSIBLE GROUP	TICKET REMARKS
●	FirstSampleFileForFieldLearning.xlsx	GL17_Y1059_CNL_DEVLET_HAST (SAMPLE)	FIELD (SAMPLE)	LTE 1-2-3. sektörlerde CPRI kablo (SFP) bandwith 1,25 kullanılmış, 2,5 ile değiştirilmesi gerekli (SAMPLE)
○	SecondSampleFileForFieldLearning.xlsx	GL17_Y1059_CNL_DEVLET_HAST (SAMPLE)	FIELD (SAMPLE)	LTE 1-2-3. sektörlerde CPRI kablo (SFP) bandwith 1,25 kullanılmış, 2,5 ile değiştirilmesi gerekli (SAMPLE)

CAN
User
Administrator
Developer
Saved Files
Active Files
Duplicate Records
SecondSampleFileForFieldLearning.xlsx
TechnicalAnalysedCauses.json
FirstSampleFileForFieldLearning.xlsx

Figure 6.19 - Duplicate Record Verification



Detailed Information

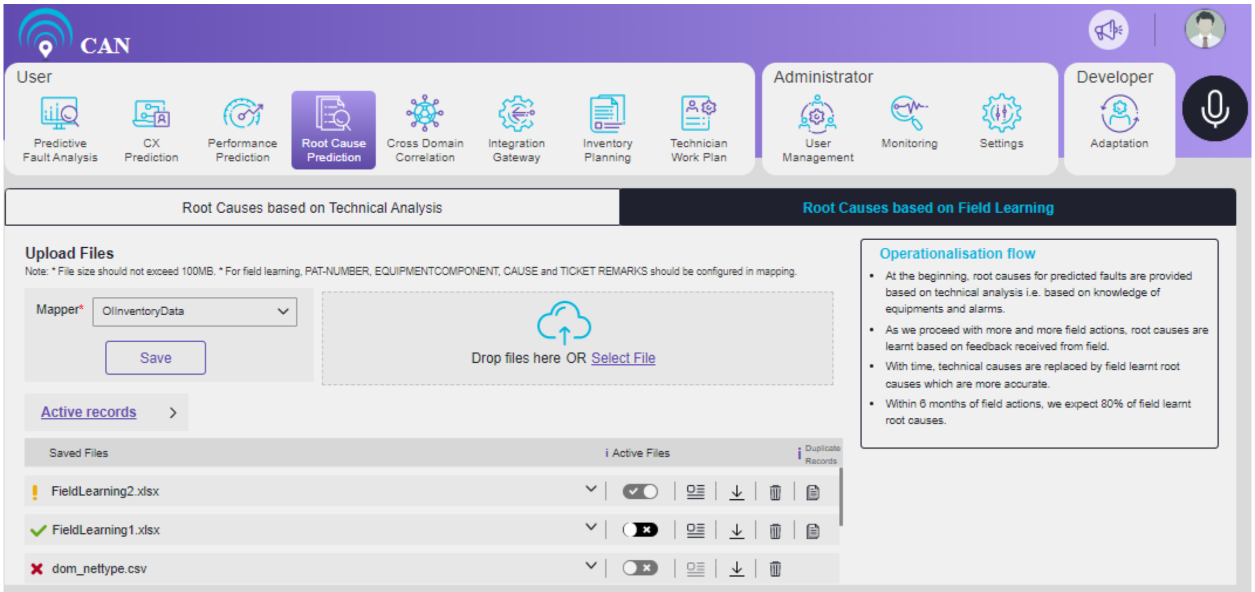
Active records: 1/5 | Errored records: 5/5

● All ○ Error

ACTIVE RECORD?	PAT-NUMBER	EQUIPMENT_COMPONENT	CAUSE	OFFICECODE	PREDICTIVE TT RESPON
✓	PAT000008984 (SAMPLE)	SUBRACK NO.=0,SLOT NO.=18,SUBSYSTEM NO.=0,PORT NO.=22 (SAMPLE)	BOARD HARDWARE FAULT (SAMPLE)	GL17_Y1059_CNL_DEVLET_HAST (SAMPLE)	FIELD (SAMPLE)
✗	PAT000009211 (SAMPLE)	IDENTITY=TOGGLING ALARM, CABINET NO.=0, SUBRACK NO.=83, SLOT NO.=0, PORT NO.=PORT 0(WEST), BOARD TYPE=MRRU, PORT TYPE=UPLINK, SPECIFIC PROBLEM=CPRI INTERFACE RECEPTION ERROR (SAMPLE)	RF UNIT CPRI INTERFACE ERROR (SAMPLE)	SR16_03916_YESILYAYLA_TT (SAMPLE)	FIELD (SAMPLE)
✗	PAT000010750 (SAMPLE)	NODEB ID=4997,RNC ID=1095,CELL ID=49976	UMTS CELL UNAVAILABLE (SAMPLE)	N1695_04997_B3821_BRSORGSA N3 (SAMPLE)	FIELD (SAMPLE)

Figure 6.20 - 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.



Upload Files

Note: * File size should not exceed 100MB. * For field learning, PAT-NUMBER, EQUIPMENTCOMPONENT, CAUSE and TICKET REMARKS should be configured in mapping.

Mapper*: OIInventoryData

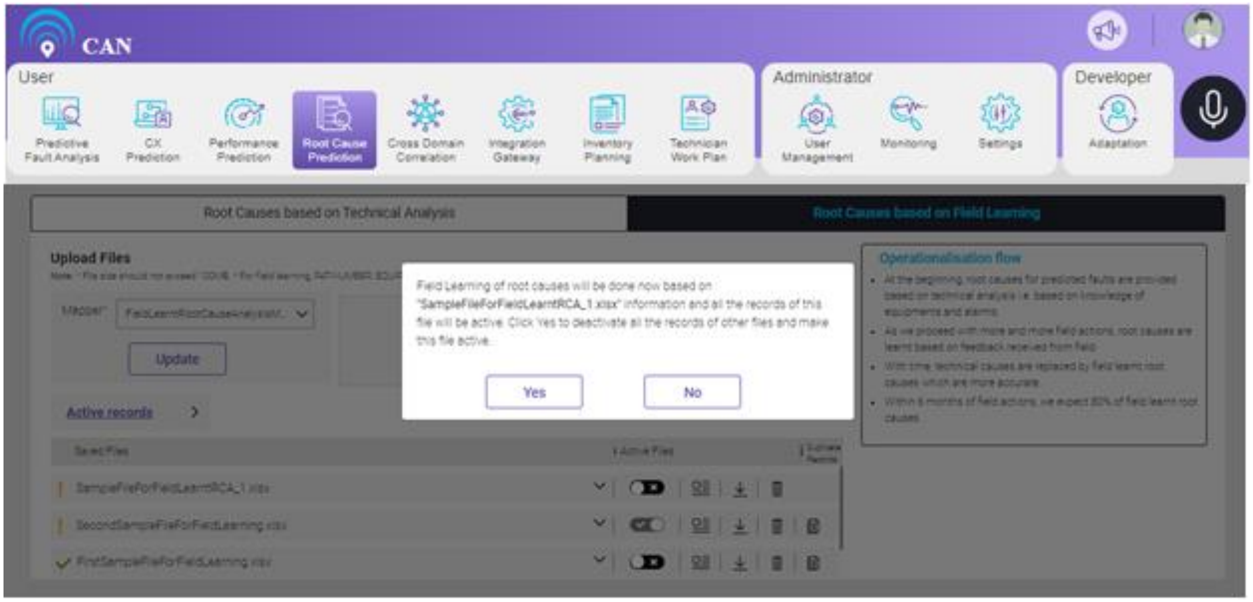
Saved Files	Active Files	Duplicate Records
! FieldLearning2.xlsx	✓	
✓ FieldLearning1.xlsx	✗	
✗ dom_nettype.csv	✗	

Operationalisation flow

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

Figure 6.21 - 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.



Field Learning of root causes will be done now based on "SampleFileForFieldLearntRCA_1.xlsx" information and all the records of this file will be active. Click Yes to deactivate all the records of other files and make this file active.

Mapper*: FieldLearntRootCauseAnalysisM...

Operationalisation flow

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

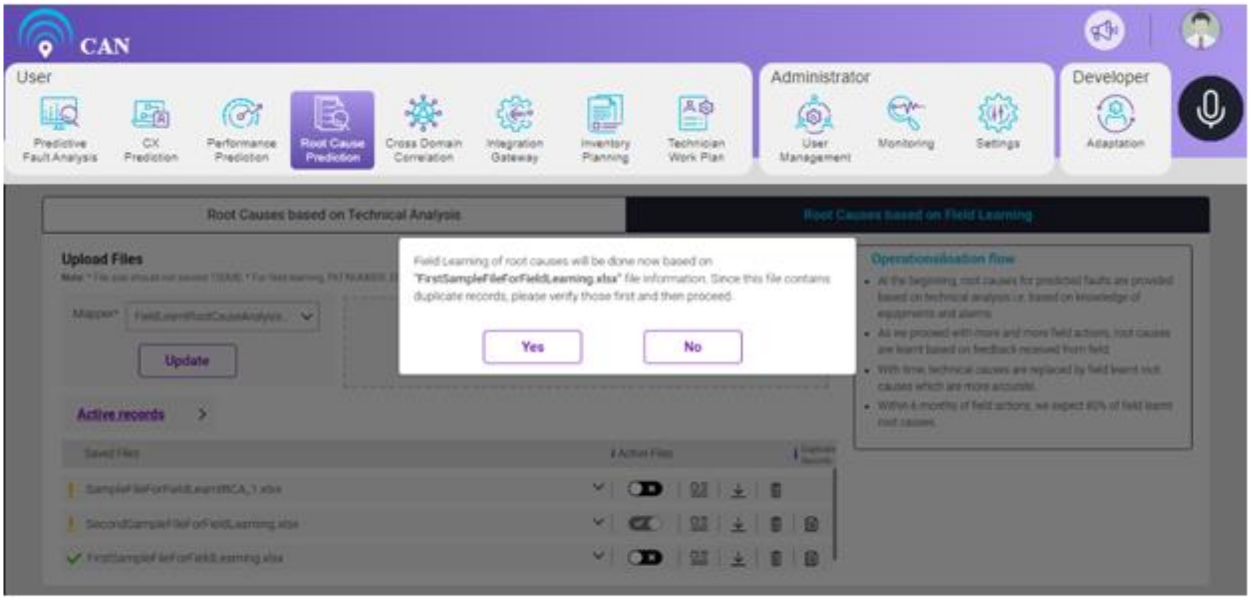
SampleFileForFieldLearntRCA_1.xlsx

SecondSampleFileForFieldLearning.xlsx

FirstSampleFileForFieldLearning.xlsx

Figure 6.22 - 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**.**



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.

Mapper*: FieldLearntRootCauseAnalysis...

Operationalisation flow

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

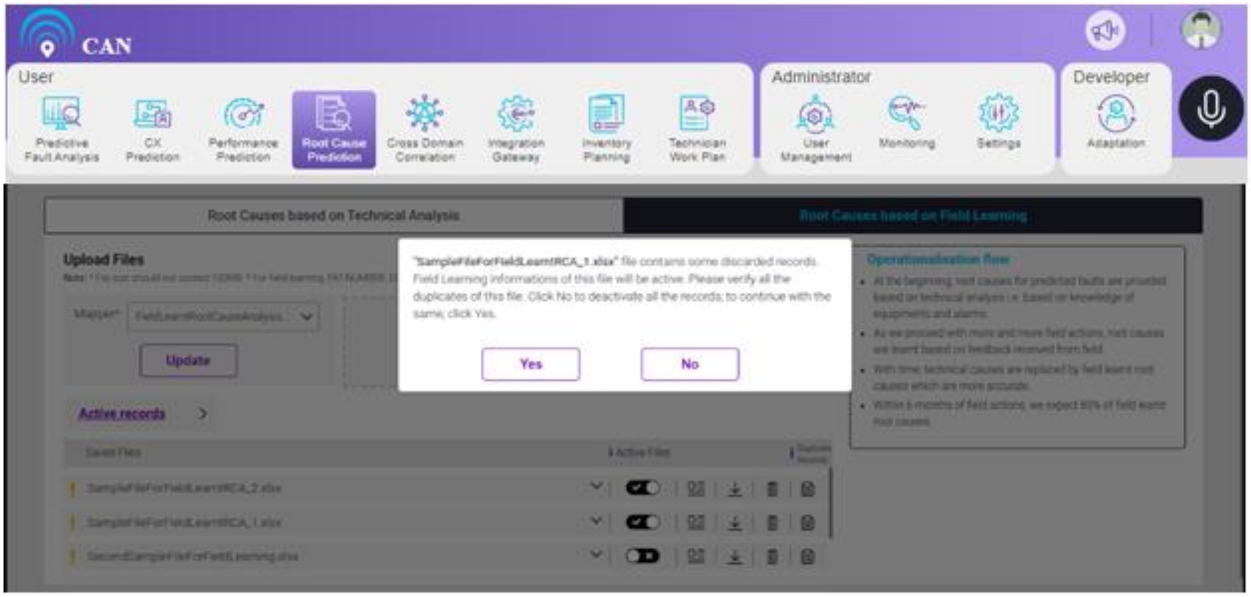
SampleFileForFieldLearntRCA_1.xlsx

SecondSampleFileForFieldLearning.xlsx

FirstSampleFileForFieldLearning.xlsx

Figure 6.23 - 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.



"SampleFileForFieldLearntRCA_1.xlsx" file contains some discarded records. Field Learning informations of this file will be active. Please verify all the duplicates of this file. Click No to deactivate all the records; to continue with the same, click Yes.

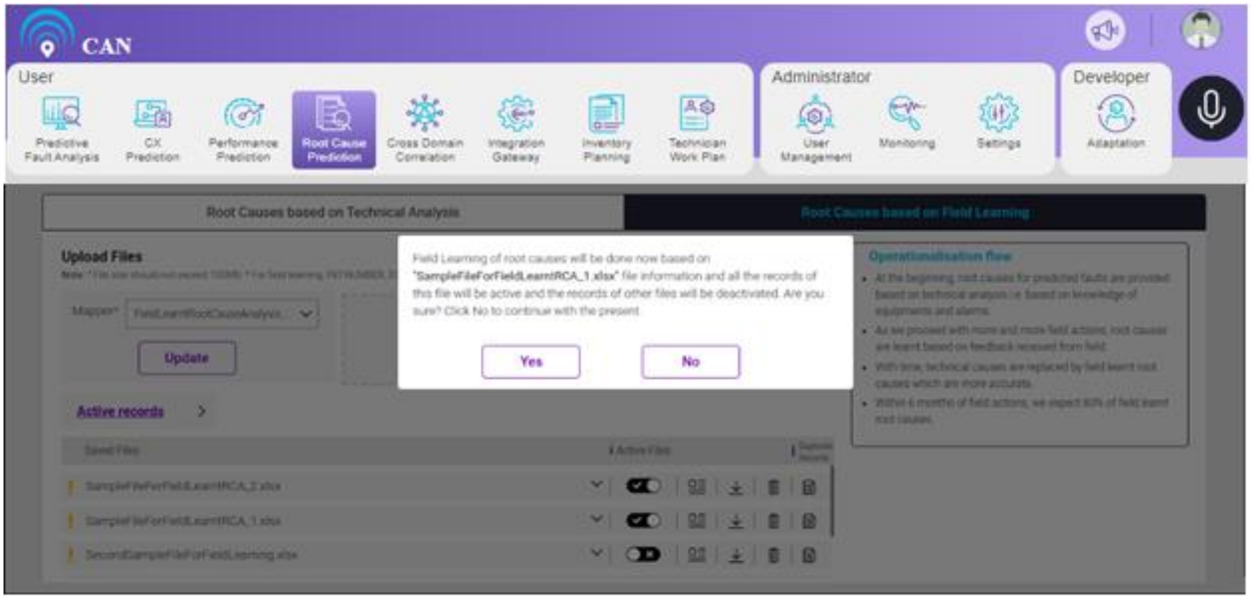
Yes No

Operationalisation flow

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

Figure 6.24 - 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).



Field Learning of root causes will be done now based on "SampleFileForFieldLearntRCA_1.xlsx" file information and all the records of this file will be active and the records of other files will be deactivated. Are you sure? Click No to continue with the present.

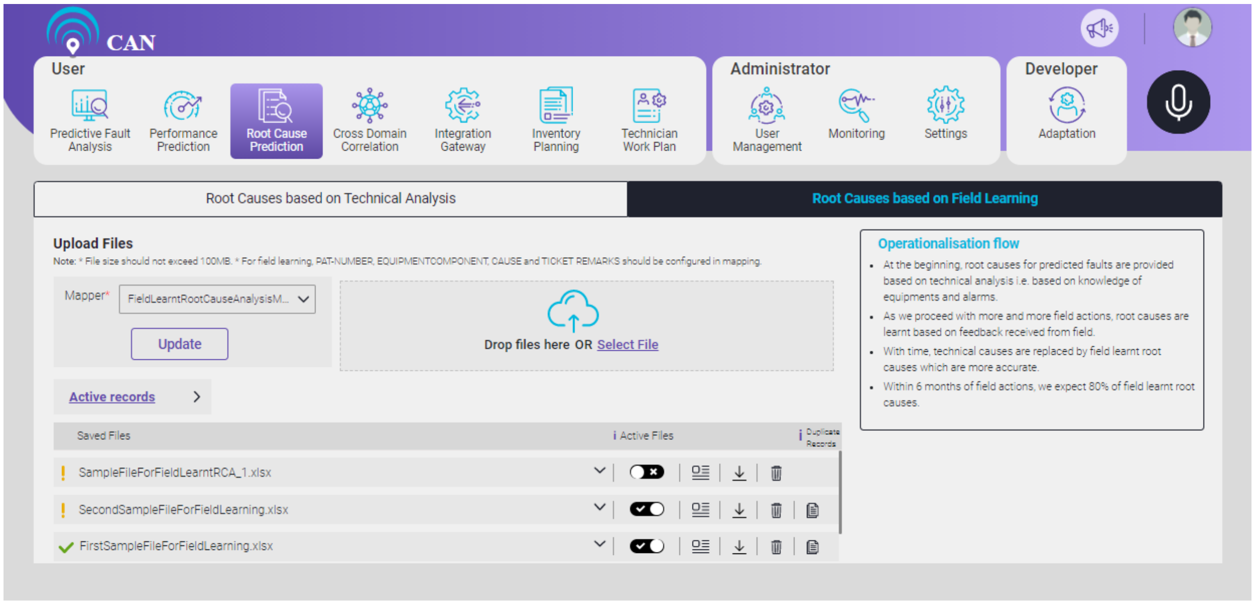
Yes No

Operationalisation flow

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

Figure 6.25 - 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.



Note: * File size should not exceed 100MB. * For field learning, PAT-NUMBER, EQUIPMENTCOMPONENT, CAUSE and TICKET REMARKS should be configured in mapping.

Mapper*: FieldLearntRootCauseAnalysisM...

Operationalisation flow

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

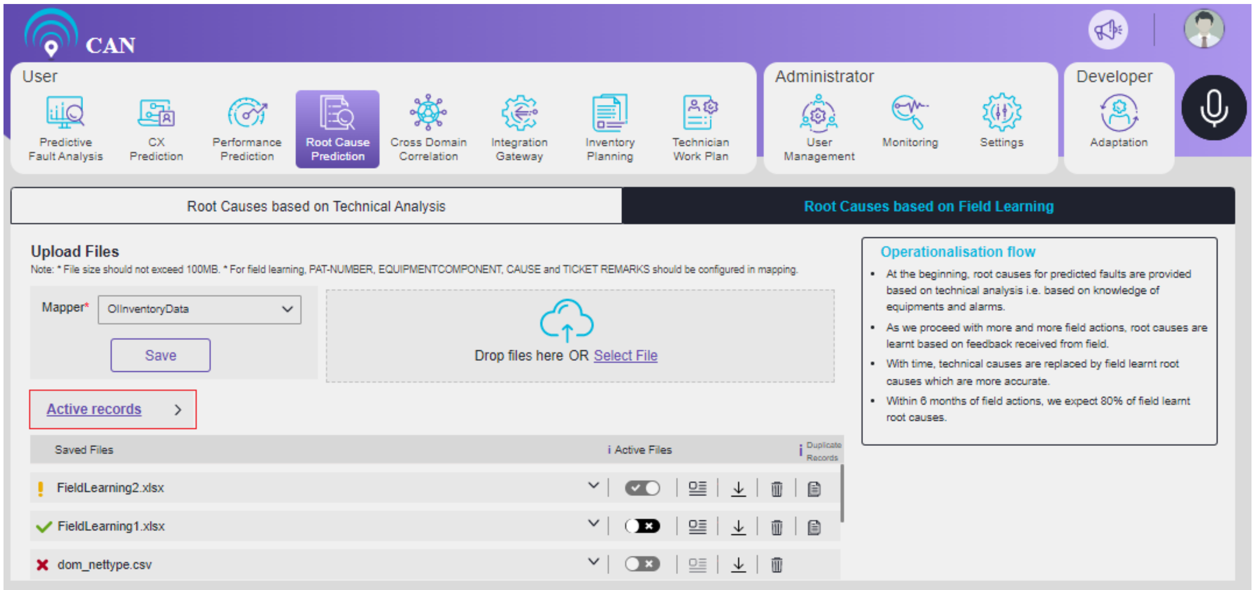
Saved Files	Active Files
! SampleFileForFieldLearntRCA_1.xlsx	☒
! SecondSampleFileForFieldLearning.xlsx	✓
✓ FirstSampleFileForFieldLearning.xlsx	✓

Figure 6.26 - 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.



Note: * File size should not exceed 100MB. * For field learning, PAT-NUMBER, EQUIPMENTCOMPONENT, CAUSE and TICKET REMARKS should be configured in mapping.

Mapper*: OIInventoryData

Operationalisation flow

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

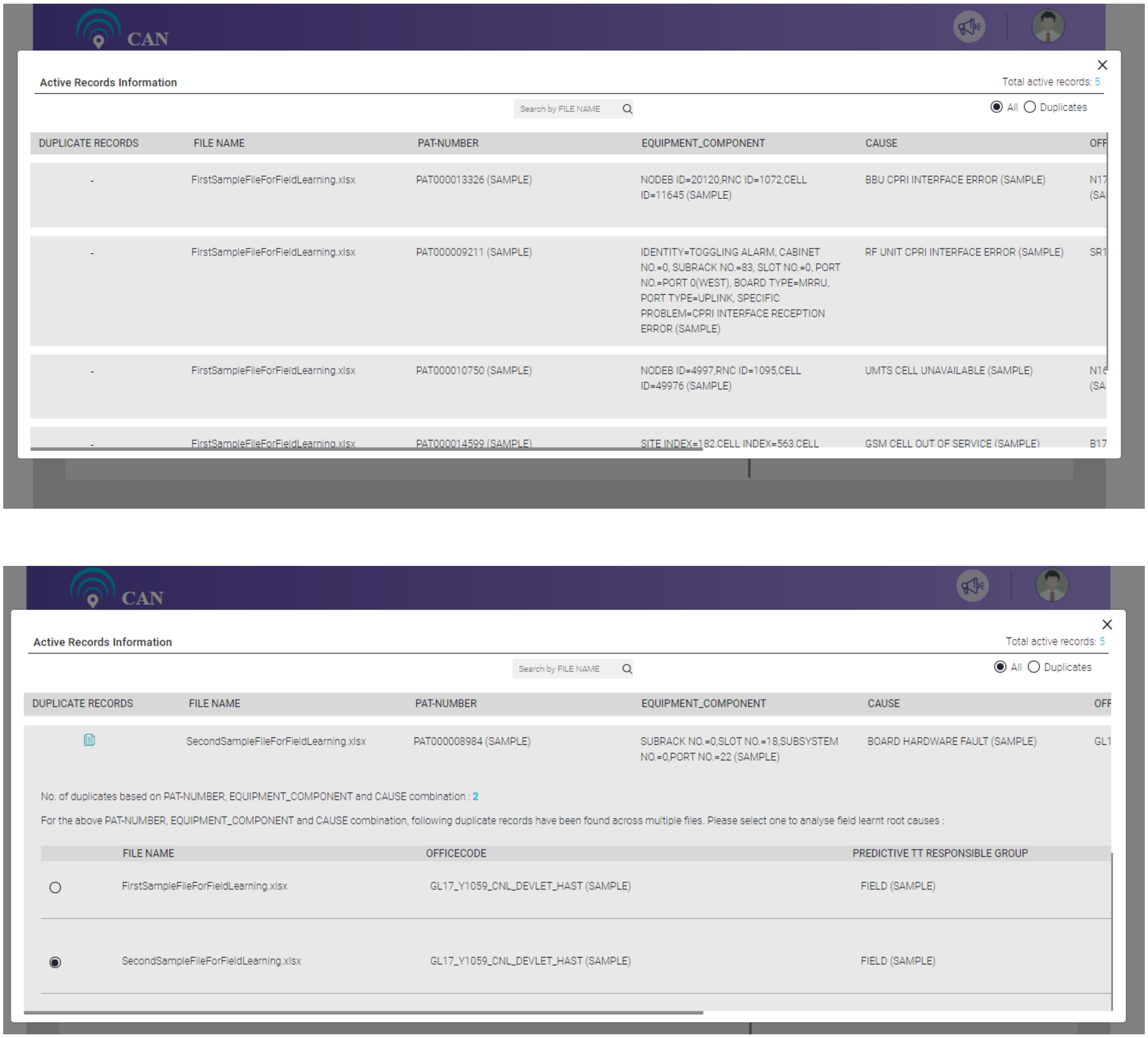
Saved Files	Active Files
! FieldLearning2.xlsx	✓
✓ FieldLearning1.xlsx	☒
✗ dom_nettype.csv	☒

Figure 6.27 - 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 Search by FILE NAME .

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



Active Records Information

Total active records: 5

Search by FILE NAME

● All ○ Duplicates

DUPLICATE RECORDS	FILE NAME	PAT-NUMBER	EQUIPMENT_COMPONENT	CAUSE	OFF
-	FirstSampleFileForFieldLearning.xlsx	PAT000013326 (SAMPLE)	NODEB ID=20120,RNC ID=1072,CELL ID=11645 (SAMPLE)	BBU CPRI INTERFACE ERROR (SAMPLE)	N17 (SA
-	FirstSampleFileForFieldLearning.xlsx	PAT000009211 (SAMPLE)	IDENTITY=TOGGLING ALARM, CABINET NO.=0, SUBRACK NO.=83, SLOT NO.=0, PORT NO.=PORT 0(WEST), BOARD TYPE=MRRU, PORT TYPE=UPLINK, SPECIFIC PROBLEM=CPRI INTERFACE RECEPTION ERROR (SAMPLE)	RF UNIT CPRI INTERFACE ERROR (SAMPLE)	SR1
-	FirstSampleFileForFieldLearning.xlsx	PAT000010750 (SAMPLE)	NODEB ID=4997,RNC ID=1095,CELL ID=49976 (SAMPLE)	UMTS CELL UNAVAILABLE (SAMPLE)	N16 (SA
-	FirstSampleFileForFieldLearning.xlsx	PAT000014599 (SAMPLE)	SITE INDEX=182,CELL INDEX=563,CELL	GSM CELL OUT OF SERVICE (SAMPLE)	B17

Active Records Information

Total active records: 5

Search by FILE NAME

● All ○ Duplicates

DUPLICATE RECORDS	FILE NAME	PAT-NUMBER	EQUIPMENT_COMPONENT	CAUSE	OFF
🗎	SecondSampleFileForFieldLearning.xlsx	PAT000008984 (SAMPLE)	SUBRACK NO.=0,SLOT NO.=18,SUBSYSTEM NO.=0,PORT NO.=22 (SAMPLE)	BOARD HARDWARE FAULT (SAMPLE)	GL1

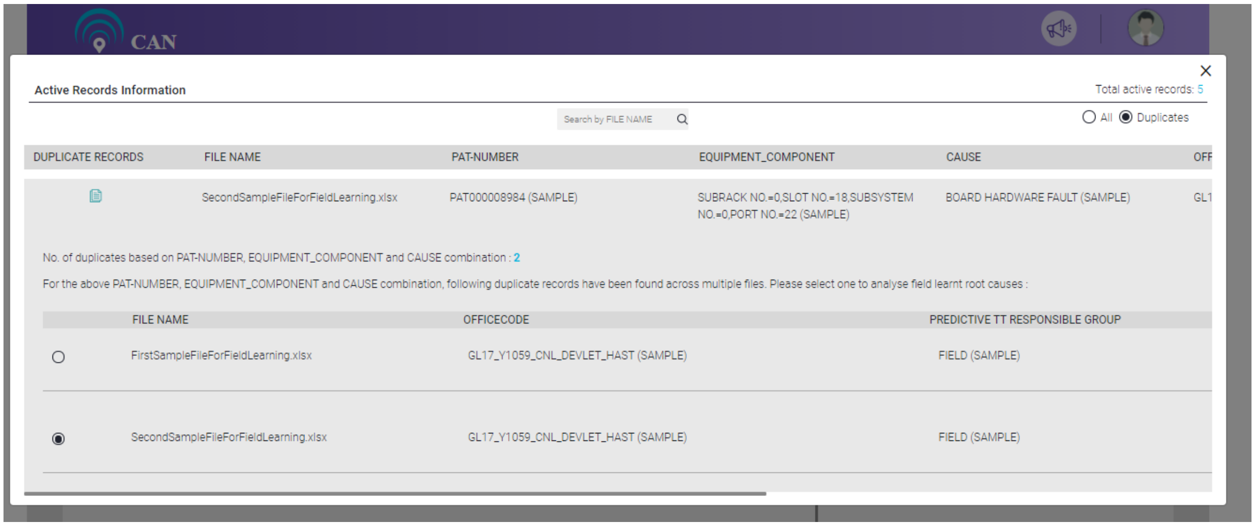
No. of duplicates based on PAT-NUMBER, EQUIPMENT_COMPONENT and CAUSE combination : 2

For the above PAT-NUMBER, EQUIPMENT_COMPONENT and CAUSE combination, following duplicate records have been found across multiple files. Please select one to analyse field learnt root causes :

	FILE NAME	OFFICECODE	PREDICTIVE TT RESPONSIBLE GROUP
○	FirstSampleFileForFieldLearning.xlsx	GL17_Y1059_CNL_DEVLET_HAST (SAMPLE)	FIELD (SAMPLE)
●	SecondSampleFileForFieldLearning.xlsx	GL17_Y1059_CNL_DEVLET_HAST (SAMPLE)	FIELD (SAMPLE)

Figure 6.28 - Active Records Information

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


CAN

Active Records Information

Total active records: 5

Search by FILE NAME

○ All ● Duplicates

DUPLICATE RECORDS	FILE NAME	PAT-NUMBER	EQUIPMENT_COMPONENT	CAUSE	OFF
	SecondSampleFileForFieldLearning.xlsx	PAT000008984 (SAMPLE)	SUBRACK NO.=0,SLOT NO.=18,SUBSYSTEM NO.=0,PORT NO.=22 (SAMPLE)	BOARD HARDWARE FAULT (SAMPLE)	GL1

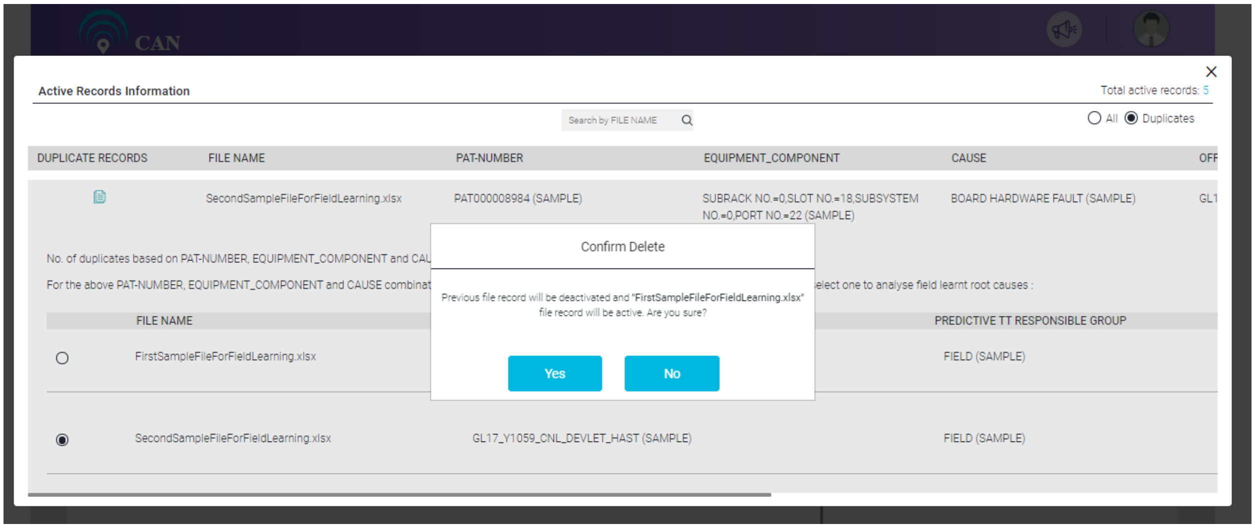
No. of duplicates based on PAT-NUMBER, EQUIPMENT_COMPONENT and CAUSE combination : 2

For the above PAT-NUMBER, EQUIPMENT_COMPONENT and CAUSE combination, following duplicate records have been found across multiple files. Please select one to analyse field learnt root causes :

	FILE NAME	OFFICECODE	PREDICTIVE TT RESPONSIBLE GROUP
○	FirstSampleFileForFieldLearning.xlsx	GL17_Y1059_CNL_DEVLET_HAST (SAMPLE)	FIELD (SAMPLE)
●	SecondSampleFileForFieldLearning.xlsx	GL17_Y1059_CNL_DEVLET_HAST (SAMPLE)	FIELD (SAMPLE)

Figure 6.29 - Duplicate records

User can verify the duplicate records across multiple files.


CAN

Active Records Information

Total active records: 5

Search by FILE NAME

○ All ● Duplicates

DUPLICATE RECORDS	FILE NAME	PAT-NUMBER	EQUIPMENT_COMPONENT	CAUSE	OFF
	SecondSampleFileForFieldLearning.xlsx	PAT000008984 (SAMPLE)	SUBRACK NO.=0,SLOT NO.=18,SUBSYSTEM NO.=0,PORT NO.=22 (SAMPLE)	BOARD HARDWARE FAULT (SAMPLE)	GL1

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

For the above PAT-NUMBER, EQUIPMENT_COMPONENT and CAUSE combinat … elect one to analyse field learnt root causes :

	FILE NAME		PREDICTIVE TT RESPONSIBLE GROUP
○	FirstSampleFileForFieldLearning.xlsx		FIELD (SAMPLE)
●	SecondSampleFileForFieldLearning.xlsx	GL17_Y1059_CNL_DEVLET_HAST (SAMPLE)	FIELD (SAMPLE)

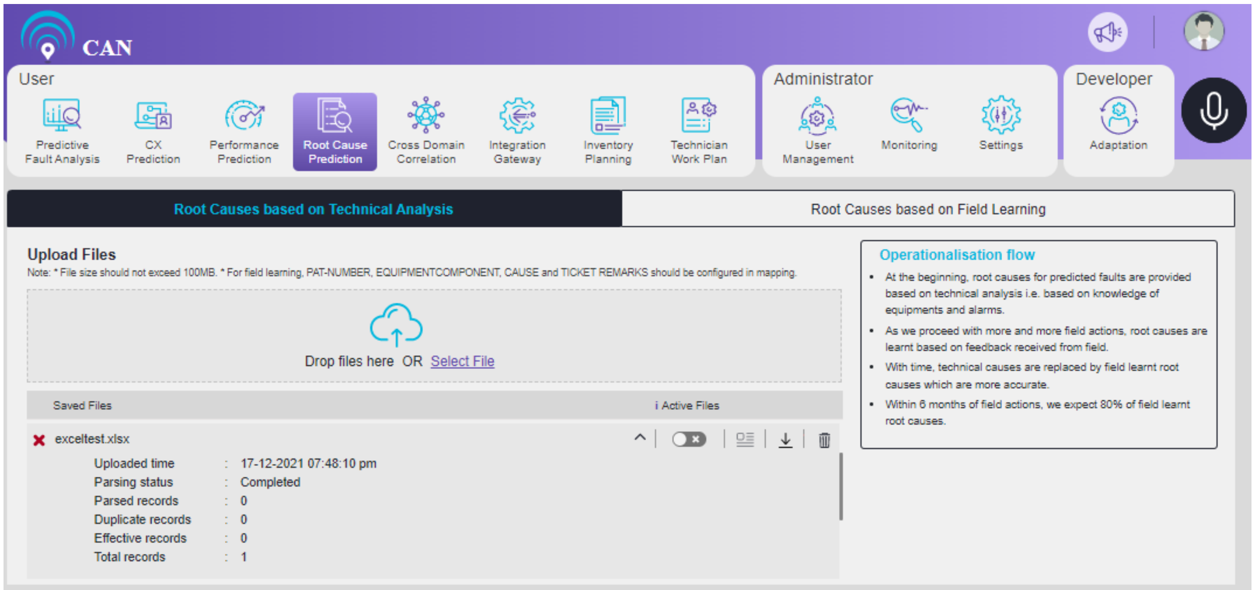
Confirm Delete

Previous file record will be deactivated and "FirstSampleFileForFieldLearning.xlsx" file record will be active. Are you sure?

Figure 6.30 - 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.



Upload Files

Note: * File size should not exceed 100MB. * For field learning, PAT-NUMBER, EQUIPMENTCOMPONENT, CAUSE and TICKET REMARKS should be configured in mapping.

✖ exceltest.xlsx

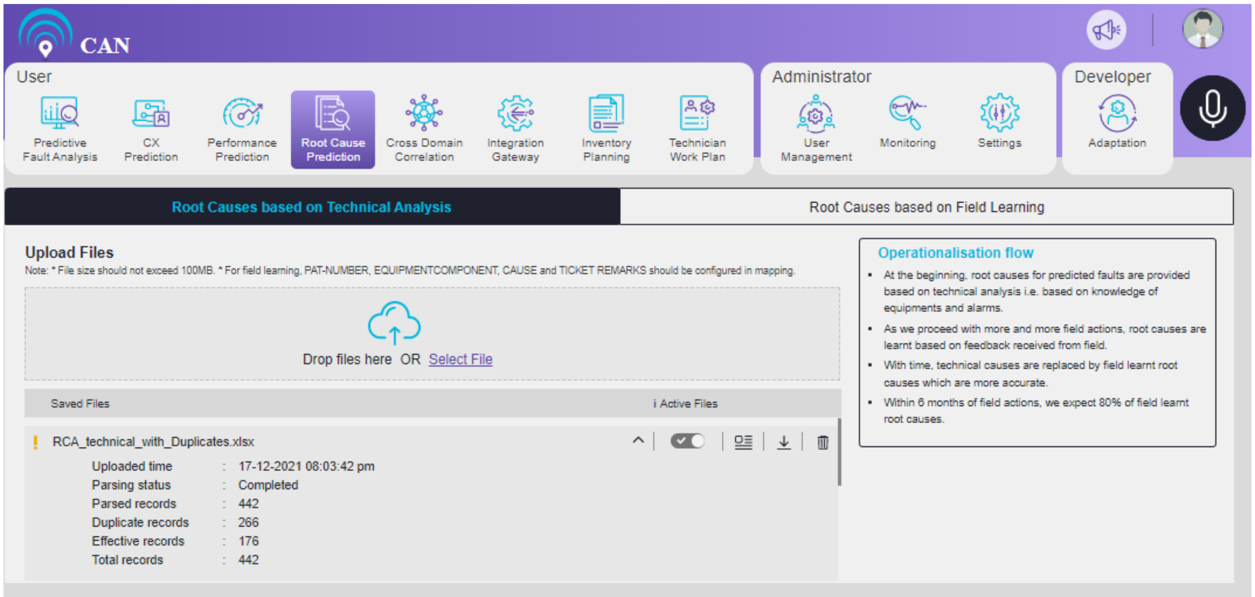
Uploaded time	:	17-12-2021 07:48:10 pm
Parsing status	:	Completed
Parsed records	:	0
Duplicate records	:	0
Effective records	:	0
Total records	:	1

Operationalisation flow

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

Figure 6.31 - 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.



Upload Files

Note: * File size should not exceed 100MB. * For field learning, PAT-NUMBER, EQUIPMENTCOMPONENT, CAUSE and TICKET REMARKS should be configured in mapping.

! RCA_technical_with_Duplicates.xlsx

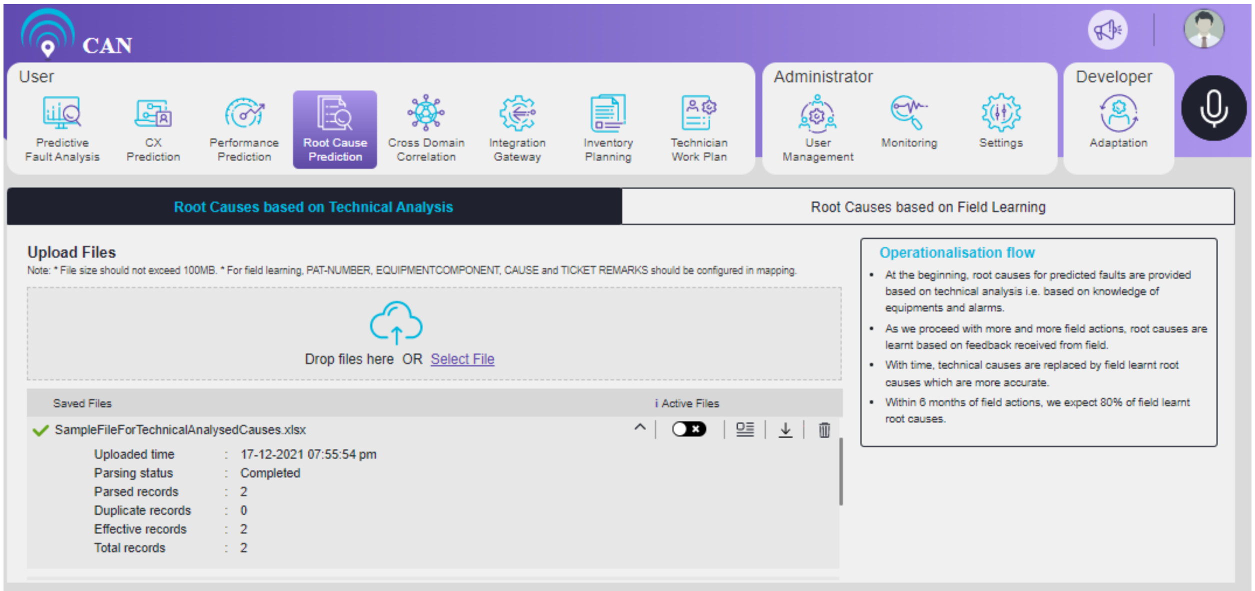
Uploaded time	:	17-12-2021 08:03:42 pm
Parsing status	:	Completed
Parsed records	:	442
Duplicate records	:	266
Effective records	:	176
Total records	:	442

Operationalisation flow

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

Figure 6.32 - 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.



Upload Files

Note: * File size should not exceed 100MB. * For field learning, PAT-NUMBER, EQUIPMENTCOMPONENT, CAUSE and TICKET REMARKS should be configured in mapping.

✓ SampleFileForTechnicalAnalysedCauses.xlsx

Uploaded time	:	17-12-2021 07:55:54 pm
Parsing status	:	Completed
Parsed records	:	2
Duplicate records	:	0
Effective records	:	2
Total records	:	2

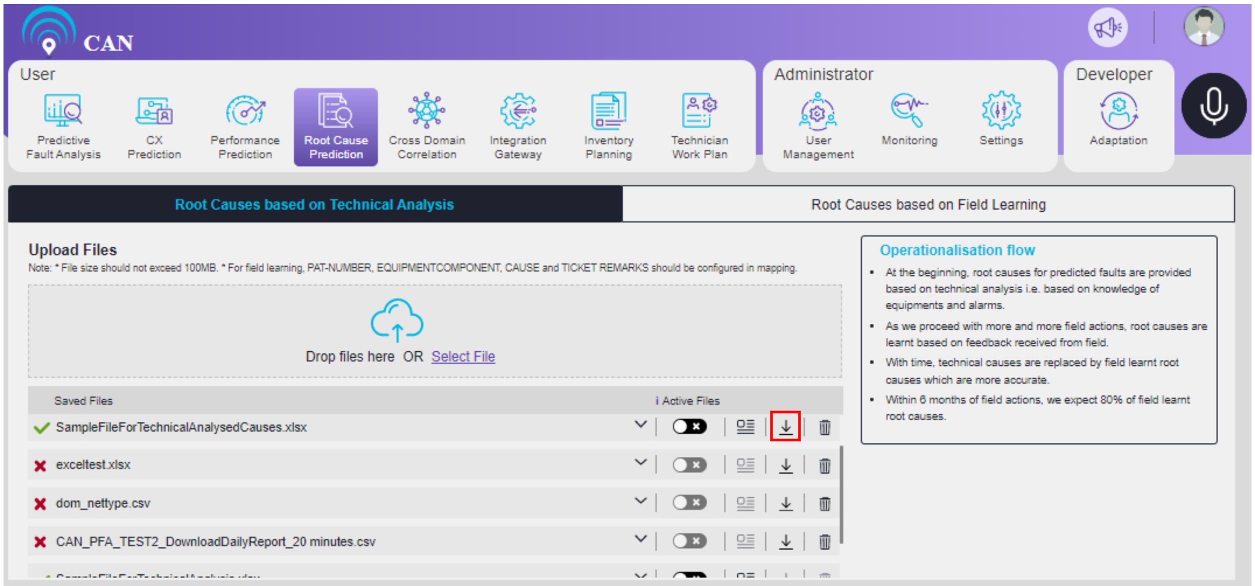
Operationalisation flow

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

Figure 6.33 - 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 ⤓.



Upload Files

Note: * File size should not exceed 100MB. * For field learning, PAT-NUMBER, EQUIPMENTCOMPONENT, CAUSE and TICKET REMARKS should be configured in mapping.

✓ SampleFileForTechnicalAnalysedCauses.xlsx

✗ exceltest.xlsx

✗ dom_nettype.csv

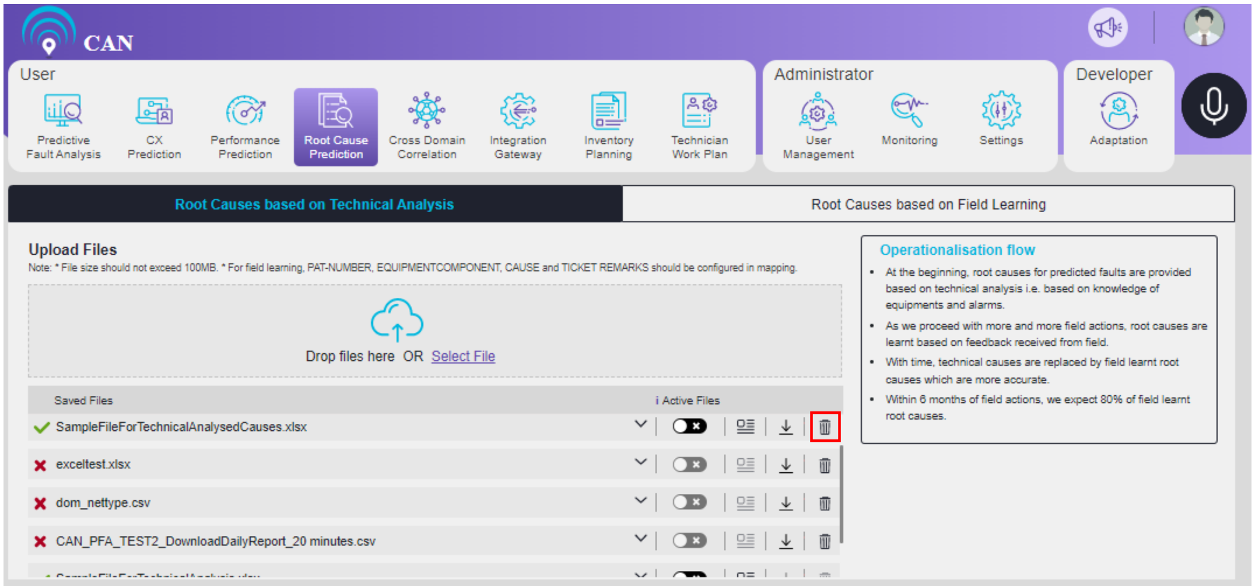
✗ CAN_PFA_TEST2_DownloadDailyReport_20 minutes.csv

Operationalisation flow

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

Figure 6.34 - Download Option

- To delete the file, click the delete icon 🗑.



Upload Files

Note: * File size should not exceed 100MB. * For field learning, PAT-NUMBER, EQUIPMENTCOMPONENT, CAUSE and TICKET REMARKS should be configured in mapping.

Saved Files
✓ SampleFileForTechnicalAnalysedCauses.xlsx
✗ exceltest.xlsx
✗ dom_nettype.csv
✗ CAN_PFA_TEST2_DownloadDailyReport_20 minutes.csv

Operationalisation flow

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

Figure 6.35 - 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.

Page Intentionally Left Blank

7. CROSS DOMAIN CORRELATION

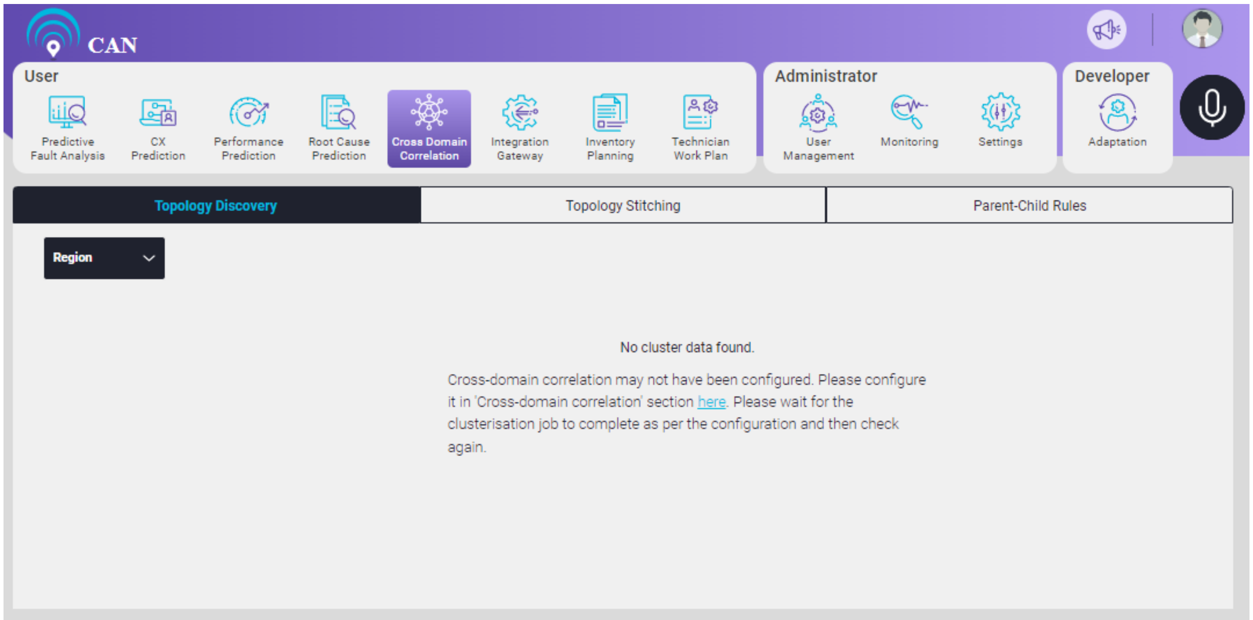
Cross Domain Correlation has three tabs:

1. Topology Discovery
2. Topology Stitching
3. Parent-Child Rules

Topology Discovery

Topology Discovery is an enhanced method by which the end-to-end network is discovered from the inventory data provided by customer and displayed. By default, Cross Domain Correlation lands on Topology Discovery tab. 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 Topology Discovery Configuration Page.

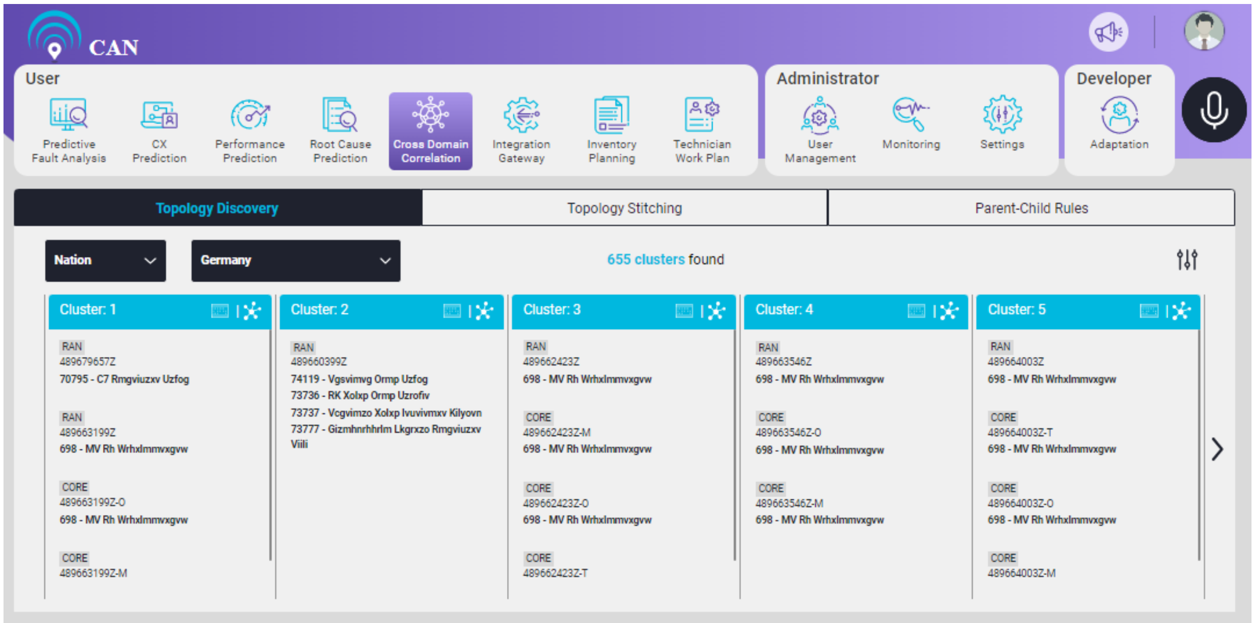


No cluster data found.

Cross-domain correlation may not have been configured. Please configure it in 'Cross-domain correlation' section here. Please wait for the clusterisation job to complete as per the configuration and then check again.

Figure 7.1 - Cross Domain Correlation Screen with No data

When adequate data is available, the page displays all the correlated faults according to the locality. If the number of clusters is less than or equal to five, then the screen displays all the clusters.



Topology Discovery | Topology Stitching | Parent-Child Rules

Nation | Germany

655 clusters found

Cluster: 1

RAN
4896796577
70795 - C7 Rmgviuzxv Uzfog

RAN
489663199Z
698 - MV Rh Wrhxlmmvxgvw

CORE
489663199Z-O
698 - MV Rh Wrhxlmmvxgvw

CORE
489663199Z-M

Cluster: 2

RAN
489660399Z
74119 - Vgsvimvg Ormp Uzfog
73736 - RK Xolxp Ormp Uzrofiv
73737 - Vcgvimzo Xolxp Ivuvivmxv Kilyovn
73777 - Gizmhnrhhrlm Lkgrxzo Rmgviuzxv Viili

Cluster: 3

RAN
489662423Z
698 - MV Rh Wrhxlmmvxgvw

CORE
489662423Z-M
698 - MV Rh Wrhxlmmvxgvw

CORE
489662423Z-O
698 - MV Rh Wrhxlmmvxgvw

CORE
489662423Z-T

Cluster: 4

RAN
489663546Z
698 - MV Rh Wrhxlmmvxgvw

CORE
489663546Z-O
698 - MV Rh Wrhxlmmvxgvw

CORE
489663546Z-M
698 - MV Rh Wrhxlmmvxgvw

Cluster: 5

RAN
489664003Z
698 - MV Rh Wrhxlmmvxgvw

CORE
489664003Z-T
698 - MV Rh Wrhxlmmvxgvw

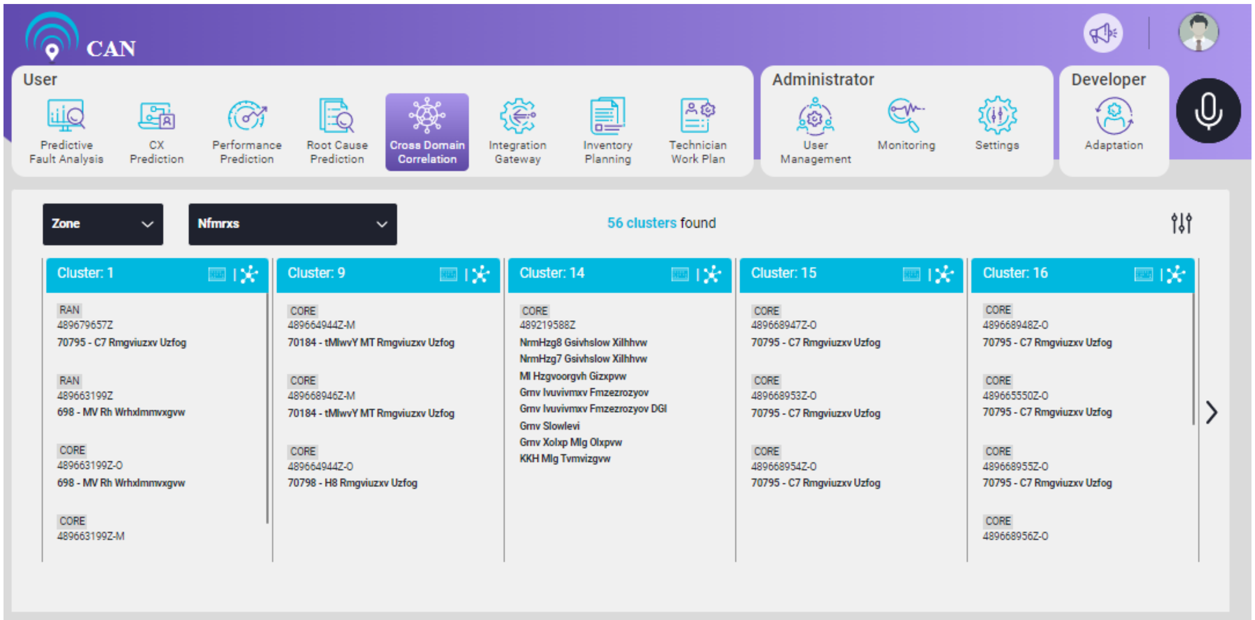
CORE
489664003Z-O
698 - MV Rh Wrhxlmmvxgvw

CORE
489664003Z-M

Figure 7.2 - Cross Domain Correlation

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

User can see total number of clusters (i.e. Cumulative sum of clusters of a particular locality) in the center of the screen.



Zone | Nfmrxs

56 clusters found

Cluster: 1

RAN
4896796577
70795 - C7 Rmgviuzxv Uzfog

RAN
489663199Z
698 - MV Rh Wrhxlmmvxgvw

CORE
489663199Z-O
698 - MV Rh Wrhxlmmvxgvw

CORE
489663199Z-M

Cluster: 9

CORE
489664944Z-M
70184 - tMlwvY MT Rmgviuzxv Uzfog

CORE
489668946Z-M
70184 - tMlwvY MT Rmgviuzxv Uzfog

CORE
489664944Z-O
70798 - H8 Rmgviuzxv Uzfog

Cluster: 14

CORE
489219588Z
NrmHzg8 Gsivhslow Xilhhvw
NrmHzg7 Gsivhslow Xilhhvw
Ml Hzgvoorgvh Gizxpvw
Grnv Ivuvivmxv Fmzezrozyov
Grnv Ivuvivmxv Fmzezrozyov DGl
Grnv Slowlevi
Grnv Xolxp Mlg Olxpvw
KKH Mlg Tvmvizgvw

Cluster: 15

CORE
489668947Z-O
70795 - C7 Rmgviuzxv Uzfog

CORE
489668953Z-O
70795 - C7 Rmgviuzxv Uzfog

CORE
489668954Z-O
70795 - C7 Rmgviuzxv Uzfog

Cluster: 16

CORE
489668948Z-O
70795 - C7 Rmgviuzxv Uzfog

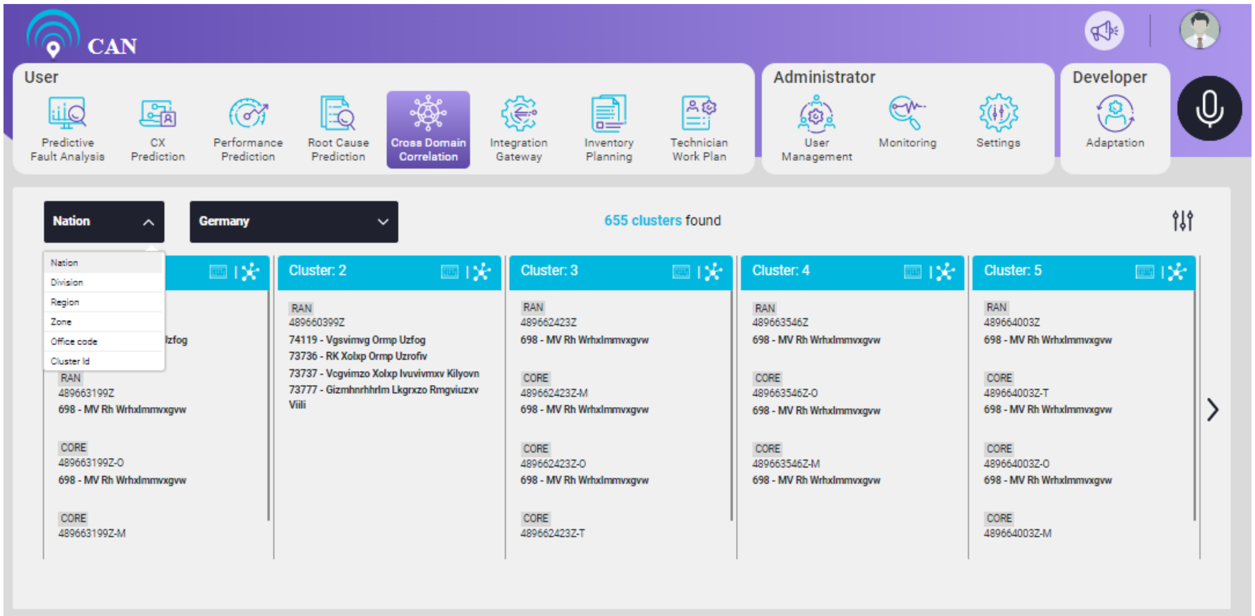
CORE
489665550Z-O
70795 - C7 Rmgviuzxv Uzfog

CORE
489668955Z-O
70795 - C7 Rmgviuzxv Uzfog

CORE
489668956Z-O

Figure 7.3 - No. of Clusters

User can select the **Locality** (Nation, Division, Region, Zone, Office Code and Cluster Id) from the drop down to view the clusters.



655 clusters found

Cluster 1 (partly hidden): …lzfog
RAN
489663199Z
698 - MV Rh Wrhxlmmvxgvw
CORE
489663199Z-O
698 - MV Rh Wrhxlmmvxgvw
CORE
489663199Z-M

Cluster: 2
RAN
489660399Z
74119 - Vgsvimvg Ormp Uzfog
73736 - RK Xolxp Ormp Uzrofiv
73737 - Vcgvimzo Xolxp Ivuvivmxv Kilyovn
73777 - Gizmhnrhhrlm Lkgrxzo Rmgviuzxv Viili

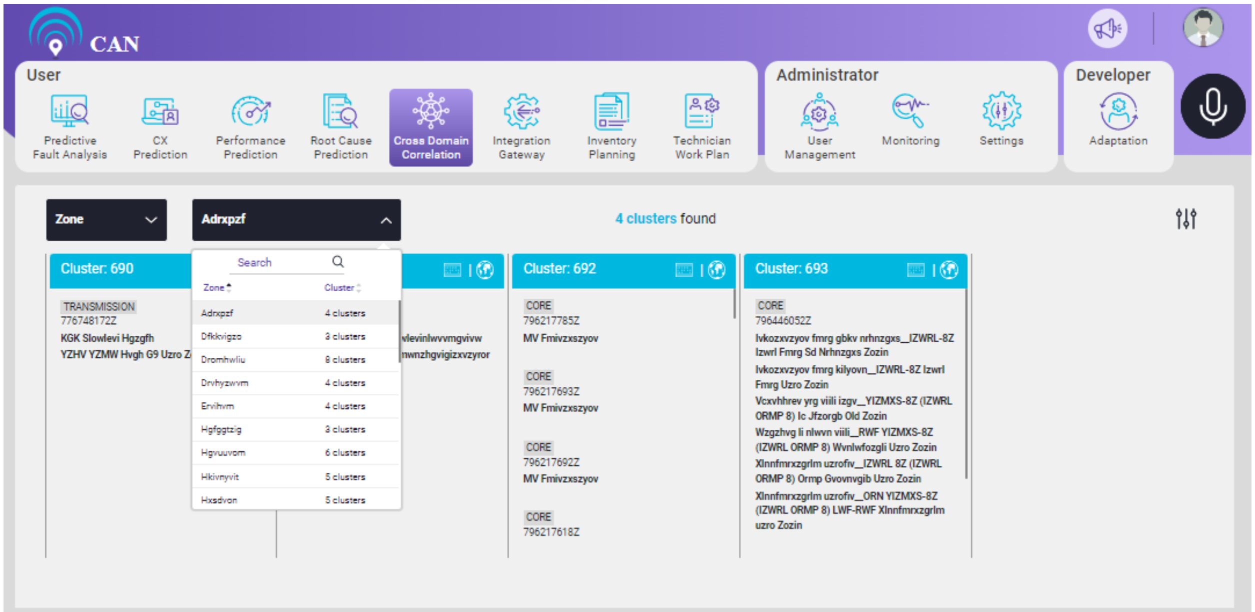
Cluster: 3
RAN
489662423Z
698 - MV Rh Wrhxlmmvxgvw
CORE
489662423Z-M
698 - MV Rh Wrhxlmmvxgvw
CORE
489662423Z-O
698 - MV Rh Wrhxlmmvxgvw
CORE
489662423Z-T

Cluster: 4
RAN
489663546Z
698 - MV Rh Wrhxlmmvxgvw
CORE
489663546Z-O
698 - MV Rh Wrhxlmmvxgvw
CORE
489663546Z-M
698 - MV Rh Wrhxlmmvxgvw

Cluster: 5
RAN
489664003Z
698 - MV Rh Wrhxlmmvxgvw
CORE
489664003Z-T
698 - MV Rh Wrhxlmmvxgvw
CORE
489664003Z-O
698 - MV Rh Wrhxlmmvxgvw
CORE
489664003Z-M

Figure 7.4 - Locality Selection

User can select a **Region, Division, Zone, Office Code or Cluster Id** from the drop down to filter the clusters based on the selection.



4 clusters found

Zone	Cluster
Adrxpzf	4 clusters
Dfkkvigzo	3 clusters
Dromhwliu	8 clusters
Drvhyzwvm	4 clusters
Ervihvm	4 clusters
Hgfggtzig	3 clusters
Hgvuuvom	6 clusters
Hkivnyvit	5 clusters
Hxsdvon	5 clusters

Cluster: 690
TRANSMISSION
776748172Z
KGK Slowlevi Hgzgfh
YZHV YZMW Hvgh G9 Uzro Z…

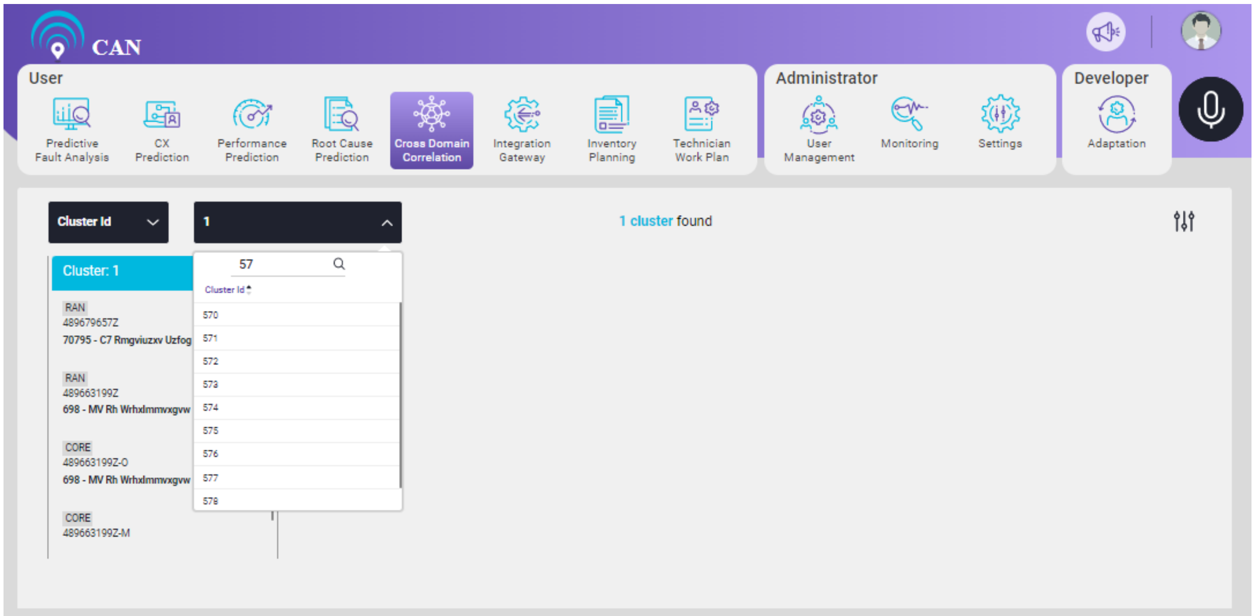
Cluster 691 (partly hidden):
…vlevinlwvvmgvivw
…nwnzhgvigizxvzyror

Cluster: 692
CORE
796217785Z
MV Fmivzxszyov
CORE
796217693Z
MV Fmivzxszyov
CORE
796217692Z
MV Fmivzxszyov
CORE
796217618Z

Cluster: 693
CORE
796446052Z
Ivkozxvzyov fmrg gbkv nrhnzgxs__IZWRL-8Z Izwrl Fmrg Sd Nrhnzgxs Zozin
Ivkozxvzyov fmrg kilyovn__IZWRL-8Z Izwrl Fmrg Uzro Zozin
Vcxvhhrev yrg viili izgv__YIZMXS-8Z (IZWRL ORMP 8) Ic Jfzorgb Old Zozin
Wzgzhvg li nlwvn viili__RWF YIZMXS-8Z (IZWRL ORMP 8) Wvnlwfozgli Uzro Zozin
Xlnnfmrxzgrlm uzrofiv__IZWRL 8Z (IZWRL ORMP 8) Ormp Gvovnvgib Uzro Zozin
Xlnnfmrxzgrlm uzrofiv__ORN YIZMXS-8Z (IZWRL ORMP 8) LWF-RWF Xlnnfmrxzgrlm uzro Zozin

Figure 7.5 - Specific Zone Selection

User can use the search text box to search the **Region, Division, Zone, Office Code or Cluster Id**. The screen will display all the clusters as per the search.



Cluster Id | 1

1 cluster found

Cluster: 1

RAN
489679657Z
70795 - C7 Rmgviuzxv Uzfog

RAN
489663199Z
698 - MV Rh Wrhxlmmvxgvw

CORE
489663199Z-O
698 - MV Rh Wrhxlmmvxgvw

CORE
489663199Z-M

57

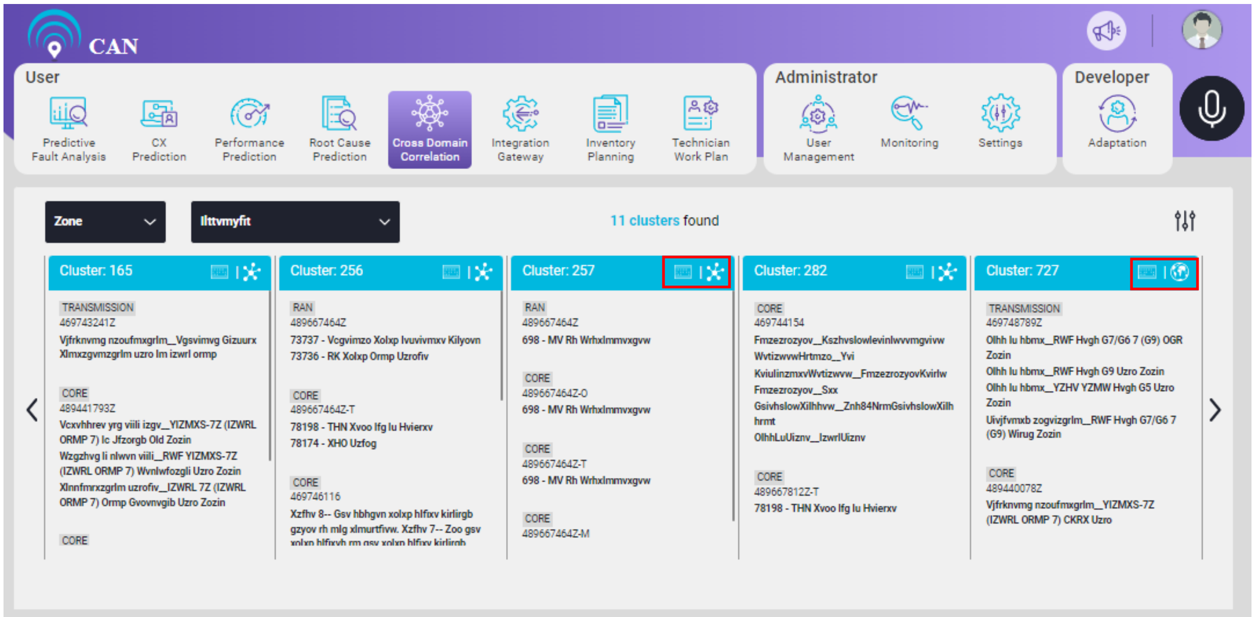
Cluster Id

570
571
572
573
574
575
576
577
578

Figure 7.6 - Search a Cluster

The screen displays the cluster details.

Each cluster has either **Bit Pattern View - Schematic View** or **Bit Pattern View - Map View**.



Zone | Ilttvmyfit

11 clusters found

Cluster: 165

TRANSMISSION
469743241Z
Vjfrknvmg nzoufmxgrlm__Vgsvimvg Gizuurx Xlmxzgvmzgrlm uzro lm izwrl ormp

CORE
489441793Z
Vcxvhhrev yrg viili izgv__YIZMXS-7Z (IZWRL ORMP 7) Ic Jfzorgb Old Zozin
Wzgzhvg li nlwvn viili__RWF YIZMXS-7Z (IZWRL ORMP 7) Wvnlwfozgli Uzro Zozin
Xlnnfmrxzgrlm uzrofiv__IZWRL 7Z (IZWRL ORMP 7) Ormp Gvovnvgib Uzro Zozin

CORE

Cluster: 256

RAN
4896674642
73737 - Vcgvimzo Xolxp Ivuvivmxv Kilyovn
73736 - RK Xolxp Ormp Uzrofiv

CORE
489667464Z-T
78198 - THN Xvoo Ifg lu Hvierxv
78174 - XHO Uzfog

CORE
469746116
Xzfhv 8-- Gsv hbhgvn xolxp hlfixv kirlirgb gzyov rh mlg xlmurtfivw. Xzfhv 7-- Zoo gsv xolxp hlfixvh rm gsv xolxp hlfixv kirlirgb

Cluster: 257

RAN
489667464Z
698 - MV Rh Wrhxlmmvxgvw

CORE
489667464Z-O
698 - MV Rh Wrhxlmmvxgvw

CORE
489667464Z-T
698 - MV Rh Wrhxlmmvxgvw

CORE
489667464Z-M

Cluster: 282

CORE
469744154
Fmzezrozyov__Kszhvslowlevinlwvvmgvivw
WvtizwvwHrtmzo__Yvi
KviulinzmxvWvtizwvw__FmzezrozyovKvirlw
Fmzezrozyov__Sxx
GsivhslowXilhhvw__Znh84NrmGsivhslowXilh hrmt
OlhhLuUiznv__IzwrlUiznv

CORE
489667812Z-T
78198 - THN Xvoo Ifg lu Hvierxv

Cluster: 727

TRANSMISSION
469748789Z
Olhh lu hbmx__RWF Hvgh G7/G6 7 (G9) OGR Zozin
Olhh lu hbmx__RWF Hvgh G9 Uzro Zozin
Olhh lu hbmx__YZHV YZMW Hvgh G5 Uzro Zozin
Uivjfvmxb zogvizgrlm__RWF Hvgh G7/G6 7 (G9) Wirug Zozin

CORE
489440078Z
Vjfrknvmg nzoufmxgrlm__YIZMXS-7Z (IZWRL ORMP 7) CKRX Uzro

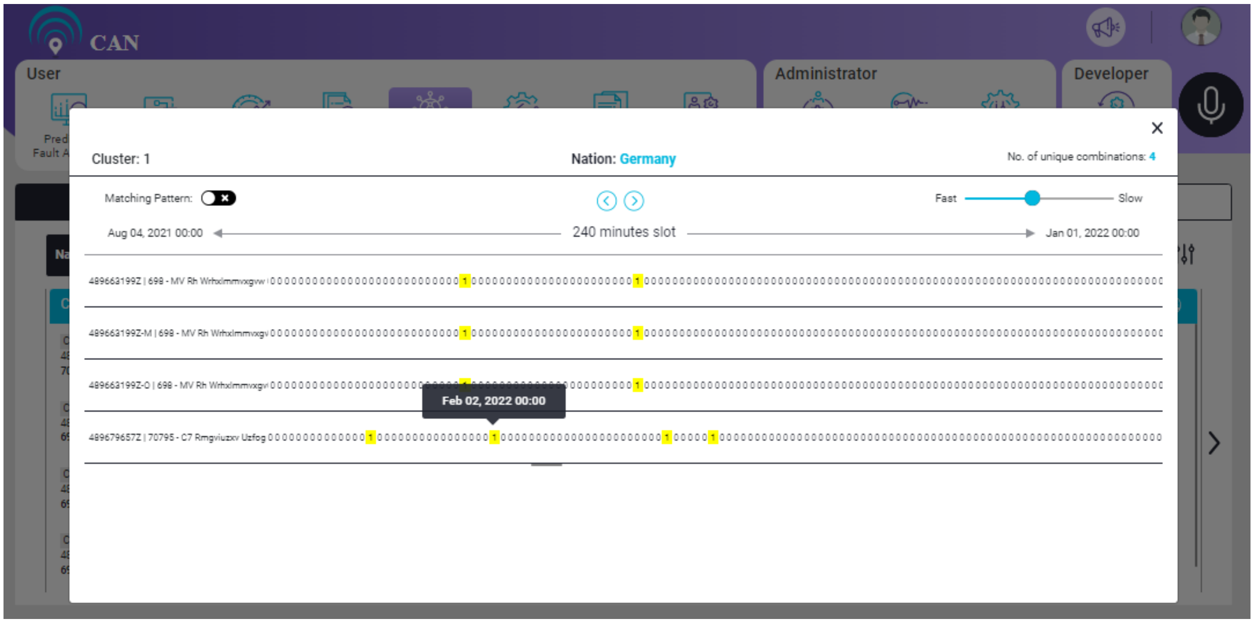
Figure 7.7 - Type of Views

Bit pattern view:

This view displays all the combinations and the corresponding bit pattern for a unique Cluster-Locality 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 240 minutes' slot. User cannot change the duration of the correlation pattern.



Cluster: 1

Nation: Germany

No. of unique combinations: 4

Matching Pattern: ☒

Fast — Slow

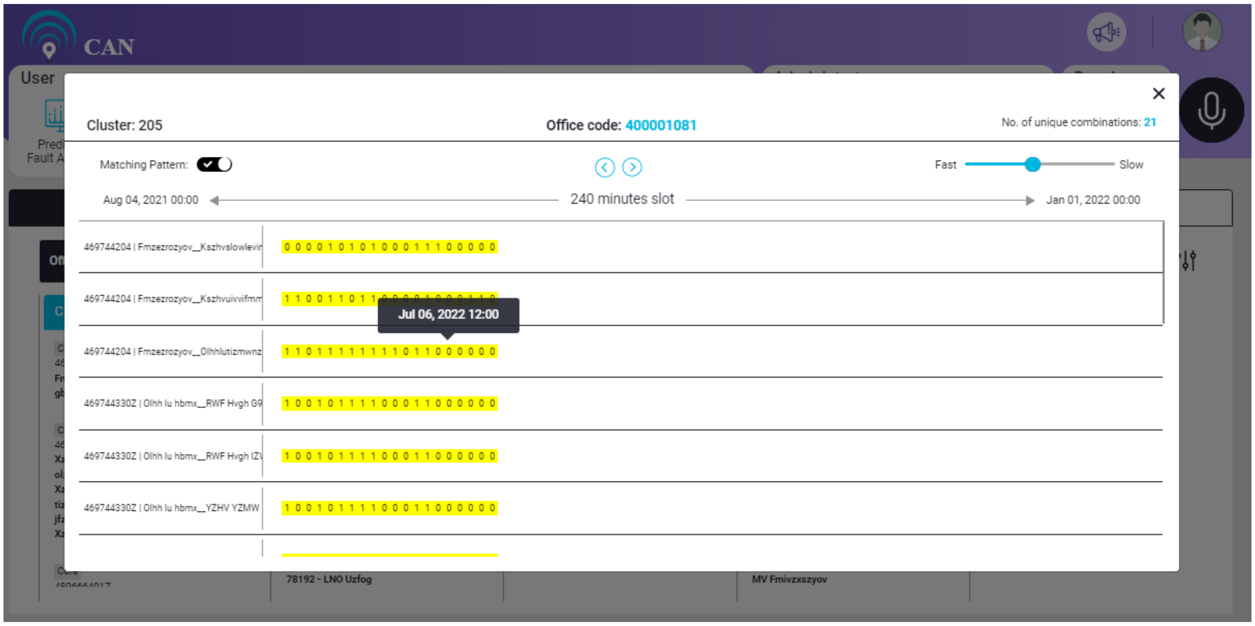
Aug 04, 2021 00:00 ◄ 240 minutes slot ► Jan 01, 2022 00:00

```
489663199Z | 698 - MV Rh Wrhxlmmvxgvw 0000000000000000000000000001000000000000000000000001000000000000000000000000000000000000000000000000000000000000000
489663199Z-M | 698 - MV Rh Wrhxlmmvxgv 0000000000000000000000000001000000000000000000000001000000000000000000000000000000000000000000000000000000000000000
489663199Z-O | 698 - MV Rh Wrhxlmmvxgv 0000000000000000000000000001000000000000000000000001000000000000000000000000000000000000000000000000000000000000000
489679657Z | 70795 - C7 Rmgviuzxv Uzfog 00000000000000100000000000000001000000000000000000000001000001000000000000000000000000000000000000000000000000000000000
```

Feb 02, 2022 00:00

Figure 7.8 - Bit Pattern View

User can view the matching bits for the filtered clusters by clicking the **Matching Pattern** toggle button ☑.



Cluster: 205

Office code: 400001081

No. of unique combinations: 21

Matching Pattern: ☑

Fast — Slow

Aug 04, 2021 00:00 ◄ 240 minutes slot ► Jan 01, 2022 00:00

```
469744204 | Fmzezrozyov__Kszhvslowlevir   0 0 0 0 1 0 1 0 1 0 0 0 1 1 1 0 0 0 0 0
469744204 | Fmzezrozyov__Kszhvuivvifmm    1 1 0 0 1 1 0 1 1 0 0 0 0 1 0 0 0 1 1 0
469744204 | Fmzezrozyov__Olhhlutizmwnz    1 1 0 1 1 1 1 1 1 1 0 1 1 0 0 0 0 0 0
469744330Z | Olhh lu hbmx__RWF Hvgh G9     1 0 0 1 0 1 1 1 1 0 0 0 1 1 0 0 0 0 0 0
469744330Z | Olhh lu hbmx__RWF Hvgh IZV    1 0 0 1 0 1 1 1 1 0 0 0 1 1 0 0 0 0 0 0
469744330Z | Olhh lu hbmx__YZHV YZMW       1 0 0 1 0 1 1 1 1 0 0 0 1 1 0 0 0 0 0 0
```

Jul 06, 2022 12:00

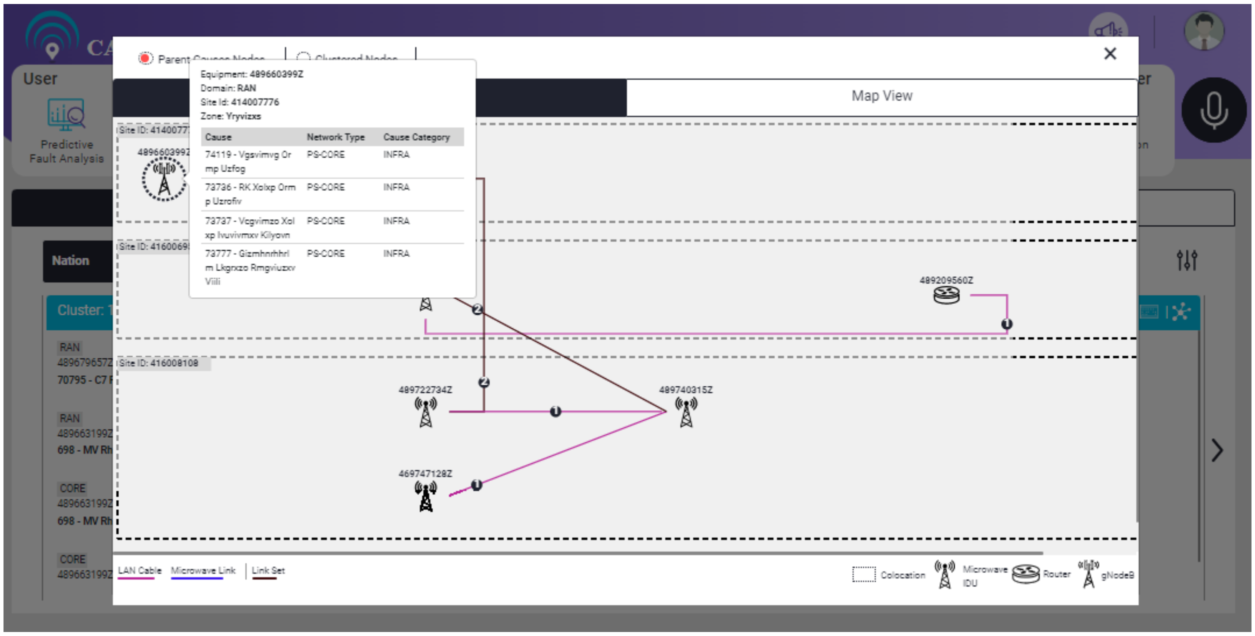
Figure 7.9 - Matching Bit Pattern

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

Schematic View

This view displays the topological connections of nodes and co-located nodes are displayed with dotted area.

In Schematic view, blinking nodes represent the **Clustered Nodes**. Click any node to view the **Node Details**.

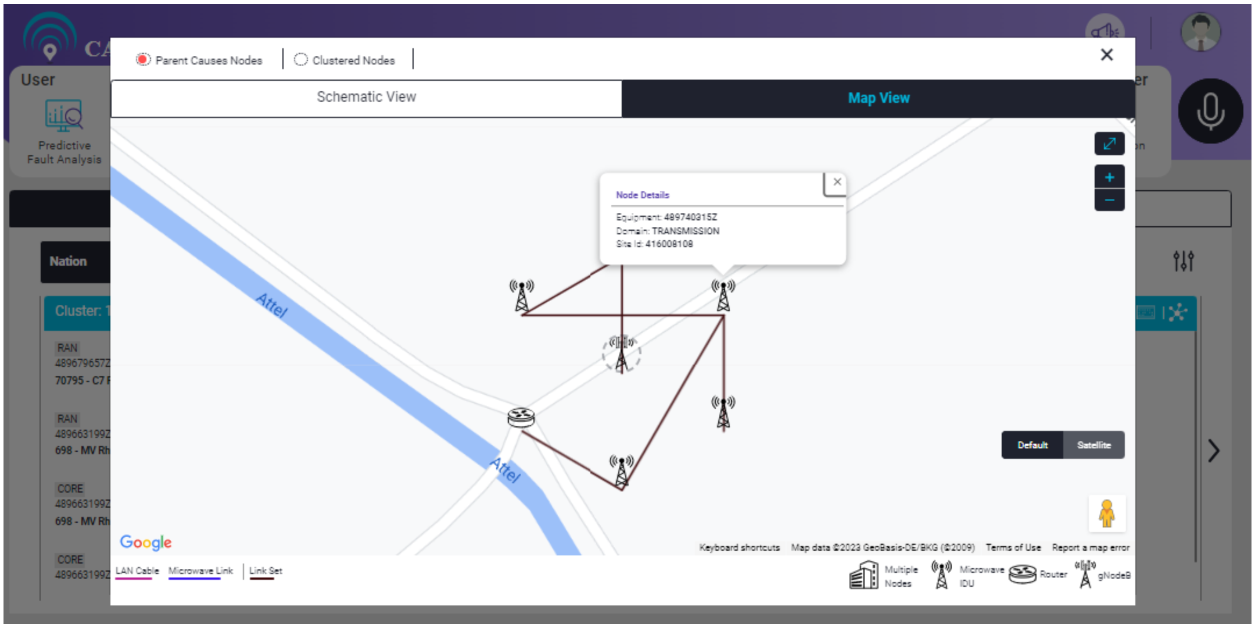


Equipment: 489660399Z
Domain: RAN
Site Id: 414007776
Zone: Yryvizxs

Cause	Network Type	Cause Category
74119 - Vgsvimvg Or mp Uzfog	PS-CORE	INFRA
73736 - RK Xolxp Orm p Uzrofiv	PS-CORE	INFRA
73737 - Vcgvimzo Xol xp Ivuvivmxv Kilyovn	PS-CORE	INFRA
73777 - Gizmhnrhhrl m Lkgrxzo Rmgviuzxv Viili	PS-CORE	INFRA

Figure 7.10 - Schematic View

Click on Map view to display the connections on a map. Click any node to view the **Node Details**.



Node Details

Equipment: 489740315Z
Domain: TRANSMISSION
Site Id: 416008108

Figure 7.11 - Map View

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

Map view:

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

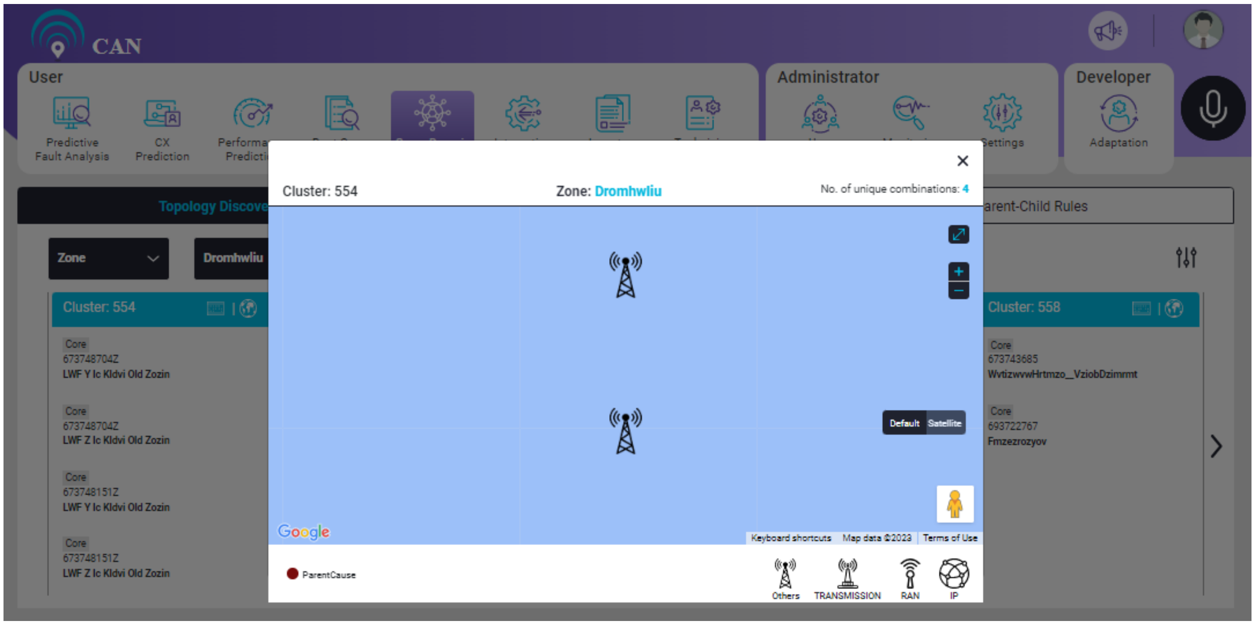
User can expand the view of the map to the full screen view with ⤢ icon.

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
- RAN
- IP



Cluster: 554 Zone: Dromhwliu No. of unique combinations: 4

● ParentCause

Cluster: 554

Core
673748704Z
LWF Y Ic Kldvi Old Zozin

Core
673748704Z
LWF Z Ic Kldvi Old Zozin

Core
673748151Z
LWF Y Ic Kldvi Old Zozin

Core
673748151Z
LWF Z Ic Kldvi Old Zozin

Cluster: 558

Core
673743685
WvtizwvwHrtmzo_VziobDzimrmt

Core
693722767
Fmzezrozyov

Figure 7.12 - Map View with Pointer

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

When user clicks the pointer, a pop-up will appear on the screen.

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

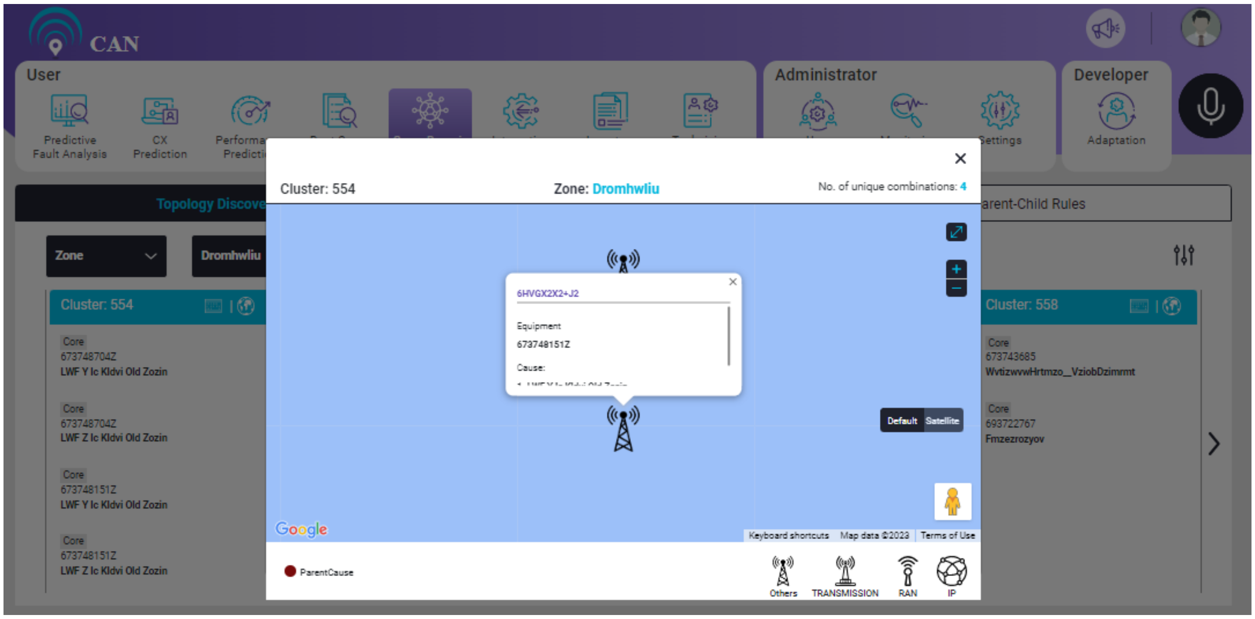


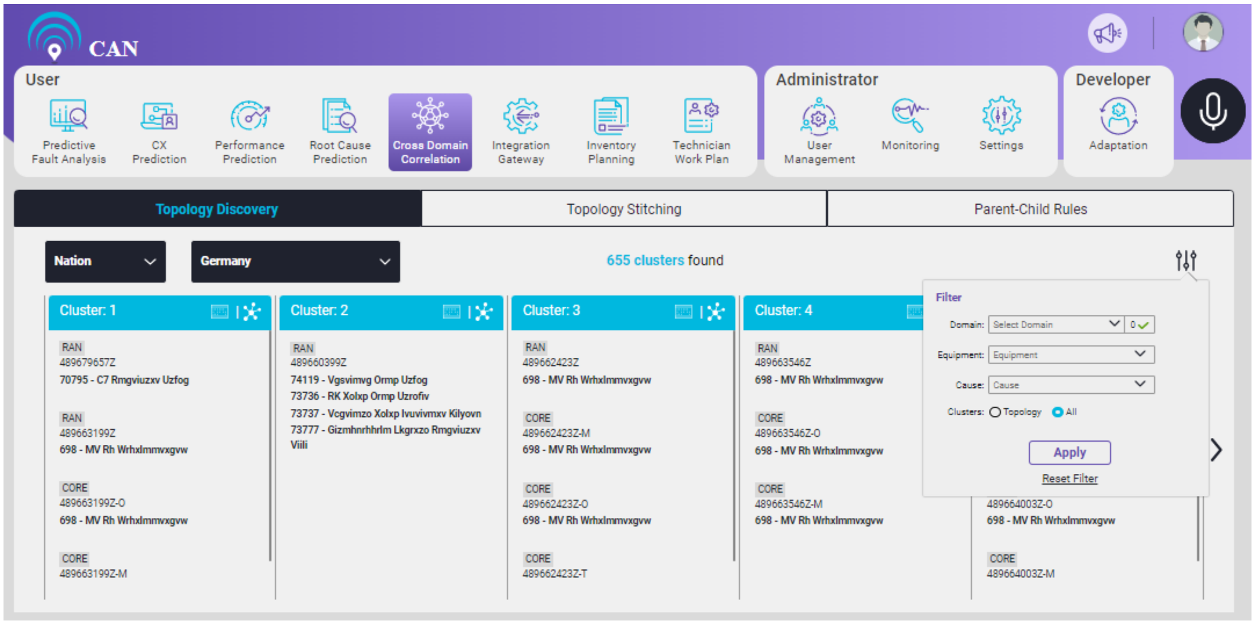
Figure 7.13 - Map View with Details

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 unique combinations present for this particular cluster is shown above.

To Filter the Clusters

1. Click on the **Filter** icon 🎚 to filter the clusters based on **Domain, Equipment, Cause** and **Clusters**.
2. Select Domain, Equipment or Cause from the drop-down.
3. Select the **Topology** radio button to view only the topology based clusters. By default, screen displays **All** clusters.
4. Click **Apply** button to filter the clusters.
5. Click Reset Filter to reset all the fields to default.



Nation: Germany

655 clusters found

Filter
Domain: Select Domain 0 ✓
Equipment: Equipment
Cause: Cause
Clusters: ○ Topology ● All

Cluster: 1
RAN
489679657Z
70795 - C7 Rmgviuzxv Uzfog
RAN
489663199Z
698 - MV Rh Wrhxlmmvxgvw
CORE
489663199Z-O
698 - MV Rh Wrhxlmmvxgvw
CORE
489663199Z-M

Cluster: 2
RAN
489660399Z
74119 - Vgsvimvg Ormp Uzfog
73736 - RK Xolxp Ormp Uzrofiv
73737 - Vcgvimzo Xolxp Ivuvivmxv Kilyovn
73777 - Gizmhnrhhrlm Lkgrxzo Rmgviuzxv Viili

Cluster: 3
RAN
489662423Z
698 - MV Rh Wrhxlmmvxgvw
CORE
489662423Z-M
698 - MV Rh Wrhxlmmvxgvw
CORE
489662423Z-O
698 - MV Rh Wrhxlmmvxgvw
CORE
489662423Z-T

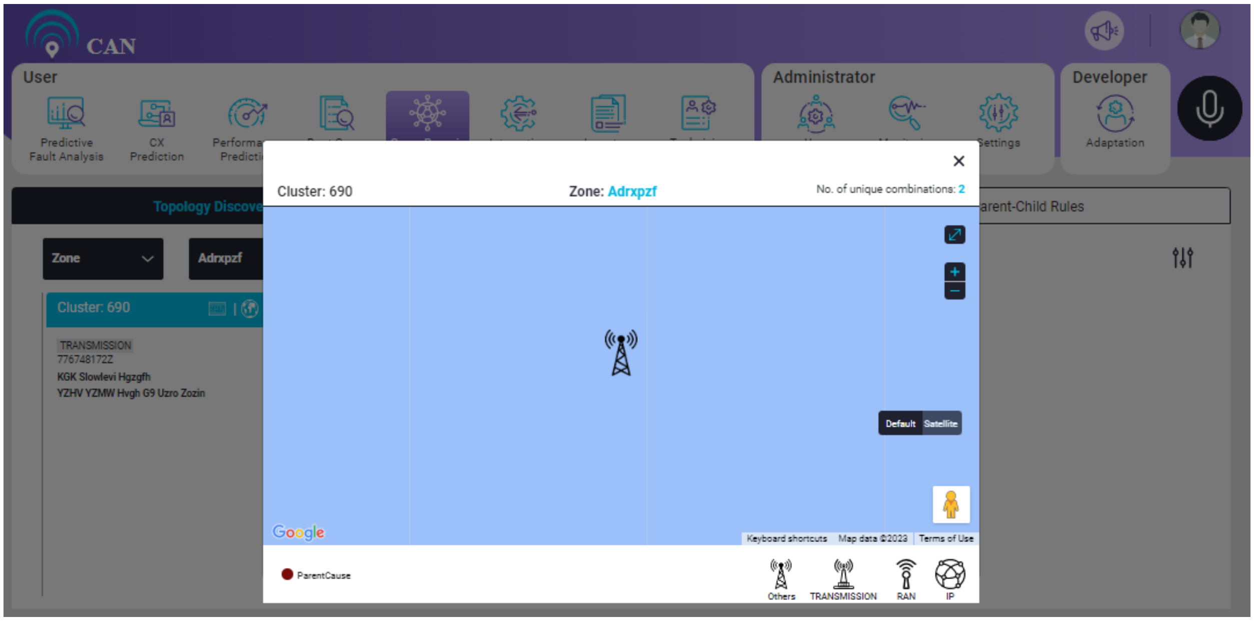
Cluster: 4
RAN
489663546Z
698 - MV Rh Wrhxlmmvxgvw
CORE
489663546Z-O
698 - MV Rh Wrhxlmmvxgvw
CORE
489663546Z-M
698 - MV Rh Wrhxlmmvxgvw

489664003Z-O
698 - MV Rh Wrhxlmmvxgvw
CORE
489664003Z-M

Figure 7.14 - Filter Option

No Marker Scenario

1. When there is no marker (Lat/Long) and the zone name is “known” or “valid”, the map locates the appropriate zone.



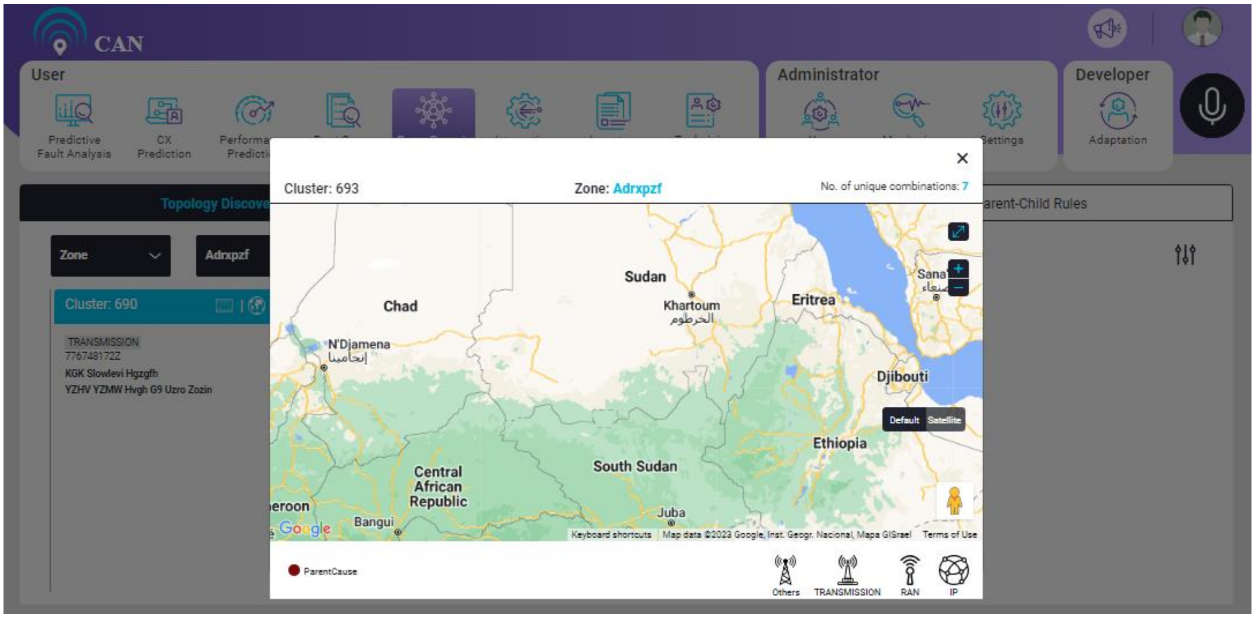
Zone: Adrxpzf

Cluster: 690
TRANSMISSION
776748172Z
KGK Slowlevi Hgzgfh
YZHV YZMW Hvgh G9 Uzro Zozin

Cluster: 690
Zone: Adrxpzf
No. of unique combinations: 2

Figure 7.15 - Valid Zone

2. When there is no marker (Lat/Long) and the zone name is “unknown” or “invalid”, the map locates the associated nation.



Cluster: 693

Zone: Adrxpzf

No. of unique combinations: 7

Zone: Adrxpzf

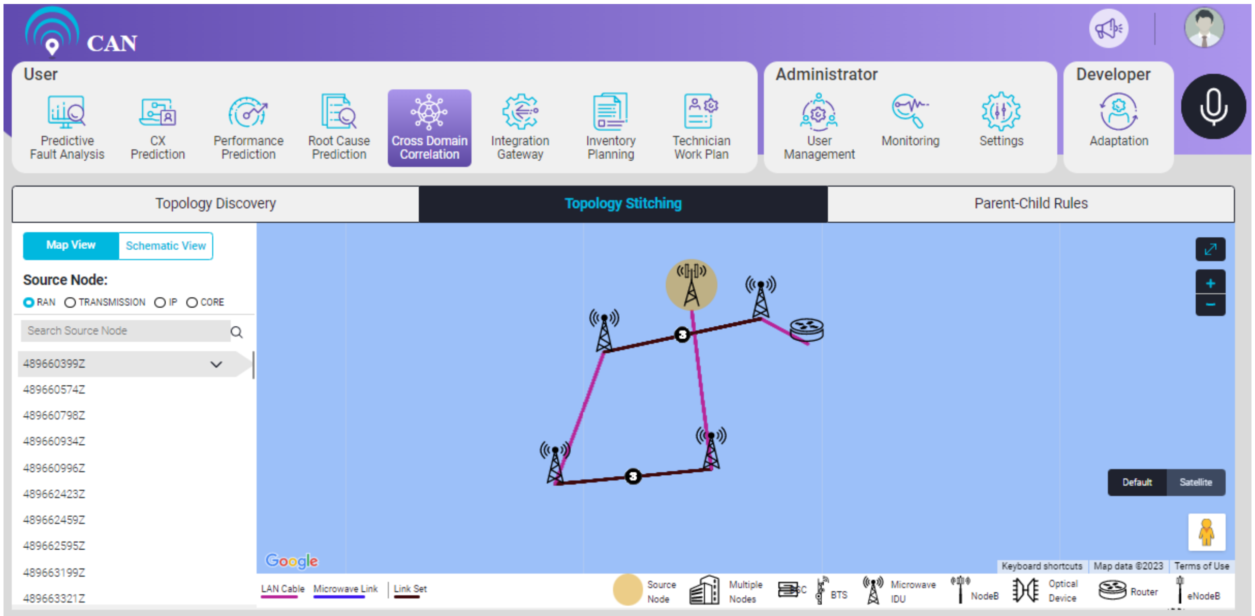
Cluster: 690

TRANSMISSION
776748172Z
KGK Slowlevi Hgzgfh
YZHV YZMW Hvgh G9 Uzro Zozin

Figure 7.16 - Invalid Zone

Topology Stitching

Topology Stitching screen visualises the discovered path. Link information is obtained from the inventory data. Based on the inventory data, topological connections across multiple domains (RAN, Transmission, IP and Core) are discovered. Connection traverse from RAN → Transmission → IP → Core (If provided). There may be single or multiple active links between any two nodes.



Source Node:

● RAN ○ TRANSMISSION ○ IP ○ CORE

489660399Z
489660574Z
489660798Z
489660934Z
489660996Z
489662423Z
489662459Z
489662595Z
489663199Z
489663321Z

Figure 7.17 - Topology Stitching Screen

User can select the required **Source Node** by clicking the radio button (RAN, TRANSMISSION, IP and CORE). By default, RAN is selected.

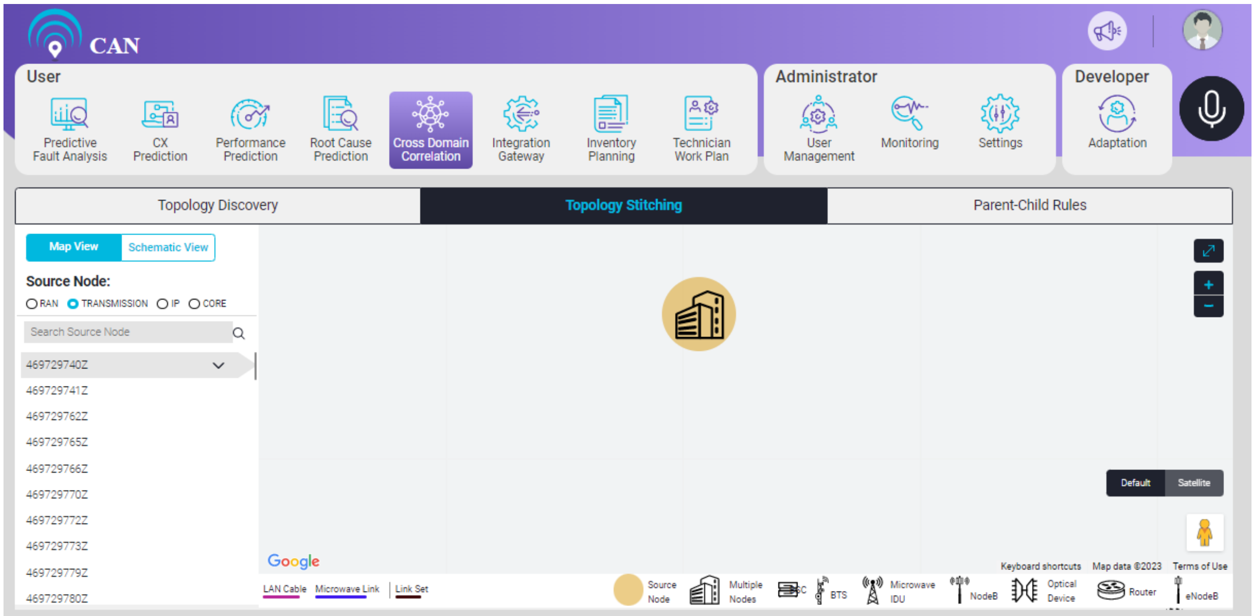
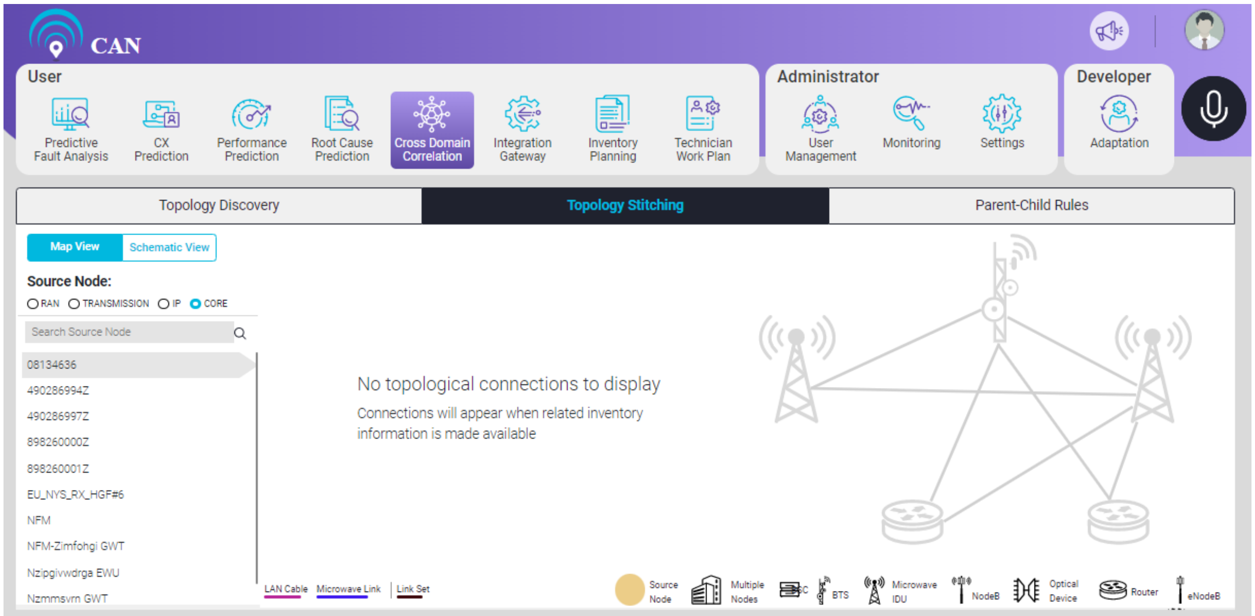


Figure 7.18 - Source Node Selection

If there are no connections, the screen displays a message “No topological connections to display”.

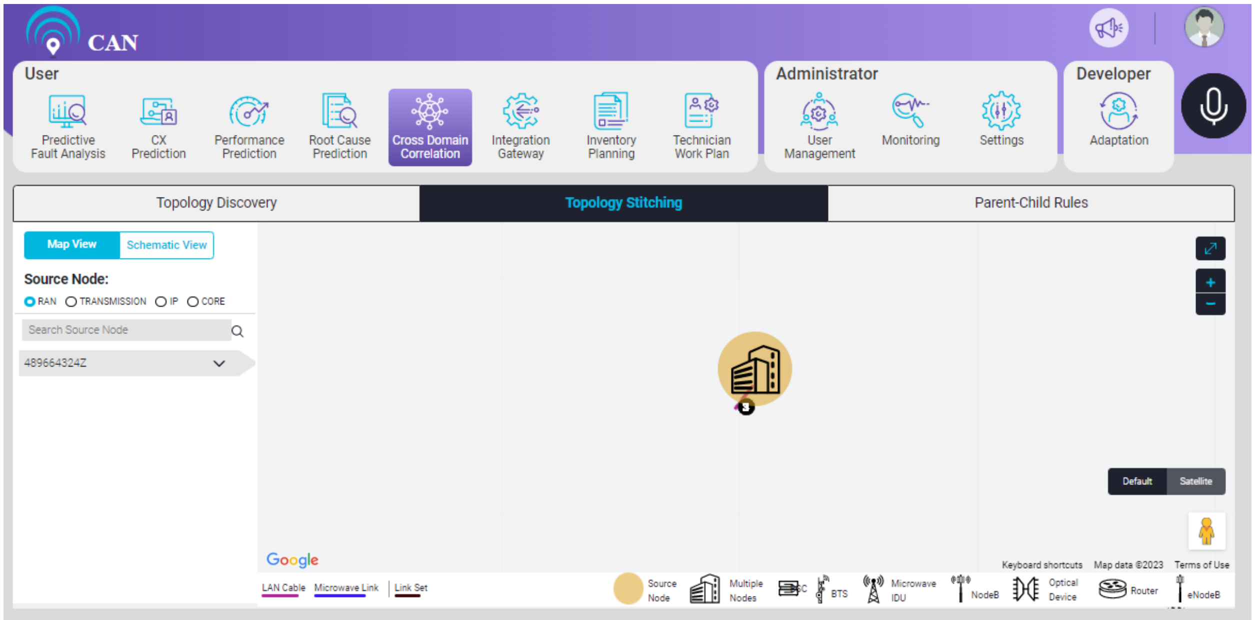


No topological connections to display

Connections will appear when related inventory information is made available

Figure 7.19 - Topology Stitching Screen with No Connections

User can use the search text box to search the Source Node. The screen will display the topological connections as per the search. To clear the search, click the 🔍 icon again.



Map View | Schematic View

Source Node:

● RAN ○ TRANSMISSION ○ IP ○ CORE

Search Source Node

489664324Z

Figure 7.20 - Search a Node

The topological connection has two views:

- Map View
- Schematic View

Map View

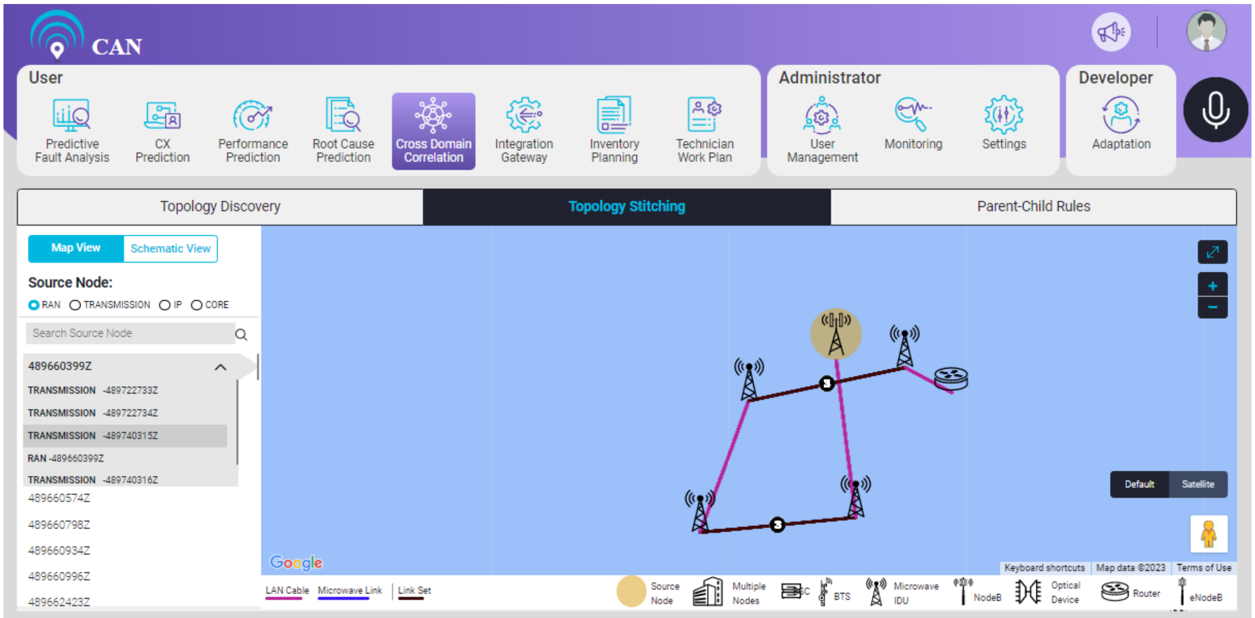
This view displays the topological connections on the map, when customer provides Lat-Long values for the nodes.

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 left side of the screen displays all the source nodes. Click the ⌄ icon to view the list of multiple nodes connected to that source node. User can click any node in the list to traverse to that node directly on the map.



Source Node:

● RAN ○ TRANSMISSION ○ IP ○ CORE

Search Source Node

489660399Z

TRANSMISSION -489722733Z

TRANSMISSION -489722734Z

TRANSMISSION -489740315Z

RAN -489660399Z

TRANSMISSION -489740316Z

489660574Z

489660798Z

489660934Z

489660996Z

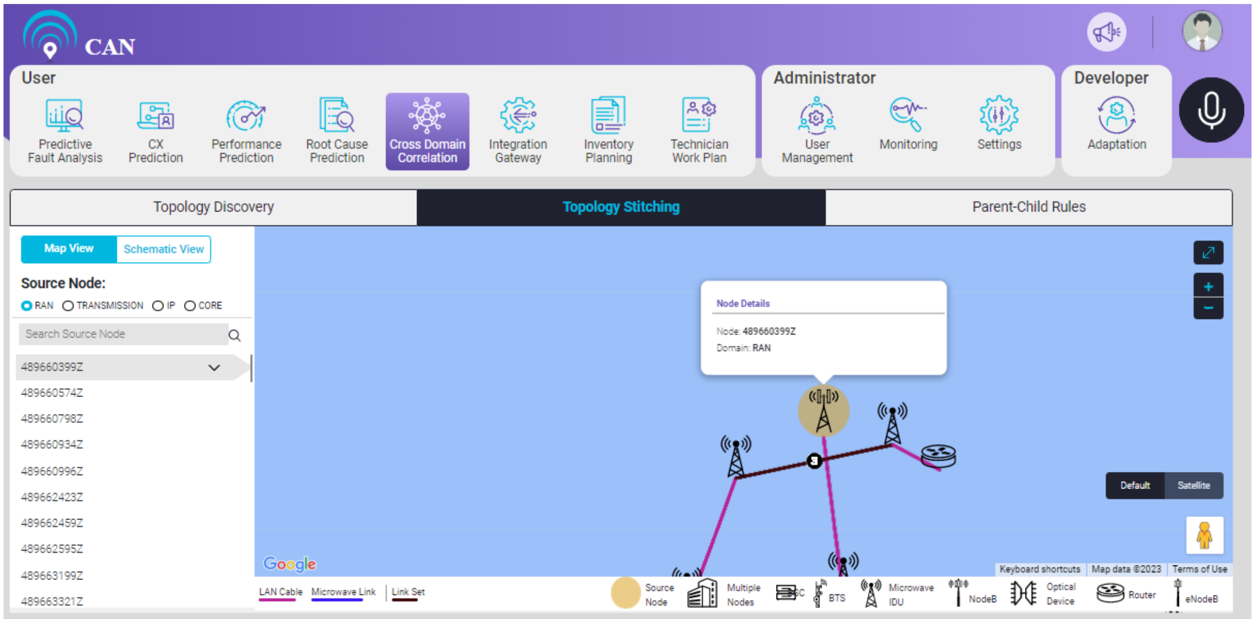
489662423Z

Figure 7.21 - Multiple Nodes within Source Node

To see the details of the particular node or link, click the pointers.

When user clicks, a pop-up will appear on the screen.

The pop-up on the screen displays the node details or active connection details.



Source Node:

● RAN ○ TRANSMISSION ○ IP ○ CORE

Search Source Node

489660399Z

489660574Z

489660798Z

489660934Z

489660996Z

489662423Z

489662459Z

489662595Z

489663199Z

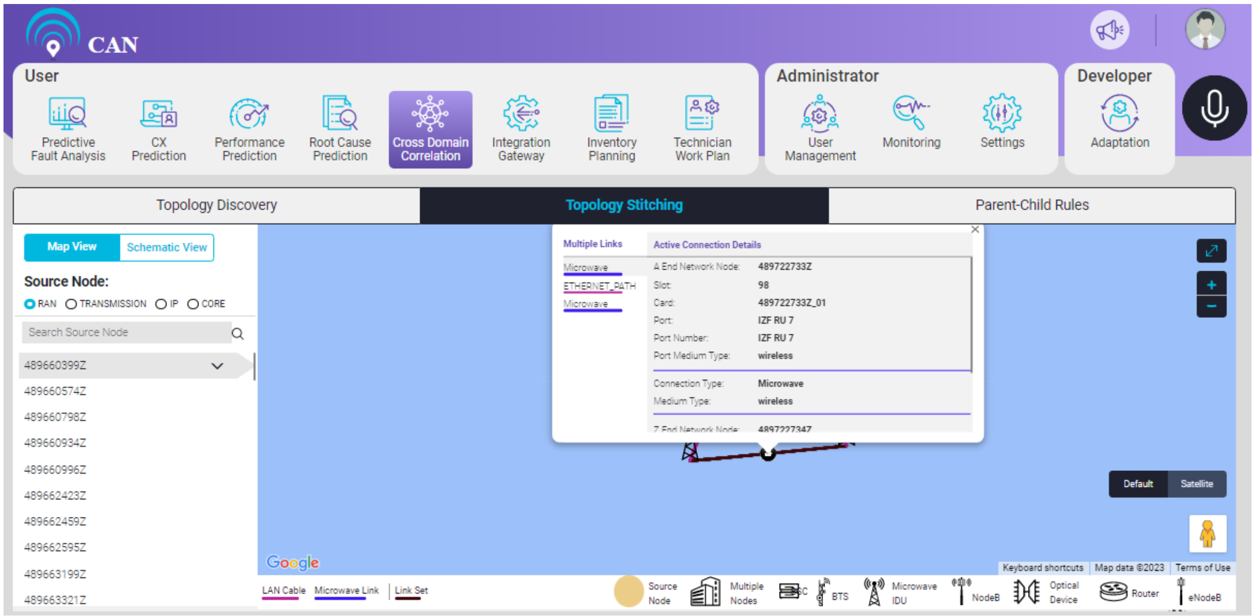
489663321Z

Node Details

Node: 489660399Z

Domain: RAN

Figure 7.22 - Node Details



Multiple Links

- Microwave
- ETHERNET_PATH
- Microwave

Active Connection Details

A End Network Node:	489722733Z
Slot:	98
Card:	489722733Z_01
Port:	IZF RU 7
Port Number:	IZF RU 7
Port Medium Type:	wireless
Connection Type:	Microwave
Medium Type:	wireless
Z End Network Node:	489722734Z

Figure 7.23 - Active Connection Details

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

Schematic View

Even if Lat-Long values are not provided for the nodes, schematic view will be displayed and co-located nodes are displayed with dotted area.

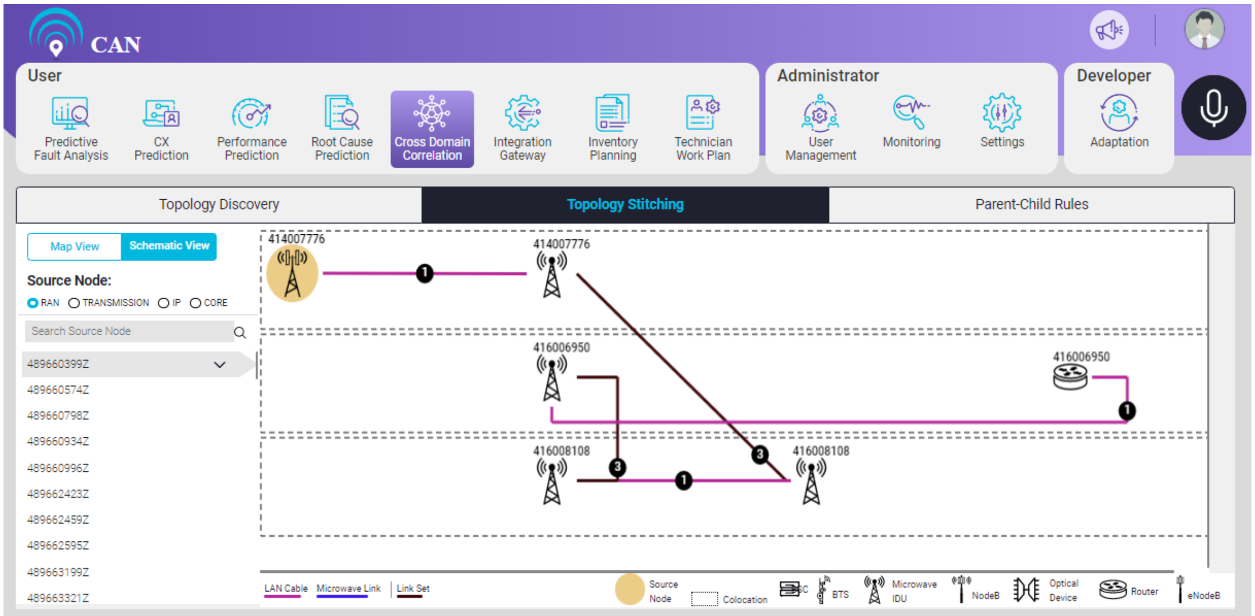
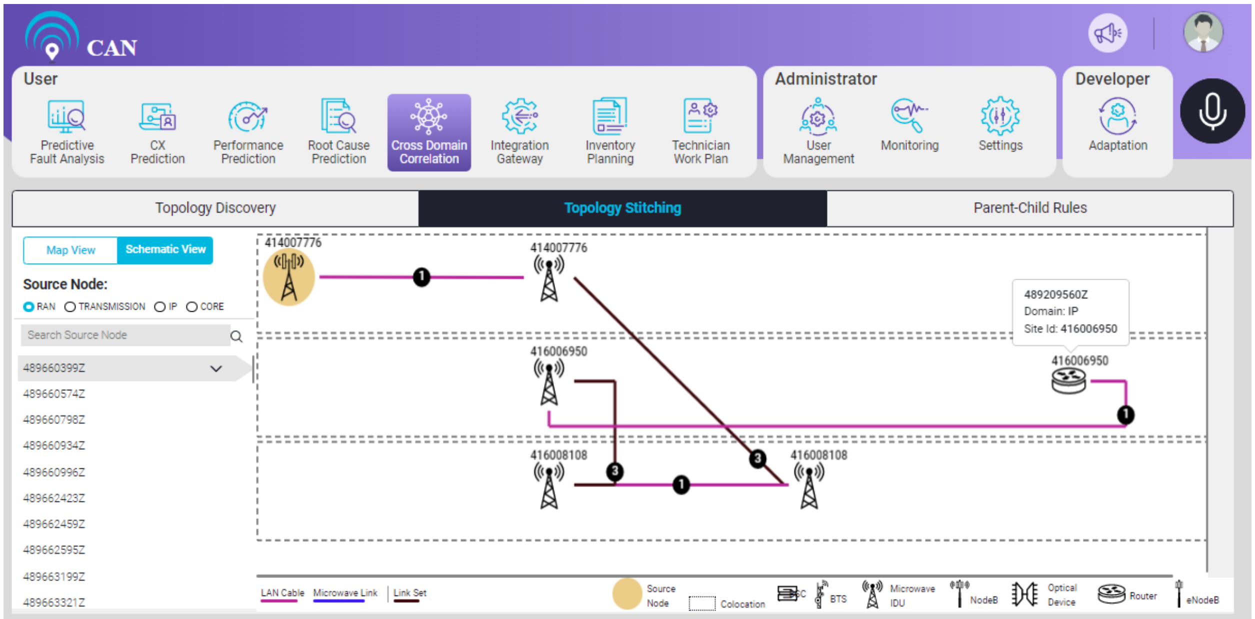


Figure 7.24 - Schematic View

To see the details of the particular node, click the pointer.

When user clicks, a pop-up will appear on the screen.

The pop-up on the screen displays the node details.



489209560Z
Domain: IP
Site Id: 416006950

Figure 7.25 - Node Details

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

Parent-Child Rules

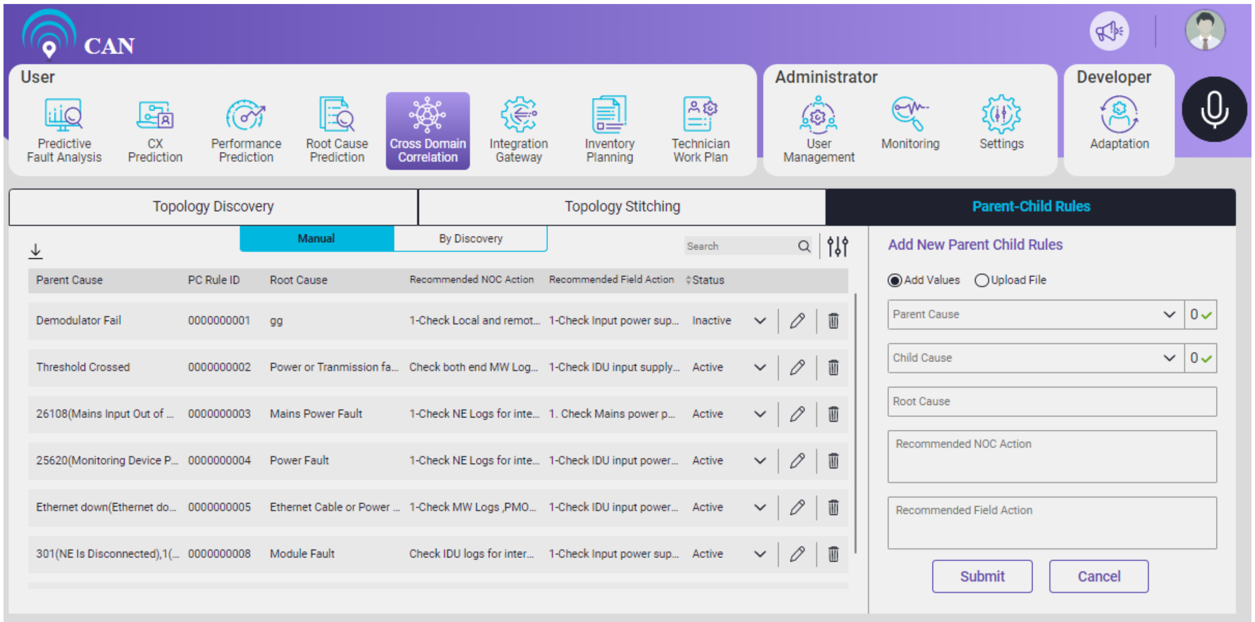
Parent-child correlation is an enhanced way of root cause analysis. The parent cause for a group of errors are configured or discovered. The rules are formed either by mapping parent-child details manually or by discovery method based on the fault logs.

Parent-Child Rules contains two tabs:

1. Manual
2. By Discovery

Manual

The parent-child details are mapped manually by using the inventory data provided by customers. The tabular view shows the list of configured parent-child rules.



Parent Cause	PC Rule ID	Root Cause	Recommended NOC Action	Recommended Field Action	⇕Status
Demodulator Fail	0000000001	gg	1-Check Local and remot...	1-Check Input power sup...	Inactive
Threshold Crossed	0000000002	Power or Tranmission fa...	Check both end MW Log...	1-Check IDU input supply...	Active
26108(Mains Input Out of ...	0000000003	Mains Power Fault	1-Check NE Logs for inte...	1. Check Mains power p...	Active
25620(Monitoring Device P...	0000000004	Power Fault	1-Check NE Logs for inte...	1-Check IDU input power...	Active
Ethernet down(Ethernet do...	0000000005	Ethernet Cable or Power ...	1-Check MW Logs ,PMO...	1-Check IDU input power...	Active
301(NE Is Disconnected),1(...	0000000008	Module Fault	Check IDU logs for inter...	1-Check Input power sup...	Active

Add New Parent Child Rules

● Add Values ○ Upload File

Parent Cause 0✓

Child Cause 0✓

Root Cause

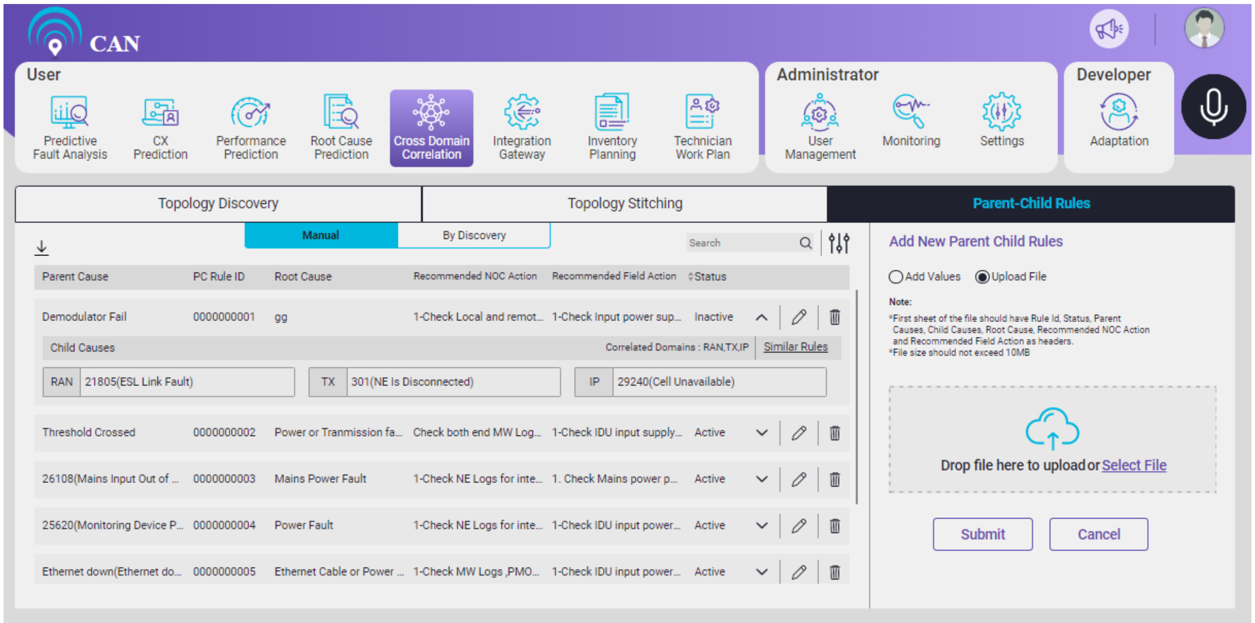
Recommended NOC Action

Recommended Field Action

Submit Cancel

Figure 7.26 - Parent-Child Correlation Manual Screen

1. To view more details of the rule click on ⌄ icon. The configured rule has following attributes:
   - Parent Cause
   - PC Rule Id
   - Root Cause
   - Recommended NOC Action
   - Recommended Field Action
   - Status
2. User can view Child Causes and the Correlated Domains.
3. User can view similar configured rules by clicking Similar Rules. If there are no similar rules, system will display “No Similar Rule found”.
4. User can sort the configured rules based on the **Status** (Active/Inactive), by clicking the sort icon ⇕.



Parent Cause	PC Rule ID	Root Cause	Recommended NOC Action	Recommended Field Action	Status
Demodulator Fail	0000000001	gg	1-Check Local and remot...	1-Check Input power sup...	Inactive
Threshold Crossed	0000000002	Power or Tranmission fa...	Check both end MW Log...	1-Check IDU input supply...	Active
26108(Mains Input Out of ...	0000000003	Mains Power Fault	1-Check NE Logs for inte...	1. Check Mains power p...	Active
25620(Monitoring Device P...	0000000004	Power Fault	1-Check NE Logs for inte...	1-Check IDU input power...	Active
Ethernet down(Ethernet do...	0000000005	Ethernet Cable or Power ...	1-Check MW Logs ,PMO...	1-Check IDU input power...	Active

Child Causes — Correlated Domains : RAN,TX,IP

RAN	21805(ESL Link Fault)	TX	301(NE Is Disconnected)	IP	29240(Cell Unavailable)

Add New Parent Child Rules

○ Add Values ● Upload File

Note:

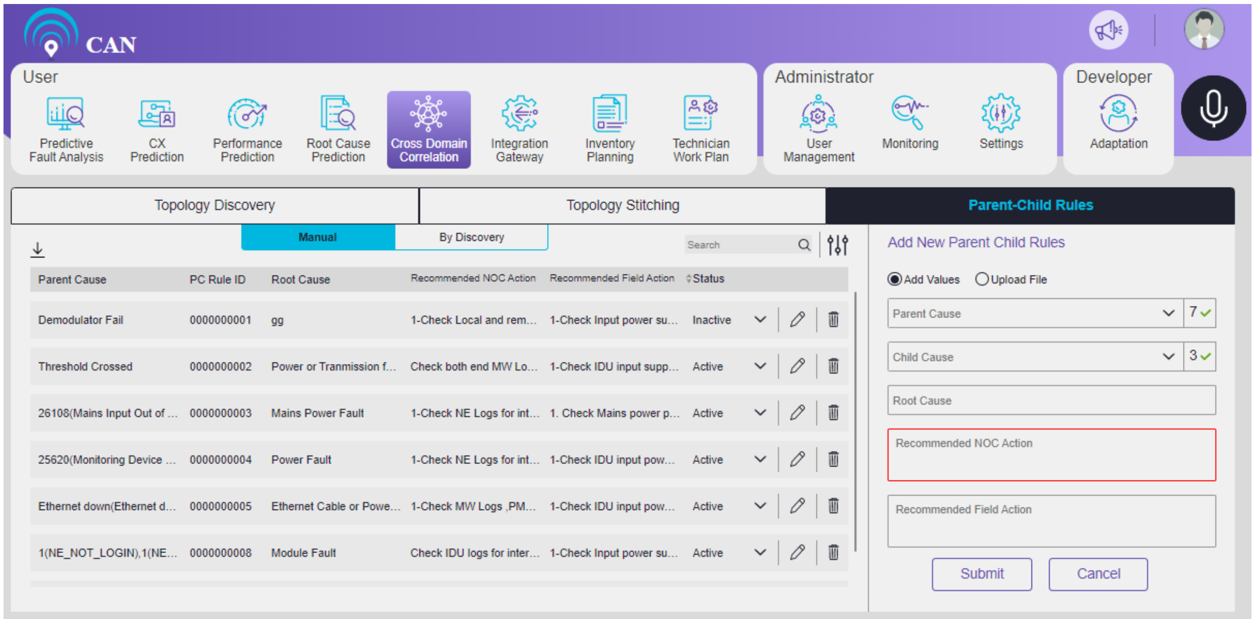
*First sheet of the file should have Rule Id, Status, Parent Causes, Child Causes, Root Cause, Recommended NOC Action and Recommended Field Action as headers.
*File size should not exceed 10MB

Figure 7.27 - Rule Details

To Add New Parent Child Rules

1. Click on **Add Values**.
2. Select one or multiple **Parent Cause** from the dropdown. Maximum number for parent causes is configurable. By default, the maximum number is 7.
3. Select one or multiple **Child Cause** from the dropdown. Any number of child causes can be selected.
4. Enter the Root Cause, Recommended NOC Action and Recommended Field Action.
5. Click **Submit** to create a new rule.

NOTE: Errors in the input file will be sent over email.



Parent Cause	PC Rule ID	Root Cause	Recommended NOC Action	Recommended Field Action	Status
Demodulator Fail	0000000001	gg	1-Check Local and rem...	1-Check Input power su...	Inactive
Threshold Crossed	0000000002	Power or Tranmission f...	Check both end MW Lo...	1-Check IDU input supp...	Active
26108(Mains Input Out of ...	0000000003	Mains Power Fault	1-Check NE Logs for int...	1. Check Mains power p...	Active
25620(Monitoring Device ...	0000000004	Power Fault	1-Check NE Logs for int...	1-Check IDU input pow...	Active
Ethernet down(Ethernet d...	0000000005	Ethernet Cable or Powe...	1-Check MW Logs ,PM...	1-Check IDU input pow...	Active
1(NE_NOT_LOGIN),1(NE...	0000000008	Module Fault	Check IDU logs for inter...	1-Check Input power su...	Active

Add New Parent Child Rules

● Add Values ○ Upload File

Parent Cause 7 ✓

Child Cause 3 ✓

Root Cause

Recommended NOC Action

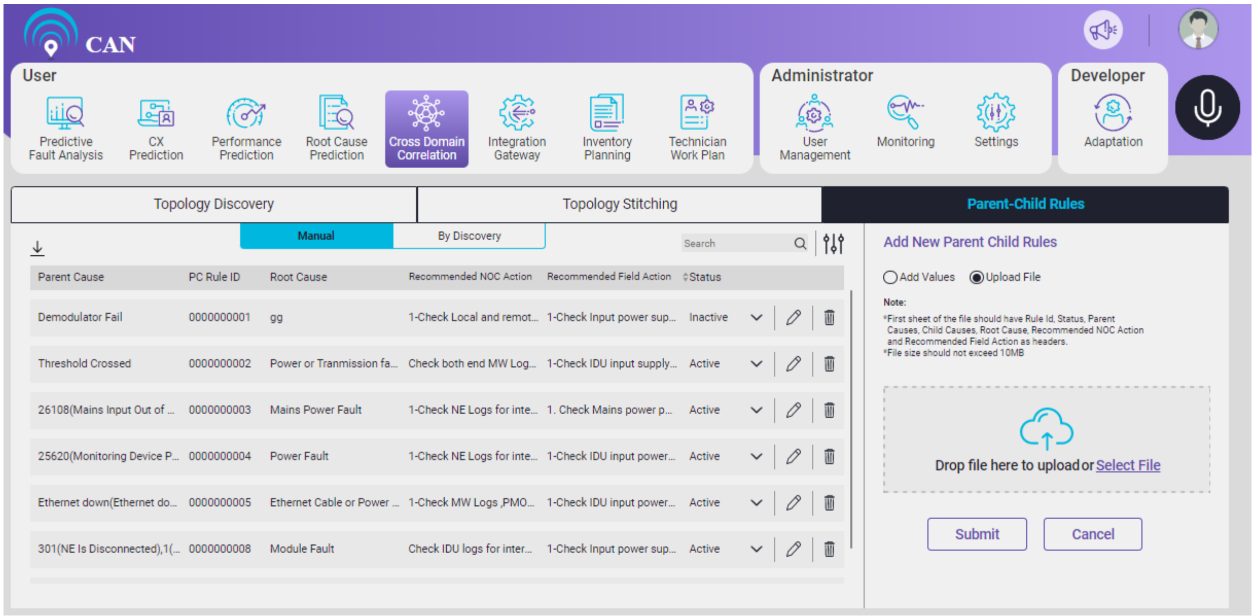
Recommended Field Action

Figure 7.28 - Add Values

1. Click on Upload File.
2. User can select the file to upload or use the drag and drop option to upload the file.
3. Click **Submit** to create new rule.

Note:

- **First sheet of the file should have Rule Id, Status, Parent Causes, Child Causes, Root Cause, Recommended NOC Action and Recommended Field Action as headers.**
- **File size should not exceed 10MB.**



Parent Cause	PC Rule ID	Root Cause	Recommended NOC Action	Recommended Field Action	Status
Demodulator Fail	0000000001	gg	1-Check Local and remot...	1-Check Input power sup...	Inactive
Threshold Crossed	0000000002	Power or Tranmission fa...	Check both end MW Log...	1-Check IDU input supply...	Active
26108(Mains Input Out of ...	0000000003	Mains Power Fault	1-Check NE Logs for inte...	1. Check Mains power p...	Active
25620(Monitoring Device P...	0000000004	Power Fault	1-Check NE Logs for inte...	1-Check IDU input power...	Active
Ethernet down(Ethernet do...	0000000005	Ethernet Cable or Power ...	1-Check MW Logs ,PMO...	1-Check IDU input power...	Active
301(NE Is Disconnected),1(...	0000000008	Module Fault	Check IDU logs for inter...	1-Check Input power sup...	Active

Add New Parent Child Rules

○ Add Values ● Upload File

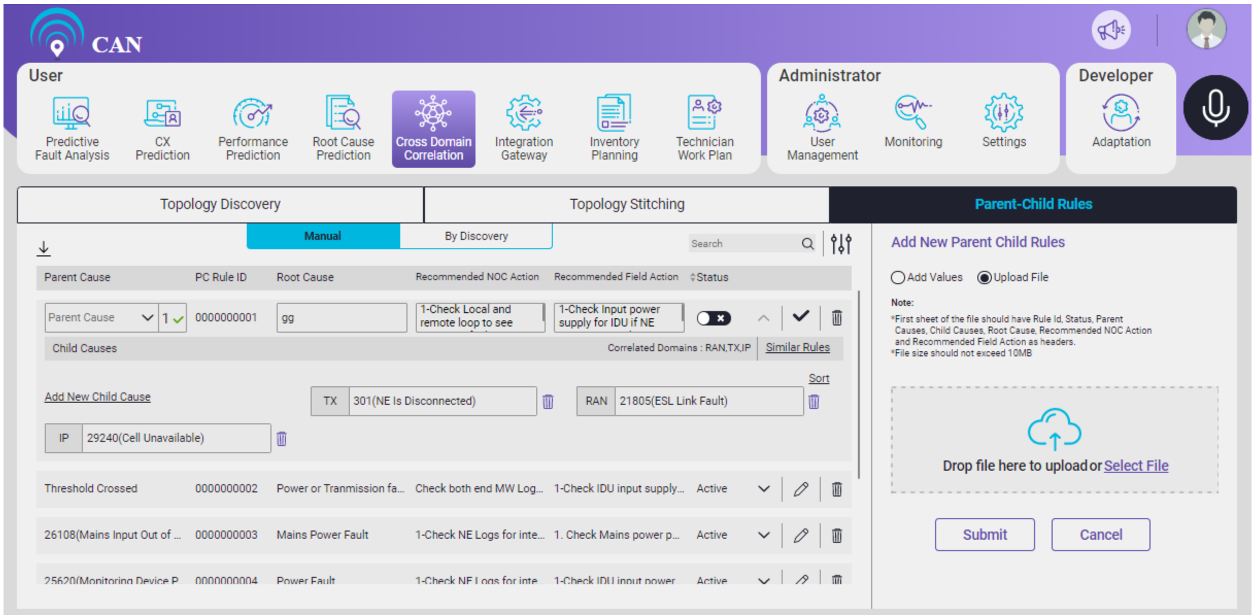
Note:

*First sheet of the file should have Rule Id, Status, Parent Causes, Child Causes, Root Cause, Recommended NOC Action and Recommended Field Action as headers.
*File size should not exceed 10MB

Figure 7.29 - Upload File

To Edit the Existing Rule

1. Edit a rule by clicking the edit icon ✎.
2. User can select/deselect the **Parent Cause** from the dropdown.
3. User can edit Root Cause, Recommended NOC Action and Recommended Field Action.
4. User can change the **Status** of the rule as Active/Inactive by clicking the toggle button ✖.
5. User can add a child cause by clicking Add New Child Cause and delete an existing child cause by clicking the delete icon 🗑.
6. User has an option to Sort the child causes based on Domain name.
7. Click the Update icon ✓ to save the changes to the rule.
8. Delete a rule configuration by clicking the delete icon 🗑.



Parent Cause	PC Rule ID	Root Cause	Recommended NOC Action	Recommended Field Action	Status
Parent Cause 1 ✓	0000000001	gg	1-Check Local and remote loop to see	1-Check Input power supply for IDU if NE	✖
Threshold Crossed	0000000002	Power or Tranmission fa...	Check both end MW Log...	1-Check IDU input supply...	Active
26108(Mains Input Out of ...	0000000003	Mains Power Fault	1-Check NE Logs for inte...	1. Check Mains power p...	Active
25620(Monitoring Device P	0000000004	Power Fault	1-Check NE Logs for inte	1-Check IDU input power	Active

Child Causes

Correlated Domains : RAN,TX,IP

Similar Rules

Sort

Add New Child Cause

TX	301(NE Is Disconnected)
RAN	21805(ESL Link Fault)
IP	29240(Cell Unavailable)

Add New Parent Child Rules

○ Add Values ● Upload File

Note:
*First sheet of the file should have Rule Id, Status, Parent Causes, Child Causes, Root Cause, Recommended NOC Action and Recommended Field Action as headers.
*File size should not exceed 10MB

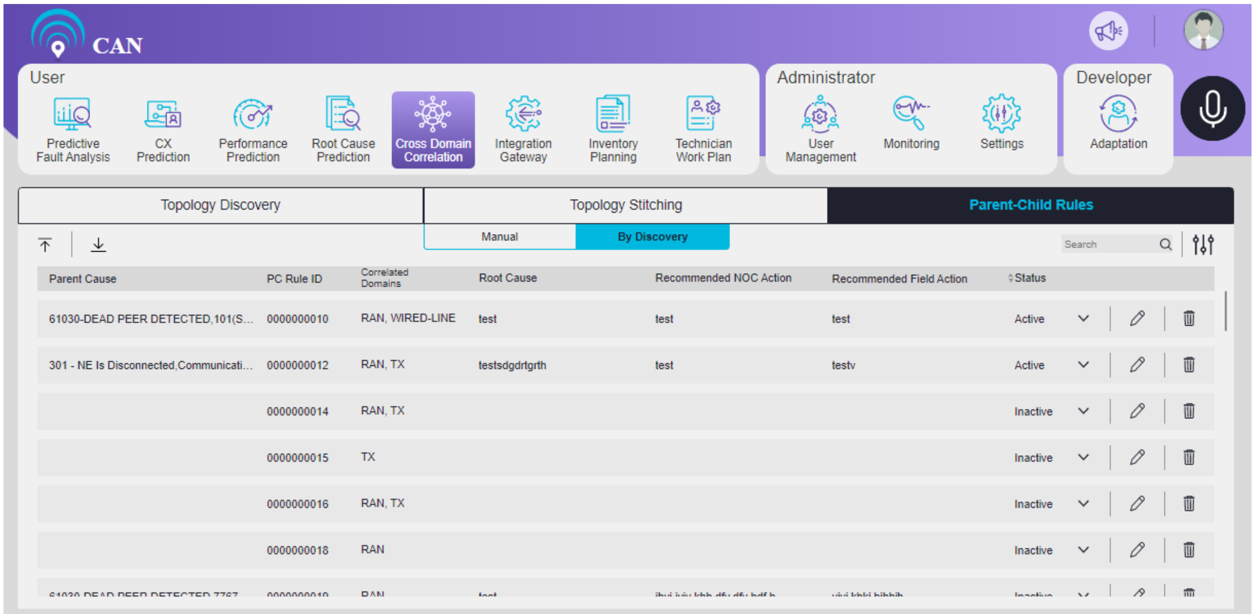
Drop file here to upload or Select File

Submit Cancel

Figure 7.30 - Edit Rule

By Discovery

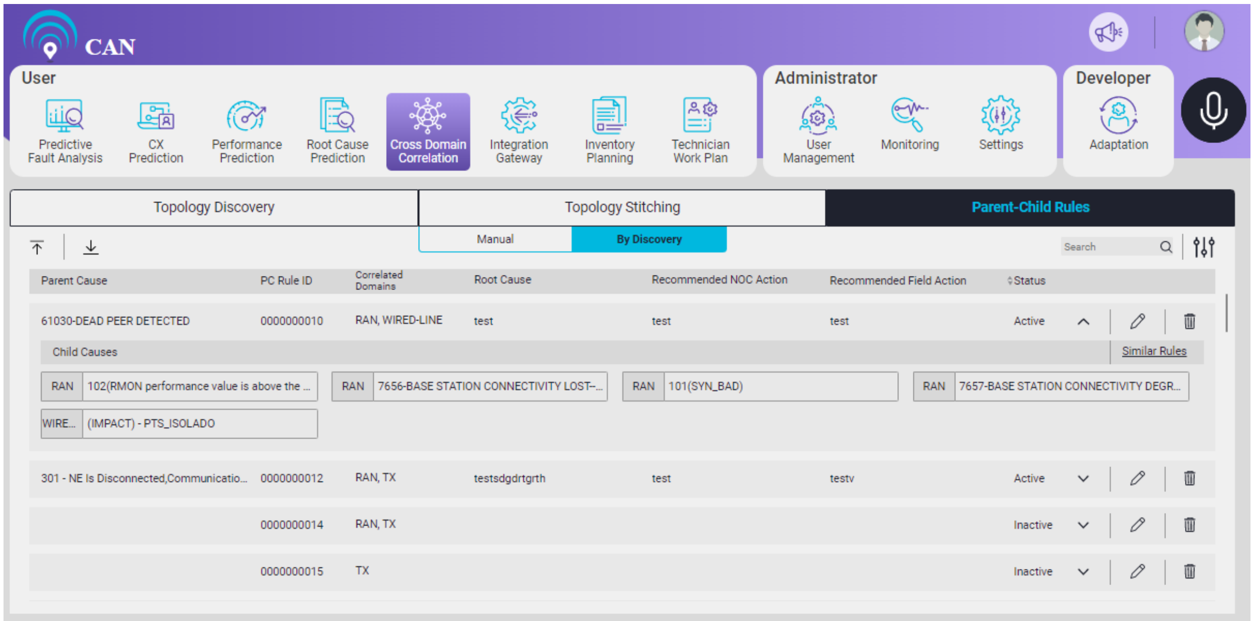
CAN discovers the child causes among the clustered faults using By Discovery method. User identifies and marks the parent cause among the child causes.



Parent Cause	PC Rule ID	Correlated Domains	Root Cause	Recommended NOC Action	Recommended Field Action	Status
61030-DEAD PEER DETECTED,101(S...	0000000010	RAN, WIRED-LINE	test	test	test	Active
301 - NE Is Disconnected,Communicati...	0000000012	RAN, TX	testsdgdrtgrth	test	testv	Active
	0000000014	RAN, TX				Inactive
	0000000015	TX				Inactive
	0000000016	RAN, TX				Inactive
	0000000018	RAN				Inactive
61030-DEAD PEER DETECTED,7767	0000000019	RAN	test	jhvi ivjv khh dfu dfu hdf h	vivi kbki hihbih	Inactive

Figure 7.31 - PC Correlation By Discovery Screen

1. To view more details of the rule click on ⌄icon. The configured rule has following attributes:
   - Parent Cause
   - PC Rule Id
   - Correlated Domains
   - Root Cause
   - Recommended NOC Action
   - Recommended Field Action
   - Status
   - Child Causes
2. User can view similar configured rules by clicking Similar Rules. If there are no similar rules, system will display "No Similar Rule found".
3. User can sort the configured rules based on the **Status** (Active/Inactive), by clicking the sort icon ⇕.

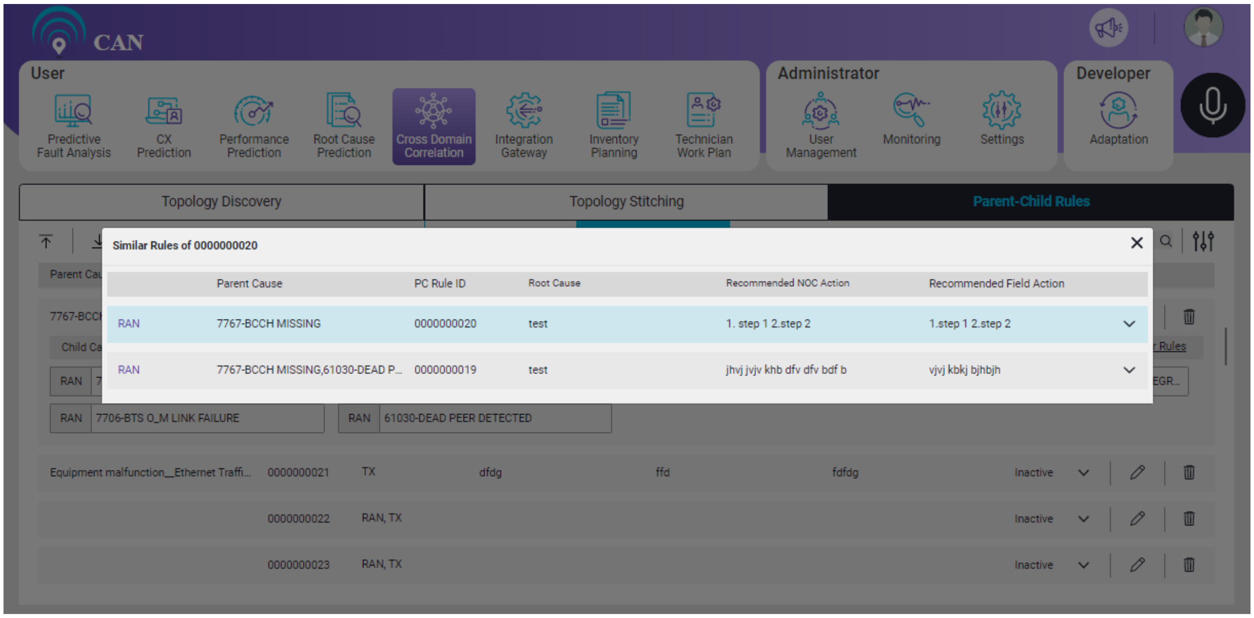


Parent Cause	PC Rule ID	Correlated Domains	Root Cause	Recommended NOC Action	Recommended Field Action	Status
61030-DEAD PEER DETECTED	0000000010	RAN, WIRED-LINE	test	test	test	Active
301 - NE Is Disconnected,Communicatio...	0000000012	RAN, TX	testsdgdrtgrth	test	testv	Active
	0000000014	RAN, TX				Inactive
	0000000015	TX				Inactive

Child Causes — Similar Rules

RAN	102(RMON performance value is above the ...
RAN	7656-BASE STATION CONNECTIVITY LOST-...
RAN	101(SYN_BAD)
RAN	7657-BASE STATION CONNECTIVITY DEGR...
WIRE...	(IMPACT) - PTS_ISOLADO

Figure 7.32 - Rule Details



Similar Rules of 0000000020

	Parent Cause	PC Rule ID	Root Cause	Recommended NOC Action	Recommended Field Action
RAN	7767-BCCH MISSING	0000000020	test	1. step 1 2.step 2	1.step 1 2.step 2
RAN	7767-BCCH MISSING,61030-DEAD P...	0000000019	test	jhvj jvjv khb dfv dfv bdf b	vjvj kbkj bjhbjh

RAN	7706-BTS O_M LINK FAILURE
RAN	61030-DEAD PEER DETECTED

Equipment malfunction__Ethernet Traffi...	0000000021	TX	dfdg	ffd	fdfdg	Inactive
	0000000022	RAN, TX				Inactive
	0000000023	RAN, TX				Inactive

Figure 7.33 - Similar Rules

To Add New Parent Child Rules

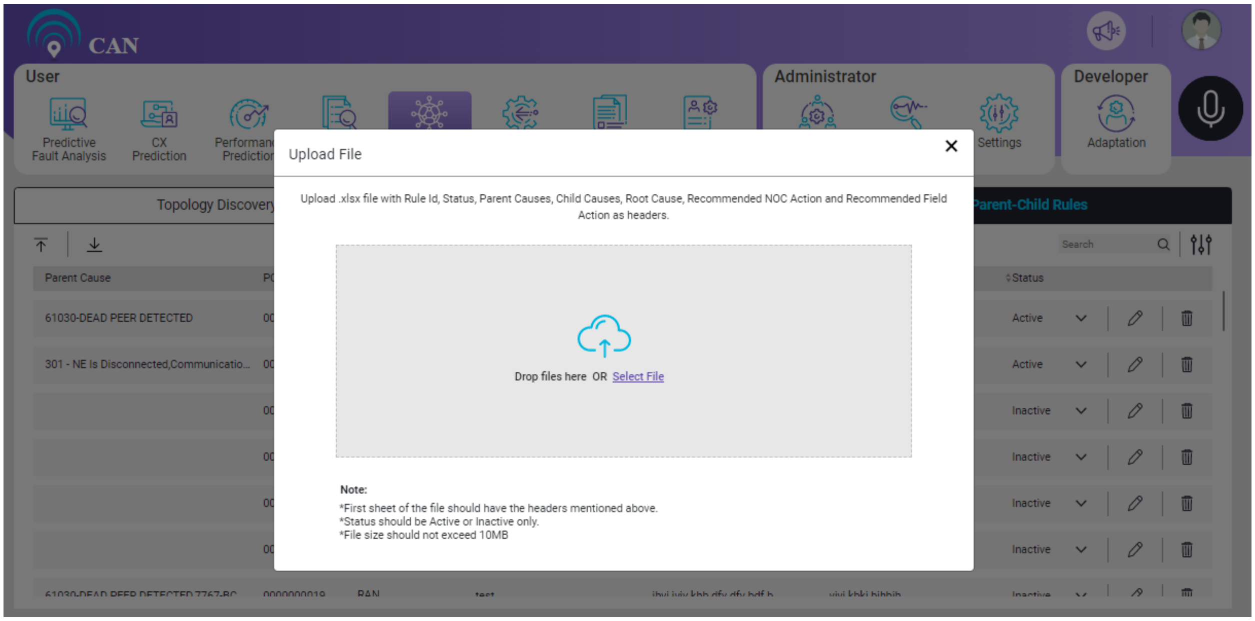
1. Click on Upload File icon ⤒ .
2. User can select the file to upload or use the drag and drop option to upload the file.
3. This is an option to create new rule or edit the existing parent-child rules.

NOTE: Errors in the input file will be sent over email.

Upload .xlsx file with Rule Id, Status, Parent Causes, Child Causes, Root Cause, Recommended NOC Action and Recommended Field Action as headers.

Note:

- First sheet of the file should have the headers mentioned above.
- Status should be Active or Inactive only.
- File size should not exceed 10MB.



Upload File

Upload .xlsx file with Rule Id, Status, Parent Causes, Child Causes, Root Cause, Recommended NOC Action and Recommended Field Action as headers.

Drop files here OR Select File

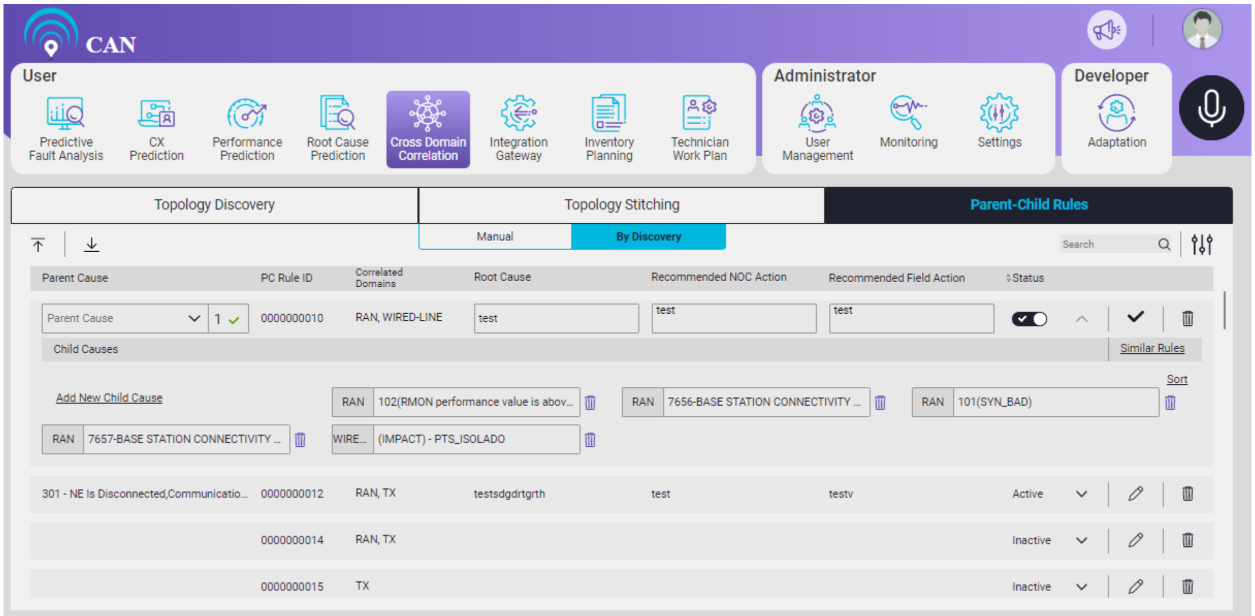
Note:

*First sheet of the file should have the headers mentioned above.
*Status should be Active or Inactive only.
*File size should not exceed 10MB

Figure 7.34 - Upload File

To Edit the Existing Rule

1. Edit a rule by clicking the edit icon ✎.
2. User can select/deselect the **Parent Cause** from the dropdown.
3. User can edit Root Cause, Recommended NOC Action and Recommended Field Action.
4. User can change the **Status** of the rule as Active/Inactive by clicking the toggle button ○✖.
5. User can add a child cause by clicking Add New Child Cause and delete an existing child cause by clicking the delete icon 🗑.
6. User has an option to Sort the child causes based on Domain name.
7. Click the Update icon ✓ to save the changes to the rule.
8. Delete a rule configuration by clicking the delete icon 🗑.



Parent Cause	PC Rule ID	Correlated Domains	Root Cause	Recommended NOC Action	Recommended Field Action	Status
Parent Cause 1 ✓	0000000010	RAN, WIRED-LINE	test	test	test	✓
301 - NE Is Disconnected,Communicatio...	0000000012	RAN, TX	testsdgdrtgrth	test	testv	Active
	0000000014	RAN, TX				Inactive
	0000000015	TX				Inactive

Child Causes

Similar Rules

Sort

Add New Child Cause

RAN 102(RMON performance value is abov...

RAN 7656-BASE STATION CONNECTIVITY ...

RAN 101(SYN_BAD)

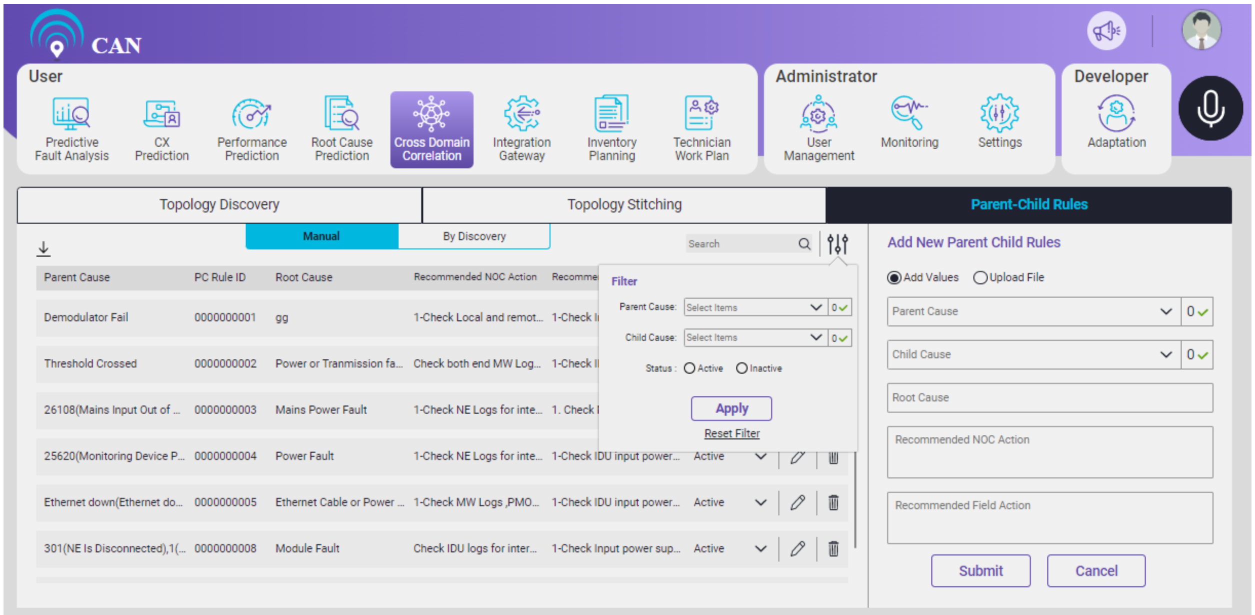
RAN 7657-BASE STATION CONNECTIVITY ...

WIRE... (IMPACT) - PTS_ISOLADO

Figure 7.35 - Edit Rule

Common Features

Click the **Filter** icon ⫶ to filter the rules based on Parent Cause, Child Cause and Status. Click **Apply** to display the filtered rules.



Parent Cause	PC Rule ID	Root Cause	Recommended NOC Action	Recomme...	
Demodulator Fail	0000000001	gg	1-Check Local and remot...	1-Check I	
Threshold Crossed	0000000002	Power or Tranmission fa...	Check both end MW Log...	1-Check I	
26108(Mains Input Out of ...	0000000003	Mains Power Fault	1-Check NE Logs for inte...	1. Check I	
25620(Monitoring Device P...	0000000004	Power Fault	1-Check NE Logs for inte...	1-Check IDU input power...	Active
Ethernet down(Ethernet do...	0000000005	Ethernet Cable or Power ...	1-Check MW Logs ,PMO...	1-Check IDU input power...	Active
301(NE Is Disconnected),1(...	0000000008	Module Fault	Check IDU logs for inter...	1-Check Input power sup...	Active

Filter

Parent Cause: Select Items 0 ✓

Child Cause: Select Items 0 ✓

Status : ○ Active ○ Inactive

Apply

Reset Filter

Add New Parent Child Rules

● Add Values ○ Upload File

Parent Cause 0 ✓

Child Cause 0 ✓

Root Cause

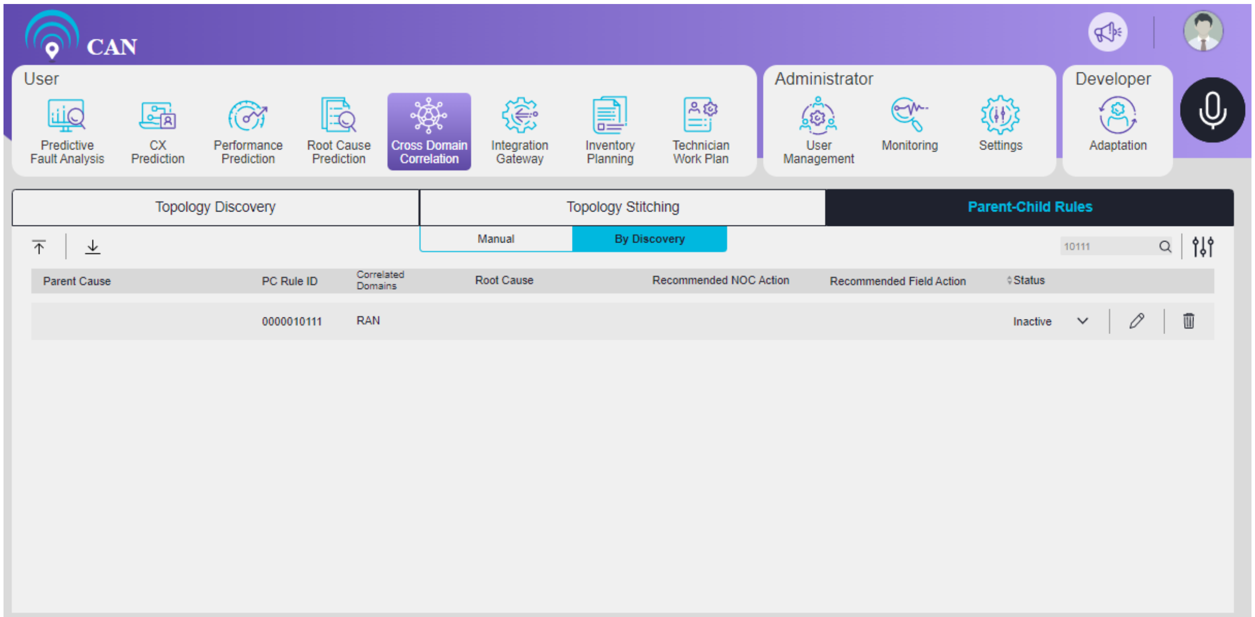
Recommended NOC Action

Recommended Field Action

Submit Cancel

Figure 7.36 - Filter Rule

User has the option to **Search** a rule based on **PC Rule Id**.

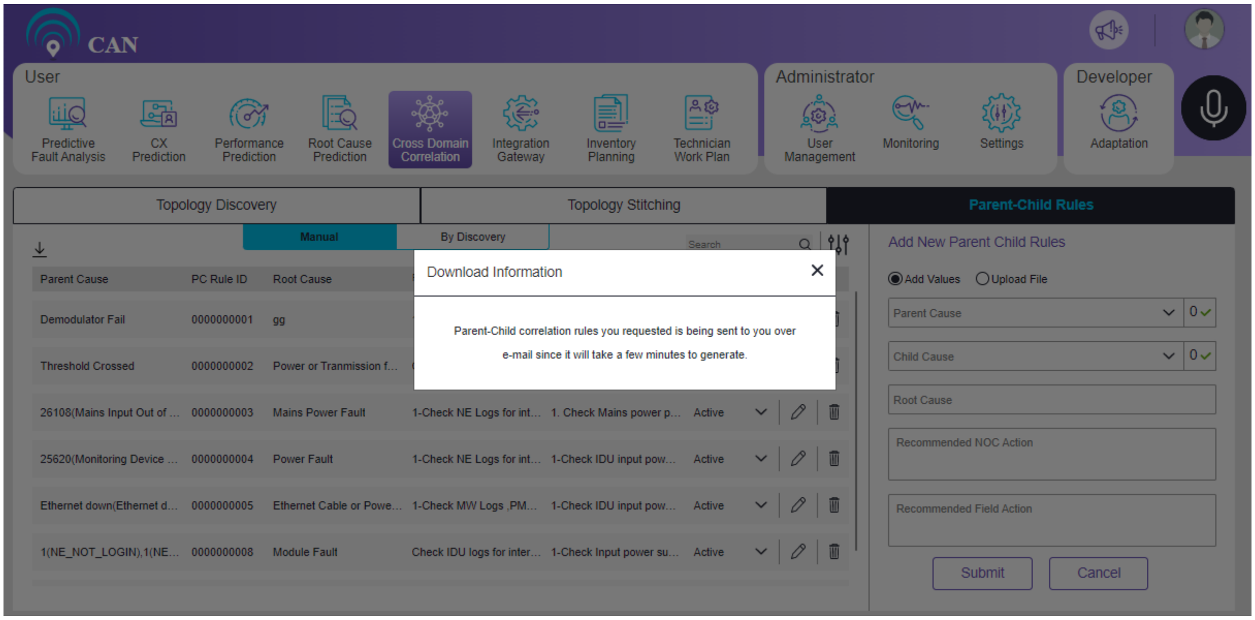


10111

Parent Cause	PC Rule ID	Correlated Domains	Root Cause	Recommended NOC Action	Recommended Field Action	Status
	0000010111	RAN				Inactive

Figure 7.37 - Search Rule

Click the **Download** icon ⤓ to download the parent and child causes. User will receive the generated report via email.



Parent Cause	PC Rule ID	Root Cause			
Demodulator Fail	0000000001	gg			
Threshold Crossed	0000000002	Power or Tranmission f...			
26108(Mains Input Out of ...	0000000003	Mains Power Fault	1-Check NE Logs for int...	1. Check Mains power p...	Active
25620(Monitoring Device ...	0000000004	Power Fault	1-Check NE Logs for int...	1-Check IDU input pow...	Active
Ethernet down(Ethernet d...	0000000005	Ethernet Cable or Powe...	1-Check MW Logs ,PM...	1-Check IDU input pow...	Active
1(NE_NOT_LOGIN),1(NE...	0000000008	Module Fault	Check IDU logs for inter...	1-Check Input power su...	Active

Download Information ✕

Parent-Child correlation rules you requested is being sent to you over e-mail since it will take a few minutes to generate.

Add New Parent Child Rules

● Add Values ○ Upload File

Parent Cause 0

Child Cause 0

Root Cause

Recommended NOC Action

Recommended Field Action

Submit Cancel

Figure 7.38 - Download File

Page Intentionally Left Blank

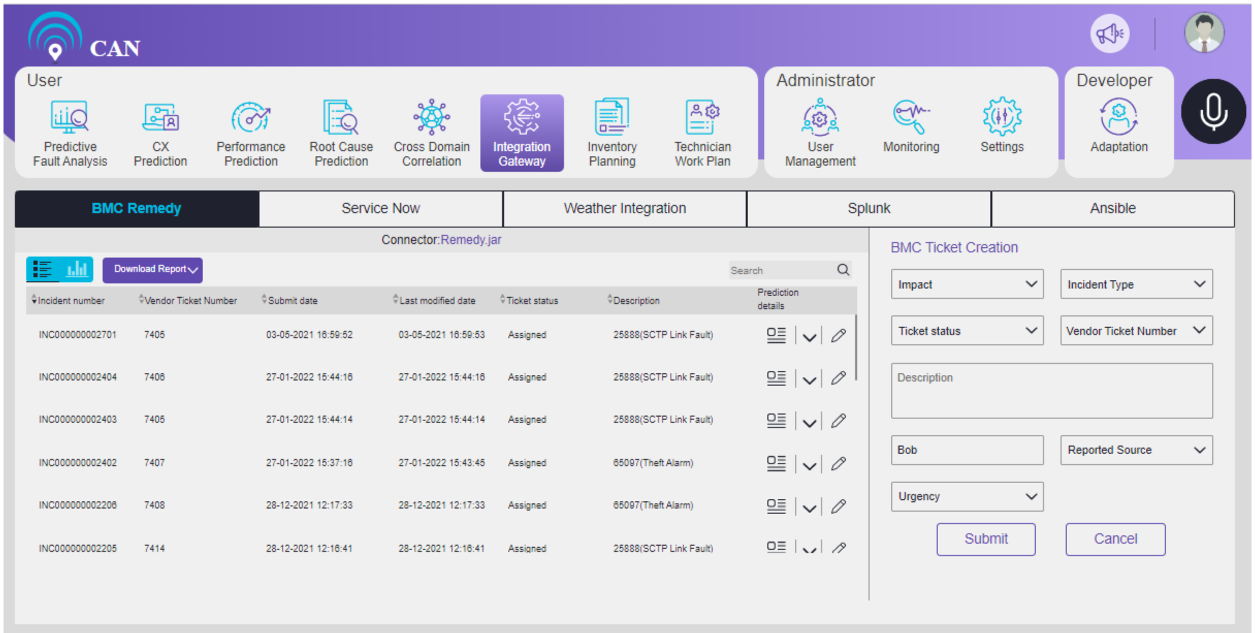
8. INTEGRATION GATEWAY

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

1. BMC Remedy
2. Service Now
3. Weather Integration
4. Splunk
5. Ansible

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 be notified through mail.



Connector:Remedy.jar

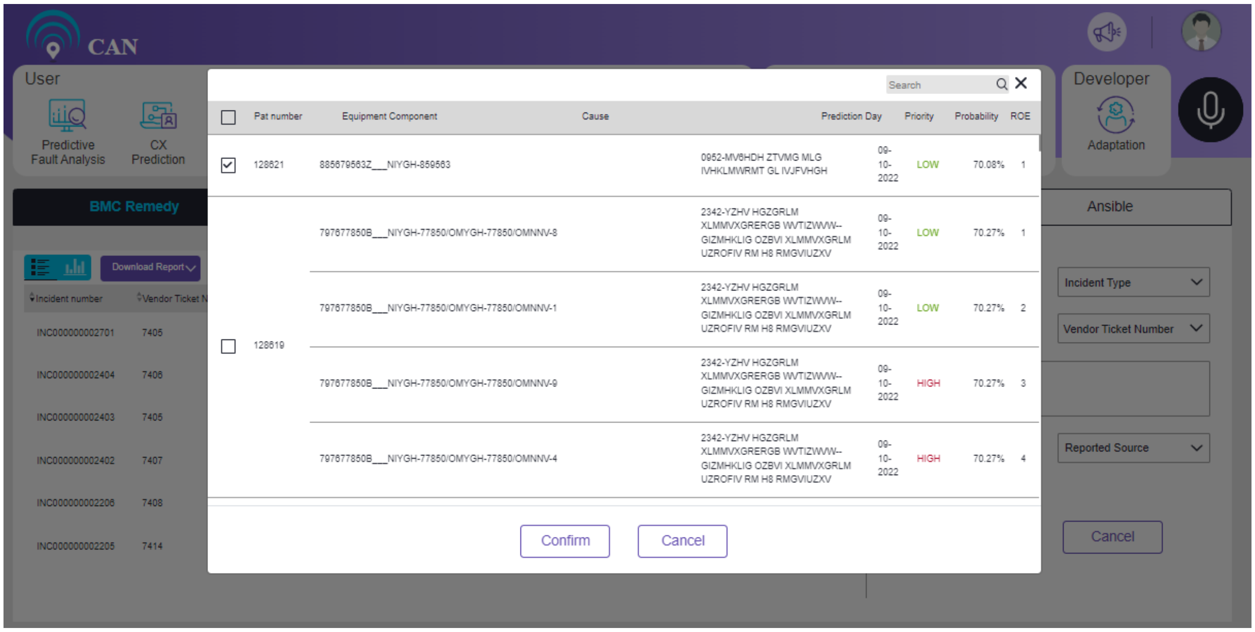
Incident number	Vendor Ticket Number	Submit date	Last modified date	Ticket status	Description	Prediction details
INC000000002701	7405	03-05-2021 16:59:52	03-05-2021 16:59:53	Assigned	25888(SCTP Link Fault)	
INC000000002404	7406	27-01-2022 15:44:16	27-01-2022 15:44:16	Assigned	25888(SCTP Link Fault)	
INC000000002403	7405	27-01-2022 15:44:14	27-01-2022 15:44:14	Assigned	25888(SCTP Link Fault)	
INC000000002402	7407	27-01-2022 15:37:16	27-01-2022 15:43:45	Assigned	65097(Theft Alarm)	
INC000000002206	7408	28-12-2021 12:17:33	28-12-2021 12:17:33	Assigned	65097(Theft Alarm)	
INC000000002205	7414	28-12-2021 12:16:41	28-12-2021 12:16:41	Assigned	25888(SCTP Link Fault)	

Bob

Figure 8.1 - BMC Remedy Screen

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.

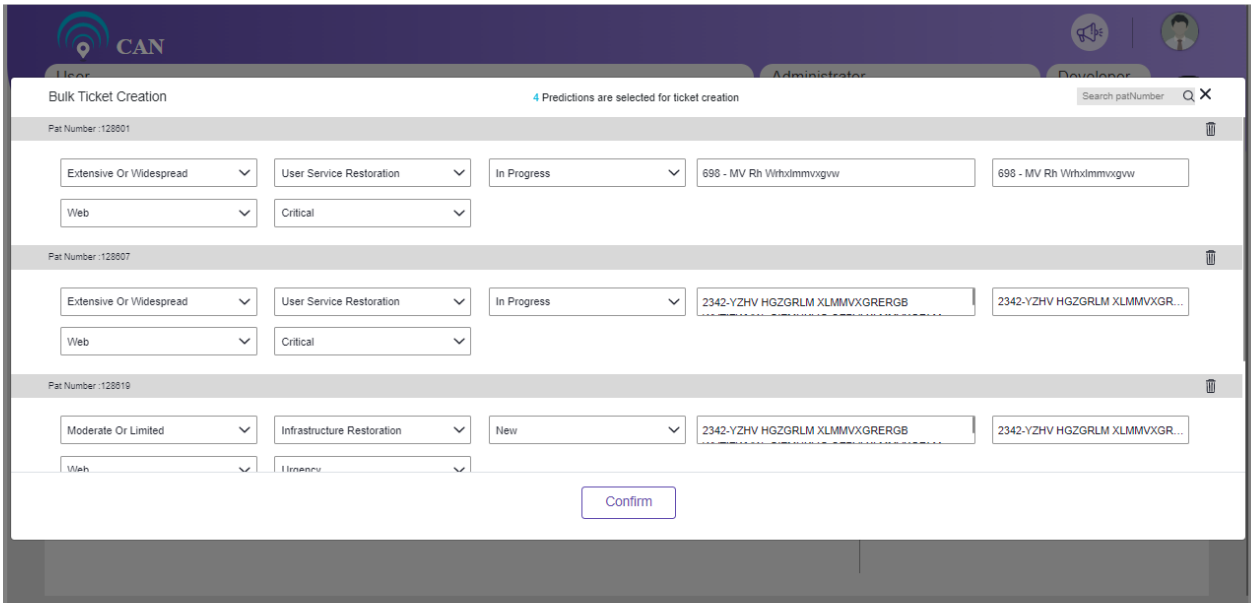


Search

□	Pat number	Equipment Component	Cause	Prediction Day	Priority	Probability	ROE
☑	128621	885679563Z___NIYGH-859563	0952-MV6HDH ZTVMG MLG IVHKLMWRMT GL IVJFVHGH	09-10-2022	LOW	70.08%	1
□	128619	797677850B___NIYGH-77850/OMYGH-77850/OMNNV-8	2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW--GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV	09-10-2022	LOW	70.27%	1
		797677850B___NIYGH-77850/OMYGH-77850/OMNNV-1	2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW--GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV	09-10-2022	LOW	70.27%	2
		797677850B___NIYGH-77850/OMYGH-77850/OMNNV-9	2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW--GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV	09-10-2022	HIGH	70.27%	3
		797677850B___NIYGH-77850/OMYGH-77850/OMNNV-4	2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW--GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV	09-10-2022	HIGH	70.27%	4

Confirm Cancel

Figure 8.2 - BMC Single Ticket Creation



Bulk Ticket Creation

4 Predictions are selected for ticket creation

Search patNumber

Pat Number : 128601

Extensive Or Widespread	User Service Restoration	In Progress	698 - MV Rh Wrhxlmmvxgvw	698 - MV Rh Wrhxlmmvxgvw
Web	Critical			

Pat Number : 128607

Extensive Or Widespread	User Service Restoration	In Progress	2342-YZHV HGZGRLM XLMMVXGRERGB	2342-YZHV HGZGRLM XLMMVXGR...
Web	Critical			

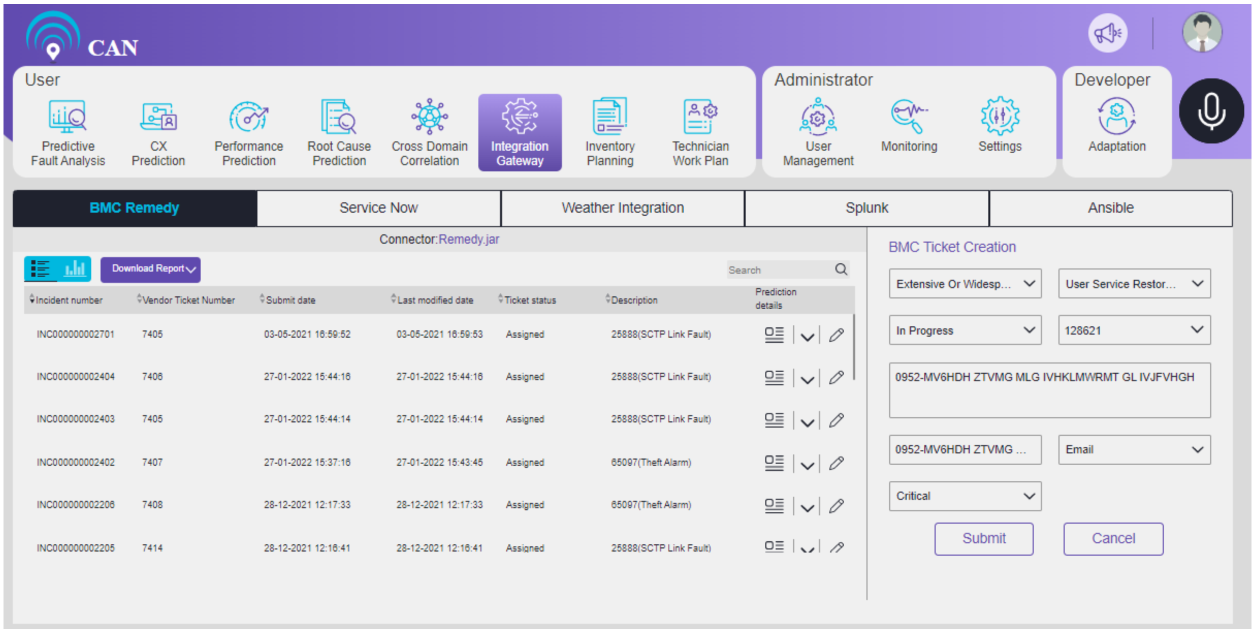
Pat Number : 128619

Moderate Or Limited	Infrastructure Restoration	New	2342-YZHV HGZGRLM XLMMVXGRERGB	2342-YZHV HGZGRLM XLMMVXGR...
Web	Urgency			

Confirm

Figure 8.3 - 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, Reported Source and Urgency will get auto filled.
6. Click the **Submit** button to create the New BMC ticket.



Connector:Remedy.jar

Incident number	Vendor Ticket Number	Submit date	Last modified date	Ticket status	Description	Prediction details
INC000000002701	7405	03-05-2021 16:59:52	03-05-2021 16:59:53	Assigned	25888(SCTP Link Fault)	
INC000000002404	7406	27-01-2022 15:44:16	27-01-2022 15:44:16	Assigned	25888(SCTP Link Fault)	
INC000000002403	7405	27-01-2022 15:44:14	27-01-2022 15:44:14	Assigned	25888(SCTP Link Fault)	
INC000000002402	7407	27-01-2022 15:37:16	27-01-2022 15:43:45	Assigned	65097(Theft Alarm)	
INC000000002206	7408	28-12-2021 12:17:33	28-12-2021 12:17:33	Assigned	65097(Theft Alarm)	
INC000000002205	7414	28-12-2021 12:16:41	28-12-2021 12:16:41	Assigned	25888(SCTP Link Fault)	

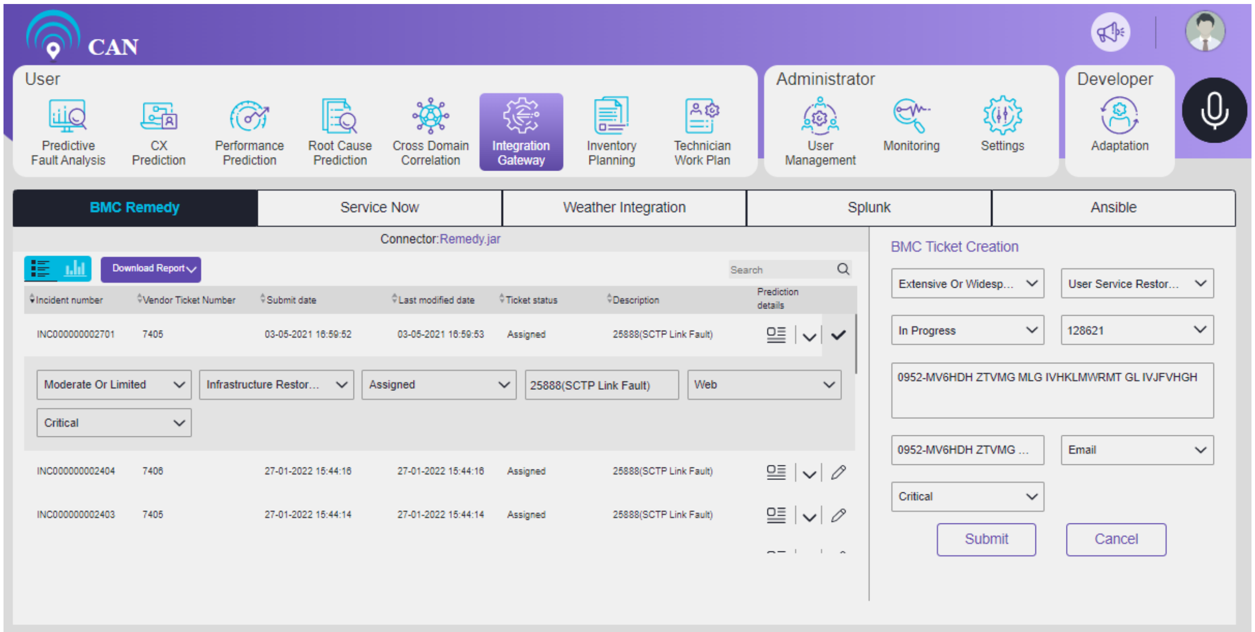
BMC Ticket Creation

Extensive Or Widesp...
User Service Restor...
In Progress
128621
0952-MV6HDH ZTVMG MLG IVHKLMWRMT GL IVJFVHGH
0952-MV6HDH ZTVMG ...
Email
Critical

Figure 8.4 - 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.



Connector:Remedy.jar

Incident number	Vendor Ticket Number	Submit date	Last modified date	Ticket status	Description	Prediction details
INC000000002701	7405	03-05-2021 16:59:52	03-05-2021 16:59:53	Assigned	25888(SCTP Link Fault)	
INC000000002404	7406	27-01-2022 15:44:16	27-01-2022 15:44:16	Assigned	25888(SCTP Link Fault)	
INC000000002403	7405	27-01-2022 15:44:14	27-01-2022 15:44:14	Assigned	25888(SCTP Link Fault)	

Moderate Or Limited
Infrastructure Restor...
Assigned
25888(SCTP Link Fault)
Web
Critical

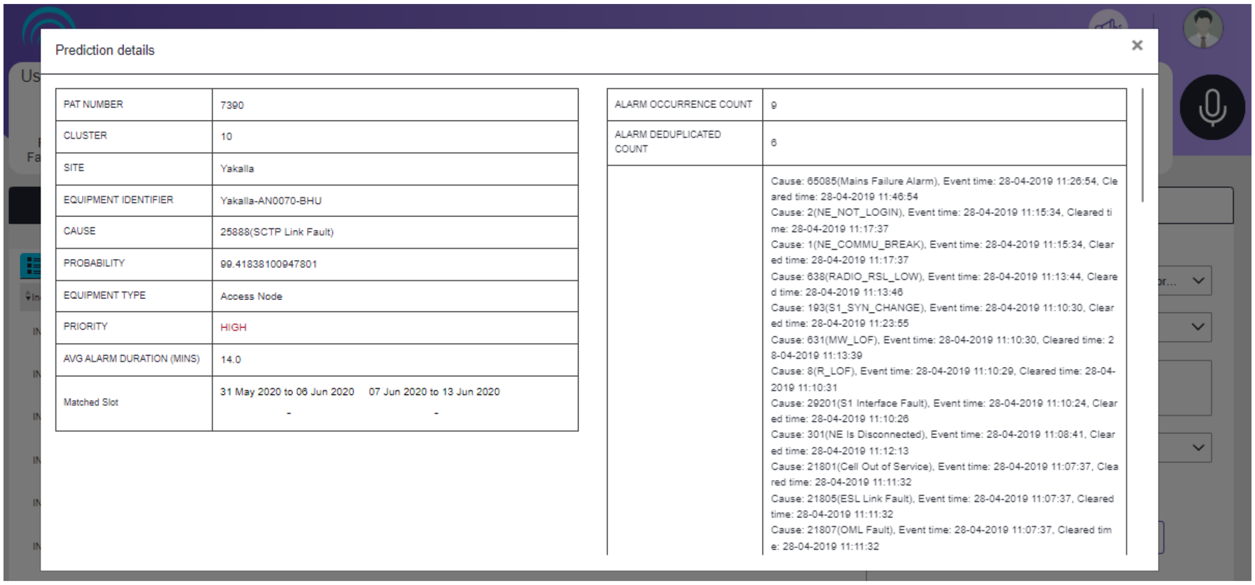
BMC Ticket Creation

Extensive Or Widesp...
User Service Restor...
In Progress
128621
0952-MV6HDH ZTVMG MLG IVHKLMWRMT GL IVJFVHGH
0952-MV6HDH ZTVMG ...
Email
Critical

Figure 8.5 - BMC Ticket Update Screen

2. After edit or update, click the save icon ✓ to save the changes.

3. User can click the prediction details icon to see the predicted fault for the particular Incident number or Vendor Ticket Number.
4. User can click the more icon 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.



Prediction details

PAT NUMBER	7390
CLUSTER	10
SITE	Yakalla
EQUIPMENT IDENTIFIER	Yakalla-AN0070-BHU
CAUSE	25888(SCTP Link Fault)
PROBABILITY	99.41838100947801
EQUIPMENT TYPE	Access Node
PRIORITY	HIGH
AVG ALARM DURATION (MINS)	14.0
Matched Slot	31 May 2020 to 06 Jun 2020 - 07 Jun 2020 to 13 Jun 2020 -

ALARM OCCURRENCE COUNT	9
ALARM DEDUPLICATED COUNT	6
	Cause: 65085(Mains Failure Alarm), Event time: 28-04-2019 11:26:54, Cleared time: 28-04-2019 11:46:54 Cause: 2(NE_NOT_LOGIN), Event time: 28-04-2019 11:15:34, Cleared time: 28-04-2019 11:17:37 Cause: 1(NE_COMMU_BREAK), Event time: 28-04-2019 11:15:34, Cleared time: 28-04-2019 11:17:37 Cause: 638(RADIO_RSL_LOW), Event time: 28-04-2019 11:13:44, Cleared time: 28-04-2019 11:13:46 Cause: 193(S1_SYN_CHANGE), Event time: 28-04-2019 11:10:30, Cleared time: 28-04-2019 11:23:55 Cause: 631(MW_LOF), Event time: 28-04-2019 11:10:30, Cleared time: 28-04-2019 11:13:39 Cause: 8(R_LOF), Event time: 28-04-2019 11:10:29, Cleared time: 28-04-2019 11:10:31 Cause: 29201(S1 Interface Fault), Event time: 28-04-2019 11:10:24, Cleared time: 28-04-2019 11:10:26 Cause: 301(NE Is Disconnected), Event time: 28-04-2019 11:08:41, Cleared time: 28-04-2019 11:12:13 Cause: 21801(Cell Out of Service), Event time: 28-04-2019 11:07:37, Cleared time: 28-04-2019 11:11:32 Cause: 21805(ESL Link Fault), Event time: 28-04-2019 11:07:37, Cleared time: 28-04-2019 11:11:32 Cause: 21807(OML Fault), Event time: 28-04-2019 11:07:37, Cleared time: 28-04-2019 11:11:32

Figure 8.6 - BMC Remedy Prediction Details

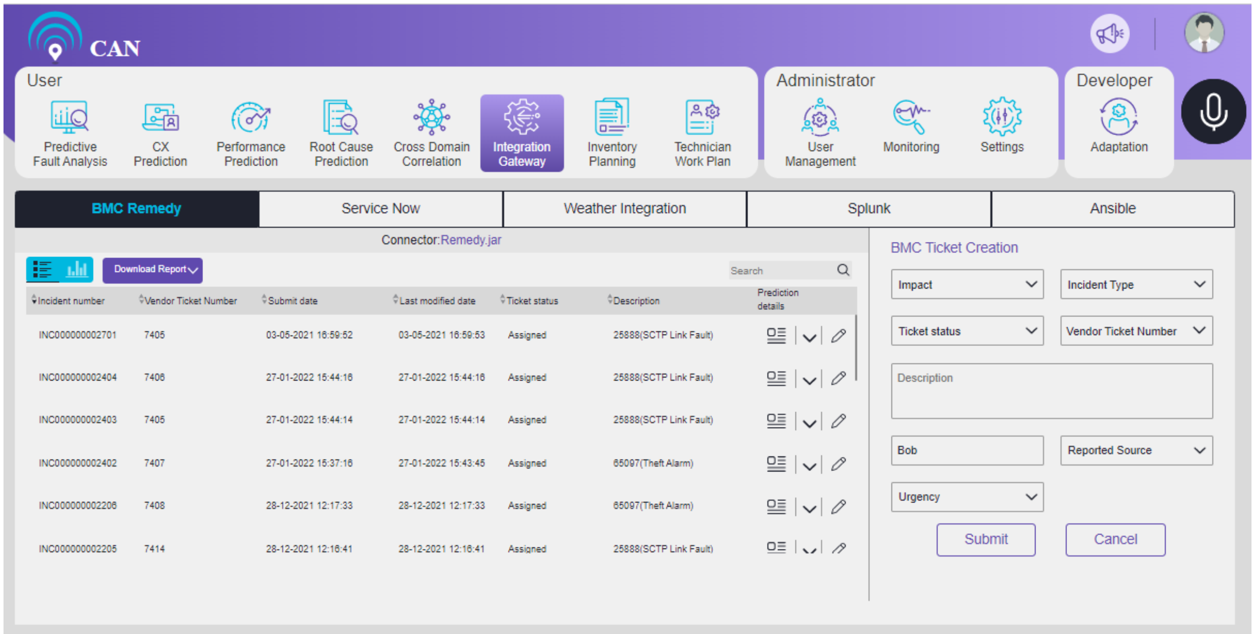
BMC Remedy screen shows the incidents or tickets in two views:

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.



Connector:Remedy.jar

Incident number	Vendor Ticket Number	Submit date	Last modified date	Ticket status	Description	Prediction details
INC000000002701	7405	03-05-2021 16:59:52	03-05-2021 16:59:53	Assigned	25888(SCTP Link Fault)	
INC000000002404	7406	27-01-2022 15:44:16	27-01-2022 15:44:16	Assigned	25888(SCTP Link Fault)	
INC000000002403	7405	27-01-2022 15:44:14	27-01-2022 15:44:14	Assigned	25888(SCTP Link Fault)	
INC000000002402	7407	27-01-2022 15:37:16	27-01-2022 15:43:45	Assigned	65097(Theft Alarm)	
INC000000002206	7408	28-12-2021 12:17:33	28-12-2021 12:17:33	Assigned	65097(Theft Alarm)	
INC000000002205	7414	28-12-2021 12:16:41	28-12-2021 12:16:41	Assigned	25888(SCTP Link Fault)	

BMC Ticket Creation

Impact | Incident Type

Ticket status | Vendor Ticket Number

Description

Bob | Reported Source

Urgency

Figure 8.7 - BMC Remedy Tabular View

2. Graph View

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

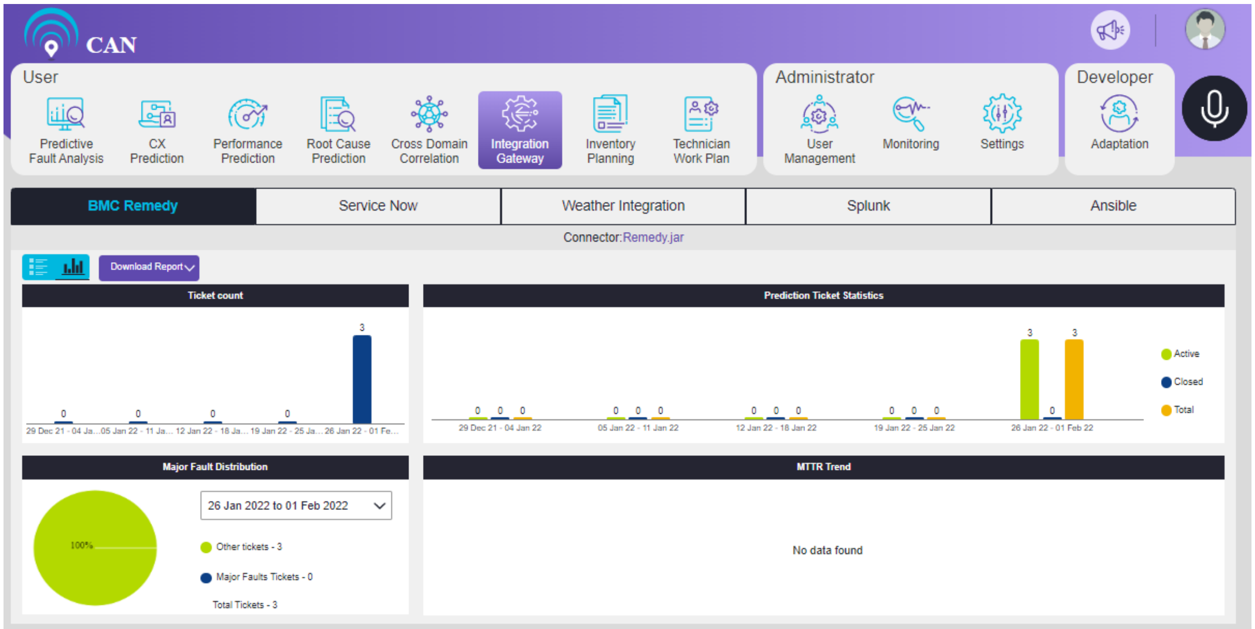


Figure 8.8 - BMC Remedy Graphical View

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.

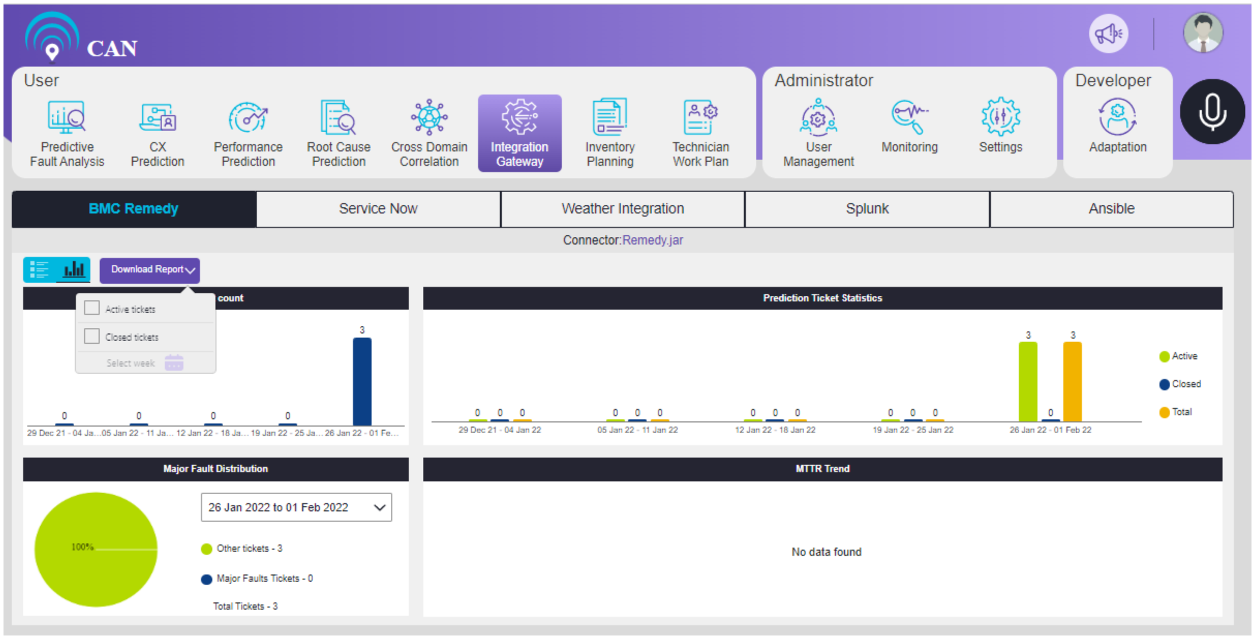
- 🟢 Green color shows the Active tickets.
- 🔵 Blue color shows the Closed tickets.
- 🟠 Orange color shows the Total tickets.

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 closing 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.



Connector:Remedy.jar

□ Active tickets
□ Closed tickets
Select week

26 Jan 2022 to 01 Feb 2022

● Other tickets - 3
● Major Faults Tickets - 0
Total Tickets - 3

No data found

Figure 8.9 - BMC Remedy Download Reports

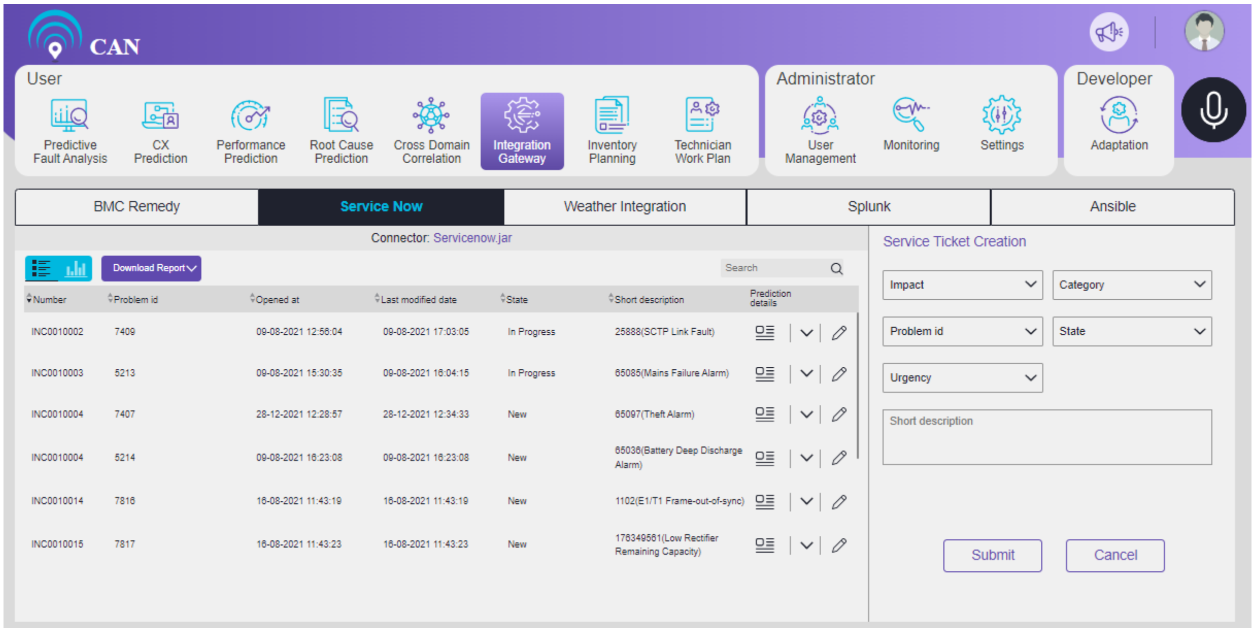
ServiceNow Integration

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 Service Now includes the IT Service Management Tool that helps the telecom, IT customers to log in fault incidents, track and close them through the digital workflows.

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.

Service Now 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.



Connector: Servicenow.jar

Number	Problem id	Opened at	Last modified date	State	Short description	Prediction details
INC0010002	7409	09-08-2021 12:56:04	09-08-2021 17:03:05	In Progress	25888(SCTP Link Fault)	
INC0010003	5213	09-08-2021 15:30:35	09-08-2021 16:04:15	In Progress	65085(Mains Failure Alarm)	
INC0010004	7407	28-12-2021 12:28:57	28-12-2021 12:34:33	New	65097(Theft Alarm)	
INC0010004	5214	09-08-2021 16:23:08	09-08-2021 16:23:08	New	65036(Battery Deep Discharge Alarm)	
INC0010014	7816	16-08-2021 11:43:19	16-08-2021 11:43:19	New	1102(E1/T1 Frame-out-of-sync)	
INC0010015	7817	16-08-2021 11:43:23	16-08-2021 11:43:23	New	176349561(Low Rectifier Remaining Capacity)	

Service Ticket Creation

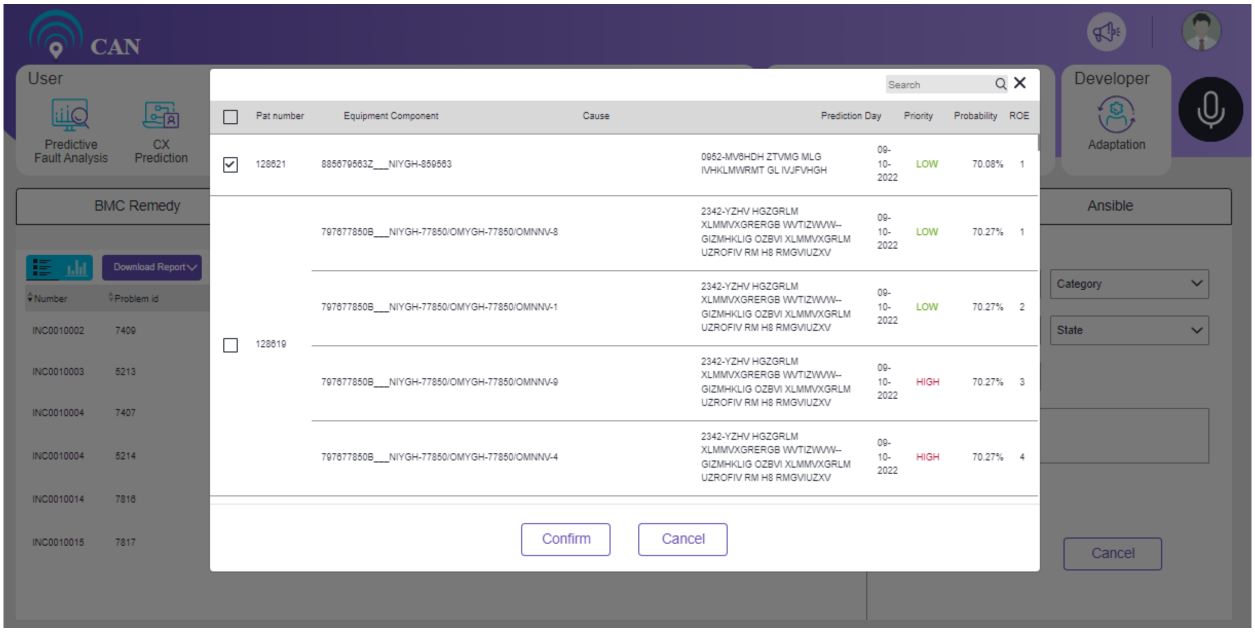
Impact
Category
Problem id
State
Urgency
Short description

Submit Cancel

Figure 8.10 - ServiceNow Screen

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.



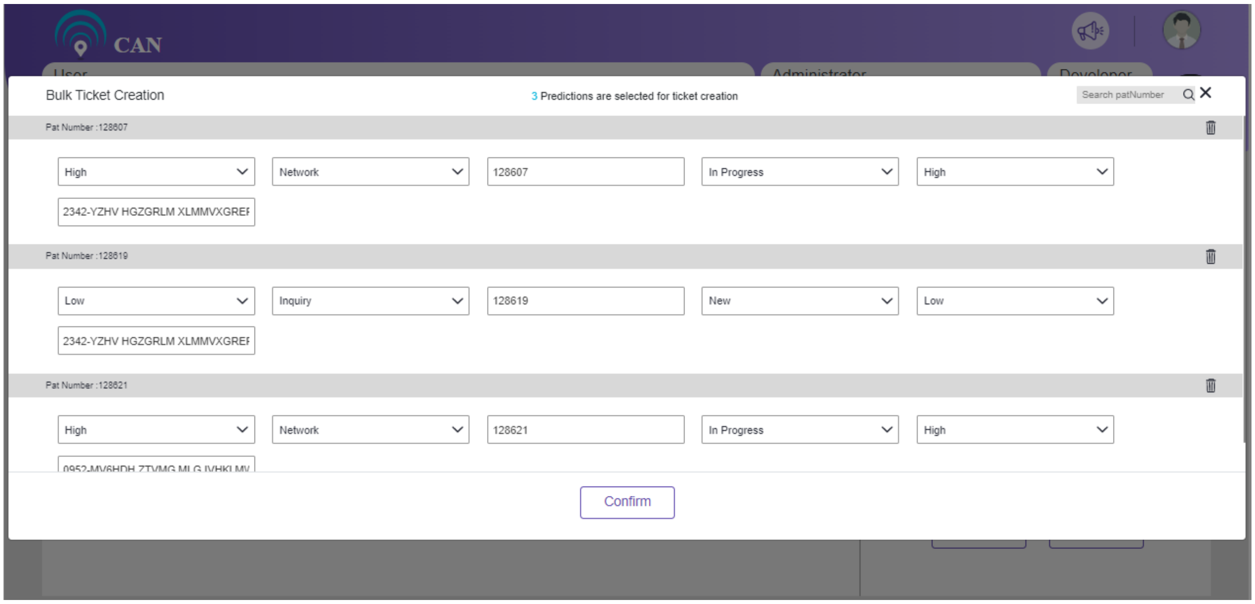
Search

☐	Pat number	Equipment Component	Cause	Prediction Day	Priority	Probability	ROE
☑	128621	885679563Z___NIYGH-859563	0952-MV6HDH ZTVMG MLG IVHKLMWRMT GL IVJFVHGH	09-10-2022	LOW	70.08%	1
☐	128619	797677850B___NIYGH-77850/OMYGH-77850/OMNNV-8	2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW--GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV	09-10-2022	LOW	70.27%	1
		797677850B___NIYGH-77850/OMYGH-77850/OMNNV-1	2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW--GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV	09-10-2022	LOW	70.27%	2
		797677850B___NIYGH-77850/OMYGH-77850/OMNNV-9	2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW--GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV	09-10-2022	HIGH	70.27%	3
		797677850B___NIYGH-77850/OMYGH-77850/OMNNV-4	2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW--GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV	09-10-2022	HIGH	70.27%	4

Confirm Cancel

Figure 8.11 – 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.



Bulk Ticket Creation

3 Predictions are selected for ticket creation

Search patNumber

Pat Number :128607

High | Network | 128607 | In Progress | High

2342-YZHV HGZGRLM XLMMVXGREF

Pat Number :128619

Low | Inquiry | 128619 | New | Low

2342-YZHV HGZGRLM XLMMVXGREF

Pat Number :128621

High | Network | 128621 | In Progress | High

0952-MV6HDH ZTVMG MLG IVHKLMV

Confirm

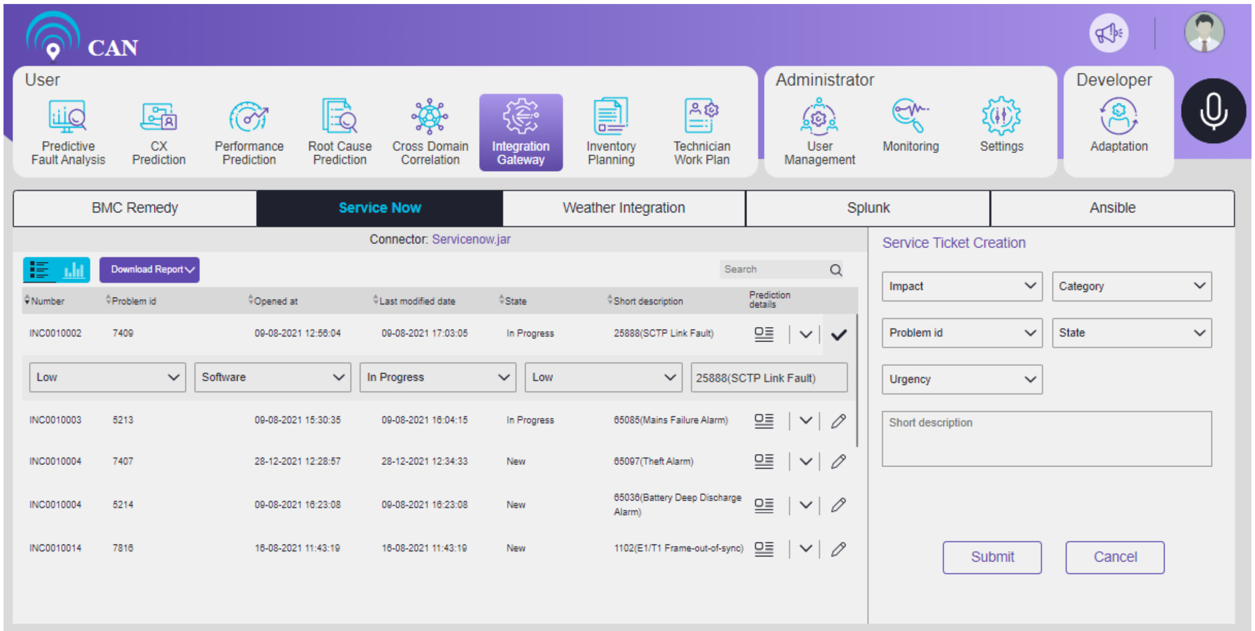
Figure 8.12 – ServiceNow Bulk Ticket Creation

7. After updating the values, click the **Confirm** button. The Pop up Screen will close.
8. You will be directed to Service Now ticket screen; the values will be auto populated in the Service Now 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 Service Now Ticket.

To Update/Edit the Existing Service Now 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.



Connector: Servicenow.jar

Number	Problem id	Opened at	Last modified date	State	Short description	Prediction details
INC0010002	7409	09-08-2021 12:56:04	09-08-2021 17:03:05	In Progress	25888(SCTP Link Fault)	
Low	Software	In Progress	Low	25888(SCTP Link Fault)		
INC0010003	5213	09-08-2021 15:30:35	09-08-2021 16:04:15	In Progress	65085(Mains Failure Alarm)	
INC0010004	7407	28-12-2021 12:28:57	28-12-2021 12:34:33	New	65097(Theft Alarm)	
INC0010004	5214	09-08-2021 16:23:08	09-08-2021 16:23:08	New	65036(Battery Deep Discharge Alarm)	
INC0010014	7816	16-08-2021 11:43:19	16-08-2021 11:43:19	New	1102(E1/T1 Frame-out-of-sync)	

Impact
Category
Problem id
State
Urgency
Short description

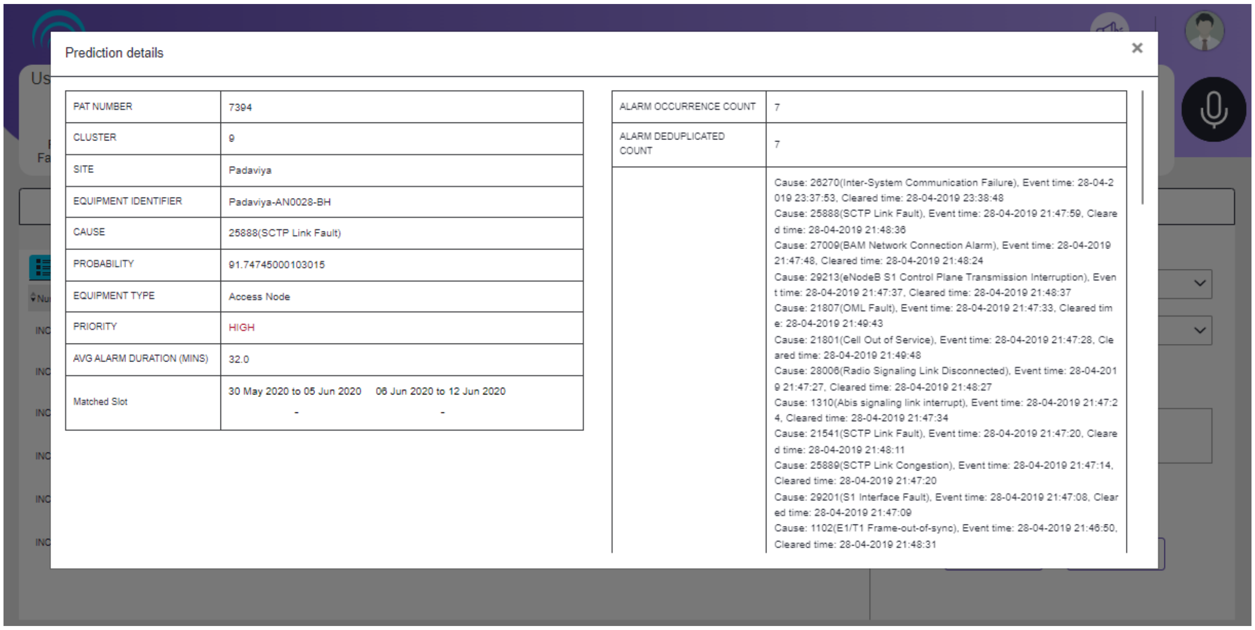
Figure 8.13 – ServiceNow Ticket Update Screen

2. After edit or update, click the save icon ✓ to save the changes.

3. User can click the prediction details icon ☰ to see the predicted fault for the particular Incident number or Problem id.

4. User can click the more icon⌄ 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.



Prediction details

PAT NUMBER	7394
CLUSTER	9
SITE	Padaviya
EQUIPMENT IDENTIFIER	Padaviya-AN0028-BH
CAUSE	25888(SCTP Link Fault)
PROBABILITY	91.74745000103015
EQUIPMENT TYPE	Access Node
PRIORITY	HIGH
AVG ALARM DURATION (MINS)	32.0
Matched Slot	30 May 2020 to 05 Jun 2020 - 06 Jun 2020 to 12 Jun 2020 -

ALARM OCCURRENCE COUNT	7
ALARM DEDUPLICATED COUNT	7
	Cause: 26270(Inter-System Communication Failure), Event time: 28-04-2019 23:37:53, Cleared time: 28-04-2019 23:38:48 Cause: 25888(SCTP Link Fault), Event time: 28-04-2019 21:47:59, Cleared time: 28-04-2019 21:48:36 Cause: 27009(BAM Network Connection Alarm), Event time: 28-04-2019 21:47:48, Cleared time: 28-04-2019 21:48:24 Cause: 29213(eNodeB S1 Control Plane Transmission Interruption), Event time: 28-04-2019 21:47:37, Cleared time: 28-04-2019 21:48:37 Cause: 21807(OML Fault), Event time: 28-04-2019 21:47:33, Cleared time: 28-04-2019 21:49:43 Cause: 21801(Cell Out of Service), Event time: 28-04-2019 21:47:28, Cleared time: 28-04-2019 21:49:48 Cause: 28006(Radio Signaling Link Disconnected), Event time: 28-04-2019 21:47:27, Cleared time: 28-04-2019 21:48:27 Cause: 1310(Abis signaling link interrupt), Event time: 28-04-2019 21:47:24, Cleared time: 28-04-2019 21:47:34 Cause: 21541(SCTP Link Fault), Event time: 28-04-2019 21:47:20, Cleared time: 28-04-2019 21:48:11 Cause: 25889(SCTP Link Congestion), Event time: 28-04-2019 21:47:14, Cleared time: 28-04-2019 21:47:20 Cause: 29201(S1 Interface Fault), Event time: 28-04-2019 21:47:08, Cleared time: 28-04-2019 21:47:09 Cause: 1102(E1/T1 Frame-out-of-sync), Event time: 28-04-2019 21:46:50, Cleared time: 28-04-2019 21:48:31

Figure 8.14 – ServiceNow Prediction Details

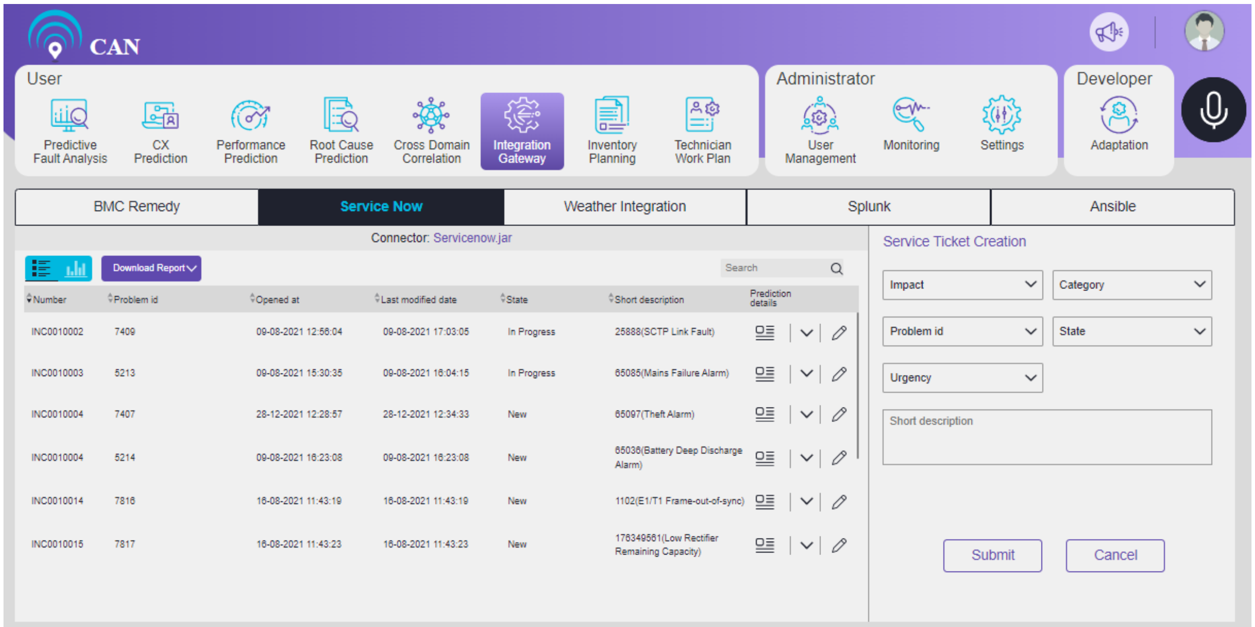
ServiceNow screen shows the incidents or tickets in two views:

1. Tabular View

   By default the tabular icon ☰ is selected on the screen.

   The Tabular view shows the below attributes of the Service Now:

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



Connector: Servicenow.jar

Number	Problem id	Opened at	Last modified date	State	Short description	Prediction details
INC0010002	7409	09-08-2021 12:56:04	09-08-2021 17:03:05	In Progress	25888(SCTP Link Fault)	
INC0010003	5213	09-08-2021 15:30:35	09-08-2021 16:04:15	In Progress	65085(Mains Failure Alarm)	
INC0010004	7407	28-12-2021 12:28:57	28-12-2021 12:34:33	New	65097(Theft Alarm)	
INC0010004	5214	09-08-2021 16:23:08	09-08-2021 16:23:08	New	65036(Battery Deep Discharge Alarm)	
INC0010014	7816	16-08-2021 11:43:19	16-08-2021 11:43:19	New	1102(E1/T1 Frame-out-of-sync)	
INC0010015	7817	16-08-2021 11:43:23	16-08-2021 11:43:23	New	176349561(Low Rectifier Remaining Capacity)	

Figure 8.15 – ServiceNow Tabular View

2. Graph View

Click the graph icon 📊 to view the graph view of the Service Now tickets.

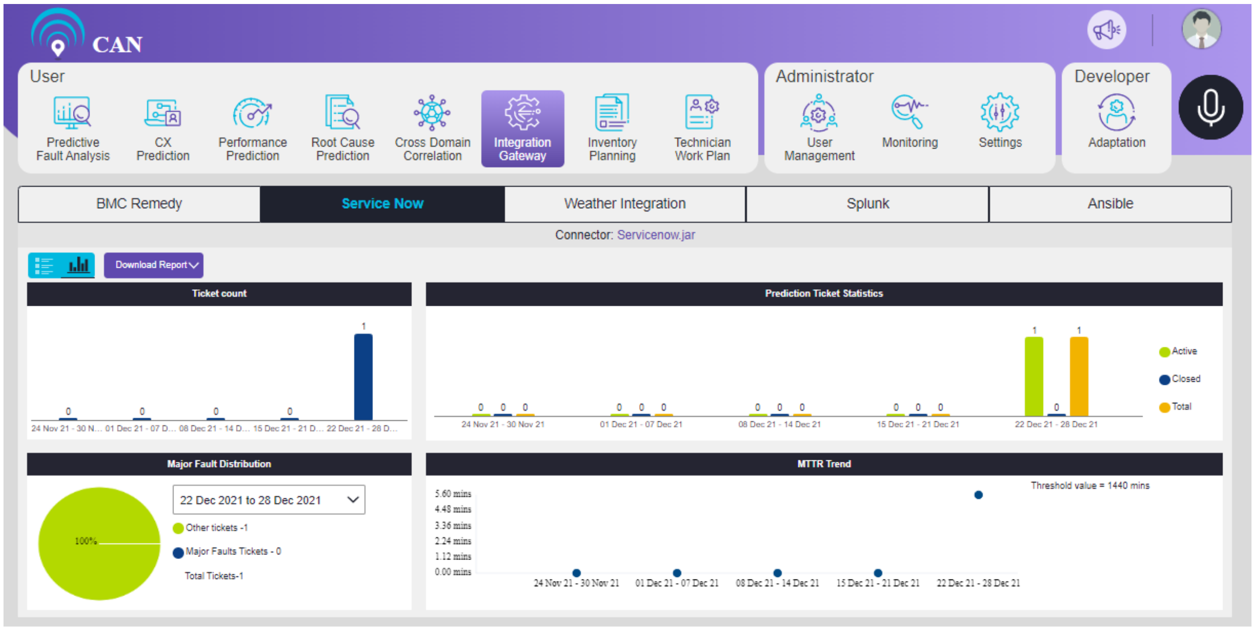


Figure 8.16 – ServiceNow Graphical View

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 closing 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.

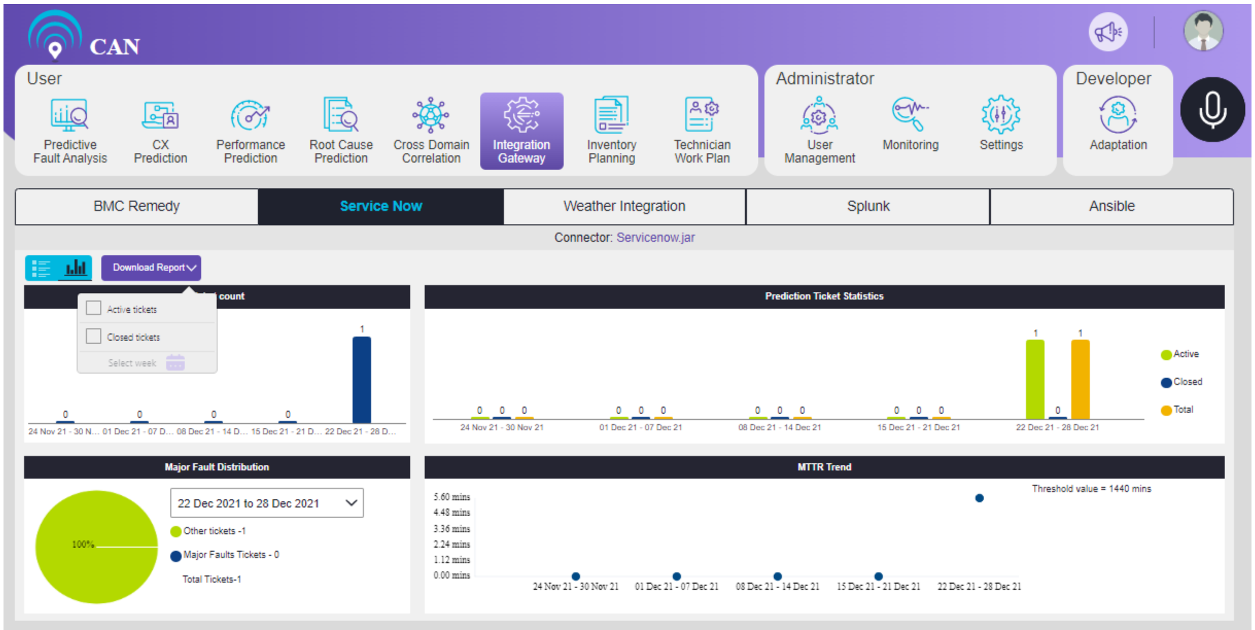
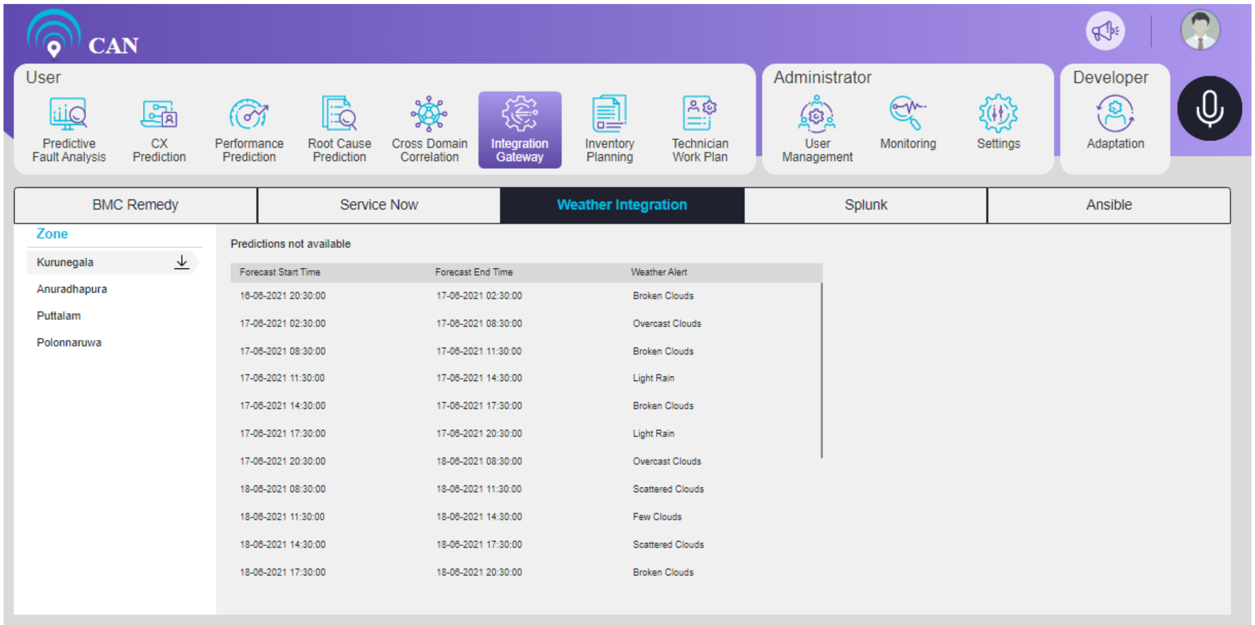


Figure 8.17 – ServiceNow Download Reports

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.



Predictions not available

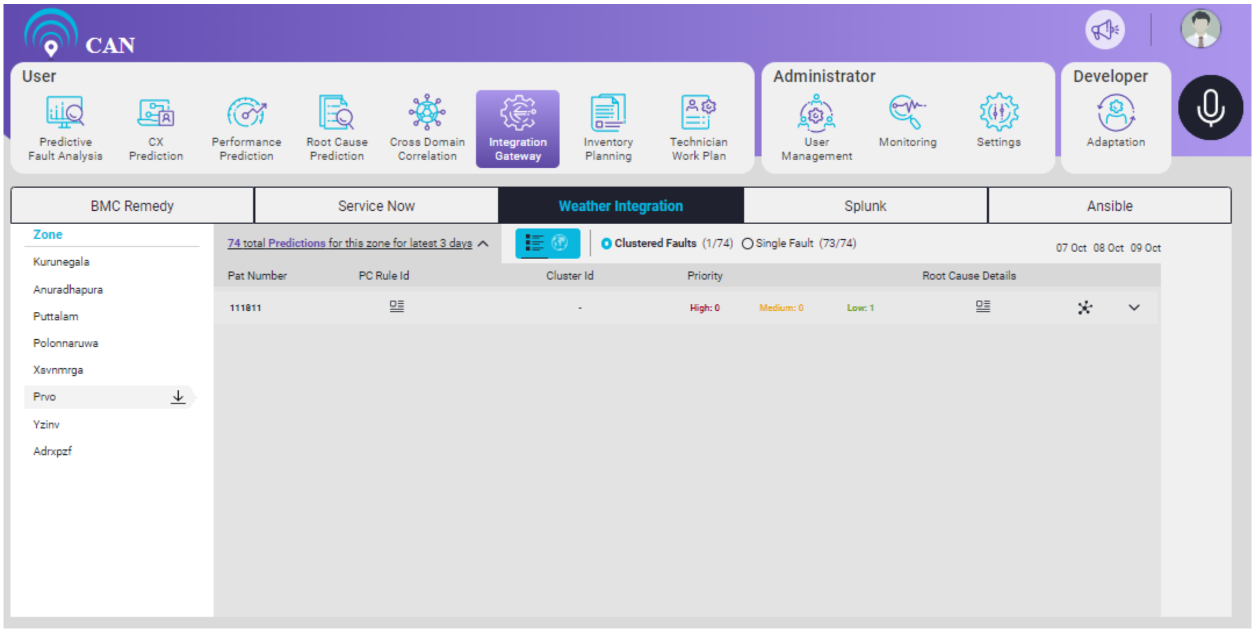
Forecast Start Time	Forecast End Time	Weather Alert
16-06-2021 20:30:00	17-06-2021 02:30:00	Broken Clouds
17-06-2021 02:30:00	17-06-2021 08:30:00	Overcast Clouds
17-06-2021 08:30:00	17-06-2021 11:30:00	Broken Clouds
17-06-2021 11:30:00	17-06-2021 14:30:00	Light Rain
17-06-2021 14:30:00	17-06-2021 17:30:00	Broken Clouds
17-06-2021 17:30:00	17-06-2021 20:30:00	Light Rain
17-06-2021 20:30:00	18-06-2021 08:30:00	Overcast Clouds
18-06-2021 08:30:00	18-06-2021 11:30:00	Scattered Clouds
18-06-2021 11:30:00	18-06-2021 14:30:00	Few Clouds
18-06-2021 14:30:00	18-06-2021 17:30:00	Scattered Clouds
18-06-2021 17:30:00	18-06-2021 20:30:00	Broken Clouds

Figure 8.18 - 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.



74 total Predictions for this zone for latest 3 days

● Clustered Faults (1/74) ○ Single Fault (73/74)

07 Oct 08 Oct 09 Oct

Pat Number	PC Rule Id	Cluster Id	Priority			Root Cause Details		
111811		-	High: 0	Medium: 0	Low: 1			

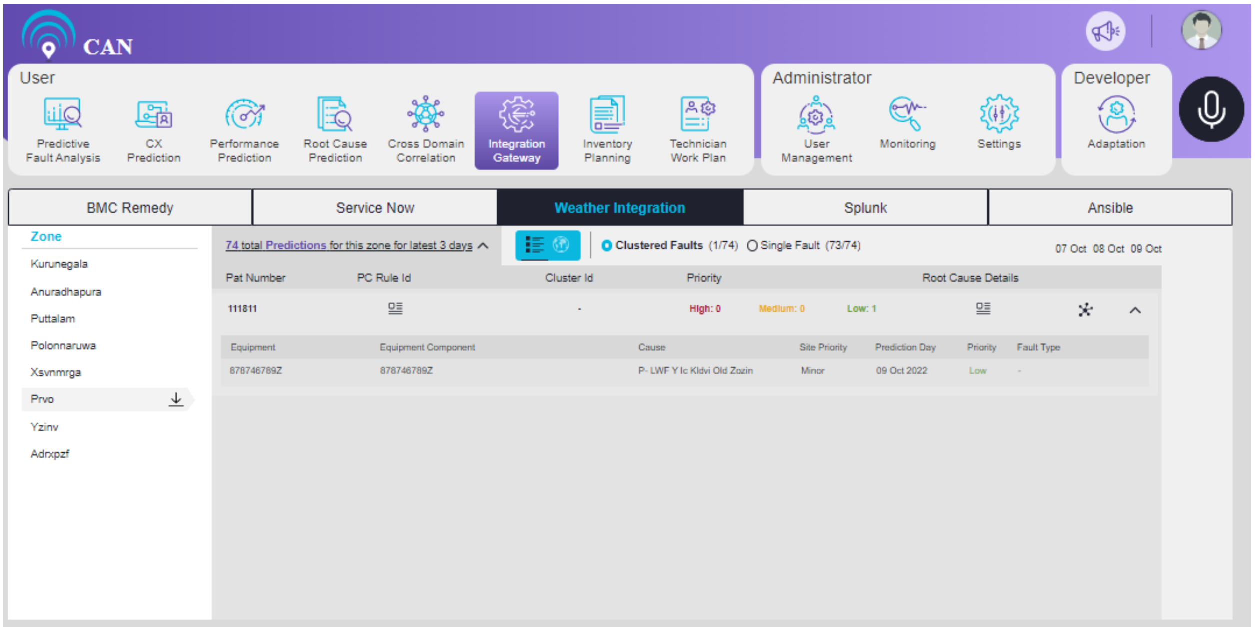
Figure 8.19 - Weather Prediction Tabular View

Tabular View

User can select **Clustered Faults** or **Single Fault** by clicking the radio button.

Clustered Faults

For a particular equipment, user can view the detailed information by clicking the ⌄ icon.

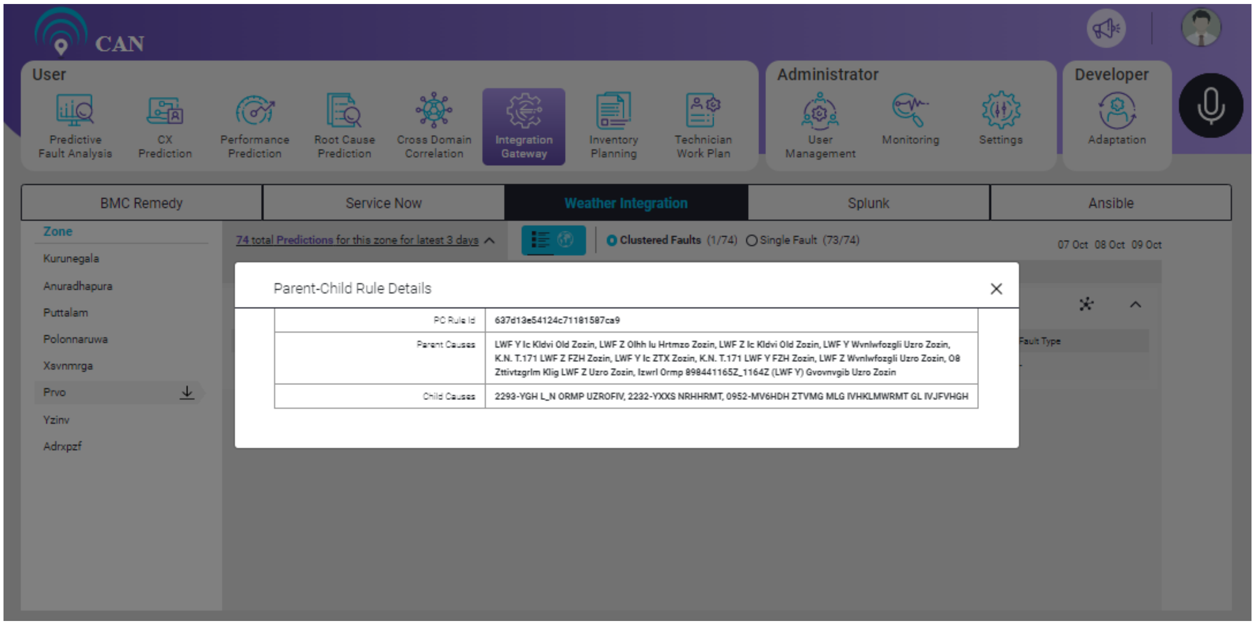


Pat Number	PC Rule Id	Cluster Id	Priority			Root Cause Details
111811	☰	-	High: 0	Medium: 0	Low: 1	☰

Equipment	Equipment Component	Cause	Site Priority	Prediction Day	Priority	Fault Type
878746789Z	878746789Z	P- LWF Y Ic Kldvi Old Zozin	Minor	09 Oct 2022	Low	-

Figure 8.20 - Prediction for Clustered Faults

Click the **PC Rule Id** icon ☰ to view the Parent-Child Rule Details of that equipment.

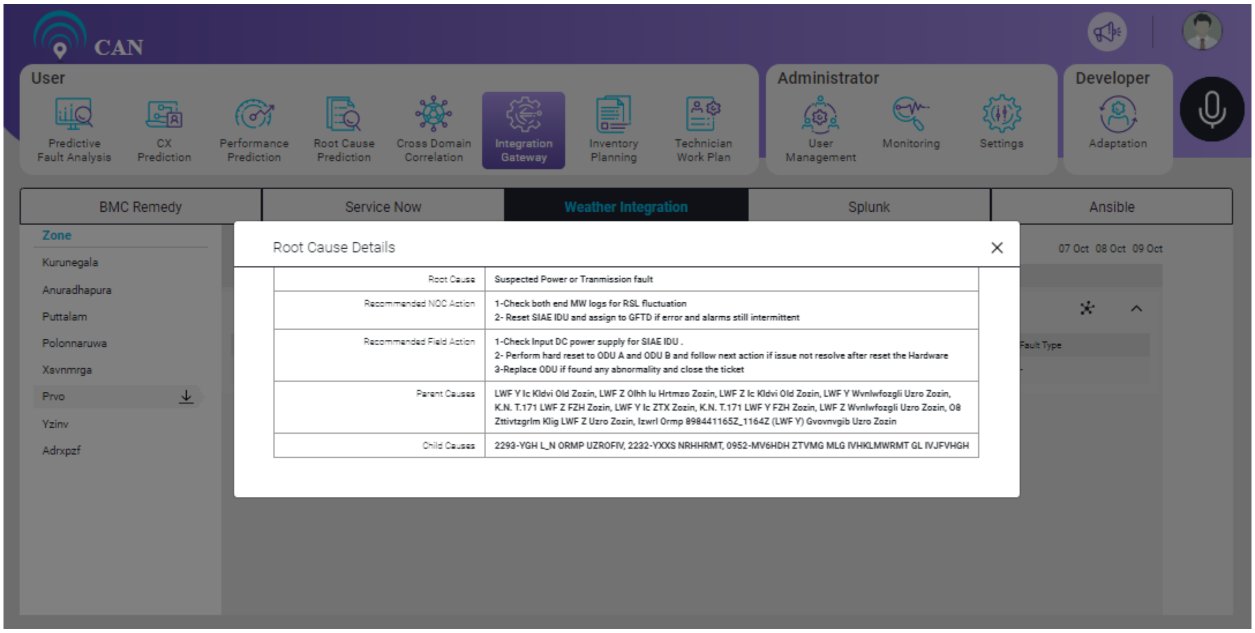


Parent-Child Rule Details

PC Rule Id	637d13e54124c71181587ca9
Parent Causes	LWF Y Ic Kldvi Old Zozin, LWF Z Olhh Iu Hrtmzo Zozin, LWF Z Ic Kldvi Old Zozin, LWF Y Wvnlwfozgli Uzro Zozin, K.N. T.171 LWF Z FZH Zozin, LWF Y Ic ZTX Zozin, K.N. T.171 LWF Y FZH Zozin, LWF Z Wvnlwfozgli Uzro Zozin, O8 Zttivtzgrlm Klig LWF Z Uzro Zozin, Izwrl Ormp 898441165Z_1164Z (LWF Y) Gvovnvgib Uzro Zozin
Child Causes	2293-YGH L_N ORMP UZROFIV, 2232-YXXS NRHHRMT, 0952-MV6HDH ZTVMG MLG IVHKLMWRMT GL IVJFVHGH

Figure 8.21 - Parent-Child Rule Details

Click on **Root Cause Details** icon ☷ to view the root cause details of that equipment.

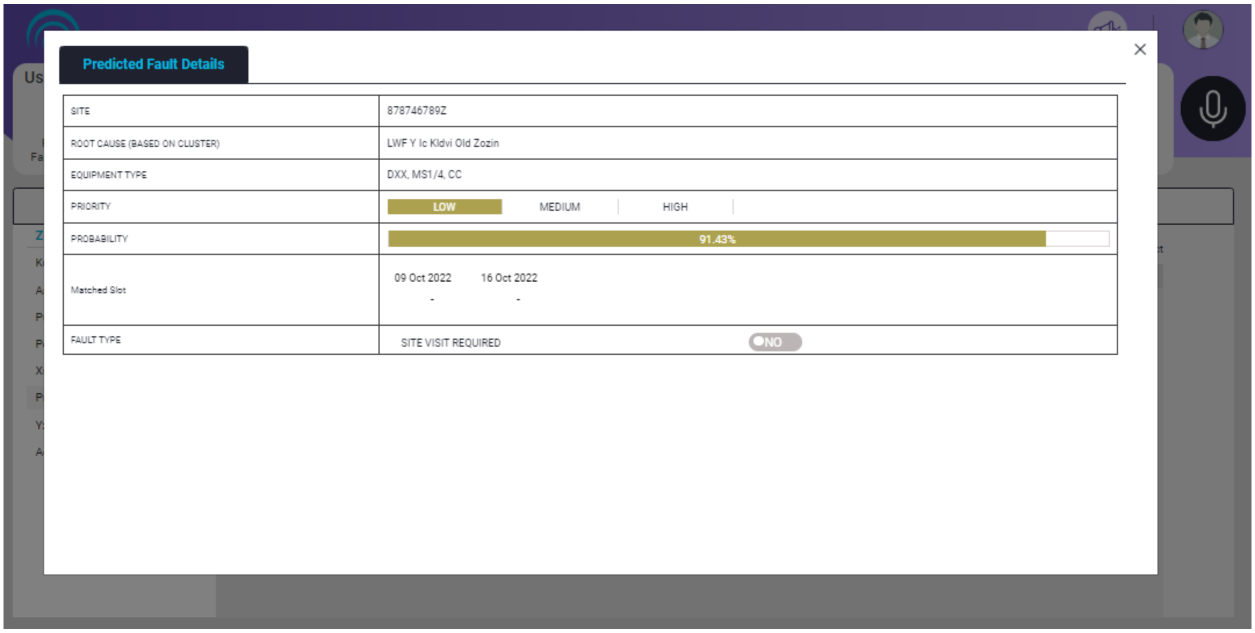


Root Cause Details

Root Cause	Suspected Power or Tranmission fault
Recommended NOC Action	1-Check both end MW logs for RSL fluctuation 2- Reset SIAE IDU and assign to GFTD if error and alarms still intermittent
Recommended Field Action	1-Check Input DC power supply for SIAE IDU . 2- Perform hard reset to ODU A and ODU B and follow next action if issue not resolve after reset the Hardware 3-Replace ODU if found any abnormality and close the ticket
Parent Causes	LWF Y Ic Kldvi Old Zozin, LWF Z Olhh Iu Hrtmzo Zozin, LWF Z Ic Kldvi Old Zozin, LWF Y Wvnlwfozgli Uzro Zozin, K.N. T.171 LWF Z FZH Zozin, LWF Y Ic ZTX Zozin, K.N. T.171 LWF Y FZH Zozin, LWF Z Wvnlwfozgli Uzro Zozin, O8 Zttivtzgrlm Klig LWF Z Uzro Zozin, Izwrl Ormp 898441165Z_1164Z (LWF Y) Gvovnvgib Uzro Zozin
Child Causes	2293-YGH L_N ORMP UZROFIV, 2232-YXXS NRHHRMT, 0952-MV6HDH ZTVMG MLG IVHKLMWRMT GL IVJFVHGH

Figure 8.22 - Root Cause Details

Click on any particular equipment to view the **Predicted Fault Details**.



Predicted Fault Details

SITE	878746789Z
ROOT CAUSE (BASED ON CLUSTER)	LWF Y Ic Kldvi Old Zozin
EQUIPMENT TYPE	DXX, MS1/4, CC
PRIORITY	LOW MEDIUM HIGH
PROBABILITY	91.43%
Matched Slot	09 Oct 2022 - 16 Oct 2022 -
FAULT TYPE	SITE VISIT REQUIRED NO

Figure 8.23 - Predicted Fault Details

Tabular view displays the network view ⁜ for every fault.

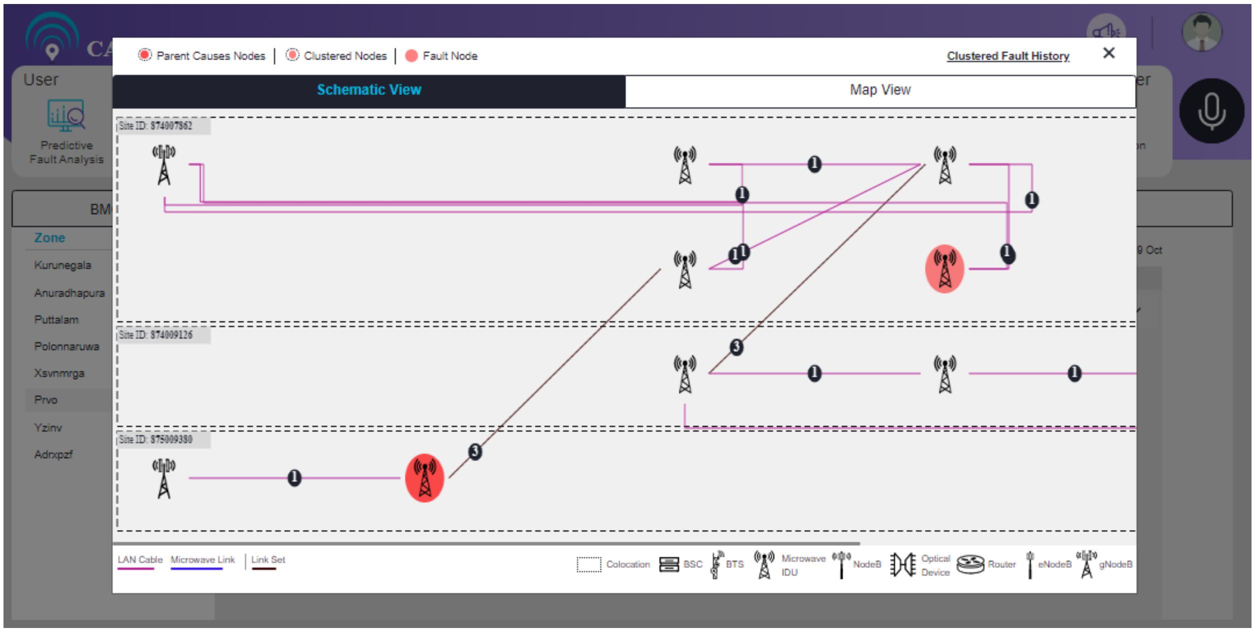


Figure 8.24 - Schematic View

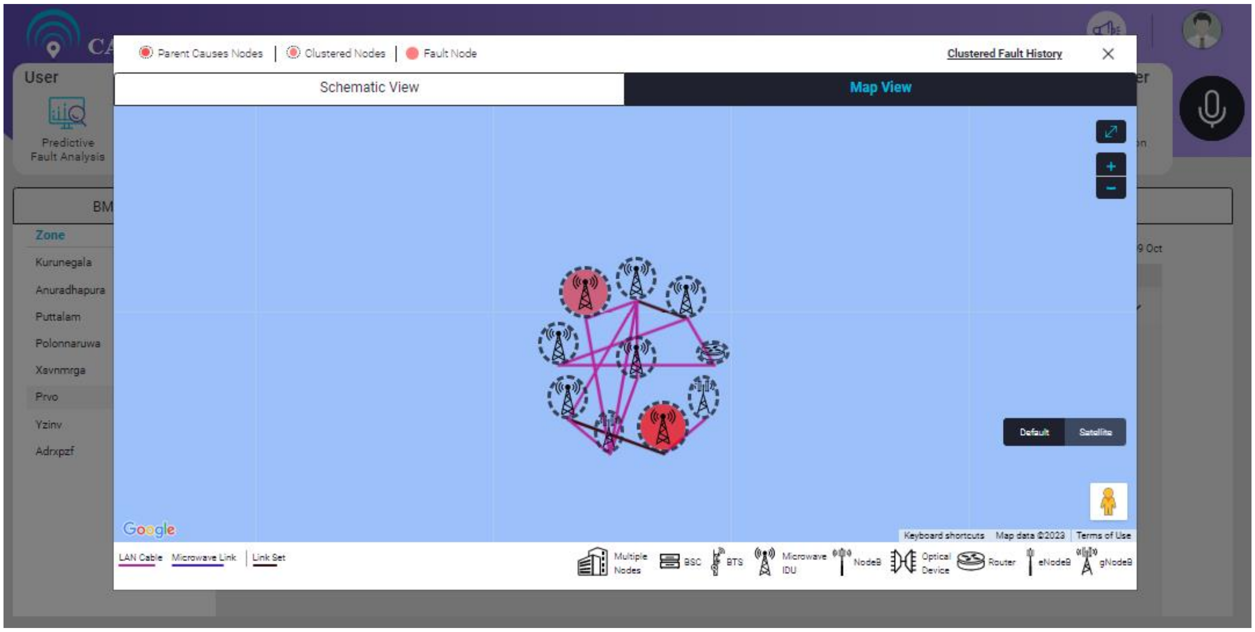
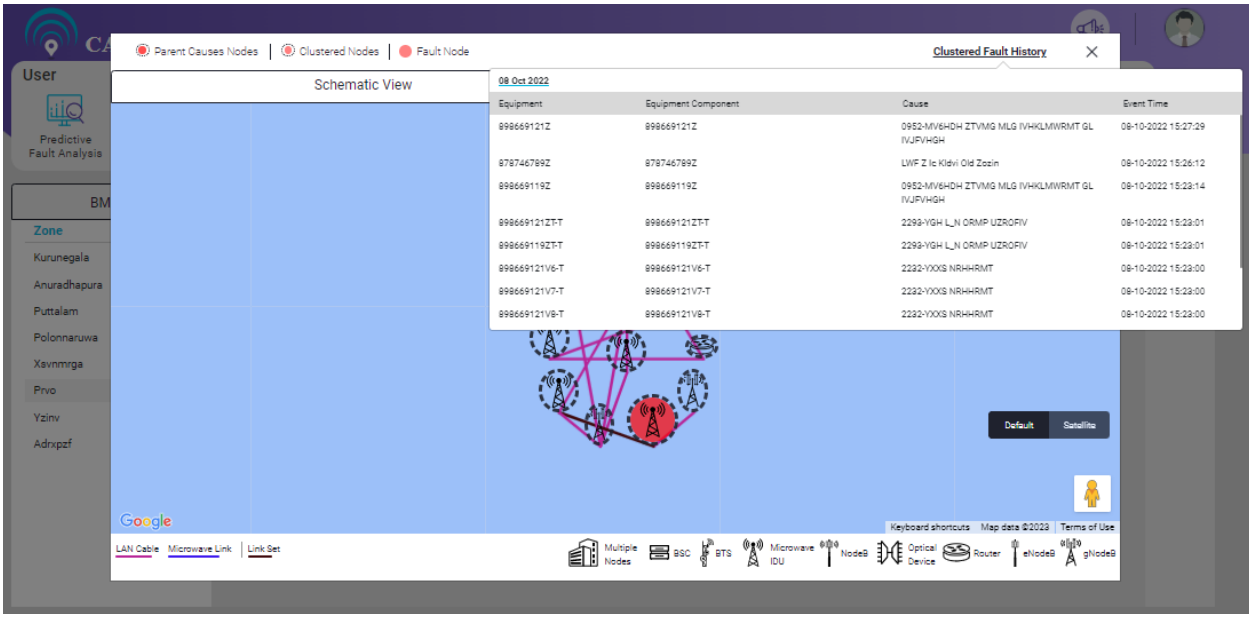


Figure 8.25 - Map View

Click on the **Clustered Fault History** to view the fault history details.



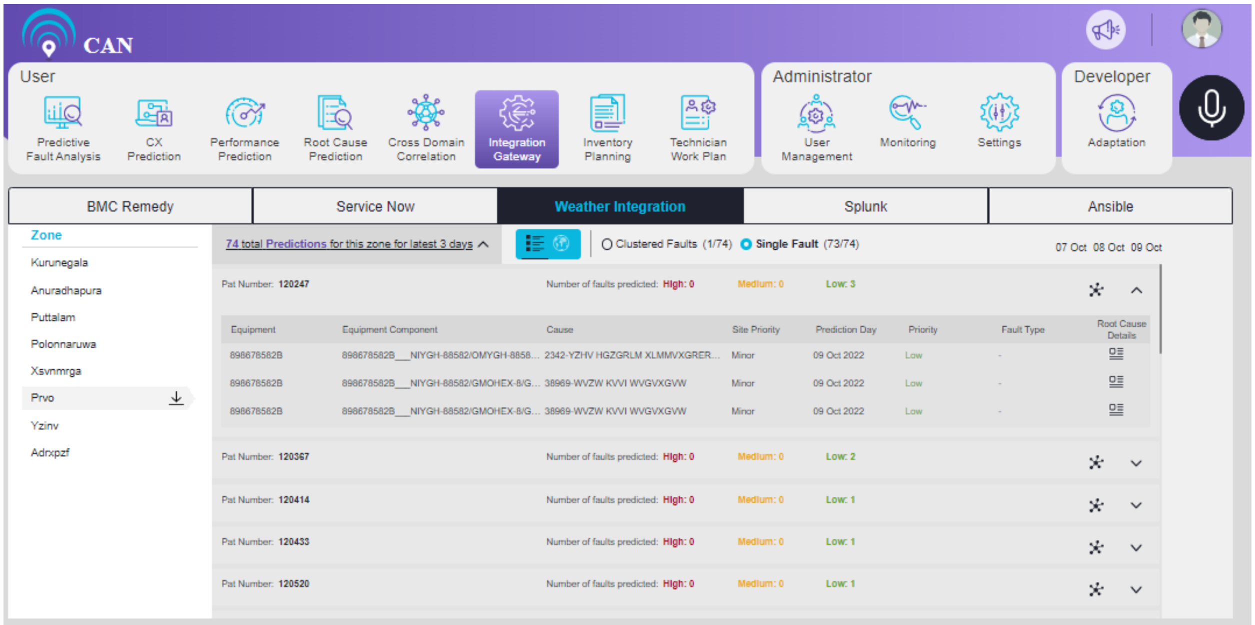
08 Oct 2022

Equipment	Equipment Component	Cause	Event Time
898669121Z	898669121Z	0952-MV6HDH ZTVMG MLG IVHKLMWRMT GL IVJFVHGH	08-10-2022 15:27:29
878746789Z	878746789Z	LWF Z Ic Kldvi Old Zozin	08-10-2022 15:26:12
898669119Z	898669119Z	0952-MV6HDH ZTVMG MLG IVHKLMWRMT GL IVJFVHGH	08-10-2022 15:23:14
898669121ZT-T	898669121ZT-T	2293-YGH L_N ORMP UZROFIV	08-10-2022 15:23:01
898669119ZT-T	898669119ZT-T	2293-YGH L_N ORMP UZROFIV	08-10-2022 15:23:01
898669121V6-T	898669121V6-T	2232-YXXS NRHHRMT	08-10-2022 15:23:00
898669121V7-T	898669121V7-T	2232-YXXS NRHHRMT	08-10-2022 15:23:00
898669121V8-T	898669121V8-T	2232-YXXS NRHHRMT	08-10-2022 15:23:00

Figure 8.26 - Clustered Fault History

Single Fault

For a particular equipment, user can view the detailed information by clicking the ⌄ icon.



74 total Predictions for this zone for latest 3 days ○ Clustered Faults (1/74) ● Single Fault (73/74) 07 Oct 08 Oct 09 Oct

Pat Number: 120247 Number of faults predicted: High: 0 Medium: 0 Low: 3

Equipment	Equipment Component	Cause	Site Priority	Prediction Day	Priority	Fault Type	Root Cause Details
898678582B	898678582B__NIYGH-88582/OMYGH-8858...	2342-YZHV HGZGRLM XLMMVXGRER...	Minor	09 Oct 2022	Low	-	▤
898678582B	898678582B__NIYGH-88582/GMOHEX-8/G...	38969-WVZW KVVI WVGVXGVW	Minor	09 Oct 2022	Low	-	▤
898678582B	898678582B__NIYGH-88582/GMOHEX-8/G...	38969-WVZW KVVI WVGVXGVW	Minor	09 Oct 2022	Low	-	▤

Pat Number: 120367 Number of faults predicted: High: 0 Medium: 0 Low: 2

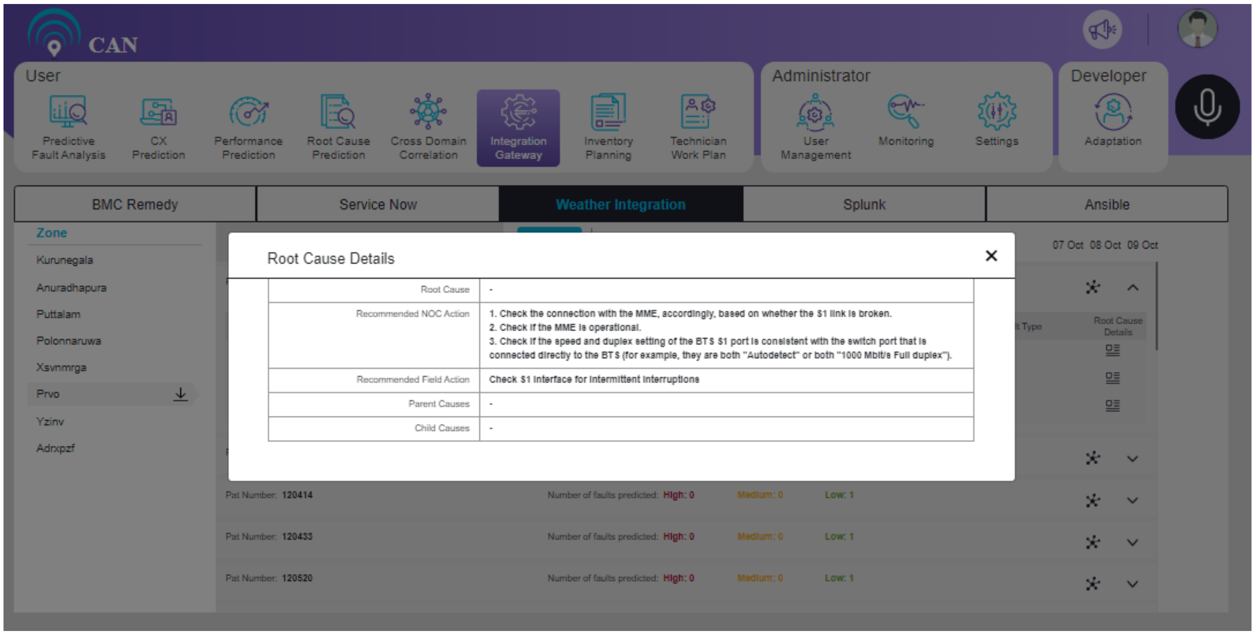
Pat Number: 120414 Number of faults predicted: High: 0 Medium: 0 Low: 1

Pat Number: 120433 Number of faults predicted: High: 0 Medium: 0 Low: 1

Pat Number: 120520 Number of faults predicted: High: 0 Medium: 0 Low: 1

Figure 8.27 - Prediction for Single Fault

Click on **Root Cause Details** icon ▤ to view the root cause details of that equipment.

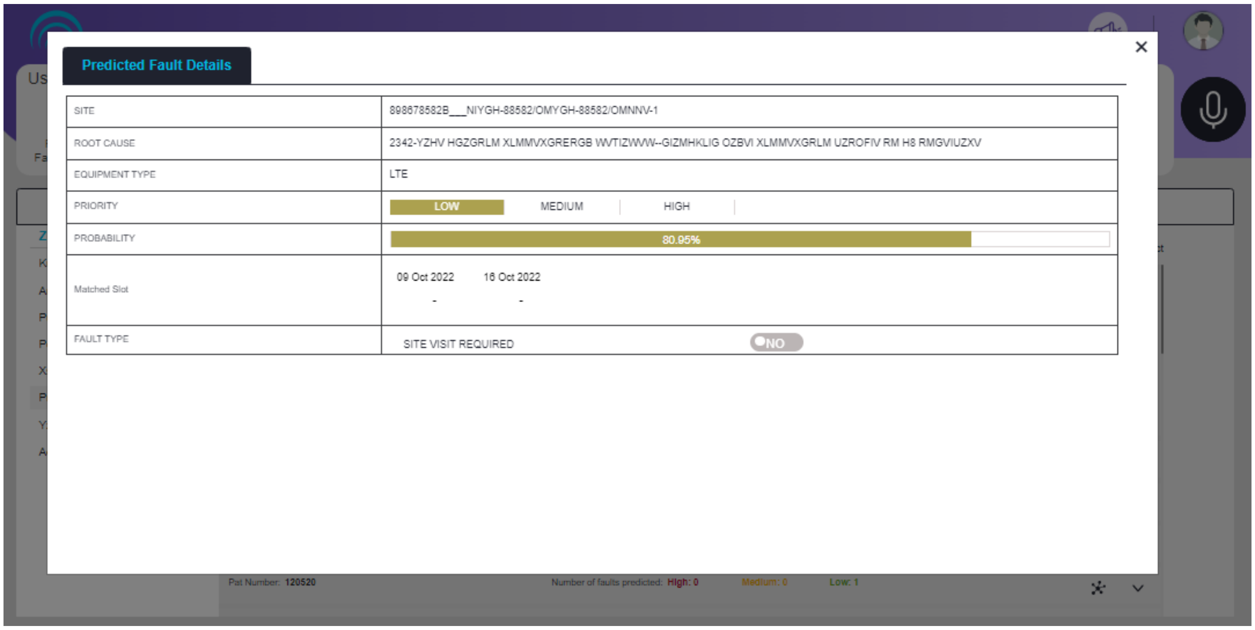


Root Cause Details

Root Cause	-
Recommended NOC Action	1. Check the connection with the MME, accordingly, based on whether the S1 link is broken. 2. Check if the MME is operational. 3. Check if the speed and duplex setting of the BTS S1 port is consistent with the switch port that is connected directly to the BTS (for example, they are both "Autodetect" or both "1000 Mbit/s Full duplex").
Recommended Field Action	Check S1 interface for intermittent interruptions
Parent Causes	-
Child Causes	-

Figure 8.28 - Root Cause Details

Click on any particular equipment to view the **Predicted Fault Details**.



Predicted Fault Details

SITE	898678582B___NIYGH-88582/OMYGH-88582/OMNNV-1
ROOT CAUSE	2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW--GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV
EQUIPMENT TYPE	LTE
PRIORITY	LOW MEDIUM HIGH
PROBABILITY	80.95%
Matched Slot	09 Oct 2022 16 Oct 2022 - -
FAULT TYPE	SITE VISIT REQUIRED NO

Figure 8.29 - Predictive Fault Details

Tabular view displays the network view ⁜ for every fault.

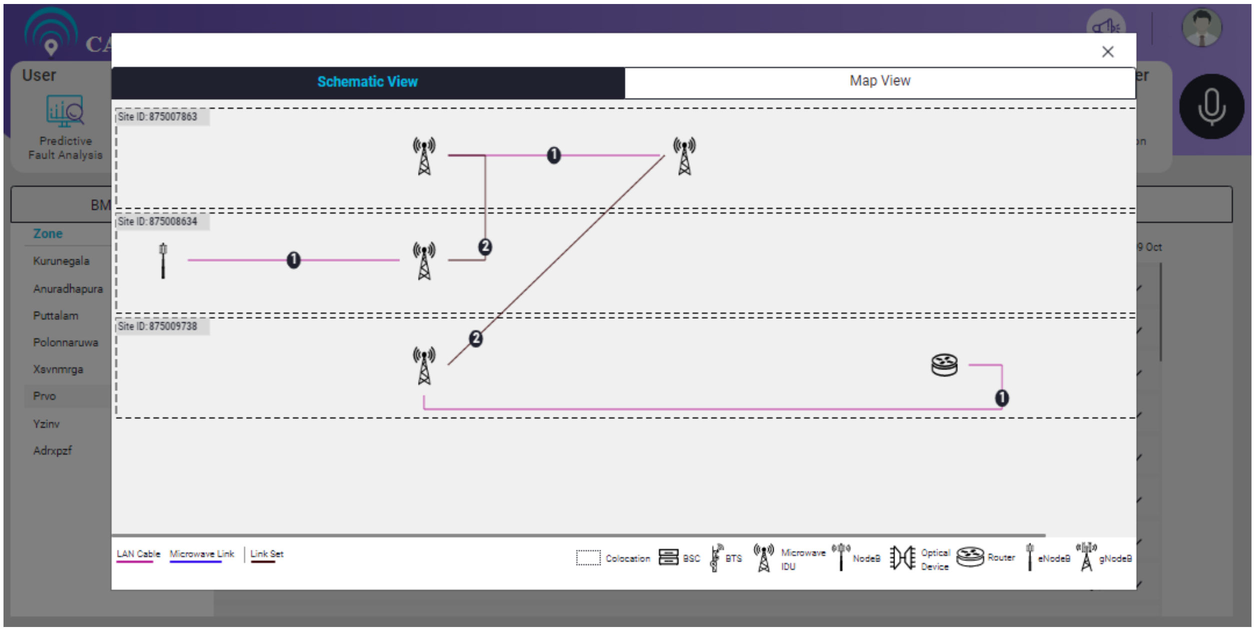


Figure 8.30 - Schematic View for Single Fault

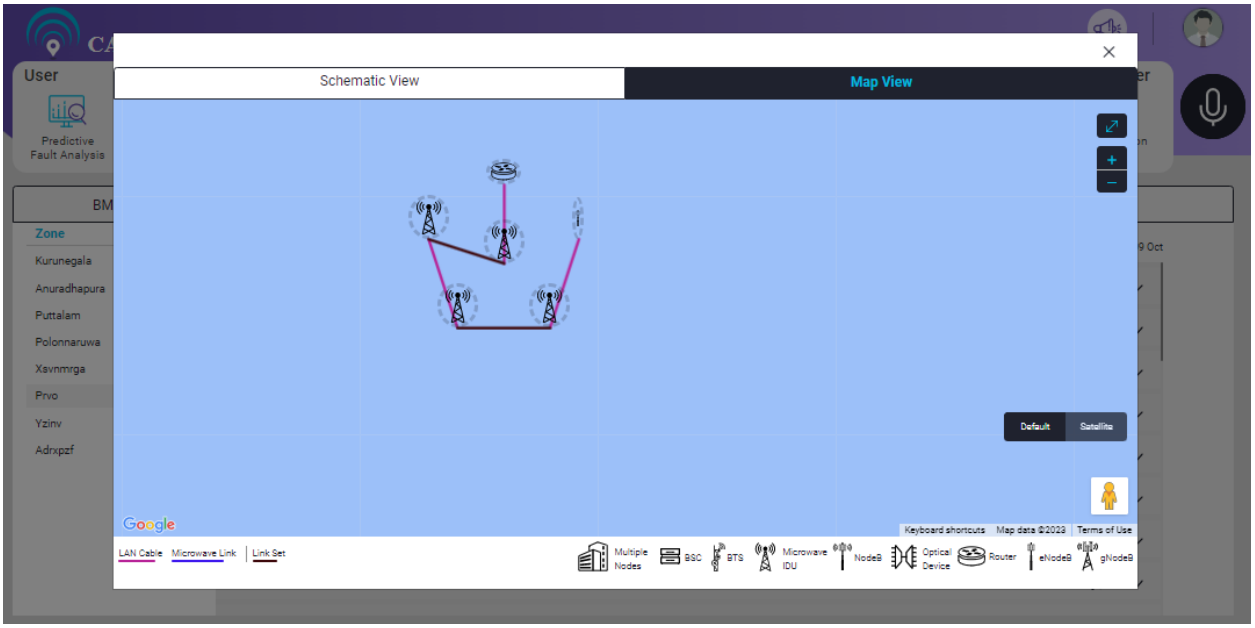


Figure 8.31 - Map View for Single Fault

Map View

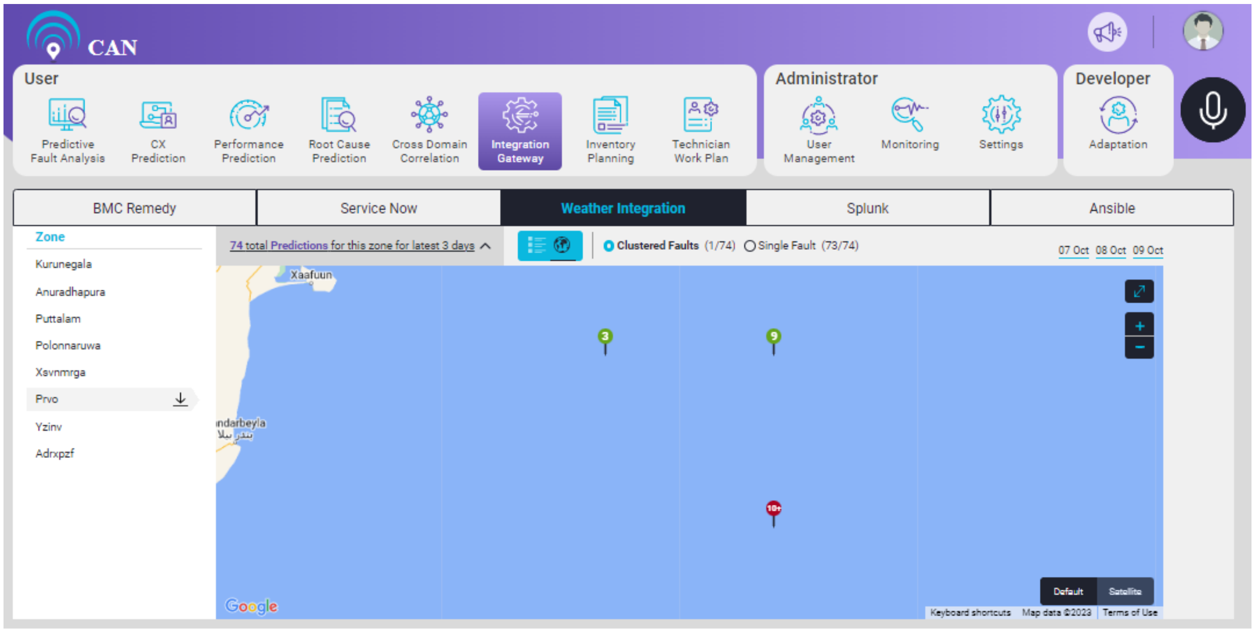
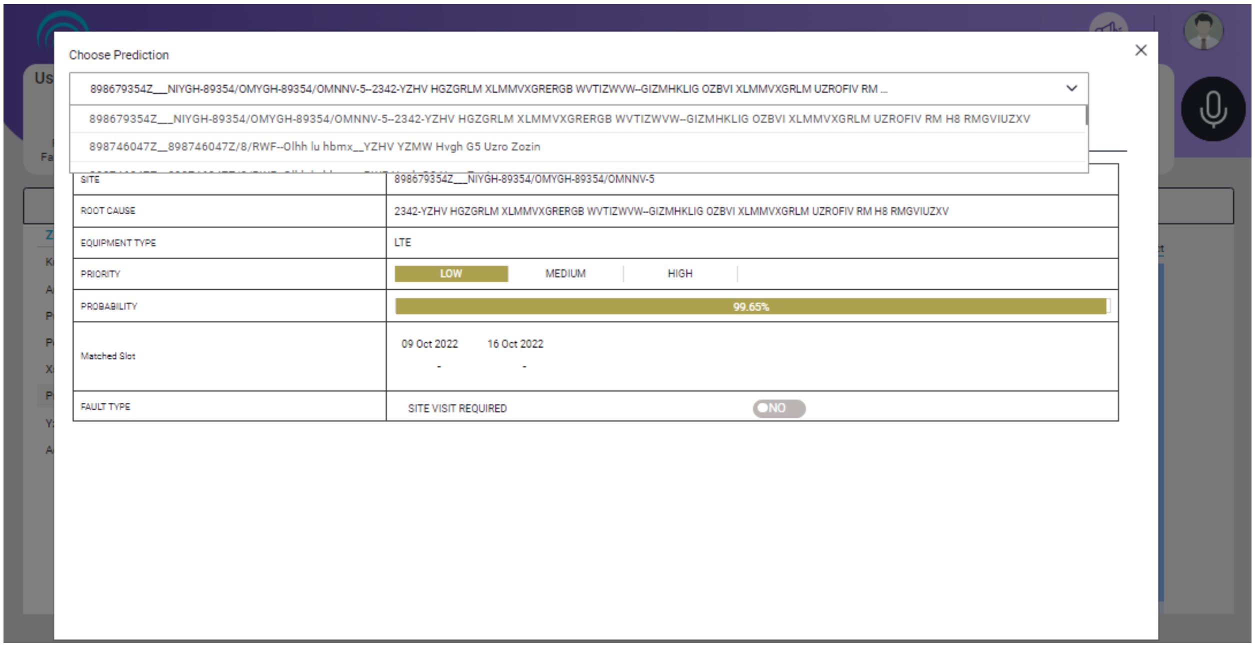


Figure 8.32 - Weather Prediction Map View

Click on any pointer to view the Predicted Fault Details. Choose a prediction from the dropdown.


Choose Prediction

898679354Z__NIYGH-89354/OMYGH-89354/OMNNV-5--2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW--GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM ...

898679354Z__NIYGH-89354/OMYGH-89354/OMNNV-5--2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW--GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV

898746047Z__898746047Z/8/RWF--Olhh lu hbmx__YZHV YZMW Hvgh G5 Uzro Zozin

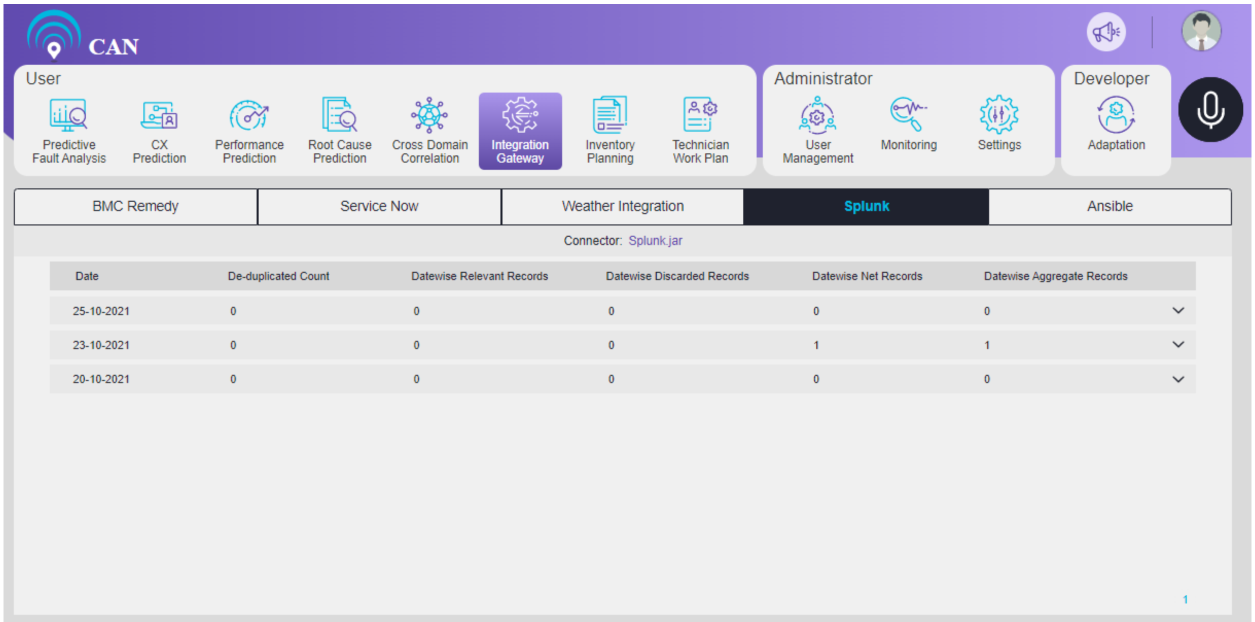
SITE	898679354Z__NIYGH-89354/OMYGH-89354/OMNNV-5
ROOT CAUSE	2342-YZHV HGZGRLM XLMMVXGRERGB WVTIZWVW--GIZMHKLIG OZBVI XLMMVXGRLM UZROFIV RM H8 RMGVIUZXV
EQUIPMENT TYPE	LTE
PRIORITY	LOW MEDIUM HIGH
PROBABILITY	99.65%
Matched Slot	09 Oct 2022 16 Oct 2022 - -
FAULT TYPE	SITE VISIT REQUIRED NO

Figure 8.33 - Prediction Dropdown with Fault Details

Splunk

By default, the Splunk screen shows the data.

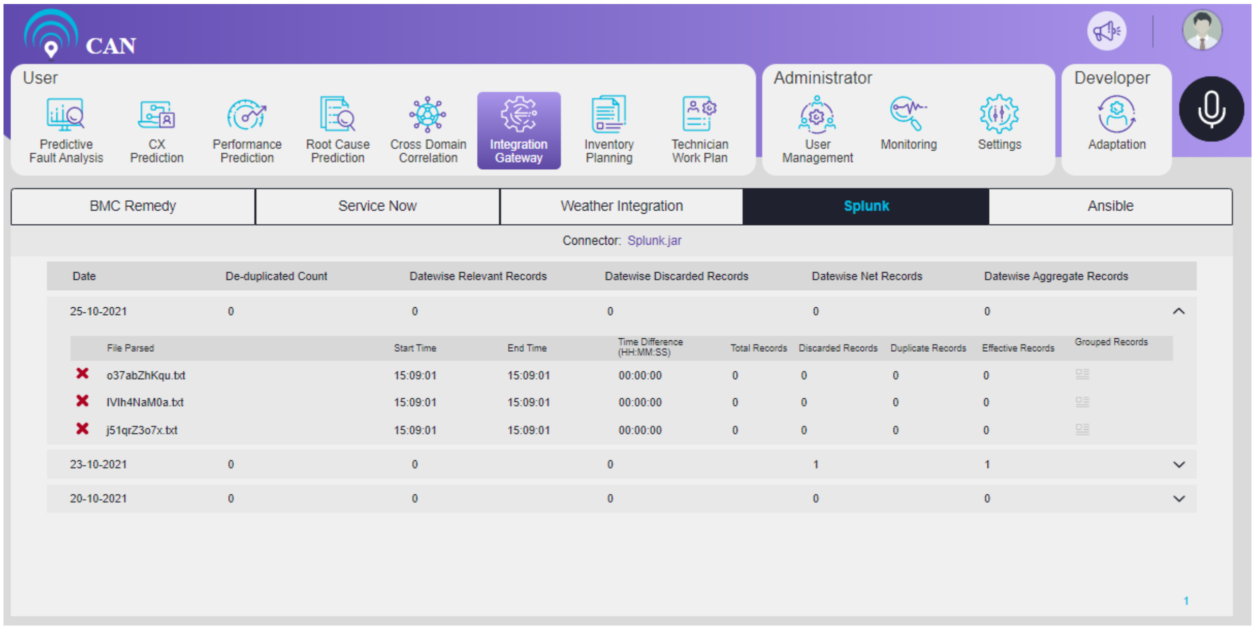
This screen displays the Date, De-Duplicated Count, Datewise Relevant Records, Datewise Discarded Records, Datewise Net Records and Datewise Aggregated Records on a daily basis.



Connector: Splunk.jar

Date	De-duplicated Count	Datewise Relevant Records	Datewise Discarded Records	Datewise Net Records	Datewise Aggregate Records
25-10-2021	0	0	0	0	0
23-10-2021	0	0	0	1	1
20-10-2021	0	0	0	0	0

Figure 8.34 - Splunk Logs Screen



Connector: Splunk.jar

Date	De-duplicated Count	Datewise Relevant Records	Datewise Discarded Records	Datewise Net Records	Datewise Aggregate Records
25-10-2021	0	0	0	0	0

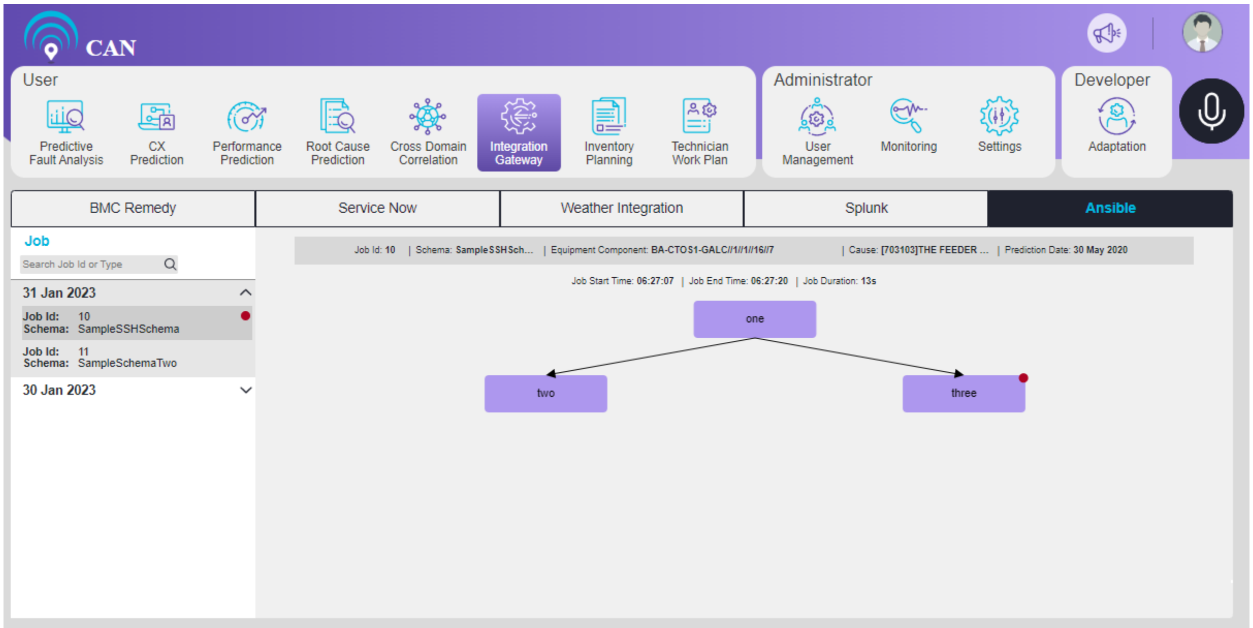
	File Parsed	Start Time	End Time	Time Difference (HH:MM:SS)	Total Records	Discarded Records	Duplicate Records	Effective Records	Grouped Records
✗	o37abZhKqu.txt	15:09:01	15:09:01	00:00:00	0	0	0	0	▤
✗	IVIh4NaM0a.txt	15:09:01	15:09:01	00:00:00	0	0	0	0	▤
✗	j51qrZ3o7x.txt	15:09:01	15:09:01	00:00:00	0	0	0	0	▤

Date	De-duplicated Count	Datewise Relevant Records	Datewise Discarded Records	Datewise Net Records	Datewise Aggregate Records
23-10-2021	0	0	0	1	1
20-10-2021	0	0	0	0	0

Figure 8.35 - Splunk Log Details

Ansible

Ansible Gateway screen displays the jobs that are executed.



Job Id: 10 | Schema: SampleSSHSch... | Equipment Component: BA-CTOS1-GALC//1//1//16//7 | Cause: [703103]THE FEEDER ... | Prediction Date: 30 May 2020

Job Start Time: 06:27:07 | Job End Time: 06:27:20 | Job Duration: 13s

31 Jan 2023

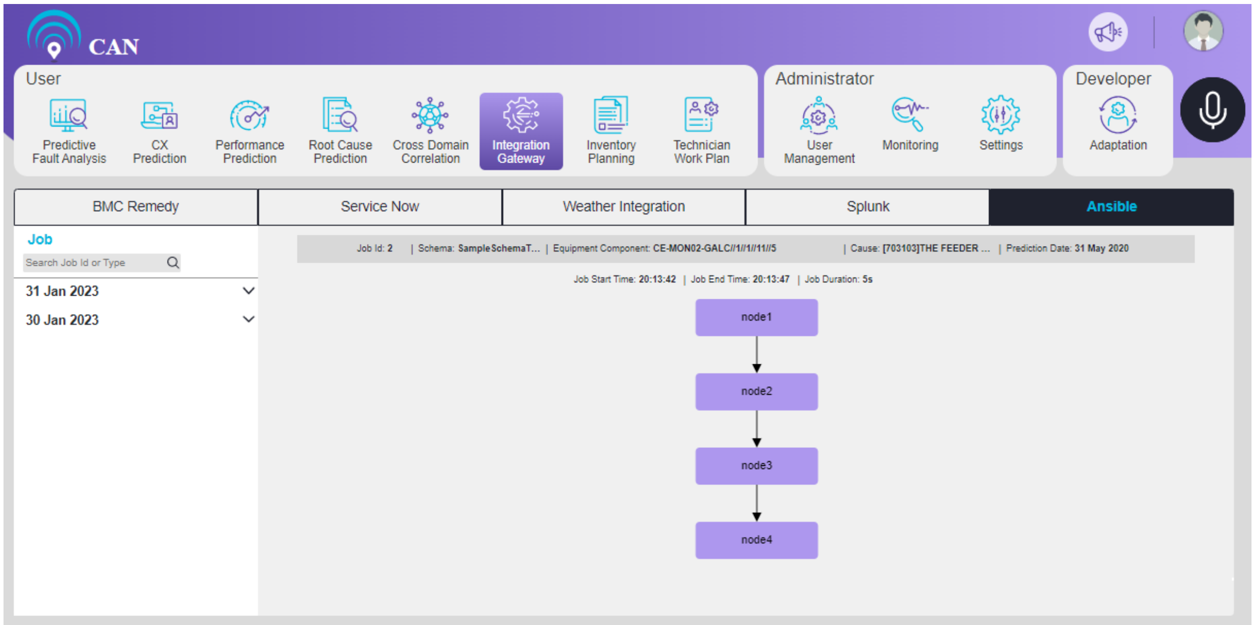
Job Id: 10 ●
Schema: SampleSSHSchema

Job Id: 11
Schema: SampleSchemaTwo

30 Jan 2023

Figure 8.36 - Ansible Screen

The jobs are listed on the left side of the screen. They are grouped and displayed based on date.



Job Id: 2 | Schema: SampleSchemaT... | Equipment Component: CE-MON02-GALC//1//1//11//5 | Cause: [703103]THE FEEDER ... | Prediction Date: 31 May 2020

Job Start Time: 20:13:42 | Job End Time: 20:13:47 | Job Duration: 5s

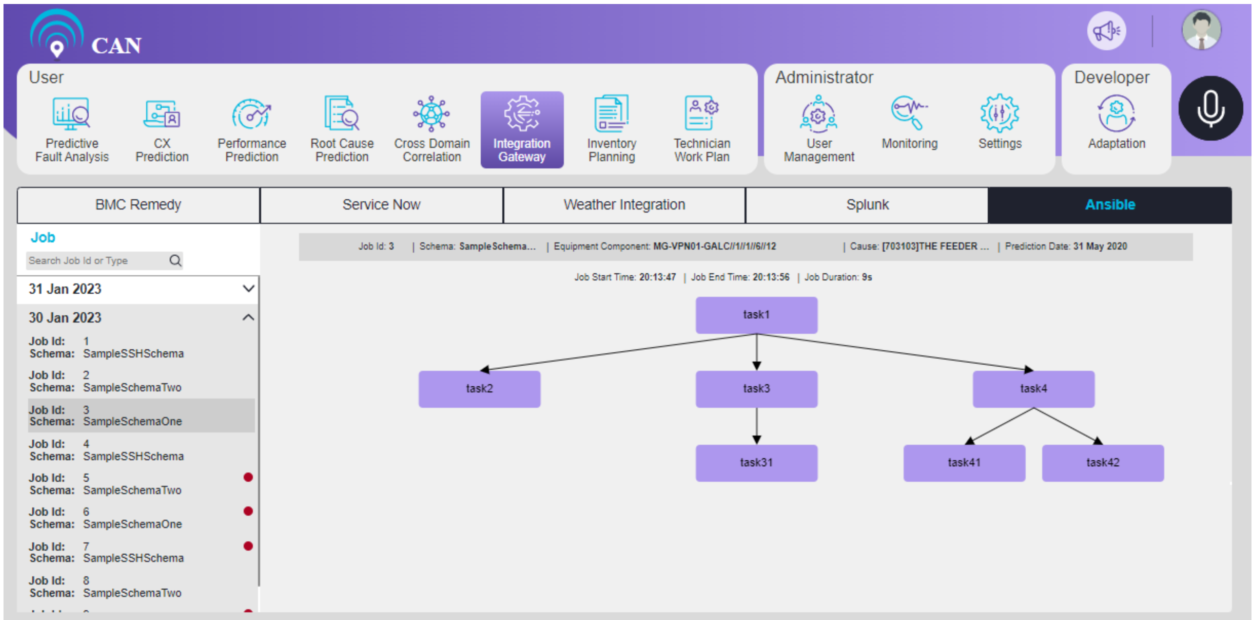
31 Jan 2023

30 Jan 2023

Figure 8.37 - Jobs Based on Date

Click on a particular date to view the list of executed jobs. Job that has a failed task is indicated by ● icon.

Click on a **Job Id** to display the executed tasks workflow diagram that shows the job execution flow.



31 Jan 2023

30 Jan 2023

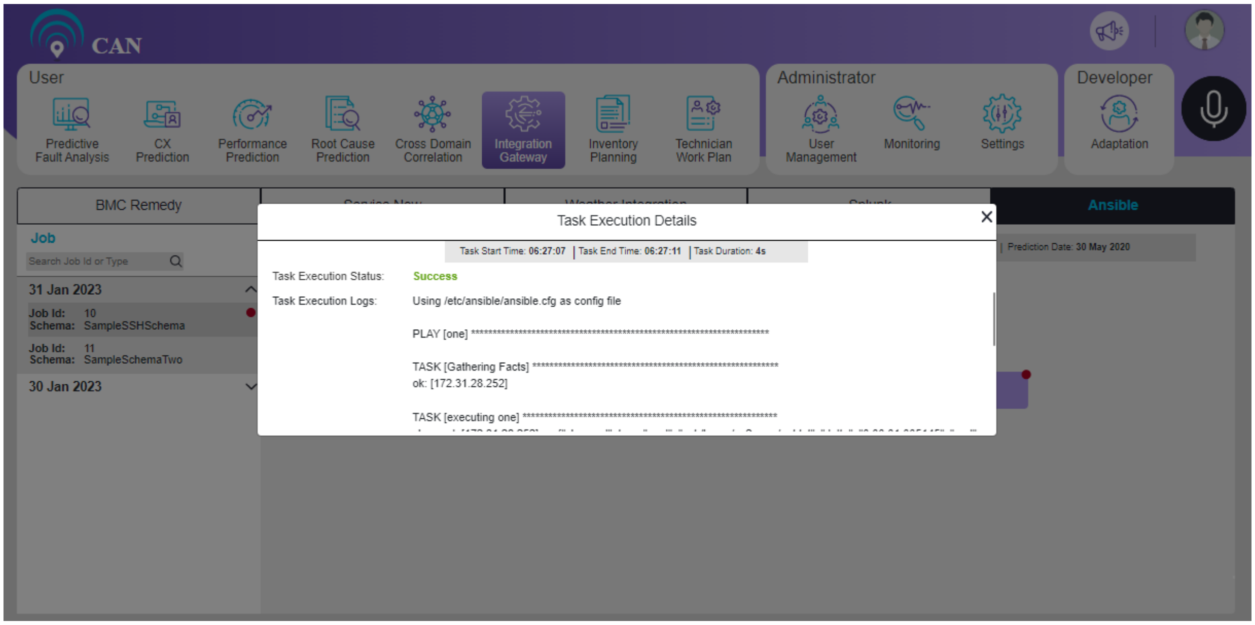
Job Id: 1 Schema: SampleSSHSchema
Job Id: 2 Schema: SampleSchemaTwo
Job Id: 3 Schema: SampleSchemaOne
Job Id: 4 Schema: SampleSSHSchema
Job Id: 5 Schema: SampleSchemaTwo
Job Id: 6 Schema: SampleSchemaOne
Job Id: 7 Schema: SampleSSHSchema
Job Id: 8 Schema: SampleSchemaTwo

Job Id: 3 | Schema: SampleSchema... | Equipment Component: MG-VPN01-GALC//1//1//6//12 | Cause: [703103]THE FEEDER ... | Prediction Date: 31 May 2020

Job Start Time: 20:13:47 | Job End Time: 20:13:56 | Job Duration: 9s

Figure 8.38 - List of Jobs

Click on each task to display the **Task Execution Details** as a popup. Click on X to close the popup.



31 Jan 2023

Job Id: 10 Schema: SampleSSHSchema
Job Id: 11 Schema: SampleSchemaTwo

30 Jan 2023

Prediction Date: 30 May 2020

Task Start Time: 06:27:07 | Task End Time: 06:27:11 | Task Duration: 4s

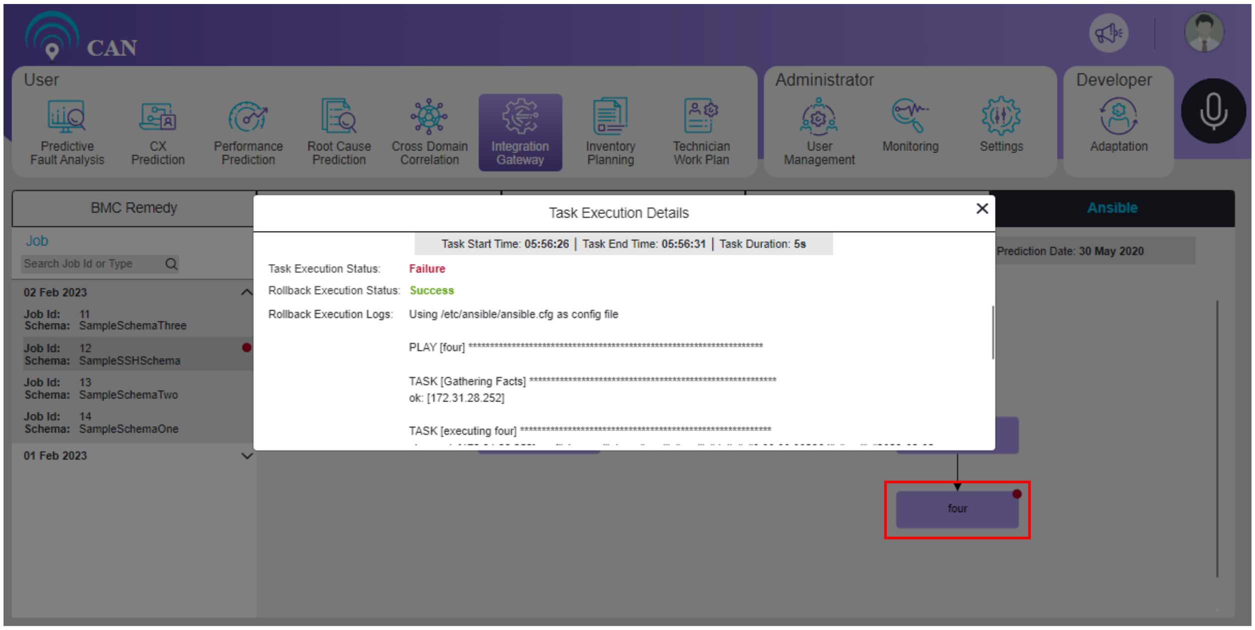
Task Execution Status: Success

Task Execution Logs:

```
Using /etc/ansible/ansible.cfg as config file

PLAY [one] *********************************************************************

TASK [Gathering Facts] *********************************************************
ok: [172.31.28.252]

TASK [executing one] ***********************************************************
```

Figure 8.39 - Task Execution Details

A failed task is highlighted on the workflow. Task configured below a failed task is not executed.



02 Feb 2023

Job Id: 11
Schema: SampleSchemaThree

Job Id: 12
Schema: SampleSSHSchema

Job Id: 13
Schema: SampleSchemaTwo

Job Id: 14
Schema: SampleSchemaOne

01 Feb 2023

Prediction Date: 30 May 2020

Task Execution Details

Task Start Time: **05:56:26** | Task End Time: **05:56:31** | Task Duration: **5s**

Task Execution Status: **Failure**

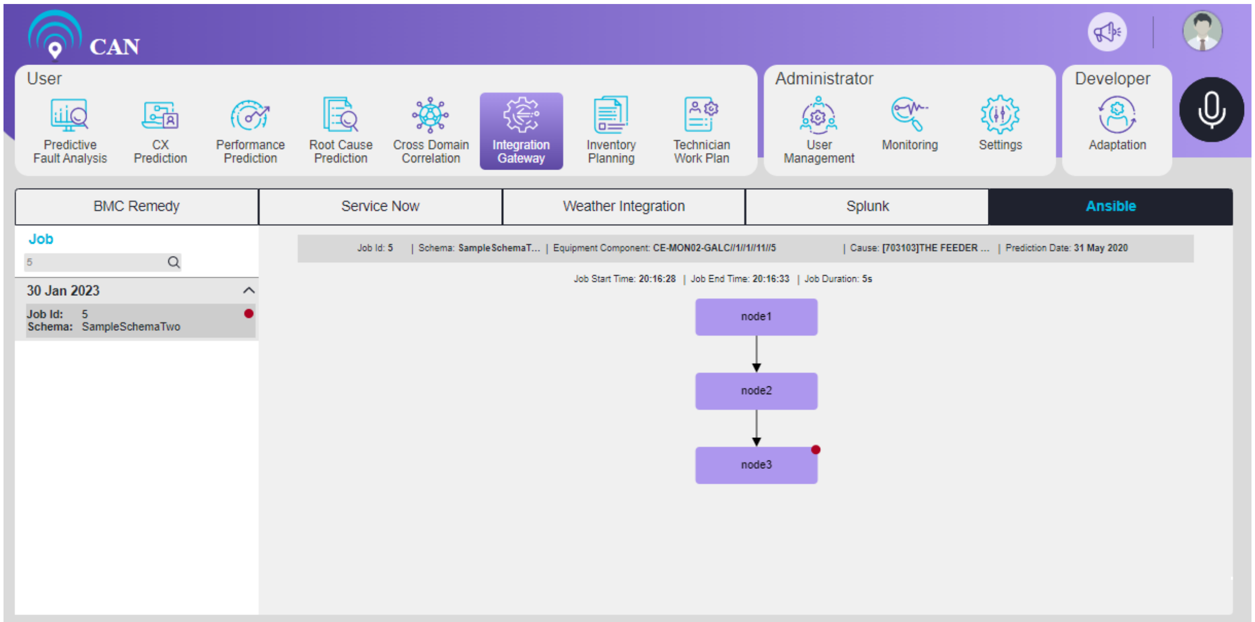
Rollback Execution Status: **Success**

Rollback Execution Logs:

```
Using /etc/ansible/ansible.cfg as config file

PLAY [four] *********************************************************************

TASK [Gathering Facts] *****************************************************************
ok: [172.31.28.252]

TASK [executing four] *****************************************************************
```

Figure 8.40 - Task Failure

User can Search a job based on **Job Id** or **Type**.



5

30 Jan 2023

Job Id: 5
Schema: SampleSchemaTwo

Job Id: **5** | Schema: **SampleSchemaT...** | Equipment Component: **CE-MON02-GALC//1//1//11//5** | Cause: **[703103]THE FEEDER ...** | Prediction Date: **31 May 2020**

Job Start Time: **20:16:28** | Job End Time: **20:16:33** | Job Duration: **5s**

Figure 8.41 - Search a Job

Page Intentionally Left Blank

9. 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:

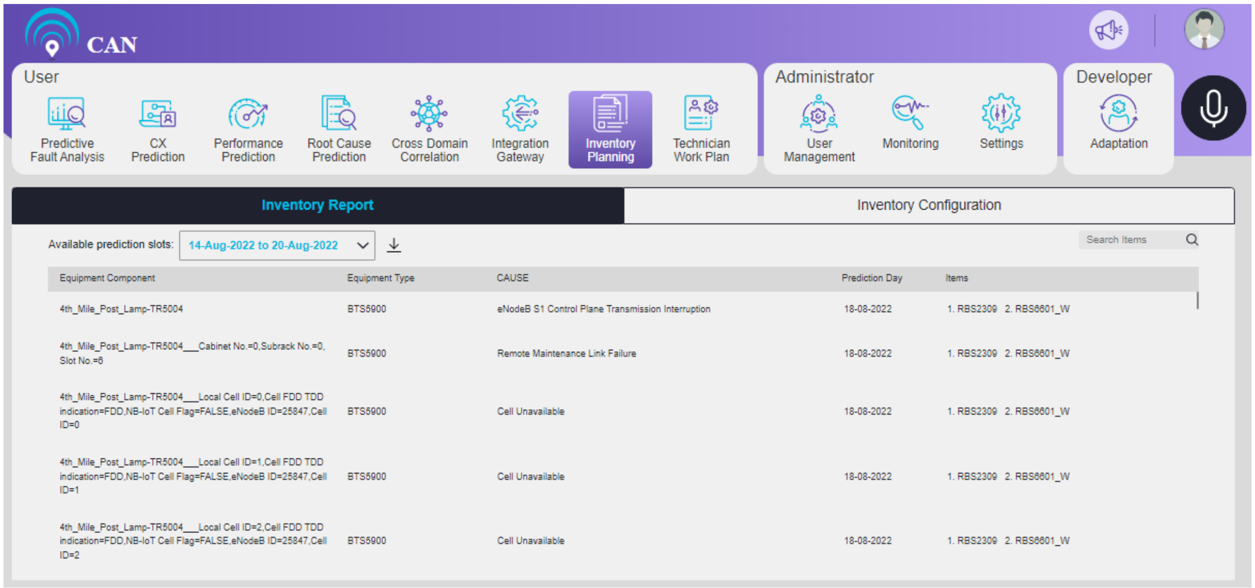
1. Inventory Report
2. Inventory Configuration

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.



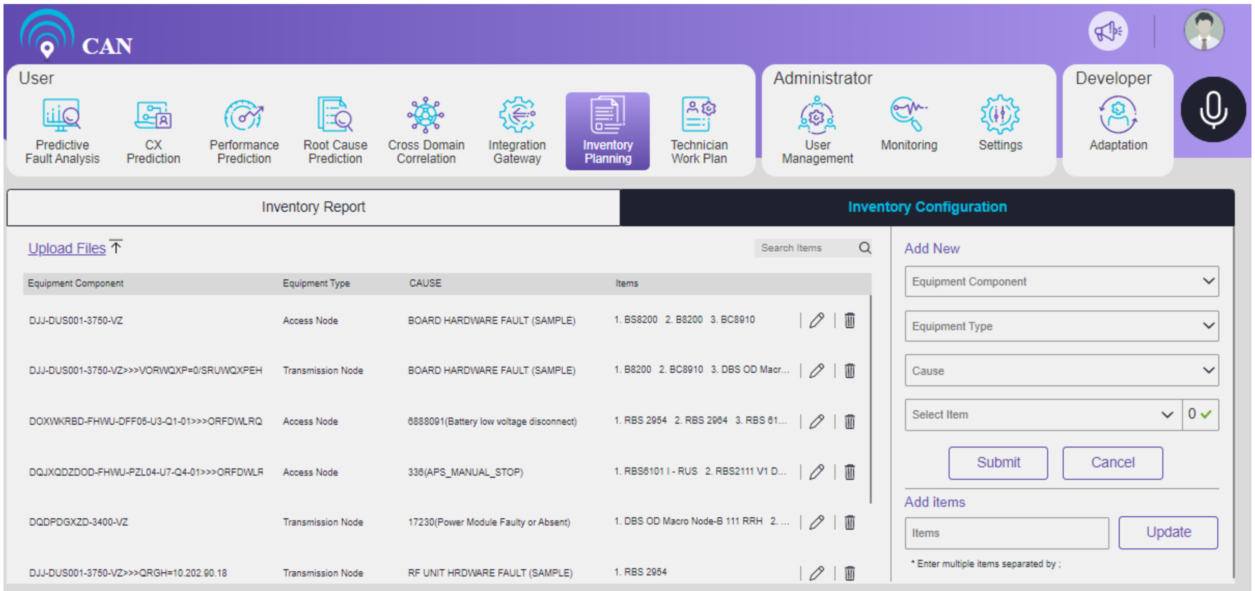
Available prediction slots: 14-Aug-2022 to 20-Aug-2022

Equipment Component	Equipment Type	CAUSE	Prediction Day	Items
4th_Mile_Post_Lamp-TR5004	BTS5900	eNodeB S1 Control Plane Transmission Interruption	18-08-2022	1. RBS2309 2. RBS6601_W
4th_Mile_Post_Lamp-TR5004___Cabinet No.=0,Subrack No.=0, Slot No.=6	BTS5900	Remote Maintenance Link Failure	18-08-2022	1. RBS2309 2. RBS6601_W
4th_Mile_Post_Lamp-TR5004___Local Cell ID=0,Cell FDD TDD indication=FDD,NB-IoT Cell Flag=FALSE,eNodeB ID=25847,Cell ID=0	BTS5900	Cell Unavailable	18-08-2022	1. RBS2309 2. RBS6601_W
4th_Mile_Post_Lamp-TR5004___Local Cell ID=1,Cell FDD TDD indication=FDD,NB-IoT Cell Flag=FALSE,eNodeB ID=25847,Cell ID=1	BTS5900	Cell Unavailable	18-08-2022	1. RBS2309 2. RBS6601_W
4th_Mile_Post_Lamp-TR5004___Local Cell ID=2,Cell FDD TDD indication=FDD,NB-IoT Cell Flag=FALSE,eNodeB ID=25847,Cell ID=2	BTS5900	Cell Unavailable	18-08-2022	1. RBS2309 2. RBS6601_W

Figure 9.1 - Inventory Planning Home Page

Inventory Configuration

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



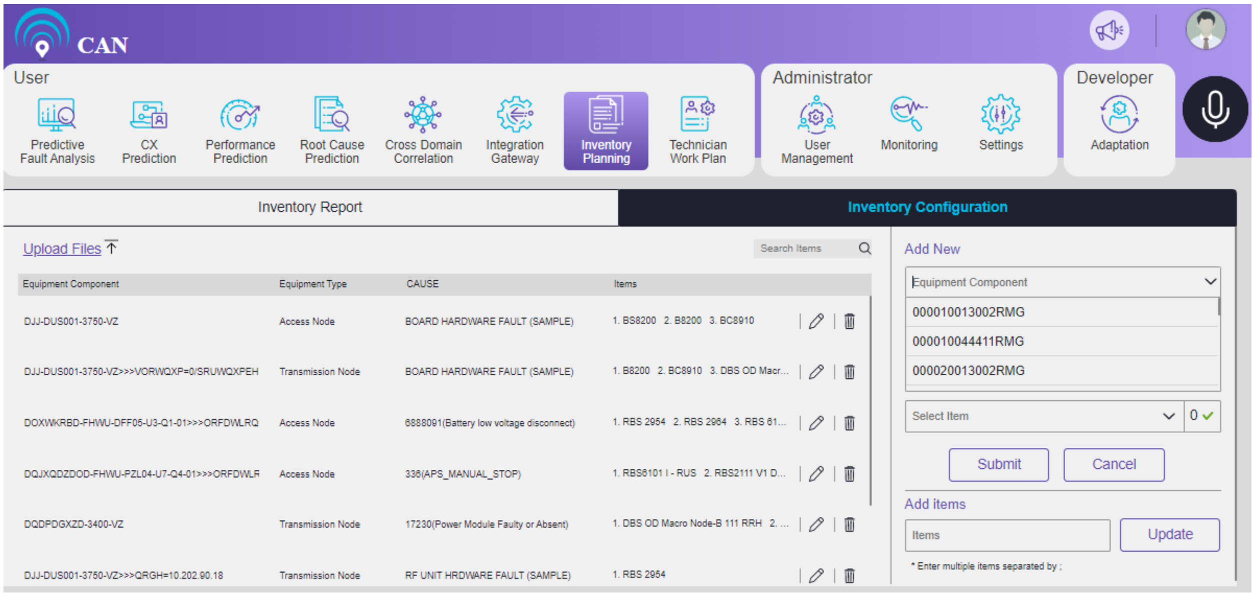
Equipment Component	Equipment Type	CAUSE	Items
DJJ-DUS001-3750-VZ	Access Node	BOARD HARDWARE FAULT (SAMPLE)	1. BS8200 2. B8200 3. BC8910
DJJ-DUS001-3750-VZ>>>VORWQXP=0/SRUWQXPEH	Transmission Node	BOARD HARDWARE FAULT (SAMPLE)	1. B8200 2. BC8910 3. DBS OD Macr...
DOXWKRBD-FHWU-DFF05-U3-Q1-01>>>ORFDWLRQ	Access Node	6888091(Battery low voltage disconnect)	1. RBS 2954 2. RBS 2964 3. RBS 61...
DQJXQDZDOD-FHWU-PZL04-U7-Q4-01>>>ORFDWLR	Access Node	336(APS_MANUAL_STOP)	1. RBS6101 I - RUS 2. RBS2111 V1 D...
DQDPDGXZD-3400-VZ	Transmission Node	17230(Power Module Faulty or Absent)	1. DBS OD Macro Node-B 111 RRH 2. ...
DJJ-DUS001-3750-VZ>>>QRGH=10.202.90.18	Transmission Node	RF UNIT HRDWARE FAULT (SAMPLE)	1. RBS 2954

* Enter multiple items separated by ;

Figure 9.2 - Inventory Configuration 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.



Equipment Component	Equipment Type	CAUSE	Items
DJJ-DUS001-3750-VZ	Access Node	BOARD HARDWARE FAULT (SAMPLE)	1. BS8200 2. B8200 3. BC8910
DJJ-DUS001-3750-VZ>>>VORWQXP=0/SRUWQXPEH	Transmission Node	BOARD HARDWARE FAULT (SAMPLE)	1. B8200 2. BC8910 3. DBS OD Macr...
DOXWKRBD-FHWU-DFF05-U3-Q1-01>>>ORFDWLRQ	Access Node	6888091(Battery low voltage disconnect)	1. RBS 2954 2. RBS 2964 3. RBS 61...
DQJXQDZDOD-FHWU-PZL04-U7-Q4-01>>>ORFDWLR	Access Node	336(APS_MANUAL_STOP)	1. RBS6101 I - RUS 2. RBS2111 V1 D...
DQDPDGXZD-3400-VZ	Transmission Node	17230(Power Module Faulty or Absent)	1. DBS OD Macro Node-B 111 RRH 2. ...
DJJ-DUS001-3750-VZ>>>QRGH=10.202.90.18	Transmission Node	RF UNIT HRDWARE FAULT (SAMPLE)	1. RBS 2954

000010013002RMG
000010044411RMG
000020013002RMG

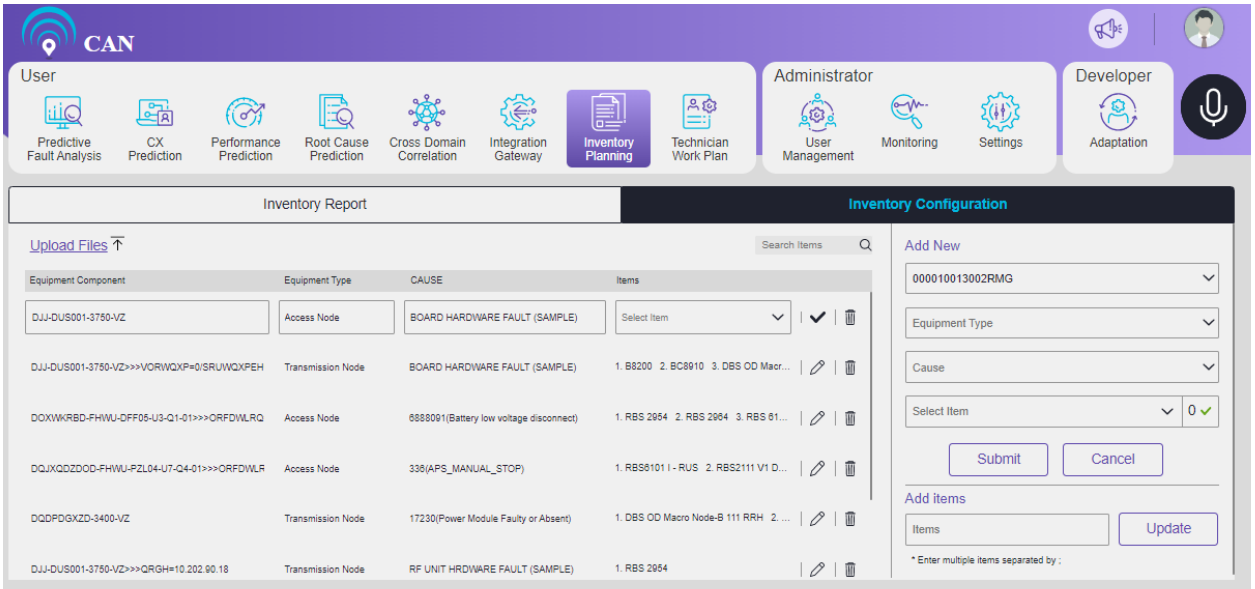
* Enter multiple items separated by ;

Figure 9.3 - New Equipment Item Addition Screen

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**.



Equipment Component	Equipment Type	CAUSE	Items
DJJ-DUS001-3750-VZ	Access Node	BOARD HARDWARE FAULT (SAMPLE)	Select Item
DJJ-DUS001-3750-VZ>>>VORWQXP=0/SRUWQXPEH	Transmission Node	BOARD HARDWARE FAULT (SAMPLE)	1. B8200 2. BC8910 3. DBS OD Macr...
DOXWKRBD-FHWU-DFF05-U3-Q1-01>>>ORFDWLRQ	Access Node	6888091(Battery low voltage disconnect)	1. RBS 2954 2. RBS 2964 3. RBS 61...
DQJXQDZDOD-FHWU-PZL04-U7-Q4-01>>>ORFDWLR	Access Node	336(APS_MANUAL_STOP)	1. RBS6101 I - RUS 2. RBS2111 V1 D...
DQDPDGXZD-3400-VZ	Transmission Node	17230(Power Module Faulty or Absent)	1. DBS OD Macro Node-B 111 RRH 2. ...
DJJ-DUS001-3750-VZ>>>QRGH=10.202.90.18	Transmission Node	RF UNIT HRDWARE FAULT (SAMPLE)	1. RBS 2954

Add New

000010013002RMG

Equipment Type

Cause

Select Item 0 ✓

Submit Cancel

Add items

Items Update

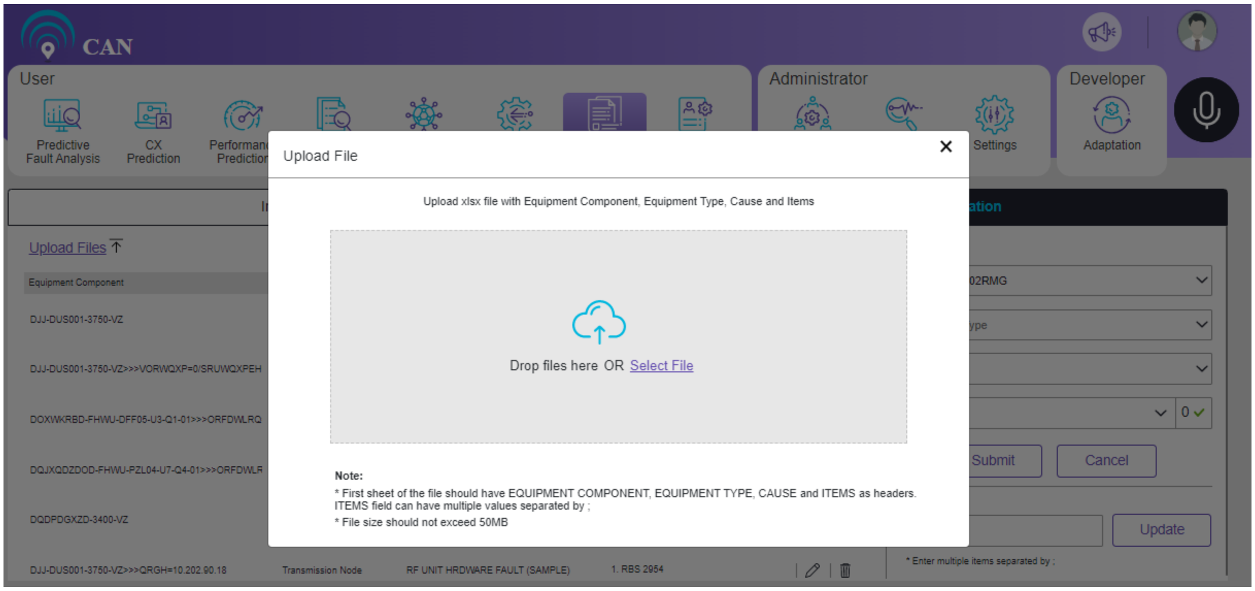
* Enter multiple items separated by ;

Figure 9.4 - 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.


CAN
User
Predictive Fault Analysis
CX Prediction
Performance Prediction
Administrator
Settings
Developer
Adaptation
Upload Files
Equipment Component
DJJ-DUS001-3750-VZ
DJJ-DUS001-3750-VZ>>>VORWQXP=0/SRUWQXPEH
DOXWKRBD-FHWU-DFF05-U3-Q1-01>>>ORFDWLRQ
DQJXQDZDOD-FHWU-PZL04-U7-Q4-01>>>ORFDWLR
DQDPDGXZD-3400-VZ
DJJ-DUS001-3750-VZ>>>QRGH=10.202.90.18
Transmission Node
RF UNIT HRDWARE FAULT (SAMPLE)
1. RBS 2954
02RMG
ype
0
Submit
Cancel
Update
* Enter multiple items separated by ;

Upload File

Upload xlsx file with Equipment Component, Equipment Type, Cause and Items

Drop files here OR Select File

Note:

* First sheet of the file should have EQUIPMENT COMPONENT, EQUIPMENT TYPE, CAUSE and ITEMS as headers. ITEMS field can have multiple values separated by ;

* File size should not exceed 50MB

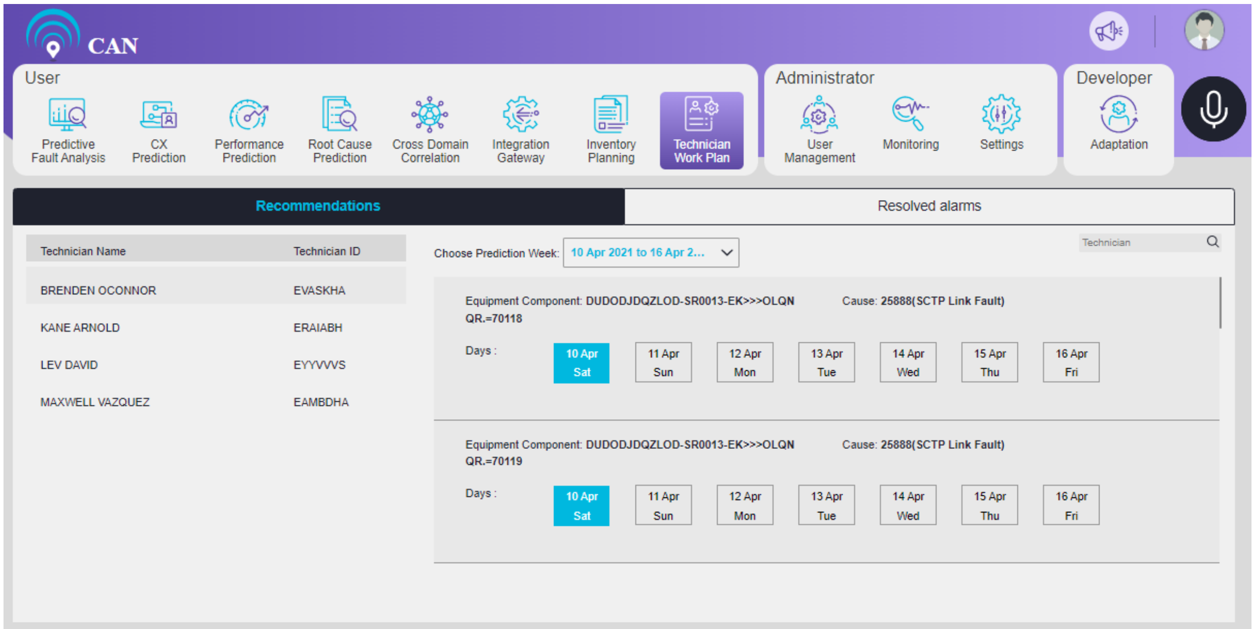
Figure 9.5 - Upload File Screen

Page Intentionally Left Blank

10. 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**.



Technician Name	Technician ID
BRENDEN OCONNOR	EVASKHA
KANE ARNOLD	ERAIABH
LEV DAVID	EYYVVVS
MAXWELL VAZQUEZ	EAMBDHA

Choose Prediction Week: 10 Apr 2021 to 16 Apr 2...

Equipment Component: **DUDODJDQZLOD-SR0013-EK>>>OLQN QR.=70118** Cause: **25888(SCTP Link Fault)**

Days : 10 Apr Sat | 11 Apr Sun | 12 Apr Mon | 13 Apr Tue | 14 Apr Wed | 15 Apr Thu | 16 Apr Fri

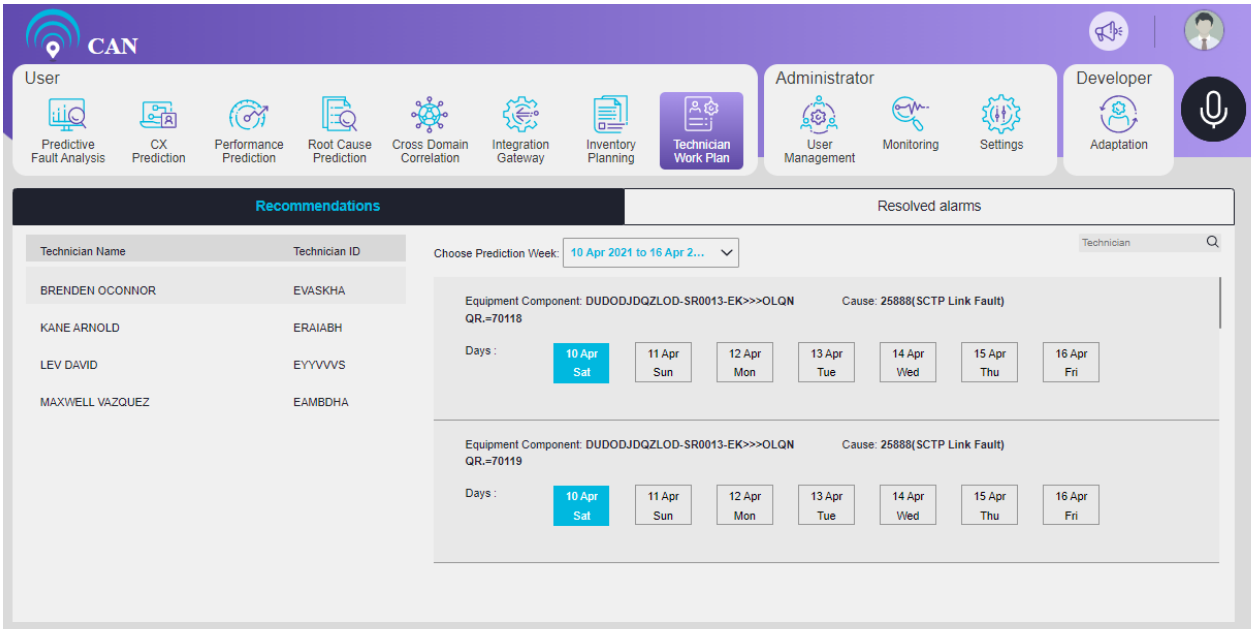
Equipment Component: **DUDODJDQZLOD-SR0013-EK>>>OLQN QR.=70119** Cause: **25888(SCTP Link Fault)**

Days : 10 Apr Sat | 11 Apr Sun | 12 Apr Mon | 13 Apr Tue | 14 Apr Wed | 15 Apr Thu | 16 Apr Fri

Figure 10.1 - 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 that can occur in the prediction week.



Technician Name	Technician ID
BRENDEN OCONNOR	EVASKHA
KANE ARNOLD	ERAIABH
LEV DAVID	EYYVVVS
MAXWELL VAZQUEZ	EAMBDHA

Choose Prediction Week: 10 Apr 2021 to 16 Apr 2...

Equipment Component: DUDODJDQZLOD-SR0013-EK>>>OLQN QR.=70118 Cause: 25888(SCTP Link Fault)

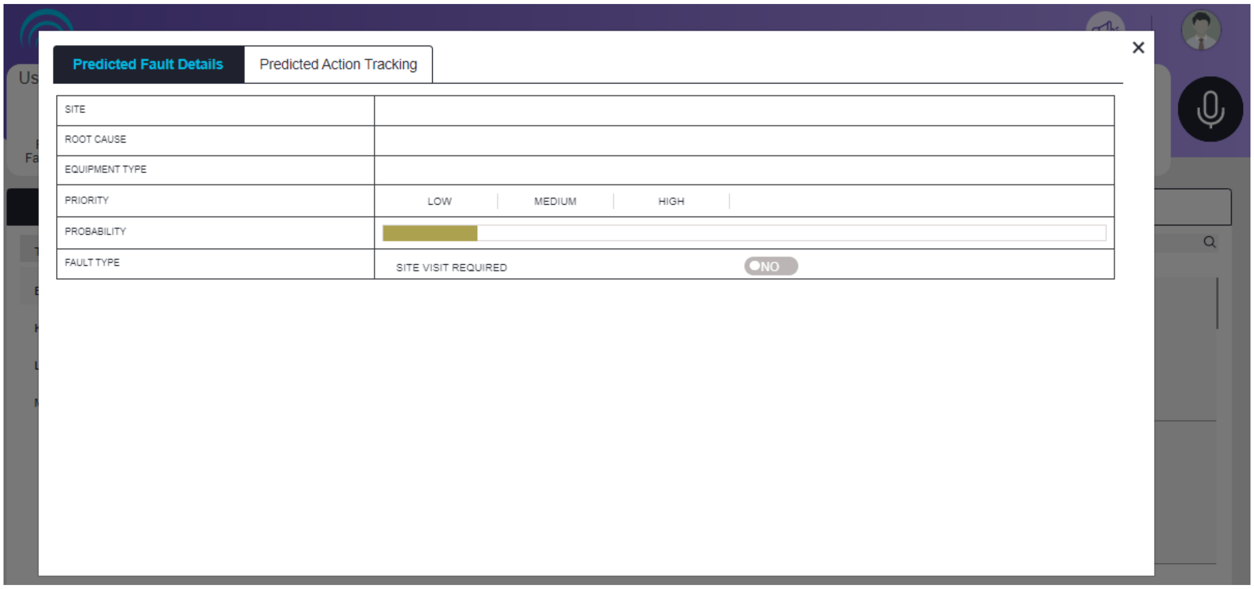
Days : 10 Apr Sat | 11 Apr Sun | 12 Apr Mon | 13 Apr Tue | 14 Apr Wed | 15 Apr Thu | 16 Apr Fri

Equipment Component: DUDODJDQZLOD-SR0013-EK>>>OLQN QR.=70119 Cause: 25888(SCTP Link Fault)

Days : 10 Apr Sat | 11 Apr Sun | 12 Apr Mon | 13 Apr Tue | 14 Apr Wed | 15 Apr Thu | 16 Apr Fri

Figure 10.2 - Recommendations

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

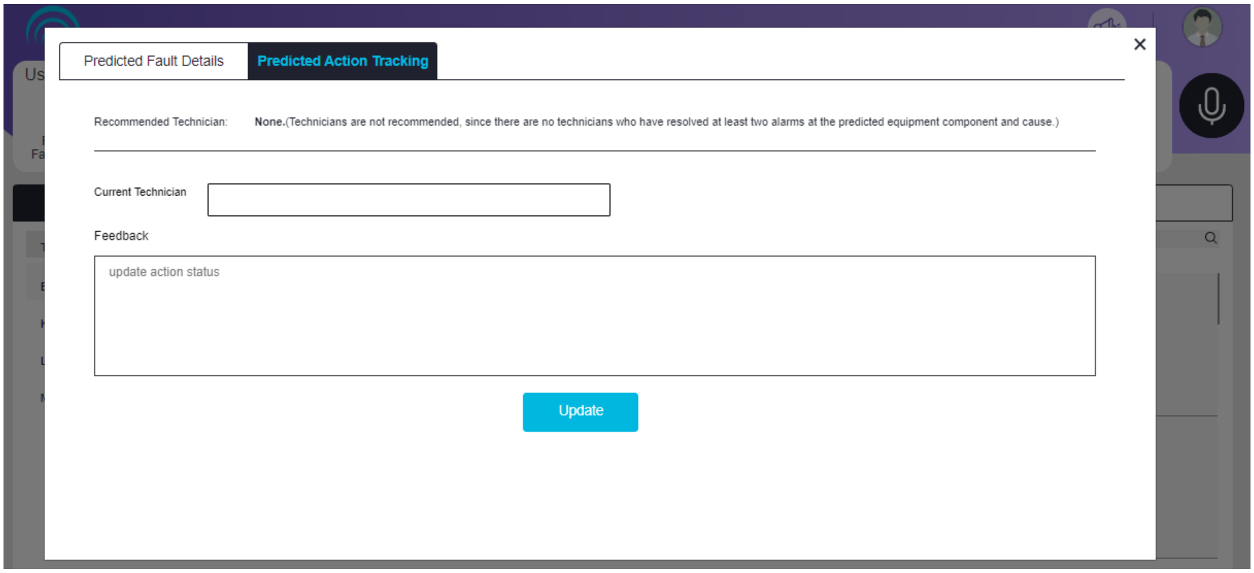


SITE	
ROOT CAUSE	
EQUIPMENT TYPE	
PRIORITY	LOW | MEDIUM | HIGH
PROBABILITY	
FAULT TYPE	SITE VISIT REQUIRED NO

Figure 10.3 - 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**.



Recommended Technician: **None.**(Technicians are not recommended, since there are no technicians who have resolved at least two alarms at the predicted equipment component and cause.)

Current Technician

Feedback

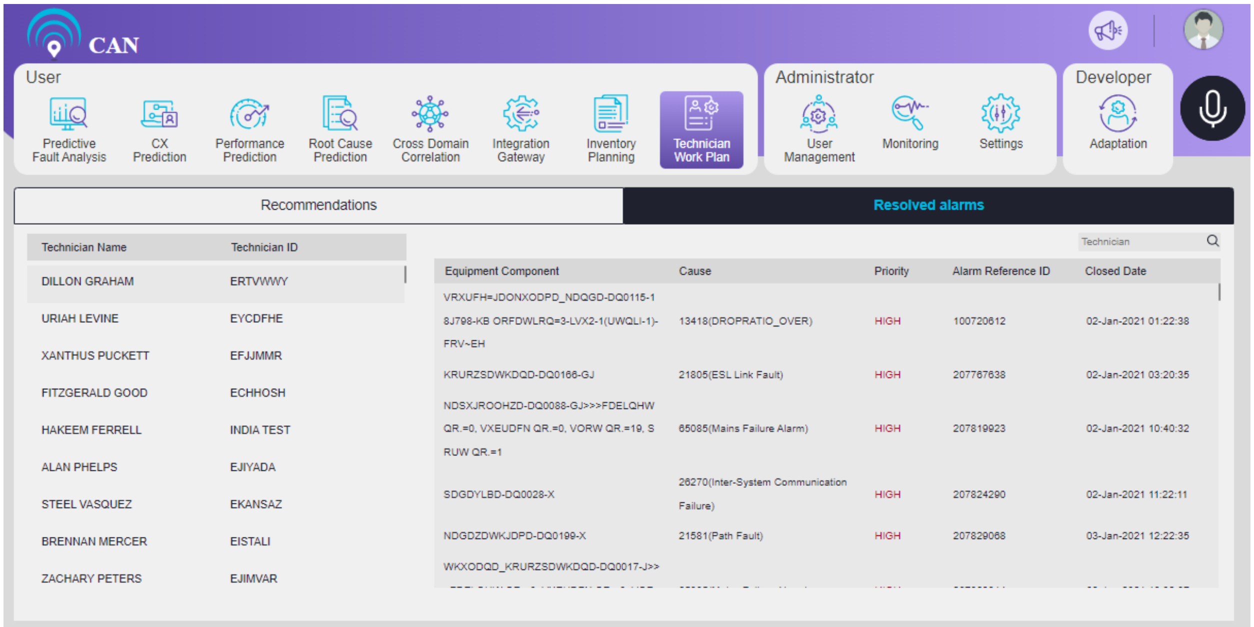
update action status

Figure 10.4 - 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.



Technician Name	Technician ID
DILLON GRAHAM	ERTVWWY
URIAH LEVINE	EYCDFHE
XANTHUS PUCKETT	EFJJMMR
FITZGERALD GOOD	ECHHOSH
HAKEEM FERRELL	INDIA TEST
ALAN PHELPS	EJIYADA
STEEL VASQUEZ	EKANSAZ
BRENNAN MERCER	EISTALI
ZACHARY PETERS	EJIMVAR

Equipment Component	Cause	Priority	Alarm Reference ID	Closed Date
VRXUFH=JDONXODPD_NDQGD-DQ0115-1 8J798-KB ORFDWLRQ=3-LVX2-1(UWQLI-1)-FRV~EH	13418(DROPRATIO_OVER)	HIGH	100720612	02-Jan-2021 01:22:38
KRURZSDWKDQD-DQ0166-GJ	21805(ESL Link Fault)	HIGH	207767638	02-Jan-2021 03:20:35
NDSXJROOHZD-DQ0088-GJ>>>FDELQHW QR.=0, VXEUDFN QR.=0, VORW QR.=19, S RUW QR.=1	65085(Mains Failure Alarm)	HIGH	207819923	02-Jan-2021 10:40:32
SDGDYLBD-DQ0028-X	26270(Inter-System Communication Failure)	HIGH	207824290	02-Jan-2021 11:22:11
NDGDZDWKJDPD-DQ0199-X	21581(Path Fault)	HIGH	207829068	03-Jan-2021 12:22:35
WKXODQD_KRURZSDWKDQD-DQ0017-J>>				

Figure 10.5 - Resolved Alarms

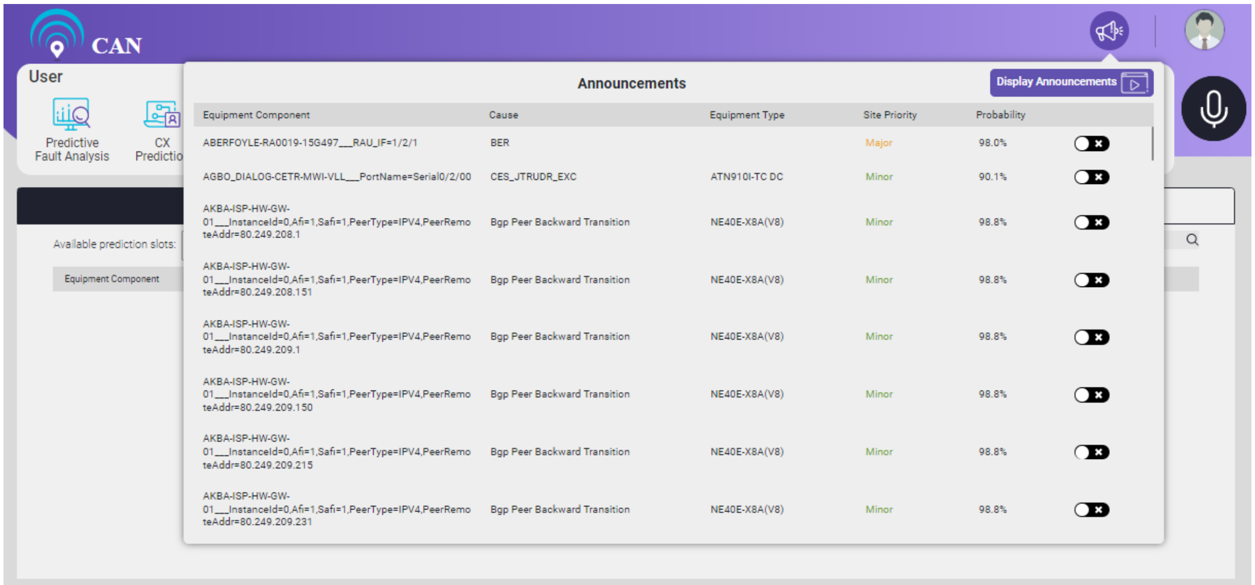
Page Intentionally Left Blank

11. 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.

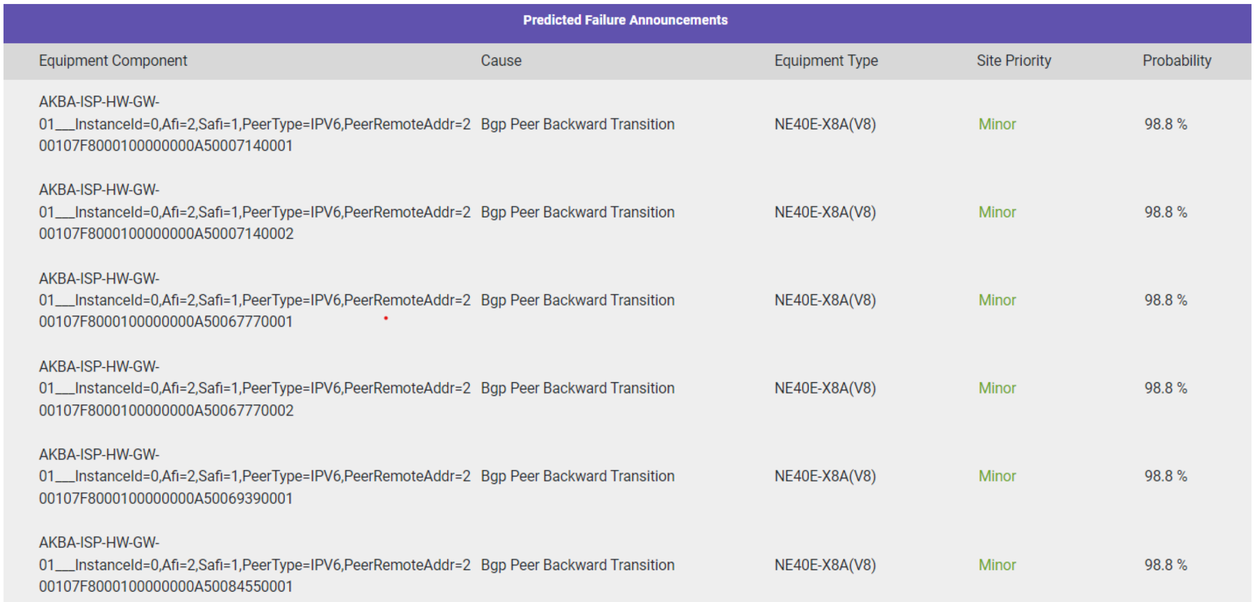


Announcements

Equipment Component	Cause	Equipment Type	Site Priority	Probability	
ABERFOYLE-RA0019-15G497___RAU_IF=1/2/1	BER		Major	98.0%	☒
AGBO_DIALOG-CETR-MWI-VLL___PortName=Serial0/2/00	CES_JTRUDR_EXC	ATN910I-TC DC	Minor	90.1%	☒
AKBA-ISP-HW-GW-01___InstanceId=0,Afi=1,Safi=1,PeerType=IPV4,PeerRemoteAddr=80.249.208.1	Bgp Peer Backward Transition	NE40E-X8A(V8)	Minor	98.8%	☒
AKBA-ISP-HW-GW-01___InstanceId=0,Afi=1,Safi=1,PeerType=IPV4,PeerRemoteAddr=80.249.208.151	Bgp Peer Backward Transition	NE40E-X8A(V8)	Minor	98.8%	☒
AKBA-ISP-HW-GW-01___InstanceId=0,Afi=1,Safi=1,PeerType=IPV4,PeerRemoteAddr=80.249.209.1	Bgp Peer Backward Transition	NE40E-X8A(V8)	Minor	98.8%	☒
AKBA-ISP-HW-GW-01___InstanceId=0,Afi=1,Safi=1,PeerType=IPV4,PeerRemoteAddr=80.249.209.150	Bgp Peer Backward Transition	NE40E-X8A(V8)	Minor	98.8%	☒
AKBA-ISP-HW-GW-01___InstanceId=0,Afi=1,Safi=1,PeerType=IPV4,PeerRemoteAddr=80.249.209.215	Bgp Peer Backward Transition	NE40E-X8A(V8)	Minor	98.8%	☒
AKBA-ISP-HW-GW-01___InstanceId=0,Afi=1,Safi=1,PeerType=IPV4,PeerRemoteAddr=80.249.209.231	Bgp Peer Backward Transition	NE40E-X8A(V8)	Minor	98.8%	☒

Figure 11.1 - Announcement Home Page

The below screen displays the Predicted Failure Announcements.



Predicted Failure Announcements

Equipment Component	Cause	Equipment Type	Site Priority	Probability
AKBA-ISP-HW-GW-01___InstanceId=0,Afi=2,Safi=1,PeerType=IPV6,PeerRemoteAddr=200107F8000100000000A50007140001	Bgp Peer Backward Transition	NE40E-X8A(V8)	Minor	98.8 %
AKBA-ISP-HW-GW-01___InstanceId=0,Afi=2,Safi=1,PeerType=IPV6,PeerRemoteAddr=200107F8000100000000A50007140002	Bgp Peer Backward Transition	NE40E-X8A(V8)	Minor	98.8 %
AKBA-ISP-HW-GW-01___InstanceId=0,Afi=2,Safi=1,PeerType=IPV6,PeerRemoteAddr=200107F8000100000000A50067770001	Bgp Peer Backward Transition	NE40E-X8A(V8)	Minor	98.8 %
AKBA-ISP-HW-GW-01___InstanceId=0,Afi=2,Safi=1,PeerType=IPV6,PeerRemoteAddr=200107F8000100000000A50067770002	Bgp Peer Backward Transition	NE40E-X8A(V8)	Minor	98.8 %
AKBA-ISP-HW-GW-01___InstanceId=0,Afi=2,Safi=1,PeerType=IPV6,PeerRemoteAddr=200107F8000100000000A50069390001	Bgp Peer Backward Transition	NE40E-X8A(V8)	Minor	98.8 %
AKBA-ISP-HW-GW-01___InstanceId=0,Afi=2,Safi=1,PeerType=IPV6,PeerRemoteAddr=200107F8000100000000A50084550001	Bgp Peer Backward Transition	NE40E-X8A(V8)	Minor	98.8 %

Figure 11.2 - Display Announcement Screen

Page Intentionally Left Blank

12. 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:

1. Manage Roles
2. Manage Users
3. View Logs

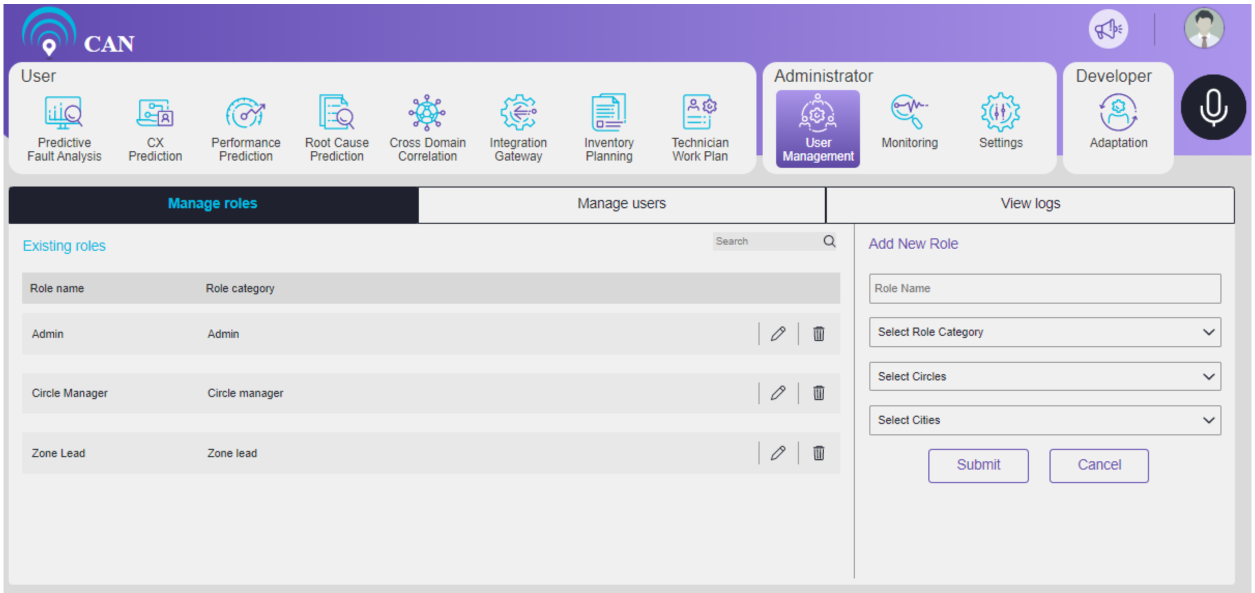
Manage Roles

This tab allows adding, deleting, searching and modifying 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.

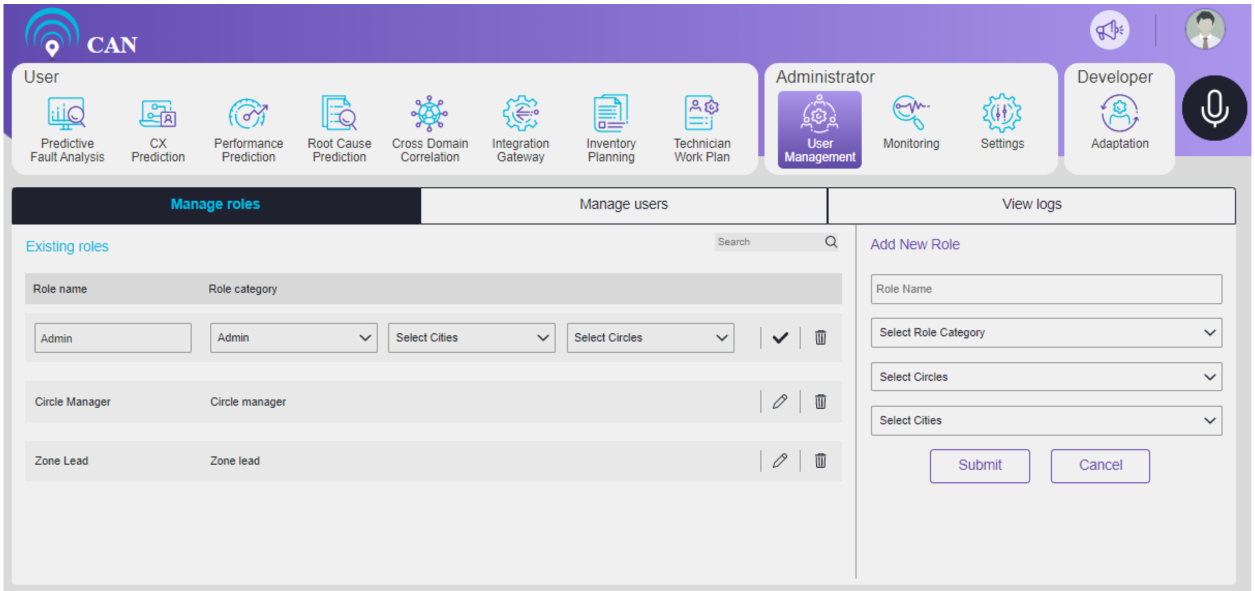


Role name	Role category
Admin	Admin
Circle Manager	Circle manager
Zone Lead	Zone lead

Figure 12.1 - 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 be saved.
4. Click the delete icon 🗑 to delete the Existing Role.



Existing roles

Role name	Role category			
Admin	Admin	Select Cities	Select Circles	✓ 🗑
Circle Manager	Circle manager			✎ 🗑
Zone Lead	Zone lead			✎ 🗑

Add New Role

Role Name

Select Role Category

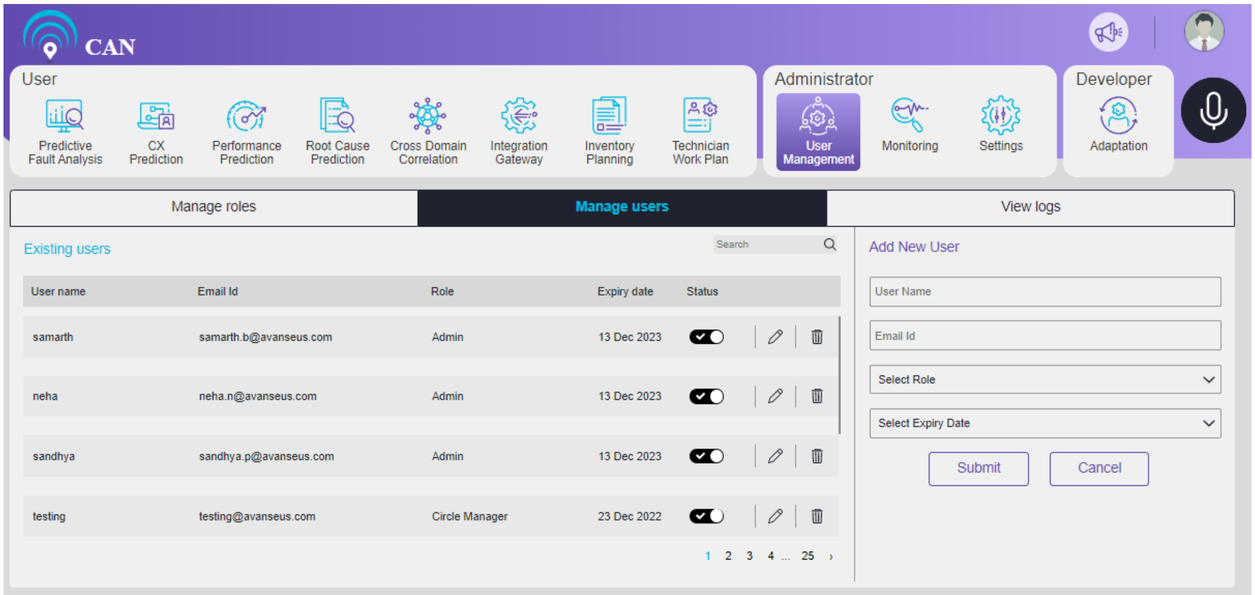
Select Circles

Select Cities

Figure 12.2 - Manage Roles of Existing Roles

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 adding a new user, modifying the existing user details and deleting the existing user.



Existing users

User name	Email Id	Role	Expiry date	Status	
samarth	samarth.b@avanseus.com	Admin	13 Dec 2023	✓	✎ 🗑
neha	neha.n@avanseus.com	Admin	13 Dec 2023	✓	✎ 🗑
sandhya	sandhya.p@avanseus.com	Admin	13 Dec 2023	✓	✎ 🗑
testing	testing@avanseus.com	Circle Manager	23 Dec 2022	✓	✎ 🗑

Add New User

User Name

Email Id

Select Role

Select Expiry Date

Figure 12.3 - Add New Users

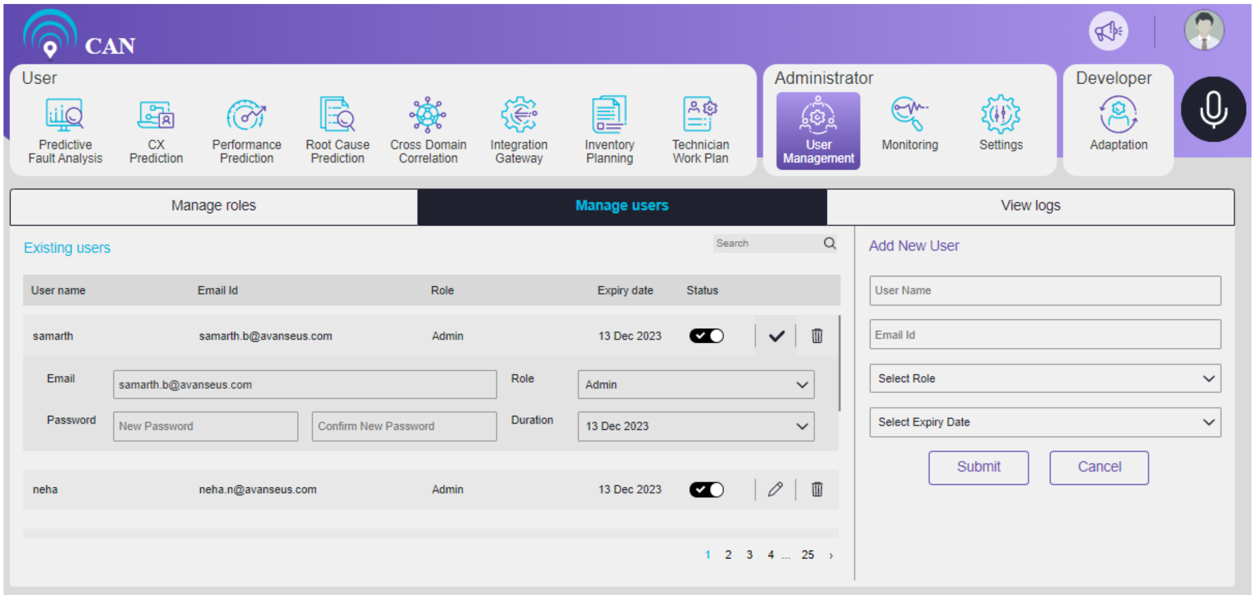
To Add New User

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 be 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.



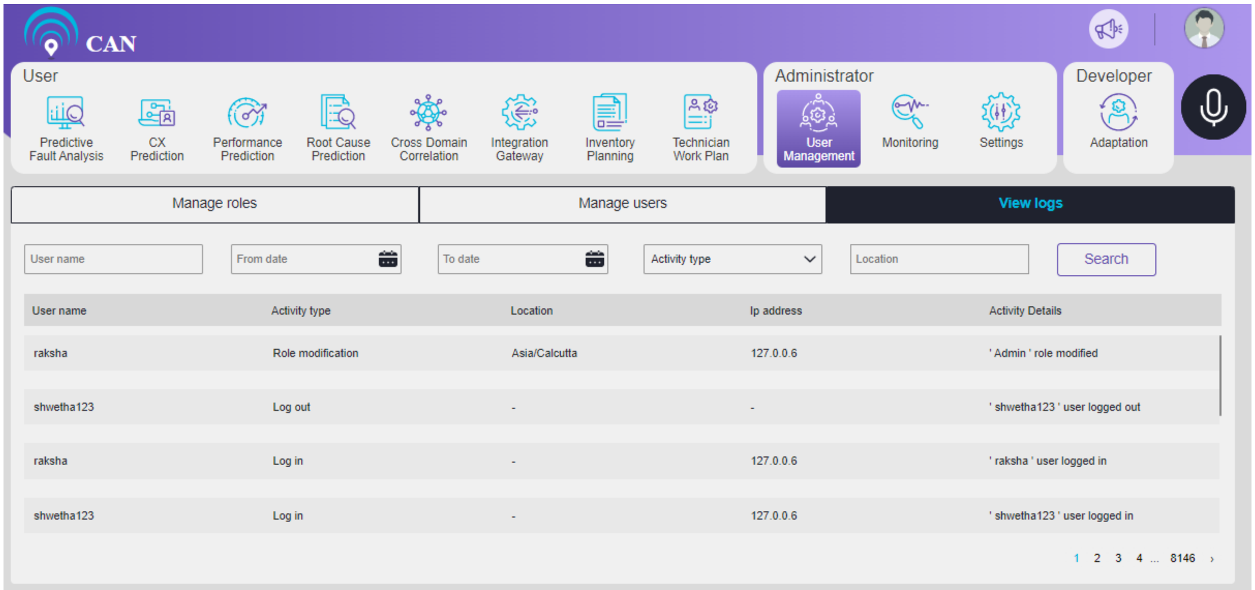
User name	Email Id	Role	Expiry date	Status
samarth	samarth.b@avanseus.com	Admin	13 Dec 2023	✓●
neha	neha.n@avanseus.com	Admin	13 Dec 2023	✓●

Email: samarth.b@avanseus.com
Role: Admin
Password: New Password / Confirm New Password
Duration: 13 Dec 2023

Figure 12.4 - 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.



User name	Activity type	Location	Ip address	Activity Details
raksha	Role modification	Asia/Calcutta	127.0.0.6	' Admin ' role modified
shwetha123	Log out	-	-	' shwetha123 ' user logged out
raksha	Log in	-	127.0.0.6	' raksha ' user logged in
shwetha123	Log in	-	127.0.0.6	' shwetha123 ' user logged in

Figure 12.5 - View Logs

Page Intentionally Left Blank

13. 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

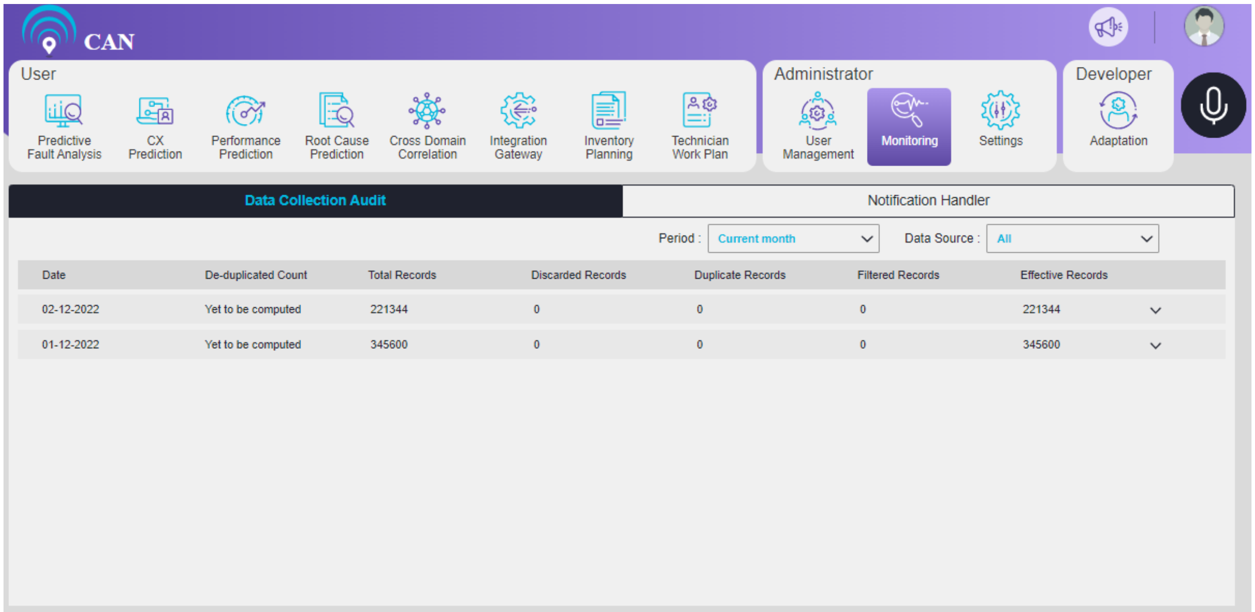
This screen has two filters: Period and Data Source.

There are three Periods available:

1. Current month
2. Current with previous month
3. Current with previous 2 months

The data sources available are:

- All
- Alarms
- Tickets
- Work Order
- Performance Counter
- Customer Experience
- Network Inventory
- Logs
- Others



Period : Current month

Data Source : All

Date	De-duplicated Count	Total Records	Discarded Records	Duplicate Records	Filtered Records	Effective Records
02-12-2022	Yet to be computed	221344	0	0	0	221344
01-12-2022	Yet to be computed	345600	0	0	0	345600

Figure 13.1 - Data Collection Audit Screen with Periods

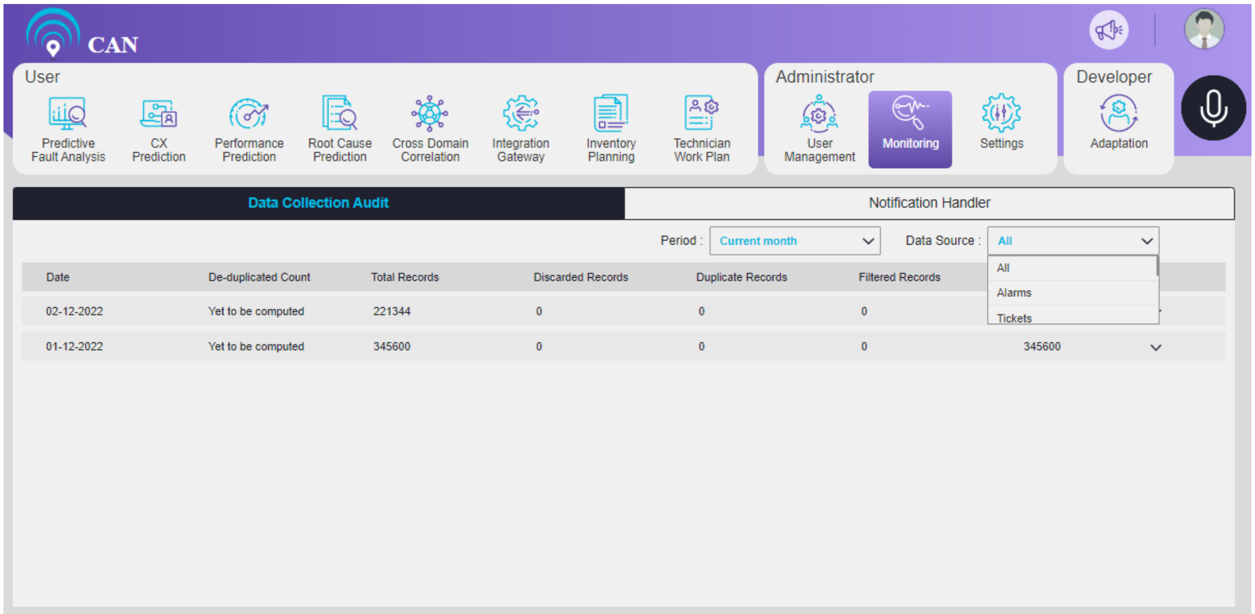
This screen displays the **Date**, **De-Duplicated Count**, **Total Records**, **Discarded Records**, **Duplicate Records**, **Filtered Records** and **Effective Records** on a daily basis (for each period and data source combination).

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**, **Start Time**, **End Time**, **Time Difference** (in HH: MM: SS format), **Total Records, Discarded Records, Duplicate Records, Effective Records, Input Records, Grouped Records, Split Records and Discarded Records Category** 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.

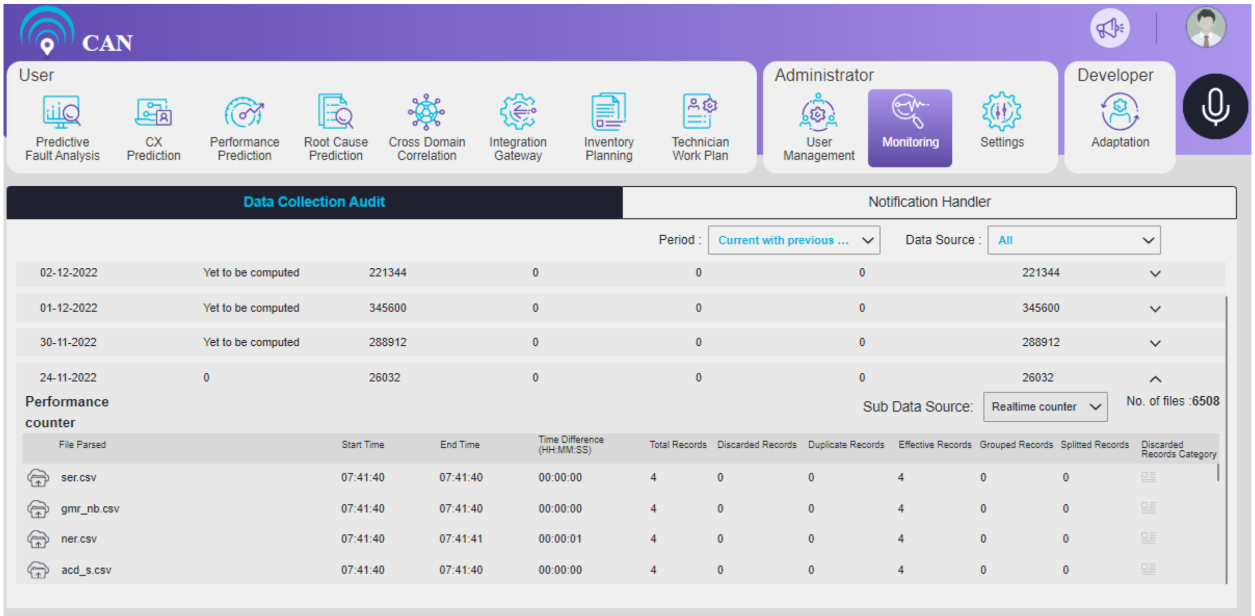


Period : Current month

Data Source : All

Date	De-duplicated Count	Total Records	Discarded Records	Duplicate Records	Filtered Records	
02-12-2022	Yet to be computed	221344	0	0	0	
01-12-2022	Yet to be computed	345600	0	0	0	345600

Figure 13.2 - Data Collection Audit Screen with Multiple Data Sources



Period : Current with previous ... Data Source : All

02-12-2022	Yet to be computed	221344	0	0	0	221344
01-12-2022	Yet to be computed	345600	0	0	0	345600
30-11-2022	Yet to be computed	288912	0	0	0	288912
24-11-2022	0	26032	0	0	0	26032

Performance counter

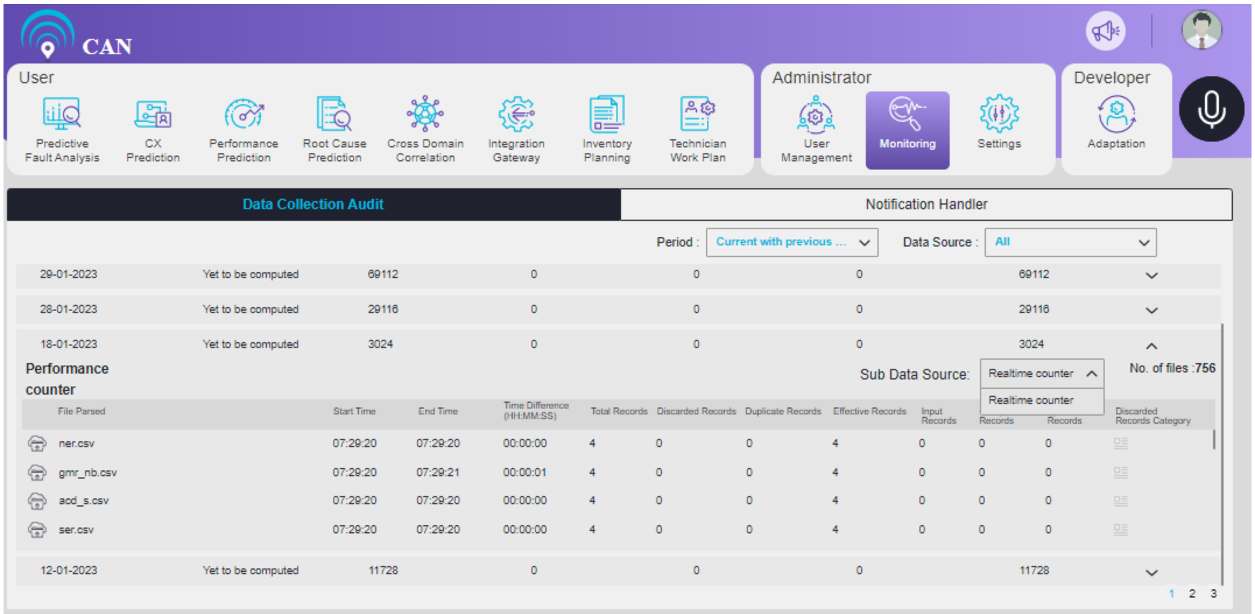
Sub Data Source: Realtime counter

No. of files :6508

File Parsed	Start Time	End Time	Time Difference (HH:MM:SS)	Total Records	Discarded Records	Duplicate Records	Effective Records	Grouped Records	Splitted Records	Discarded Records Category
ser.csv	07:41:40	07:41:40	00:00:00	4	0	0	4	0	0	
gmr_nb.csv	07:41:40	07:41:40	00:00:00	4	0	0	4	0	0	
ner.csv	07:41:40	07:41:41	00:00:01	4	0	0	4	0	0	
acd_s.csv	07:41:40	07:41:40	00:00:00	4	0	0	4	0	0	

Figure 13.3 - Data Collection Audit Screen

User can select the **Sub Data Source** from the dropdown.



Period : Current with previous ... Data Source : All

29-01-2023	Yet to be computed	69112	0	0	0	69112
28-01-2023	Yet to be computed	29116	0	0	0	29116
18-01-2023	Yet to be computed	3024	0	0	0	3024

Performance counter

Sub Data Source: Realtime counter

Realtime counter

No. of files :756

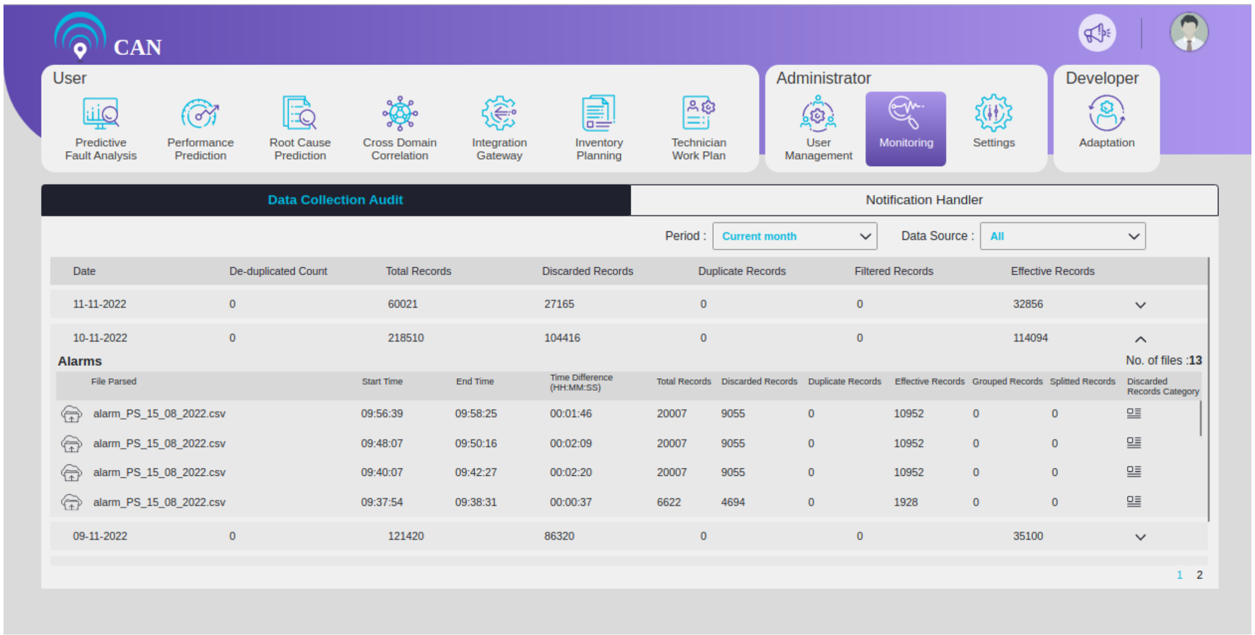
File Parsed	Start Time	End Time	Time Difference (HH:MM:SS)	Total Records	Discarded Records	Duplicate Records	Effective Records	Input Records	Records	Records	Discarded Records Category
ner.csv	07:29:20	07:29:20	00:00:00	4	0	0	4	0	0	0	
gmr_nb.csv	07:29:20	07:29:21	00:00:01	4	0	0	4	0	0	0	
acd_s.csv	07:29:20	07:29:20	00:00:00	4	0	0	4	0	0	0	
ser.csv	07:29:20	07:29:20	00:00:00	4	0	0	4	0	0	0	

12-01-2023	Yet to be computed	11728	0	0	0	11728

1 2 3

Figure 13.4 - Sub Data Source Dropdown

To view the information on **Discarded Records Category**, click the icon ☰. The rejected file is masked in the UI.



Period : Current month

Data Source : All

Date	De-duplicated Count	Total Records	Discarded Records	Duplicate Records	Filtered Records	Effective Records
11-11-2022	0	60021	27165	0	0	32856
10-11-2022	0	218510	104416	0	0	114094

Alarms

No. of files :13

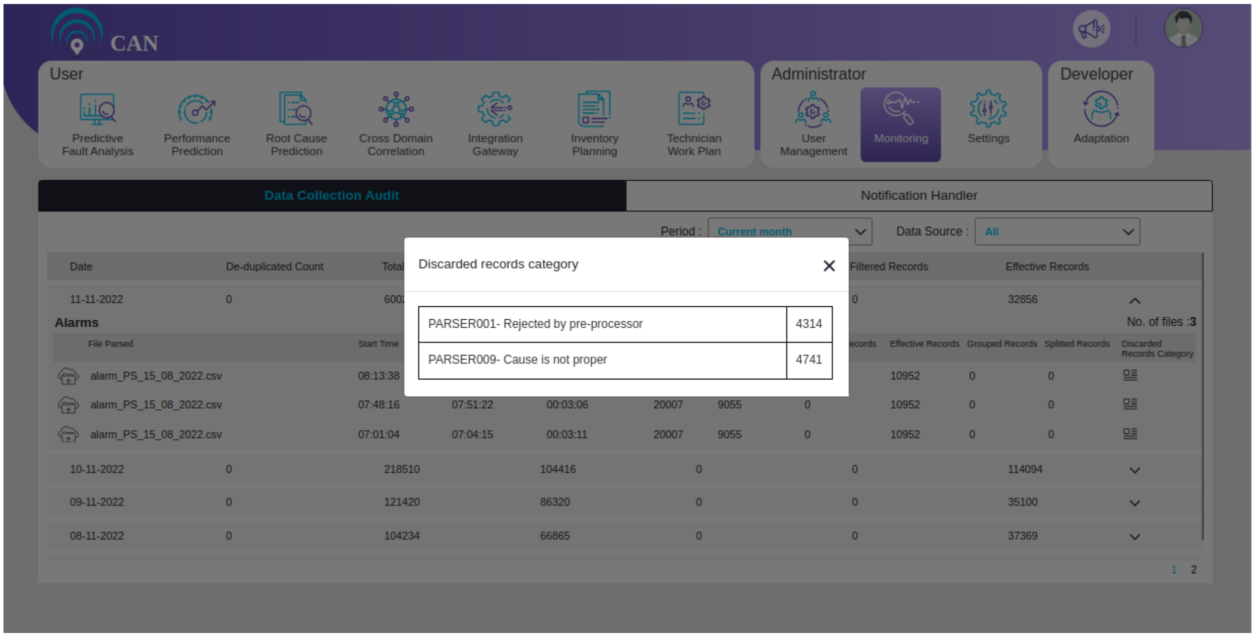
File Parsed	Start Time	End Time	Time Difference (HH:MM:SS)	Total Records	Discarded Records	Duplicate Records	Effective Records	Grouped Records	Splitted Records	Discarded Records Category
alarm_PS_15_08_2022.csv	09:56:39	09:58:25	00:01:46	20007	9055	0	10952	0	0	☰
alarm_PS_15_08_2022.csv	09:48:07	09:50:16	00:02:09	20007	9055	0	10952	0	0	☰
alarm_PS_15_08_2022.csv	09:40:07	09:42:27	00:02:20	20007	9055	0	10952	0	0	☰
alarm_PS_15_08_2022.csv	09:37:54	09:38:31	00:00:37	6622	4694	0	1928	0	0	☰

Date	De-duplicated Count	Total Records	Discarded Records	Duplicate Records	Filtered Records	Effective Records
09-11-2022	0	121420	86320	0	0	35100

1 2

Figure 13.5 - 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.



Period : Current month

Data Source : All

Discarded records category ✕

PARSER001- Rejected by pre-processor	4314
PARSER009- Cause is not proper	4741

Date	De-duplicated Count	Total			Filtered Records	Effective Records
11-11-2022	0	600			0	32856

Alarms

No. of files :3

File Parsed	Start Time					ecords	Effective Records	Grouped Records	Splitted Records	Discarded Records Category
alarm_PS_15_08_2022.csv	08:13:38						10952	0	0	☰
alarm_PS_15_08_2022.csv	07:48:16	07:51:22	00:03:06	20007	9055	0	10952	0	0	☰
alarm_PS_15_08_2022.csv	07:01:04	07:04:15	00:03:11	20007	9055	0	10952	0	0	☰

10-11-2022	0	218510	104416	0	0	114094
09-11-2022	0	121420	86320	0	0	35100
08-11-2022	0	104234	66865	0	0	37369

1 2

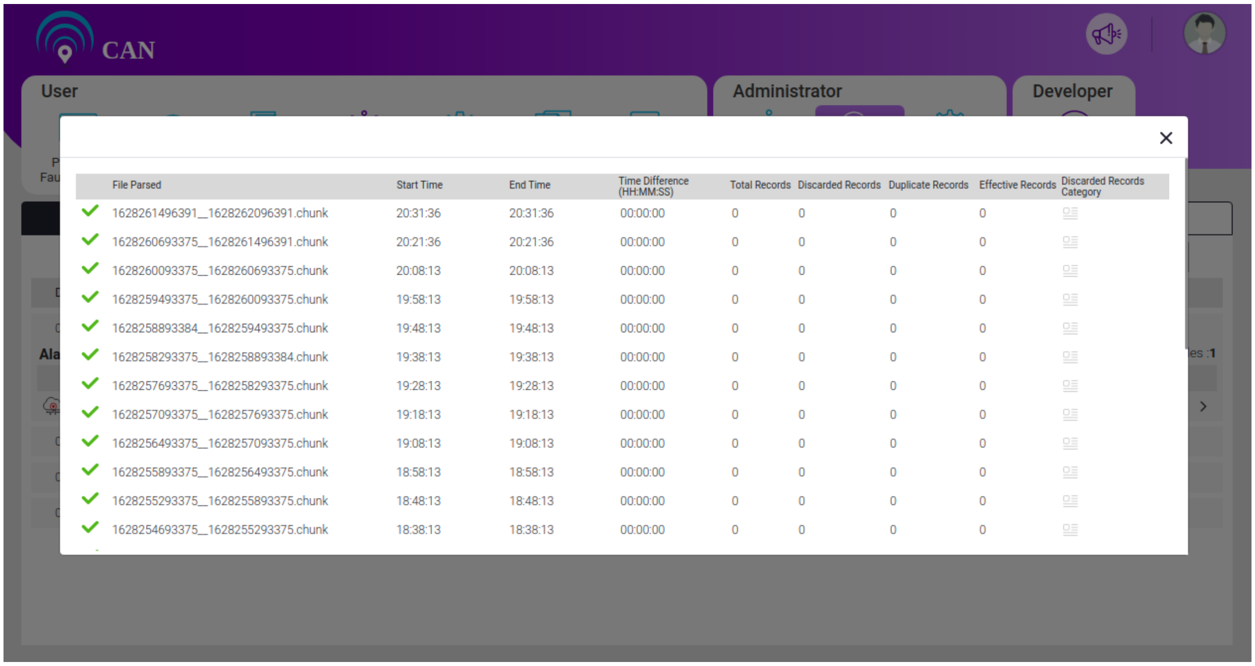
Figure 13.6 - Discarded Record Category

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:

1. Live Streaming Data - It represents the data that is live streaming. This icon ☁ is used to show live streaming data.
2. 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. 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.



	File Parsed	Start Time	End Time	Time Difference (HH:MM:SS)	Total Records	Discarded Records	Duplicate Records	Effective Records	Discarded Records Category
✓	1628261496391__1628262096391.chunk	20:31:36	20:31:36	00:00:00	0	0	0	0	☰
✓	1628260693375__1628261496391.chunk	20:21:36	20:21:36	00:00:00	0	0	0	0	☰
✓	1628260093375__1628260693375.chunk	20:08:13	20:08:13	00:00:00	0	0	0	0	☰
✓	1628259493375__1628260093375.chunk	19:58:13	19:58:13	00:00:00	0	0	0	0	☰
✓	1628258893384__1628259493375.chunk	19:48:13	19:48:13	00:00:00	0	0	0	0	☰
✓	1628258293375__1628258893384.chunk	19:38:13	19:38:13	00:00:00	0	0	0	0	☰
✓	1628257693375__1628258293375.chunk	19:28:13	19:28:13	00:00:00	0	0	0	0	☰
✓	1628257093375__1628257693375.chunk	19:18:13	19:18:13	00:00:00	0	0	0	0	☰
✓	1628256493375__1628257093375.chunk	19:08:13	19:08:13	00:00:00	0	0	0	0	☰
✓	1628255893375__1628256493375.chunk	18:58:13	18:58:13	00:00:00	0	0	0	0	☰
✓	1628255293375__1628255893375.chunk	18:48:13	18:48:13	00:00:00	0	0	0	0	☰
✓	1628254693375__1628255293375.chunk	18:38:13	18:38:13	00:00:00	0	0	0	0	☰

Figure 13.7 - 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.

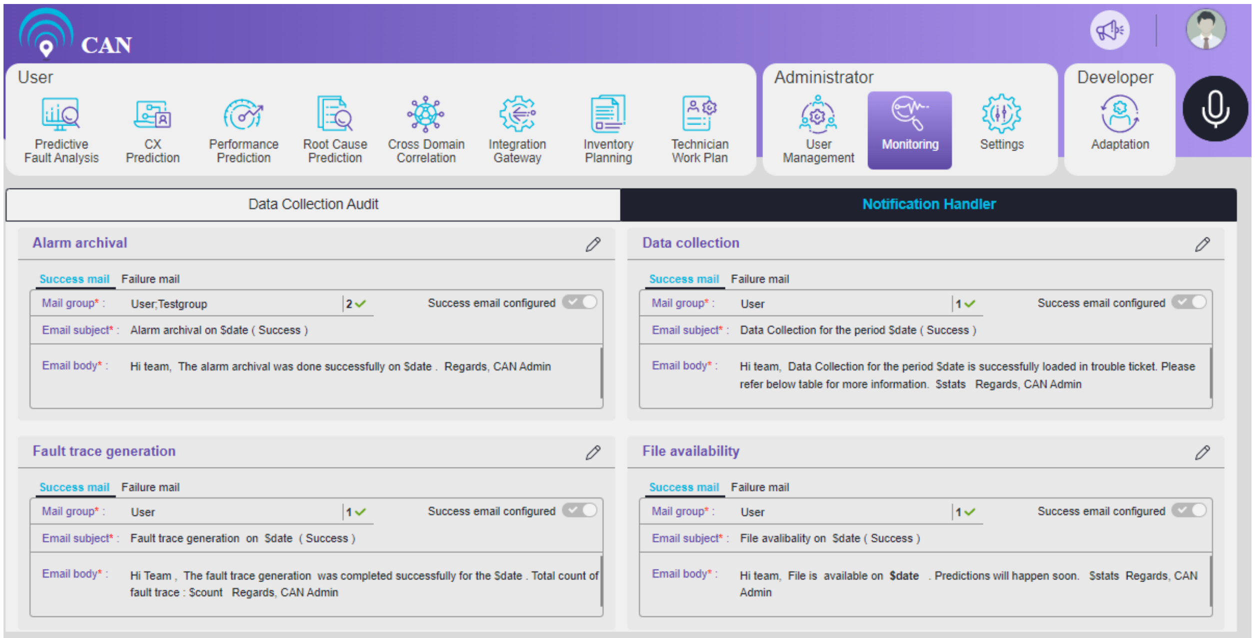
If enabled, then red star mark * will appear for the mandatory fields of the corresponding section and if disabled, then star mark will not appear.

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.



Alarm archival

Success mail Failure mail

Mail group* : User;Testgroup 2 ✓ Success email configured

Email subject* : Alarm archival on $date (Success)

Email body* : Hi team, The alarm archival was done successfully on $date . Regards, CAN Admin

Data collection

Success mail Failure mail

Mail group* : User 1 ✓ Success email configured

Email subject* : Data Collection for the period $date (Success)

Email body* : Hi team, Data Collection for the period $date is successfully loaded in trouble ticket. Please refer below table for more information. $stats Regards, CAN Admin

Fault trace generation

Success mail Failure mail

Mail group* : User 1 ✓ Success email configured

Email subject* : Fault trace generation on $date (Success)

Email body* : Hi Team , The fault trace generation was completed successfully for the $date . Total count of fault trace : $count Regards, CAN Admin

File availability

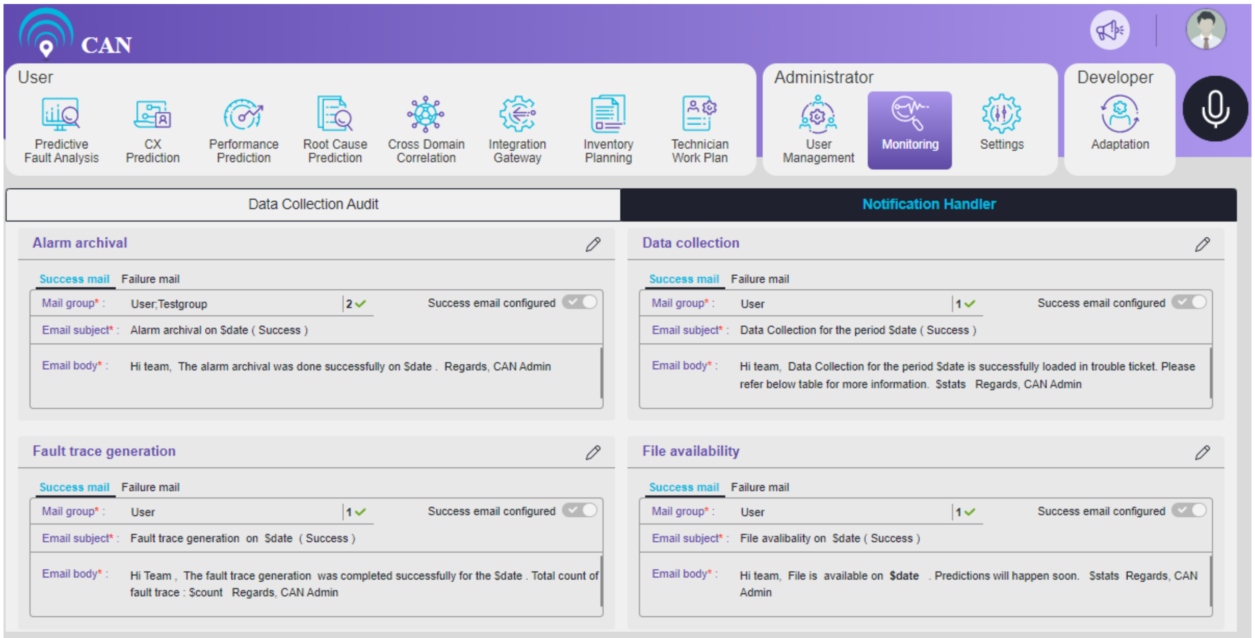
Success mail Failure mail

Mail group* : User 1 ✓ Success email configured

Email subject* : File avalibality on $date (Success)

Email body* : Hi team, File is available on **$date** . Predictions will happen soon. $stats Regards, CAN Admin

Figure 13.8 - Notification Handler



Alarm archival

Success mail Failure mail

Mail group* : User;Testgroup 2 ✓ Success email configured

Email subject* : Alarm archival on $date (Success)

Email body* : Hi team, The alarm archival was done successfully on $date . Regards, CAN Admin

Data collection

Success mail Failure mail

Mail group* : User 1 ✓ Success email configured

Email subject* : Data Collection for the period $date (Success)

Email body* : Hi team, Data Collection for the period $date is successfully loaded in trouble ticket. Please refer below table for more information. $stats Regards, CAN Admin

Fault trace generation

Success mail Failure mail

Mail group* : User 1 ✓ Success email configured

Email subject* : Fault trace generation on $date (Success)

Email body* : Hi Team , The fault trace generation was completed successfully for the $date . Total count of fault trace : $count Regards, CAN Admin

File availability

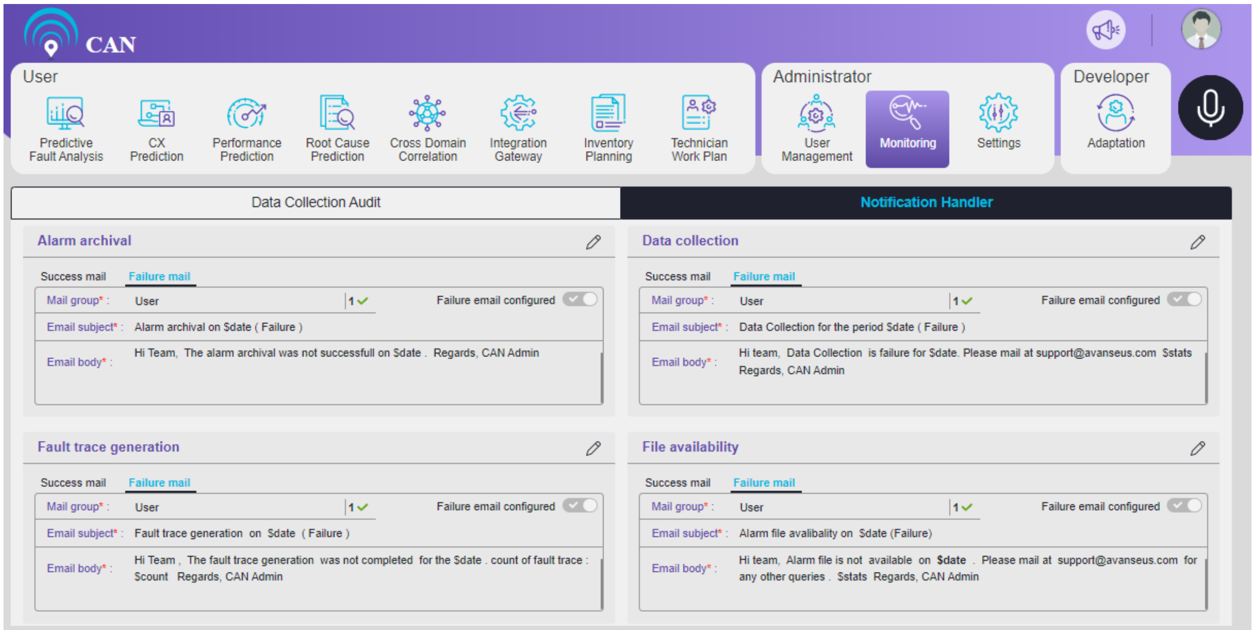
Success mail Failure mail

Mail group* : User 1 ✓ Success email configured

Email subject* : File avalibality on $date (Success)

Email body* : Hi team, File is available on **$date** . Predictions will happen soon. $stats Regards, CAN Admin

Figure 13.9 - Success Mail Template



Alarm archival

Success mail | Failure mail

Mail group* : User | 1 ✓ — Failure email configured

Email subject* : Alarm archival on $date (Failure)

Email body* : Hi Team, The alarm archival was not successfull on $date . Regards, CAN Admin

Data collection

Success mail | Failure mail

Mail group* : User | 1 ✓ — Failure email configured

Email subject* : Data Collection for the period $date (Failure)

Email body* : Hi team, Data Collection is failure for $date. Please mail at support@avanseus.com $stats Regards, CAN Admin

Fault trace generation

Success mail | Failure mail

Mail group* : User | 1 ✓ — Failure email configured

Email subject* : Fault trace generation on $date (Failure)

Email body* : Hi Team , The fault trace generation was not completed for the $date . count of fault trace : $count Regards, CAN Admin

File availability

Success mail | Failure mail

Mail group* : User | 1 ✓ — Failure email configured

Email subject* : Alarm file avalibality on $date (Failure)

Email body* : Hi team, Alarm file is not available on $date . Please mail at support@avanseus.com for any other queries . $stats Regards, CAN Admin

Figure 13.10 - Failure Mail Template

Page Intentionally Left Blank

14. SETTINGS

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

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

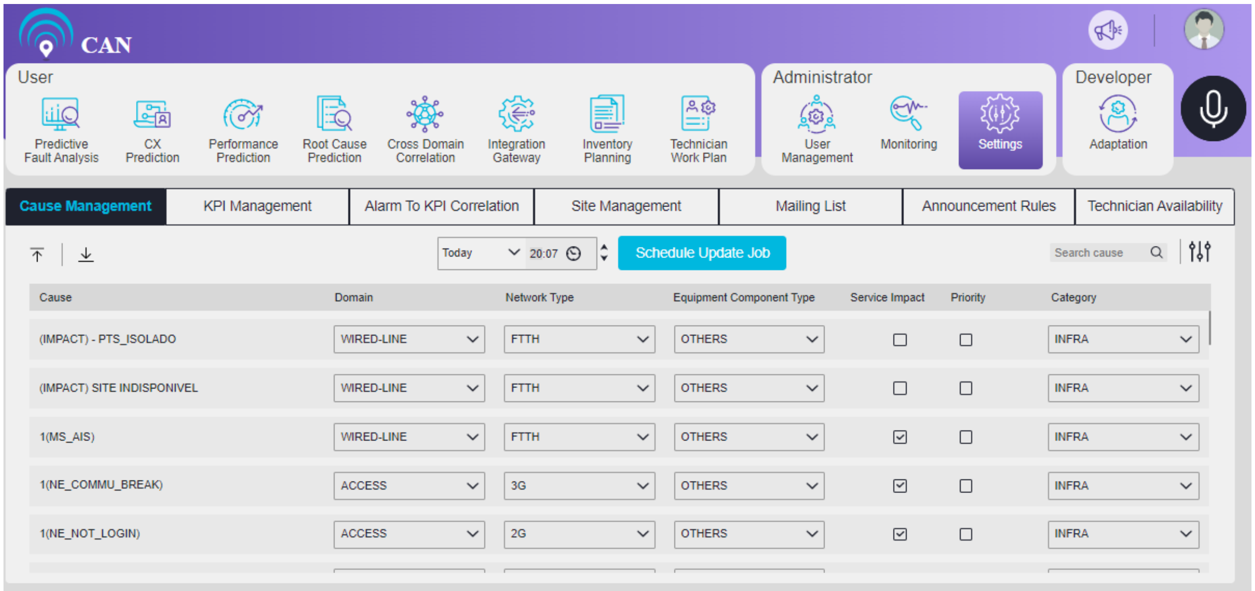
Settings are classified under seven tabs:

1. **Cause Management** - Manage the Causes relevant Configurations by giving them an alias by setting in Domain field, Network Type, Categorize 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.
2. **KPI Management** – System identifies the network KPIs from the input data and monitors for threshold breaches.
3. **Alarm to KPI Correlation** – It is a function for relating KPI and alarms as KPI is related to the performance counter configuration. It is used for performance management of KPI.
4. **Site Management** - This screen is used to view and update the site priority of the corresponding office code.
5. **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.
6. **Announcement 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.
7. **Technician Availability** - This helps to record the technician availability in real time for work assignment.

Cause Management

Cause Management 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.



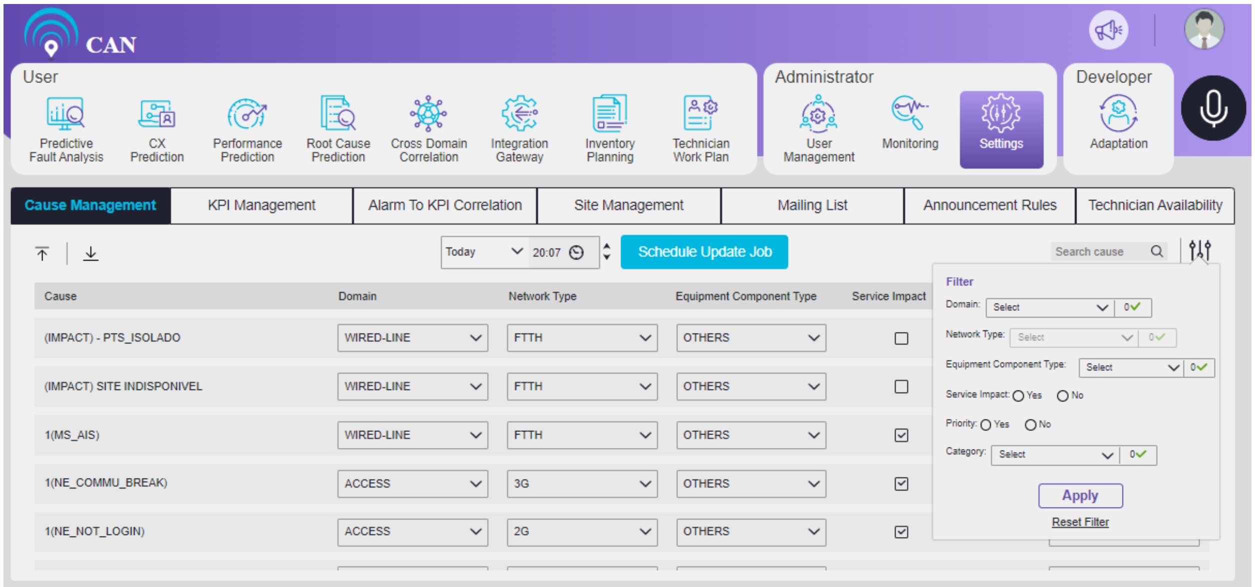
Cause	Domain	Network Type	Equipment Component Type	Service Impact	Priority	Category
(IMPACT) - PTS_ISOLADO	WIRED-LINE	FTTH	OTHERS	☐	☐	INFRA
(IMPACT) SITE INDISPONIVEL	WIRED-LINE	FTTH	OTHERS	☐	☐	INFRA
1(MS_AIS)	WIRED-LINE	FTTH	OTHERS	☑	☐	INFRA
1(NE_COMMU_BREAK)	ACCESS	3G	OTHERS	☑	☐	INFRA
1(NE_NOT_LOGIN)	ACCESS	2G	OTHERS	☑	☐	INFRA

Figure 14.1 - Cause Management

To Filter the Cause Details

1. Select the **Domain** from the drop down.
2. Display of **Network Type** as per the selected domain. 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.



Cause	Domain	Network Type	Equipment Component Type	Service Impact
(IMPACT) - PTS_ISOLADO	WIRED-LINE	FTTH	OTHERS	□
(IMPACT) SITE INDISPONIVEL	WIRED-LINE	FTTH	OTHERS	□
1(MS_AIS)	WIRED-LINE	FTTH	OTHERS	☑
1(NE_COMMU_BREAK)	ACCESS	3G	OTHERS	☑
1(NE_NOT_LOGIN)	ACCESS	2G	OTHERS	☑

Filter

Domain: Select 0✓

Network Type: Select 0✓

Equipment Component Type: Select 0✓

Service Impact: ○ Yes ○ No

Priority: ○ Yes ○ No

Category: Select 0✓

Apply

Reset Filter

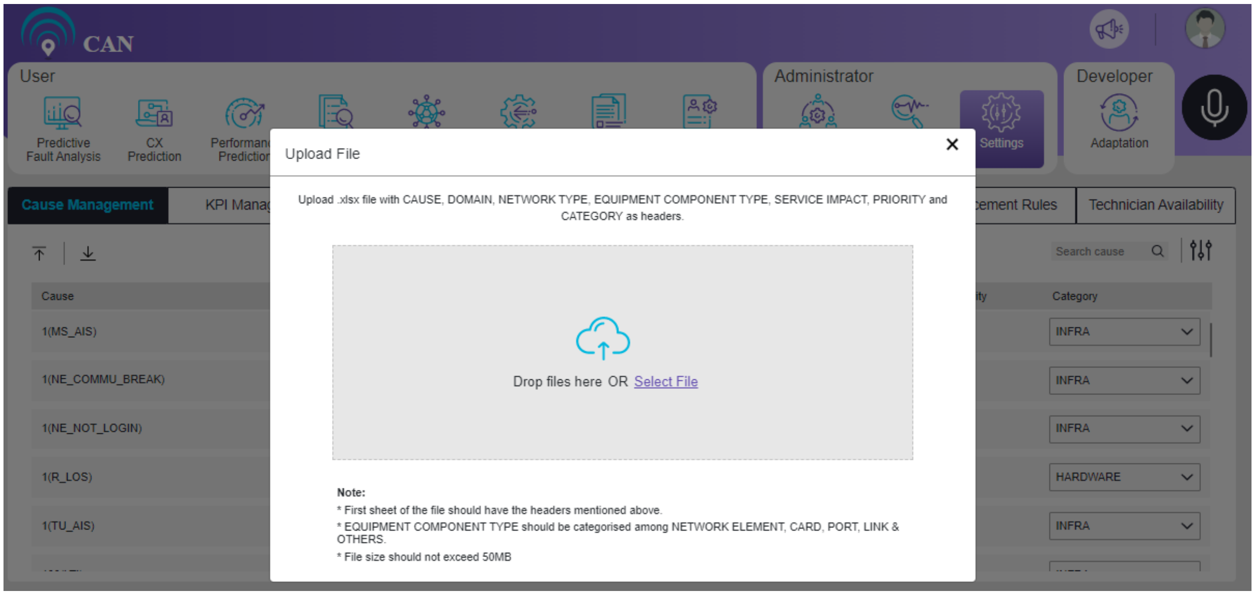
Figure 14.2 - Cause Management Filter

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, EQUIPMENT COMPONENT TYPE, SERVICE IMPACT, PRIORITY and CATEGORY.

Note:

- First sheet of the file should have the headers mentioned above.
- EQUIPMENT COMPONENT TYPE should be categorized among NETWORK ELEMENT, CARD, PORT, LINK & OTHERS.
- File size should not exceed 50MB.



Upload File ✕

Upload .xlsx file with CAUSE, DOMAIN, NETWORK TYPE, EQUIPMENT COMPONENT TYPE, SERVICE IMPACT, PRIORITY and CATEGORY as headers.

Drop files here OR Select File

Note:

* First sheet of the file should have the headers mentioned above.

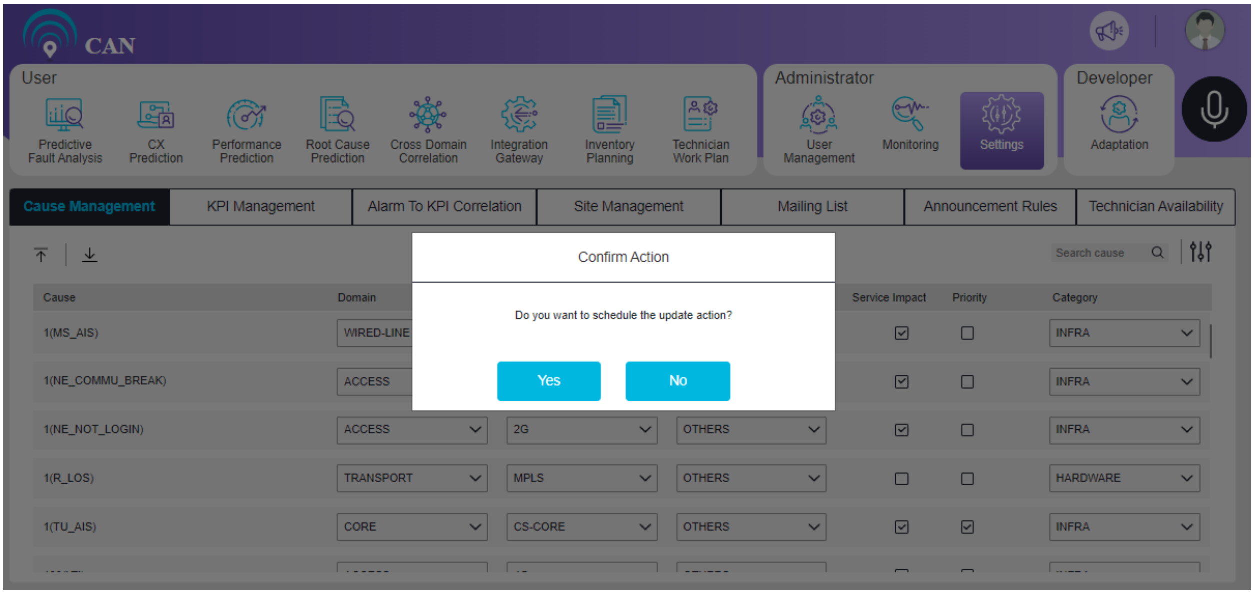
* EQUIPMENT COMPONENT TYPE should be categorised among NETWORK ELEMENT, CARD, PORT, LINK & OTHERS.

* File size should not exceed 50MB

Figure 14.3 - Cause Management Upload File

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.



Confirm Action

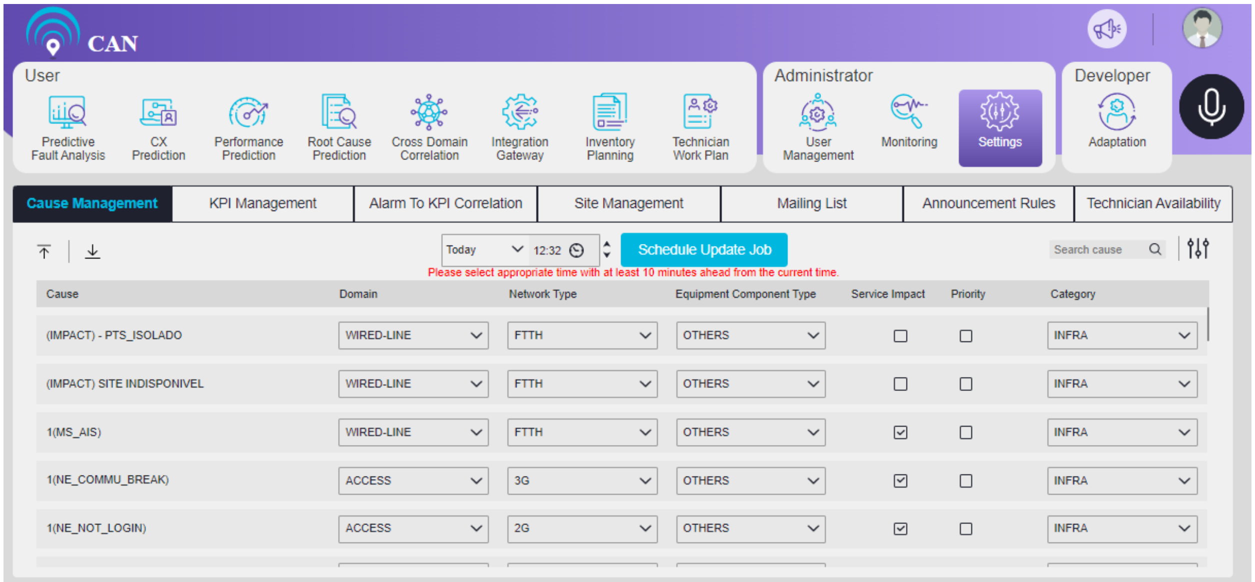
Do you want to schedule the update action?

Yes No

Cause	Domain			Service Impact	Priority	Category
1(MS_AIS)	WIRED-LINE			☑	☐	INFRA
1(NE_COMMU_BREAK)	ACCESS			☑	☐	INFRA
1(NE_NOT_LOGIN)	ACCESS	2G	OTHERS	☑	☐	INFRA
1(R_LOS)	TRANSPORT	MPLS	OTHERS	☐	☐	HARDWARE
1(TU_AIS)	CORE	CS-CORE	OTHERS	☑	☑	INFRA

Figure 14.4 - 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.



Today 12:32 Schedule Update Job

Please select appropriate time with at least 10 minutes ahead from the current time.

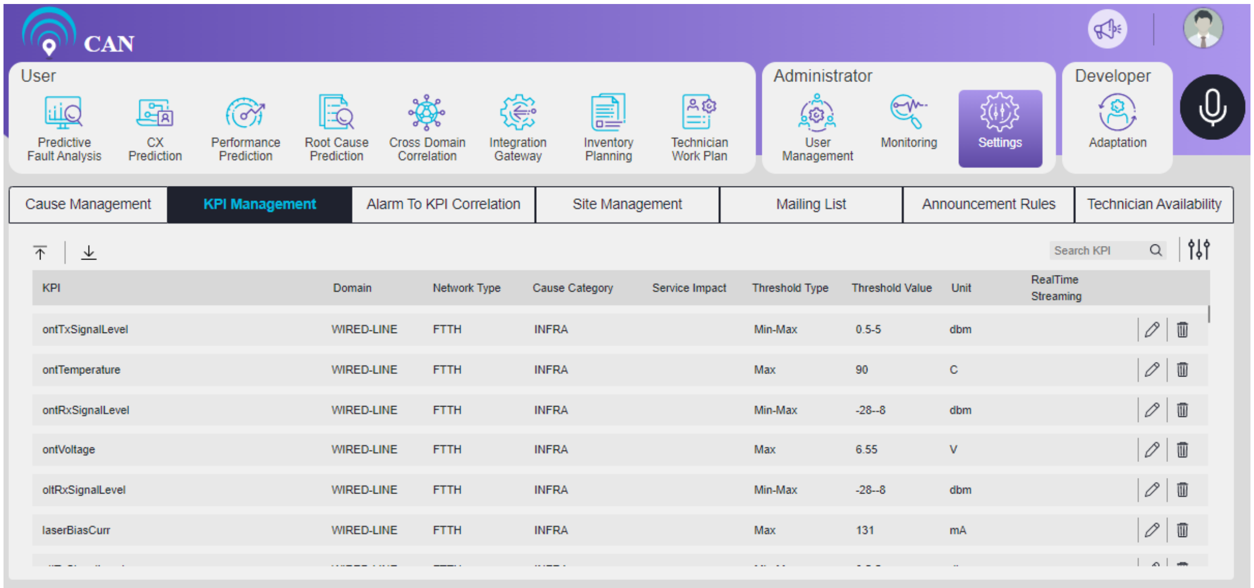
Cause	Domain	Network Type	Equipment Component Type	Service Impact	Priority	Category
(IMPACT) - PTS_ISOLADO	WIRED-LINE	FTTH	OTHERS	☐	☐	INFRA
(IMPACT) SITE INDISPONIVEL	WIRED-LINE	FTTH	OTHERS	☐	☐	INFRA
1(MS_AIS)	WIRED-LINE	FTTH	OTHERS	☑	☐	INFRA
1(NE_COMMU_BREAK)	ACCESS	3G	OTHERS	☑	☐	INFRA
1(NE_NOT_LOGIN)	ACCESS	2G	OTHERS	☑	☐	INFRA

Figure 14.5 - Schedule Update Job

KPI Management

The **KPI Management** screen supports performance KPI monitoring of the network where the KPI threshold breaches are identified by the system. It provides comprehensive support to configure the domain, network type, cause category, service impact, threshold type and threshold unit.

The network KPIs are identified by the system from the input data and the other relevant attributes. Attributes are made editable to ensure that relevant inputs are fed to the system in the most accurate way for processing. User will have options to set these values individually through edit option or to bulk upload the same as file for system to process.

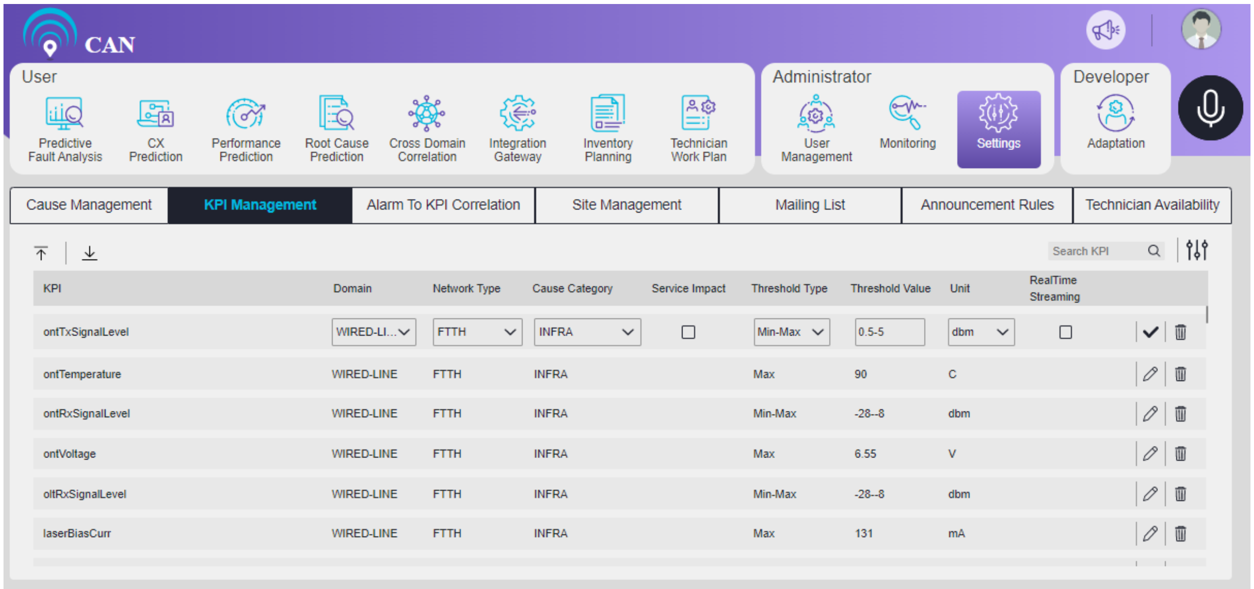


KPI	Domain	Network Type	Cause Category	Service Impact	Threshold Type	Threshold Value	Unit	RealTime Streaming
ontTxSignalLevel	WIRED-LINE	FTTH	INFRA		Min-Max	0.5-5	dbm	
ontTemperature	WIRED-LINE	FTTH	INFRA		Max	90	C	
ontRxSignalLevel	WIRED-LINE	FTTH	INFRA		Min-Max	-28--8	dbm	
ontVoltage	WIRED-LINE	FTTH	INFRA		Max	6.55	V	
oltRxSignalLevel	WIRED-LINE	FTTH	INFRA		Min-Max	-28--8	dbm	
laserBiasCurr	WIRED-LINE	FTTH	INFRA		Max	131	mA	

Figure 14.6 - KPI Management Screen

To Edit the Existing Configuration

1. Under the existing configuration section, click the edit icon ✎.
2. Select Domain, Network Type, Cause Category, Threshold Type and Unit from the drop down.
3. Enter relevant **Threshold Value**.
4. Check or uncheck Service Impact and RealTime Streaming.
5. Click the save icon ✓ to save the changes.
6. Click the delete icon 🗑 to delete the existing KPI.



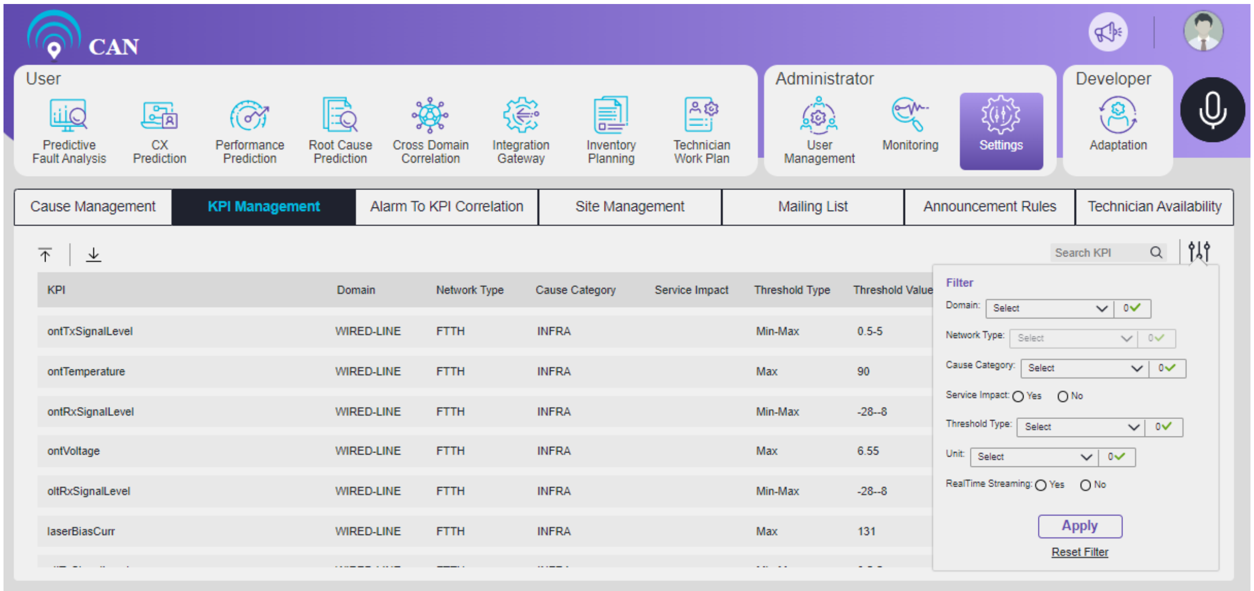
KPI	Domain	Network Type	Cause Category	Service Impact	Threshold Type	Threshold Value	Unit	RealTime Streaming	
ontTxSignalLevel	WIRED-LI...	FTTH	INFRA	□	Min-Max	0.5-5	dbm	□	✓ 🗑
ontTemperature	WIRED-LINE	FTTH	INFRA		Max	90	C		✎ 🗑
ontRxSignalLevel	WIRED-LINE	FTTH	INFRA		Min-Max	-28--8	dbm		✎ 🗑
ontVoltage	WIRED-LINE	FTTH	INFRA		Max	6.55	V		✎ 🗑
oltRxSignalLevel	WIRED-LINE	FTTH	INFRA		Min-Max	-28--8	dbm		✎ 🗑
laserBiasCurr	WIRED-LINE	FTTH	INFRA		Max	131	mA		✎ 🗑

Figure 14.7 - KPI Management Edit Screen

To Filter the KPI Details

1. Select the **Domain** from the drop down.
2. Display of **Network Type** as per the selected domain. Select the applicable **Network Type** from the drop down.
3. Check the **Service Impact** radio button (Yes or No).
4. Select the **Cause Category** from the drop down.
5. Select **Threshold Type** and **Unit** from the drop down.
6. Check the **RealTime Streaming** radio button (Yes or No).
7. Click the **Apply** button.
8. 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.



KPI	Domain	Network Type	Cause Category	Service Impact	Threshold Type	Threshold Value
ontTxSignalLevel	WIRED-LINE	FTTH	INFRA		Min-Max	0.5-5
ontTemperature	WIRED-LINE	FTTH	INFRA		Max	90
ontRxSignalLevel	WIRED-LINE	FTTH	INFRA		Min-Max	-28--8
ontVoltage	WIRED-LINE	FTTH	INFRA		Max	6.55
oltRxSignalLevel	WIRED-LINE	FTTH	INFRA		Min-Max	-28--8
laserBiasCurr	WIRED-LINE	FTTH	INFRA		Max	131

Filter

Domain: Select 0✓

Network Type: Select 0✓

Cause Category: Select 0✓

Service Impact: ○ Yes ○ No

Threshold Type: Select 0✓

Unit: Select 0✓

RealTime Streaming: ○ Yes ○ No

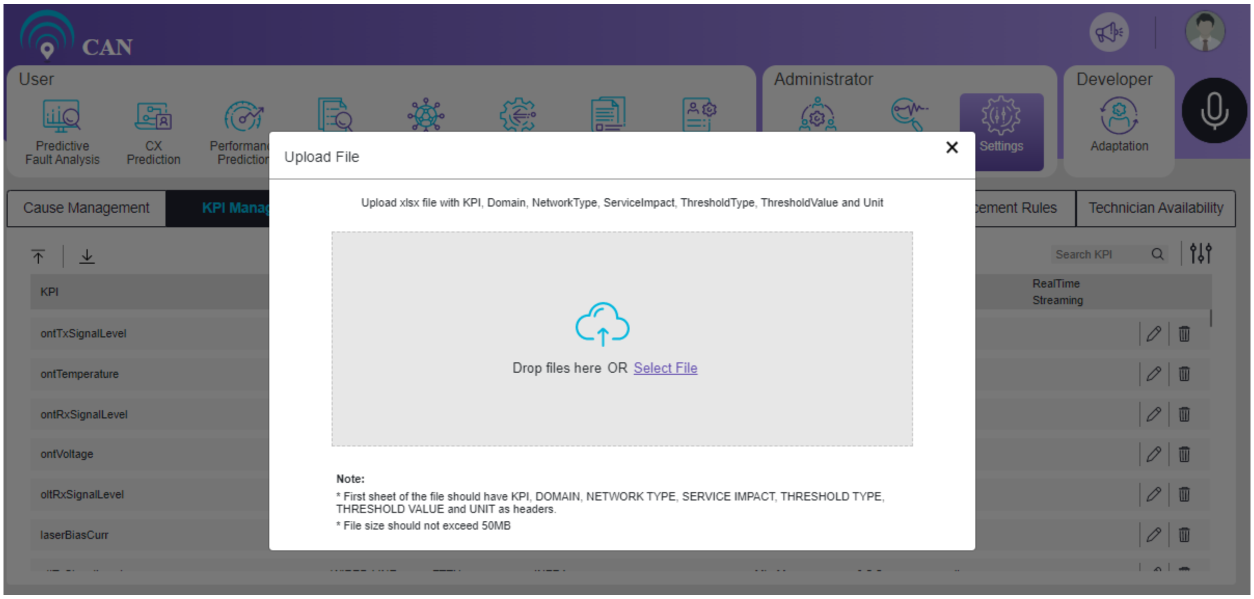
Figure 14.8 - KPI Management Filter

User can download ⤓ the pre-configured KPI details for KPI 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 KPI, Domain, Network Type, Service Impact, Threshold Type, Threshold Value and Unit.

Note:

- First sheet of the file should have KPI, DOMAIN, NETWORK TYPE, SERVICE IMPACT, THRESHOLD TYPE, THRESHOLD VALUE and UNIT as headers.
- File size should not exceed 50MB.



Upload File ×

Upload xlsx file with KPI, Domain, NetworkType, ServiceImpact, ThresholdType, ThresholdValue and Unit

Drop files here OR Select File

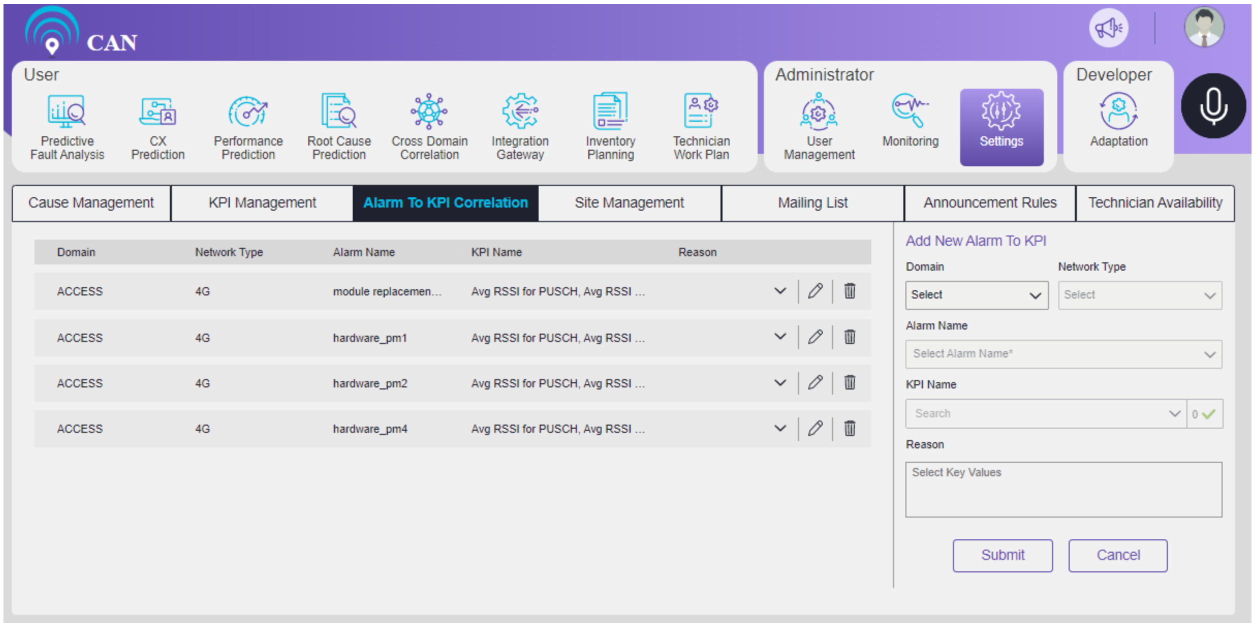
Note:
* First sheet of the file should have KPI, DOMAIN, NETWORK TYPE, SERVICE IMPACT, THRESHOLD TYPE, THRESHOLD VALUE and UNIT as headers.
* File size should not exceed 50MB

Figure 14.9 - KPI Management Upload File

Alarm to KPI Correlation

This is Alarm to KPI Correlation configuration screen. It is a function for relating KPI and alarms as KPI is related to the performance counter configuration.

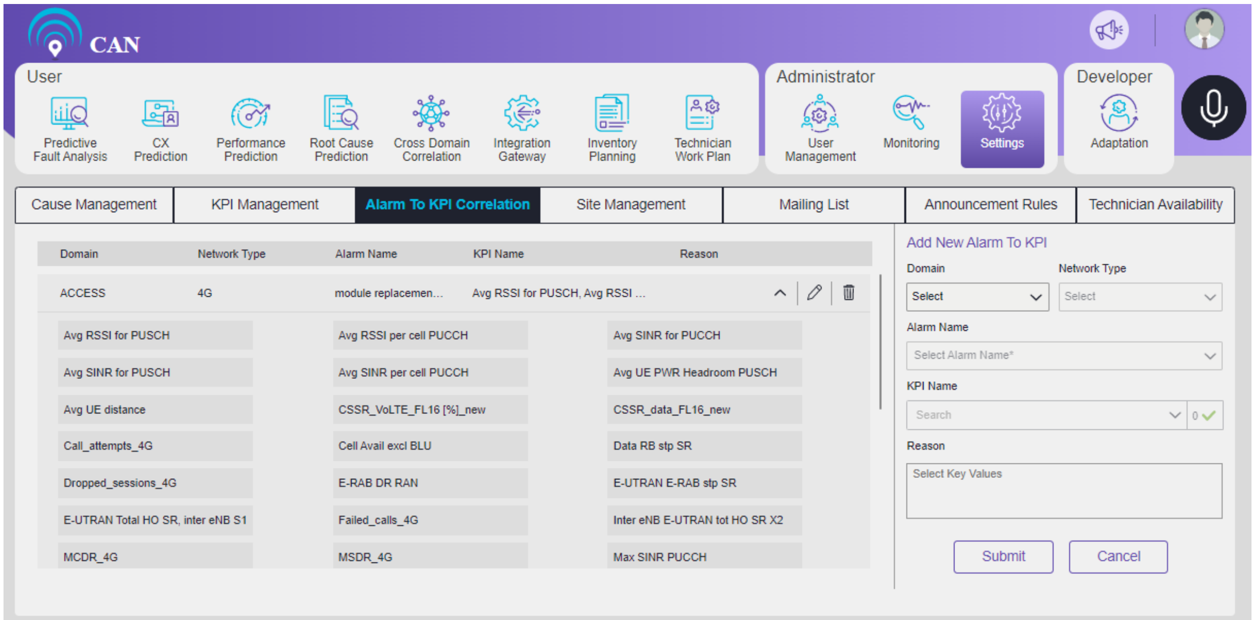
In this screen, user can view the KPIs supported for a particular alarm. Due to redundancy and tracking issue, an alarm can be selected only once. Although, KPI selection for any particular alarm can be one, many or all. Reason is listed for each KPI. KPIs and reasons can be added/deleted at any point of time.



Domain	Network Type	Alarm Name	KPI Name	Reason
ACCESS	4G	module replacemen...	Avg RSSI for PUSCH, Avg RSSI ...	
ACCESS	4G	hardware_pm1	Avg RSSI for PUSCH, Avg RSSI ...	
ACCESS	4G	hardware_pm2	Avg RSSI for PUSCH, Avg RSSI ...	
ACCESS	4G	hardware_pm4	Avg RSSI for PUSCH, Avg RSSI ...	

Figure 14.10 - Alarm to KPI Correlation Screen

Click ⌄ to see Alarm to KPI Correlation details.



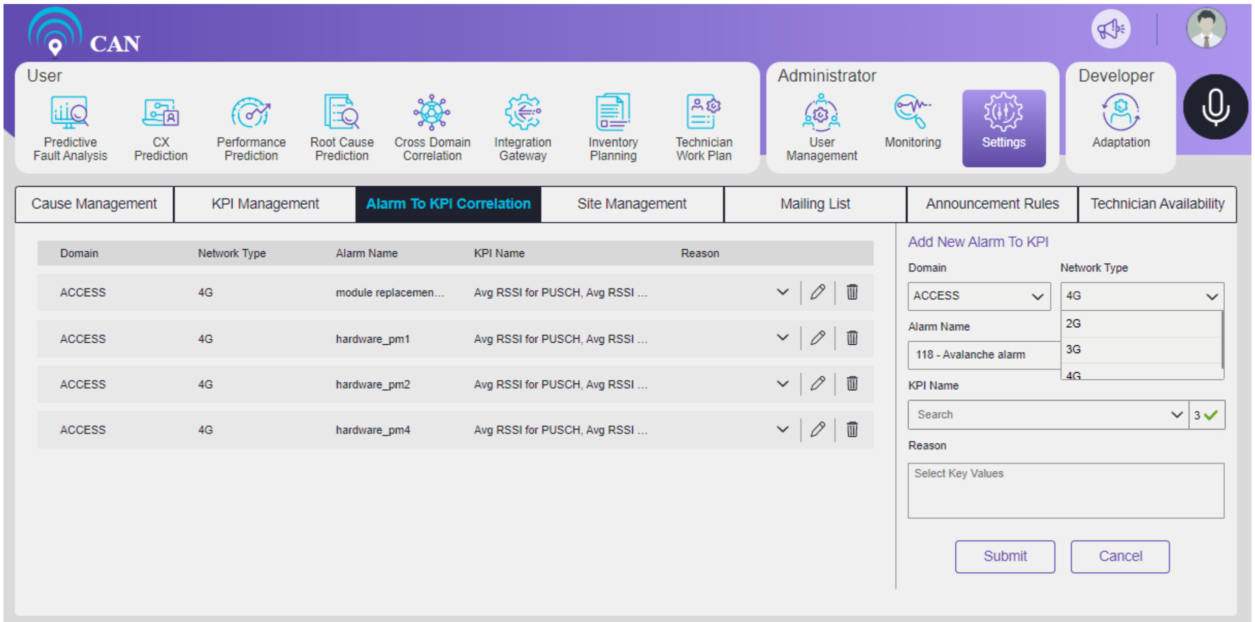
Domain	Network Type	Alarm Name	KPI Name	Reason
ACCESS	4G	module replacemen...	Avg RSSI for PUSCH, Avg RSSI ...	

Avg RSSI for PUSCH	Avg RSSI per cell PUCCH	Avg SINR for PUCCH
Avg SINR for PUSCH	Avg SINR per cell PUCCH	Avg UE PWR Headroom PUSCH
Avg UE distance	CSSR_VoLTE_FL16 [%]_new	CSSR_data_FL16_new
Call_attempts_4G	Cell Avail excl BLU	Data RB stp SR
Dropped_sessions_4G	E-RAB DR RAN	E-UTRAN E-RAB stp SR
E-UTRAN Total HO SR, inter eNB S1	Failed_calls_4G	Inter eNB E-UTRAN tot HO SR X2
MCDR_4G	MSDR_4G	Max SINR PUCCH

Figure 14.11 - Alarm to KPI Correlation Details

To Add a New Alarm to KPI Configuration

1. Go to Add New Alarm to KPI section.
2. Select the Domain, Network Type, Alarm Name and KPI Name from the drop down.
3. List the **Reason**. It is not mandatory.
4. After selecting the appropriate components, click the **Submit** button to create a new alarm to KPI configuration.



Domain	Network Type	Alarm Name	KPI Name	Reason
ACCESS	4G	module replacemen...	Avg RSSI for PUSCH, Avg RSSI ...	
ACCESS	4G	hardware_pm1	Avg RSSI for PUSCH, Avg RSSI ...	
ACCESS	4G	hardware_pm2	Avg RSSI for PUSCH, Avg RSSI ...	
ACCESS	4G	hardware_pm4	Avg RSSI for PUSCH, Avg RSSI ...	

Add New Alarm To KPI

Domain: ACCESS

Network Type: 4G (2G, 3G, 4G)

Alarm Name: 118 - Avalanche alarm

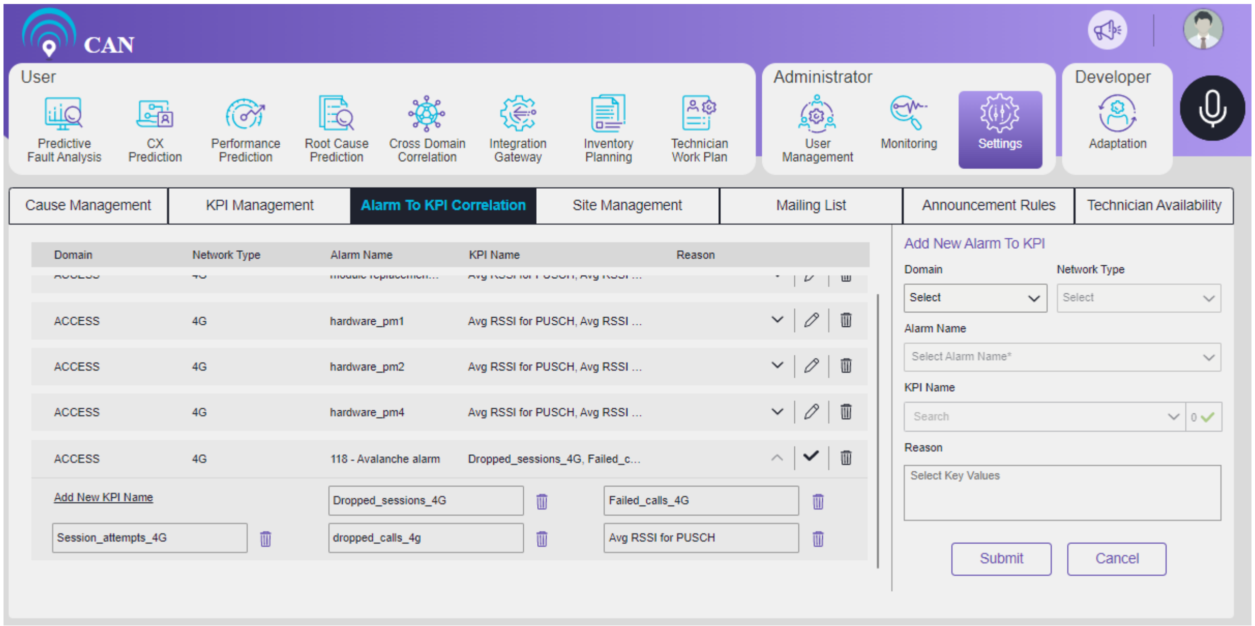
KPI Name: Search 3 ✓

Reason: Select Key Values

Figure 14.12 - Add New Alarm to KPI

To Edit the Existing Configuration

1. Under the existing configuration section, click the edit icon ✎.
2. Click **Add New KPI Name** to add a new KPI.
3. Click the delete icon 🗑 to delete an existing KPI.
4. Click the save icon ✓ to save the changes.
5. Click the delete icon 🗑 to delete the existing configuration.



Domain	Network Type	Alarm Name	KPI Name	Reason
ACCESS	4G	hardware_pm1	Avg RSSI for PUSCH, Avg RSSI ...	
ACCESS	4G	hardware_pm2	Avg RSSI for PUSCH, Avg RSSI ...	
ACCESS	4G	hardware_pm4	Avg RSSI for PUSCH, Avg RSSI ...	
ACCESS	4G	118 - Avalanche alarm	Dropped_sessions_4G, Failed_c...	

Dropped_sessions_4G

Failed_calls_4G

Session_attempts_4G

dropped_calls_4g

Avg RSSI for PUSCH

Add New Alarm To KPI

Domain: Select

Network Type: Select

Alarm Name: Select Alarm Name*

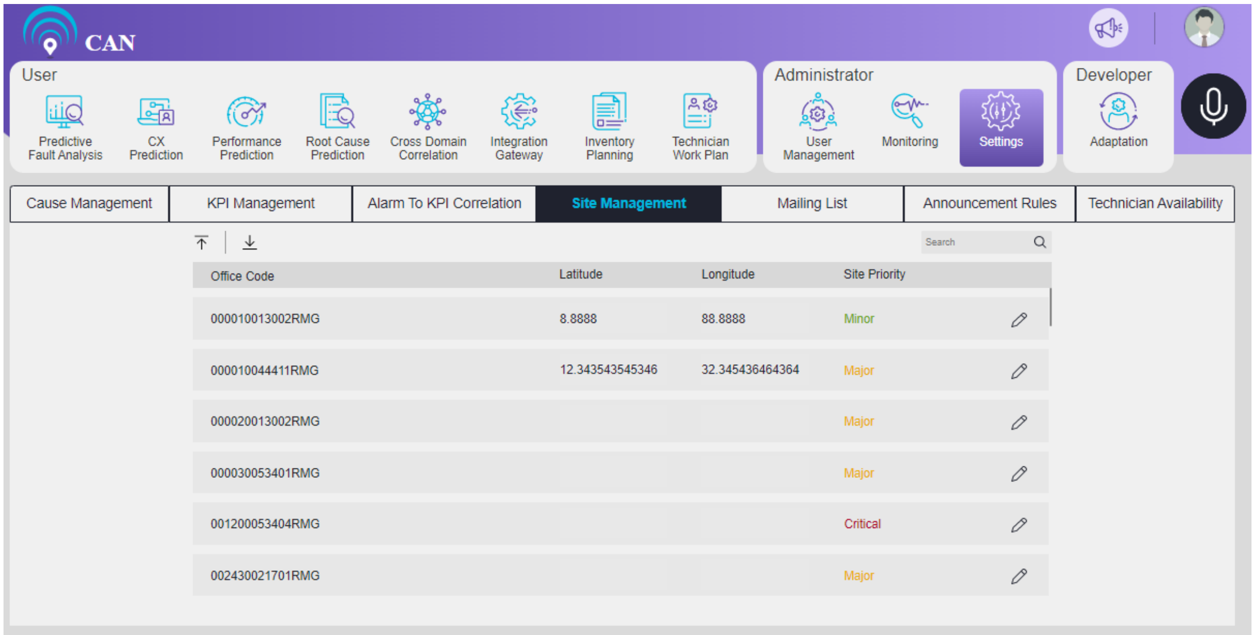
KPI Name: Search 0

Reason: Select Key Values

Figure 14.13 - Alarm to KPI Correlation Edit

Site Management

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



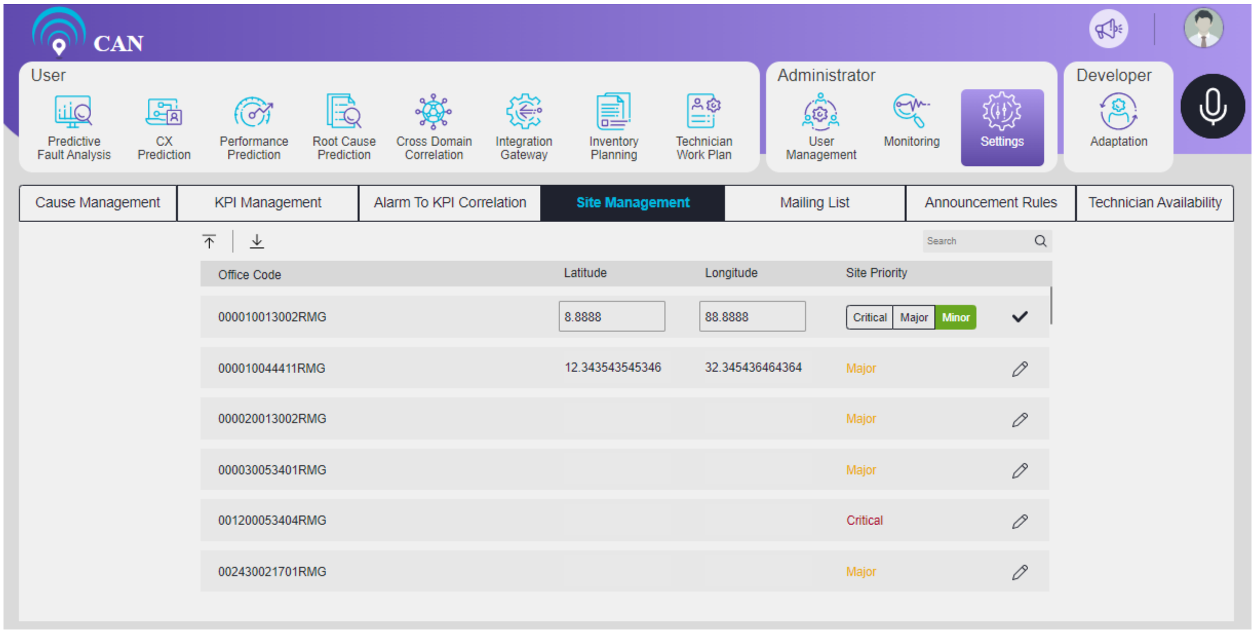
Office Code	Latitude	Longitude	Site Priority
000010013002RMG	8.8888	88.8888	Minor
000010044411RMG	12.343543545346	32.345436464364	Major
000020013002RMG			Major
000030053401RMG			Major
001200053404RMG			Critical
002430021701RMG			Major

Figure 14.14 – Site Management Screen

The first column displays the list of office codes, second & third column displays the corresponding Latitude & Longitude and last column displays the 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.

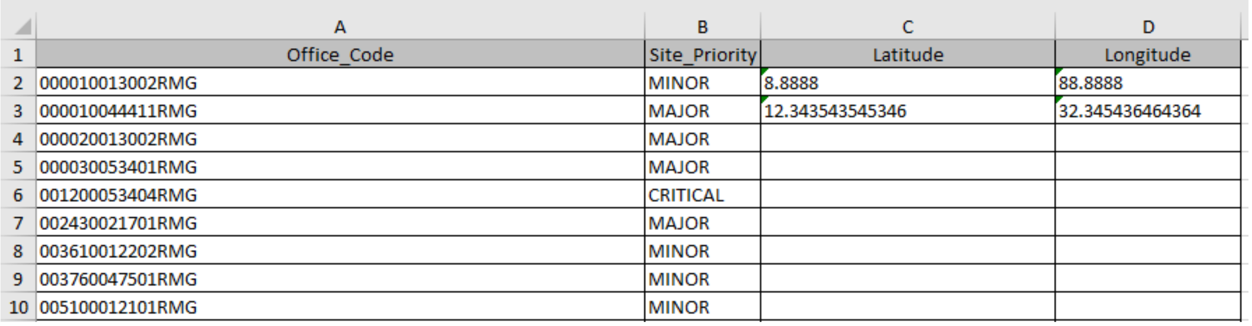
To update the site priority and latitude & longitude, click the Edit icon ✎. "**Critical**" will be marked in red, "**Major**" will be marked in yellow and "**Minor**" will be marked in green.



Office Code	Latitude	Longitude	Site Priority	
000010013002RMG	8.8888	88.8888	Critical Major [✓ Minor]	✓
000010044411RMG	12.343543545346	32.345436464364	Major	✎
000020013002RMG			Major	✎
000030053401RMG			Major	✎
001200053404RMG			Critical	✎
002430021701RMG			Major	✎

Figure 14.15 - Site Management Attributes Update

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

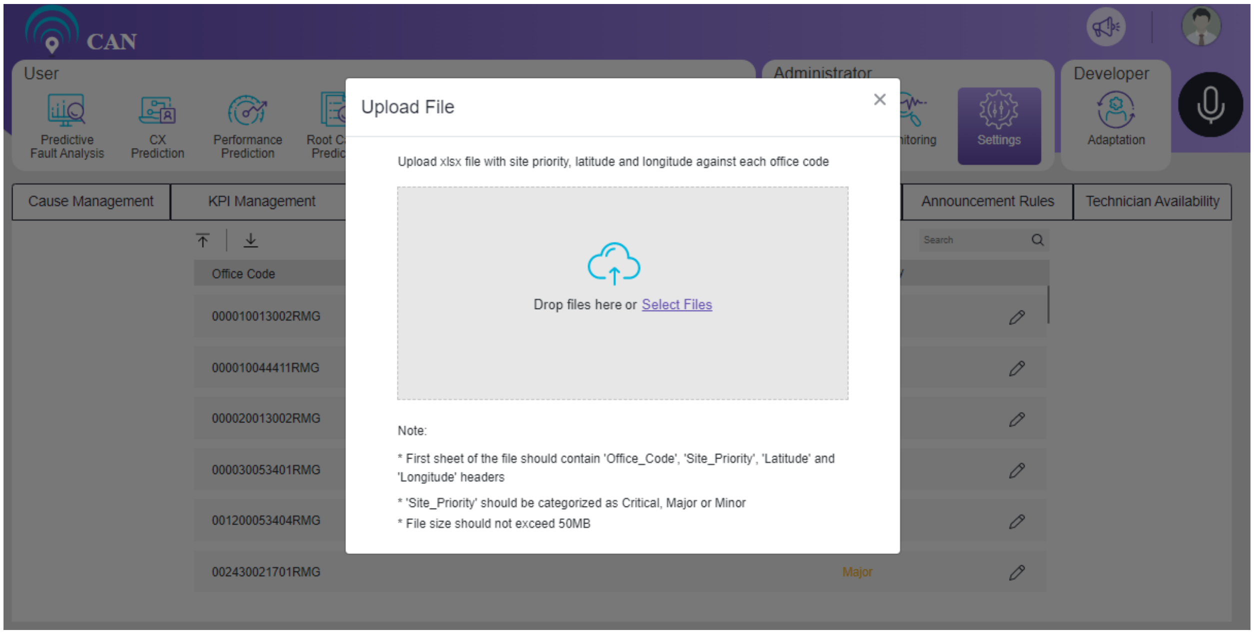


	A	B	C	D
1	Office_Code	Site_Priority	Latitude	Longitude
2	000010013002RMG	MINOR	8.8888	88.8888
3	000010044411RMG	MAJOR	12.343543545346	32.345436464364
4	000020013002RMG	MAJOR		
5	000030053401RMG	MAJOR		
6	001200053404RMG	CRITICAL		
7	002430021701RMG	MAJOR		
8	003610012202RMG	MINOR		
9	003760047501RMG	MINOR		
10	005100012101RMG	MINOR		

Figure 14.16 - Sample Downloaded File

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

CAN sends success or failure mail after uploading a file. If the file contains error entries, user can view and download the file with error entries.



Upload File

Upload xlsx file with site priority, latitude and longitude against each office code

Drop files here or Select Files

Note:

* First sheet of the file should contain 'Office_Code', 'Site_Priority', 'Latitude' and 'Longitude' headers

* 'Site_Priority' should be categorized as Critical, Major or Minor

* File size should not exceed 50MB

Office Code	
000010013002RMG	
000010044411RMG	
000020013002RMG	
000030053401RMG	
001200053404RMG	
002430021701RMG	Major

Figure 14.17 - Upload File Option

Note:

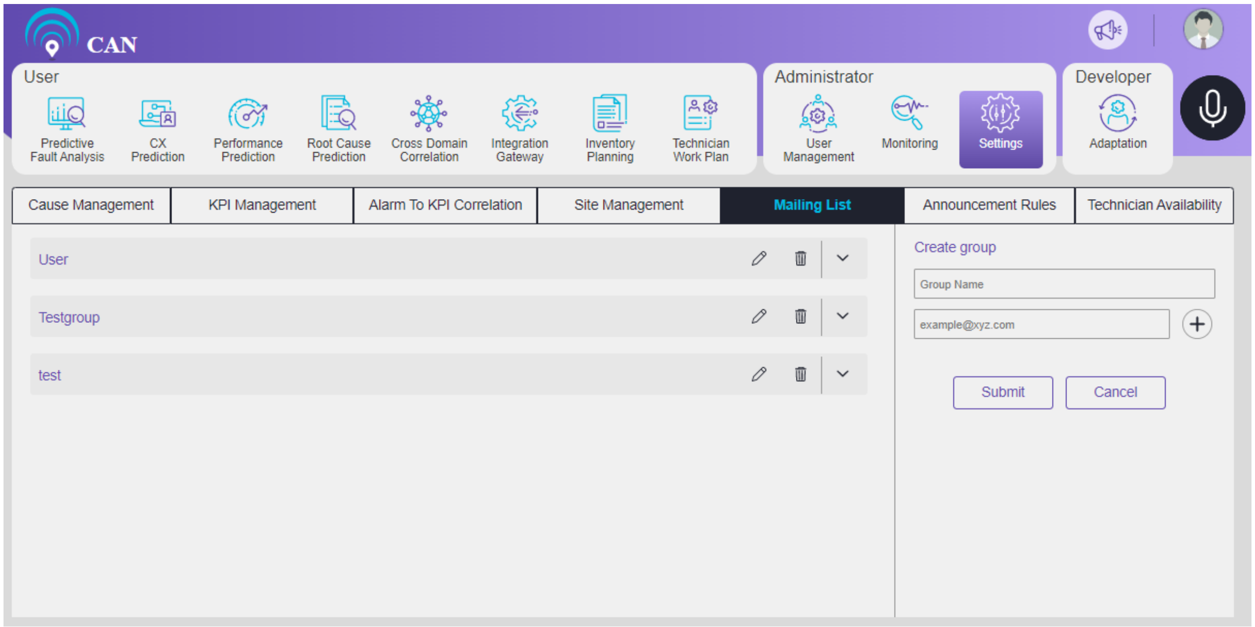
- First sheet of the xlsx file should contain Office_Code, Site_Priority, Latitude and Longitude headers.
- Site_Priority should be categorized as Critical, Major or Minor.
- File size should not exceed 50MB.
- If the file contains error entries, those entries will appear in the upload pop up. User can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

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.



User

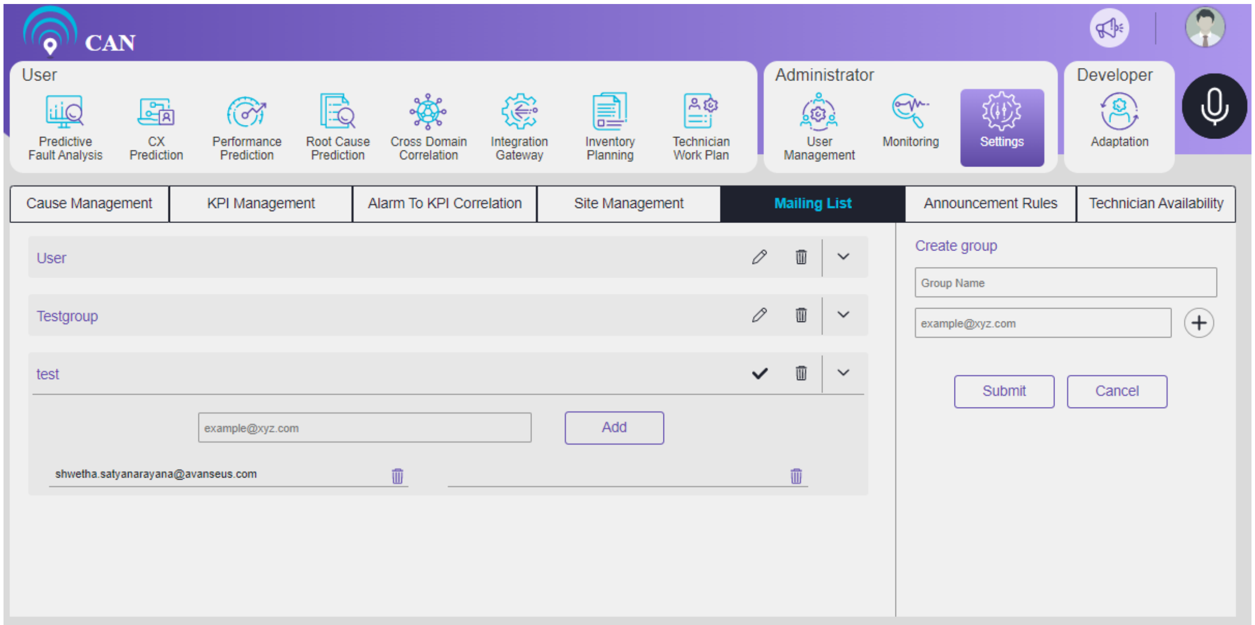
Testgroup

test

Figure 14.18 - 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.



User

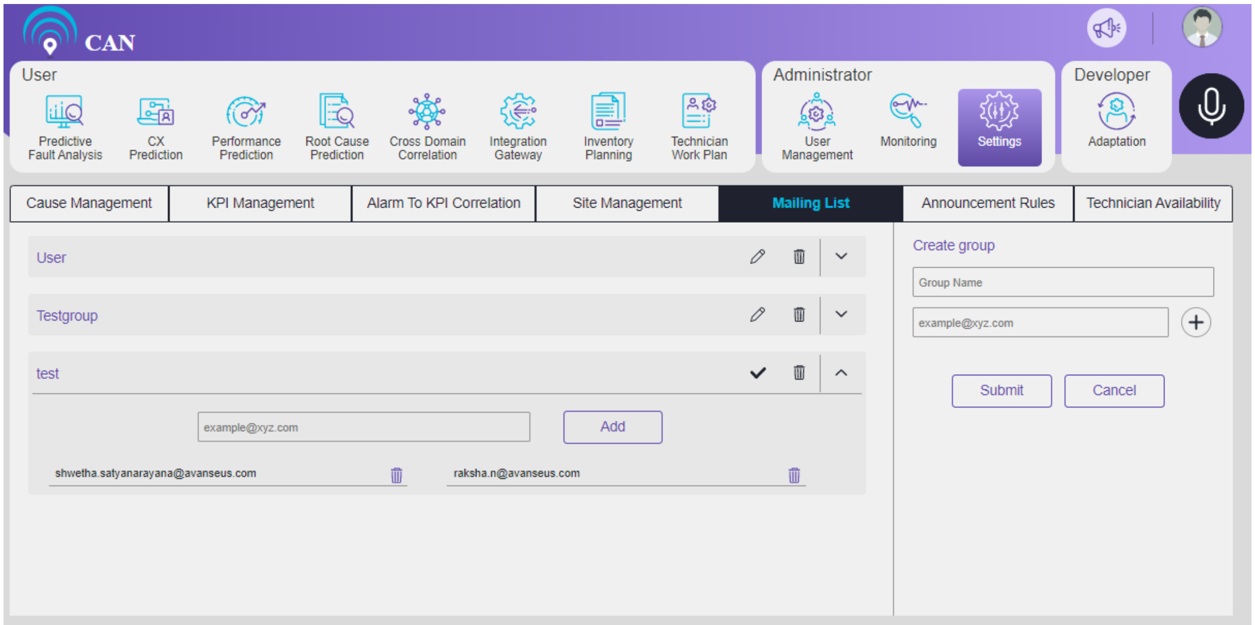
Testgroup

test

shwetha.satyanarayana@avanseus.com

Figure 14.19 - 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.



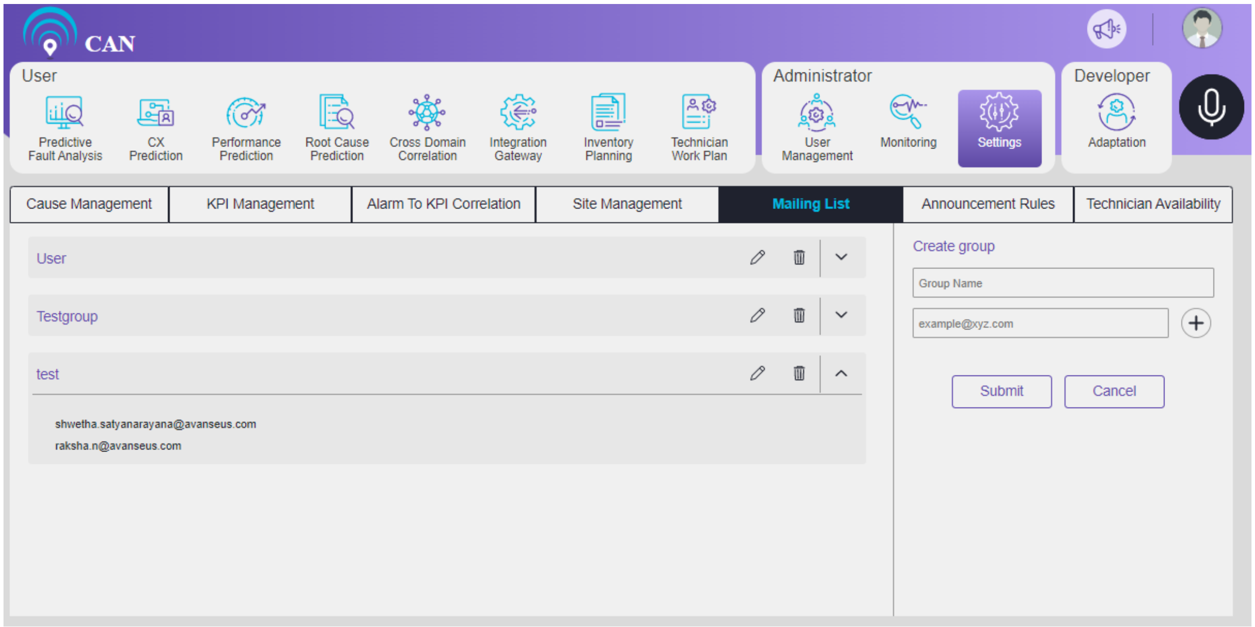
shwetha.satyanarayana@avanseus.com

raksha.n@avanseus.com

Figure 14.20 - Multiple Mail Id

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

Click ⌄ to see the details of the Mailing List.



shwetha.satyanarayana@avanseus.com
raksha.n@avanseus.com

Figure 14.21 - Mailing List Details

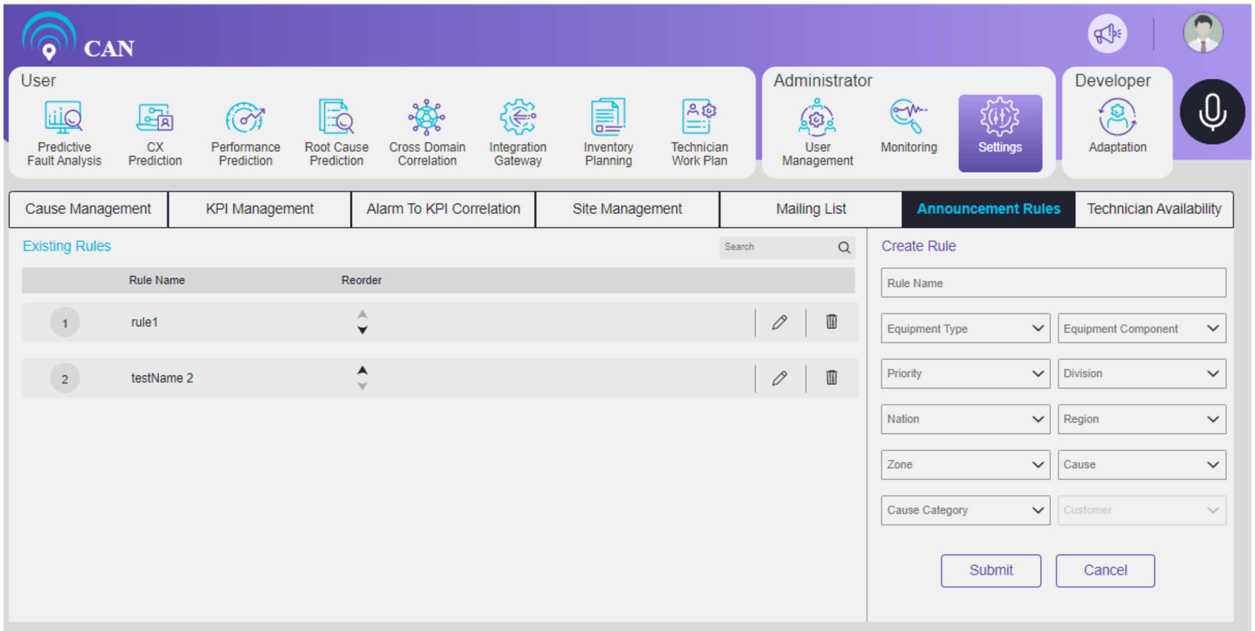
Announcement Rules

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.

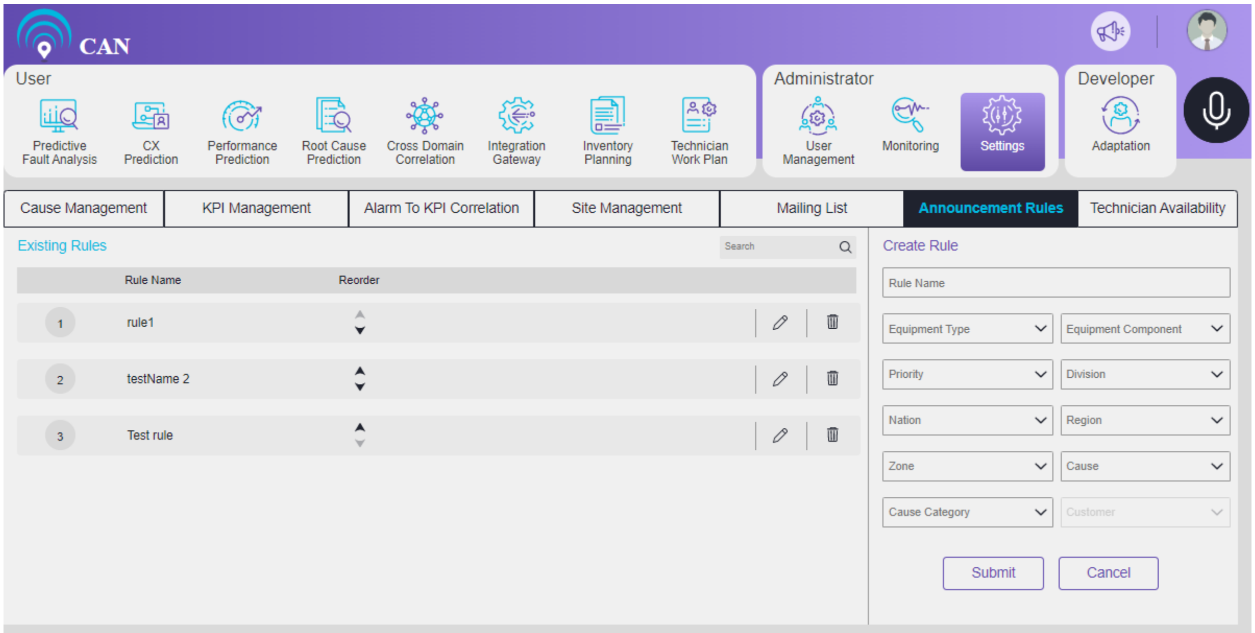


	Rule Name	Reorder
1	rule1	▲▼
2	testName 2	▲▼

Figure 14.22 - 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.

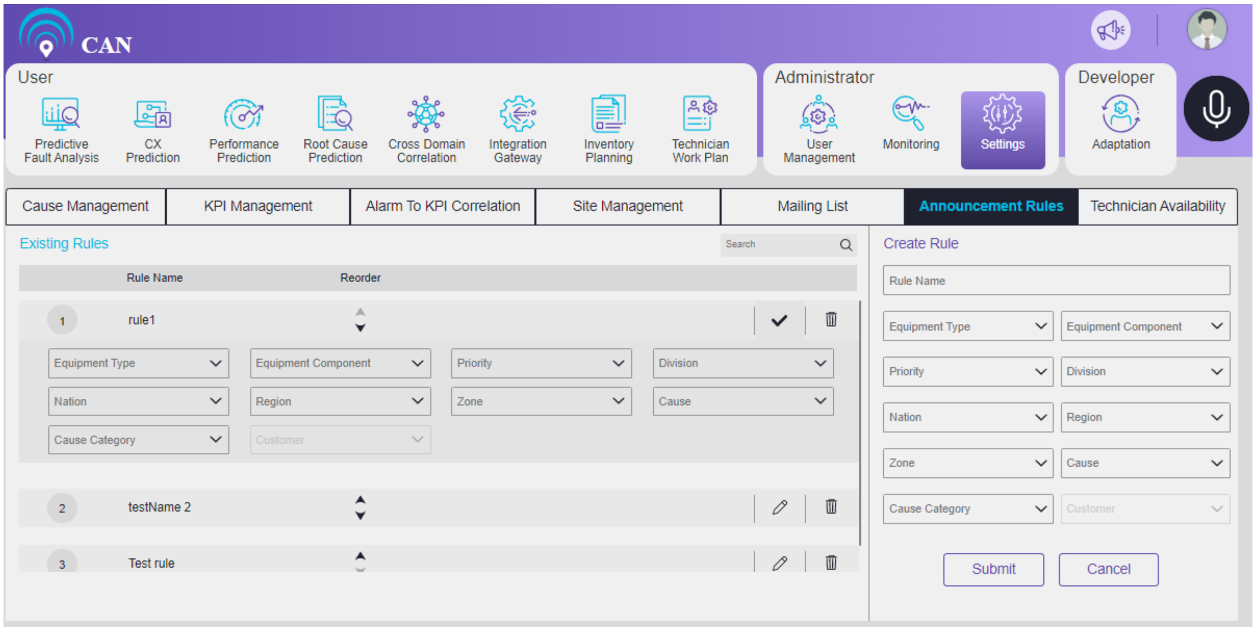


	Rule Name	Reorder
1	rule1	
2	testName 2	
3	Test rule	

Figure 14.23 - Rule Configuration for Announcement Rules

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**.



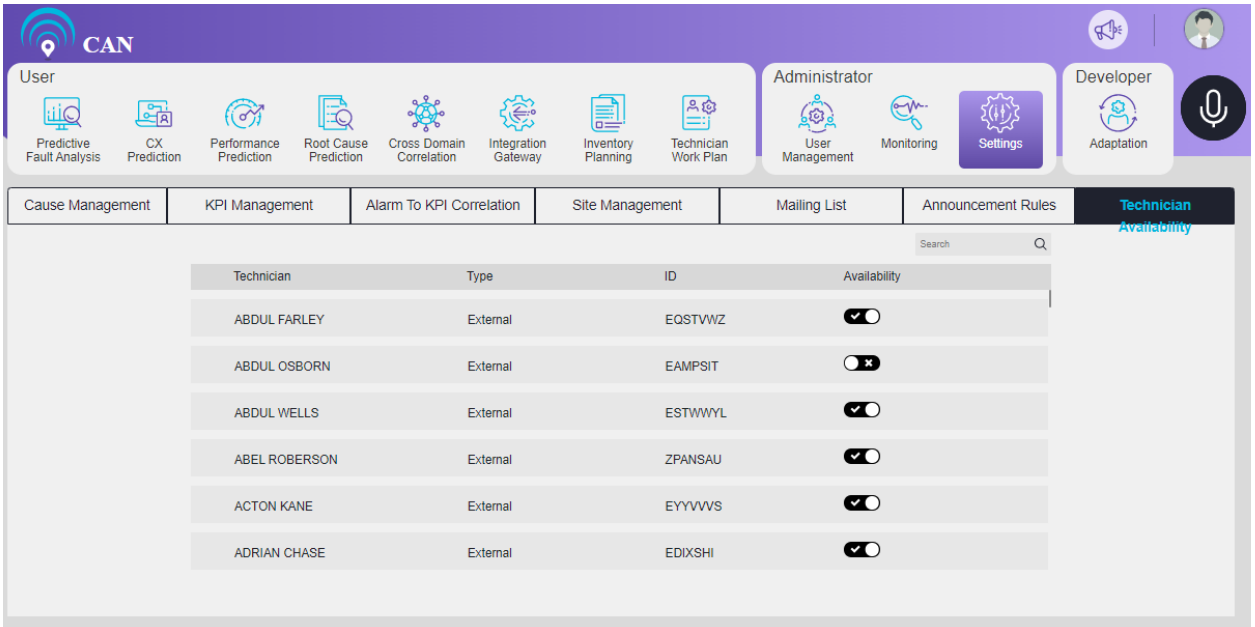
	Rule Name	Reorder
1	rule1	
2	testName 2	
3	Test rule	

Figure 14.24 - 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.



Technician	Type	ID	Availability
ABDUL FARLEY	External	EQSTVWZ	✓
ABDUL OSBORN	External	EAMPSIT	✗
ABDUL WELLS	External	ESTWWYL	✓
ABEL ROBERSON	External	ZPANSAU	✓
ACTON KANE	External	EYYVVVS	✓
ADRIAN CHASE	External	EDIXSHI	✓

Figure 14.25 - Technician Availability Screen

Page Intentionally Left Blank

15. ADAPTATION

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

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

The **Adaptation** screen has twelve tabs:

1. Input Mapper - User can set the Configurations related to loading client data files here. Four options fall under this category.
    1. File Pre-processor
    2. File Post-processor
    3. Record Parser
    4. Record Post-processor
2. Data Collection & Configuration - User can set the Configurations required to pull files from remote sources.
3. Filter Configuration - User can configure the rules to filter and optimize predictions here.
4. Post Prediction Process - User can upload the customizable code to be executed post prediction.
5. Report Configuration - The result of Prediction in Excel format is made configurable.
6. Advanced Configuration - Developer related Configurations.
7. Alarm Inclusions/Exclusions - Allows user to configure alarm filters.
8. Resource Configuration - Allows user to upload master data files that can be later used to fetch some information.
9. ROE Configuration - It helps to identify the root cause of a prediction based on multiple alarm parameters.
10. Integration Configuration - It is to integrate CAN with 3-party software (BMC Remedy, Weather Integration, Splunk and Ansible).
11. Topology Stitching Configuration
12. Topology Discovery Configuration

Input Mapper

Input Mapper has four tabs:

1. File Pre-processor
2. File Post-processor

3. Record Parser
4. Record Post-processor

File 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 select preferred code language, give name and description and write a code (similar to that of writing Record Parser code) inside the text area.

This code will implement IPreprocessor interface that 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.

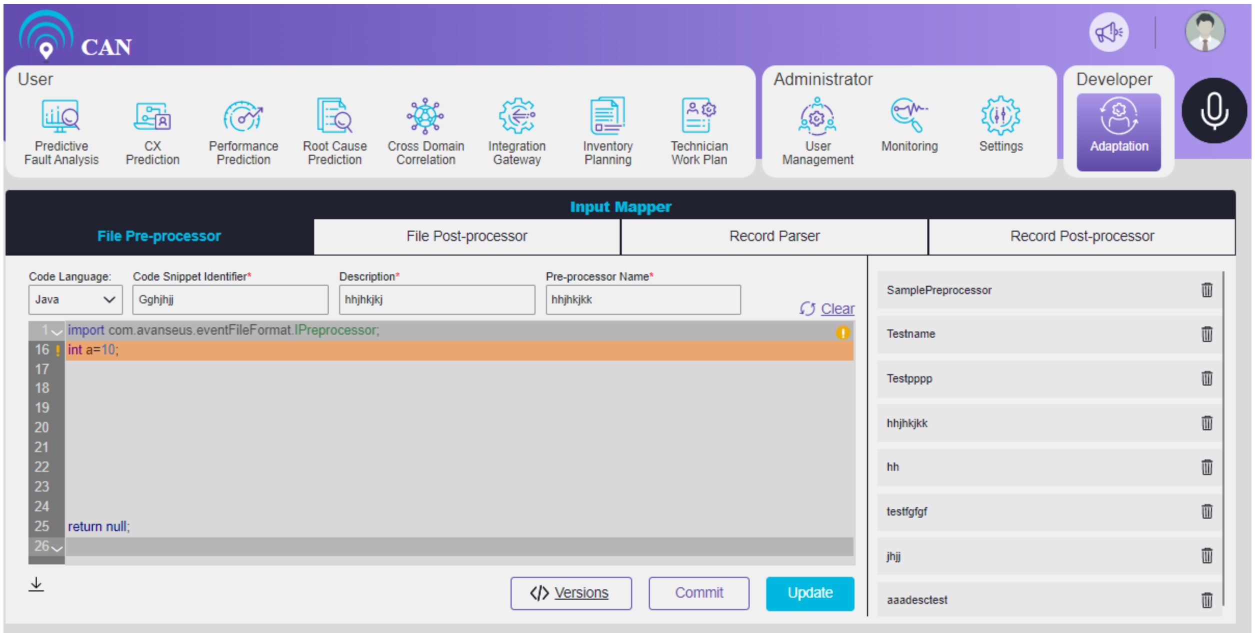
User can see a list of saved File pre-processor configurations at the right top corner.

By default, File Pre-processor is in edit mode.

Click any saved configuration on the right side of the screen.

The orange exclamatory mark 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 exclamatory mark to see the Error, Warning and Info details of the code.

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



Code Language: Java

Code Snippet Identifier*: Gghjhjj

Description*: hhjhkjkj

Pre-processor Name*: hhjhkjkk

```
import com.avanseus.eventFileFormat.IPreprocessor;
int a=10;








return null;
```

SamplePreprocessor

Testname

Testpppp

hhjhkjkk

hh

testfgfgf

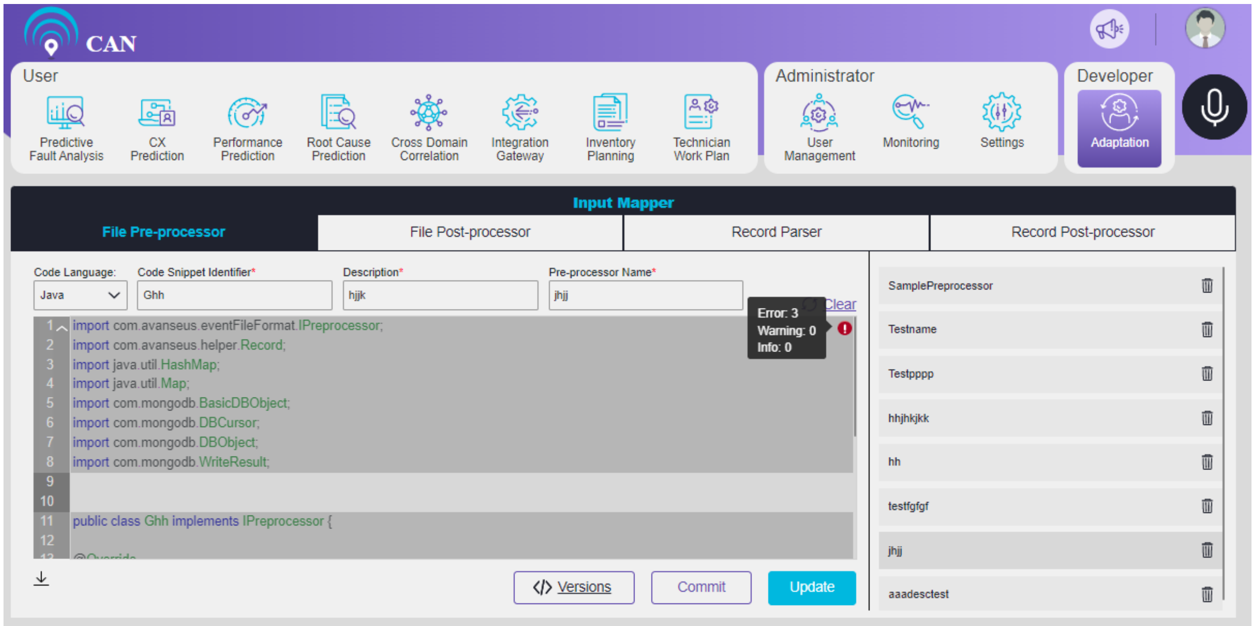
jhjj

aaadesctest

Figure 15.1 - 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 is disabled in case of the error in the code.



Code Language: Java

Code Snippet Identifier*: Ghh

Description*: hjjk

Pre-processor Name*: jhjj

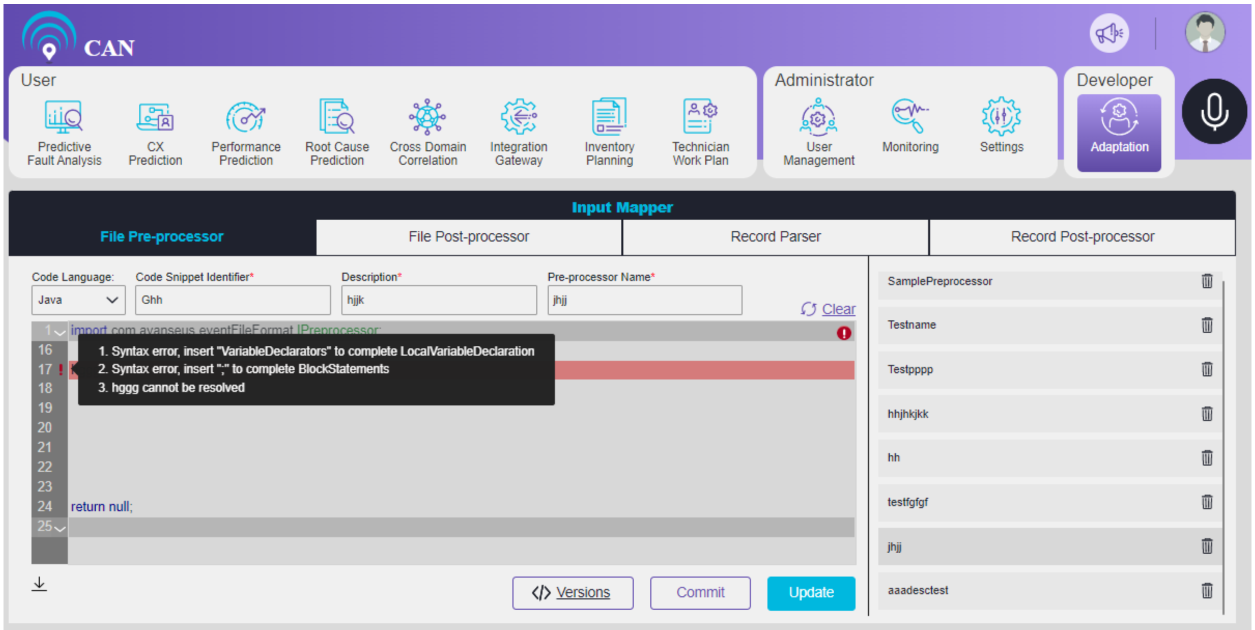
Error: 3
Warning: 0
Info: 0

```
import com.avanseus.eventFileFormat.IPreprocessor;
import com.avanseus.helper.Record;
import java.util.HashMap;
import java.util.Map;
import com.mongodb.BasicDBObject;
import com.mongodb.DBCursor;
import com.mongodb.DBObject;
import com.mongodb.WriteResult;


public class Ghh implements IPreprocessor {

@Override
```

SamplePreprocessor
Testname
Testpppp
hhjhkjkk
hh
testfgfgf
jhjj
aaadesctest

Figure 15.2 - 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.



Code Language: Java

Code Snippet Identifier*: Ghh

Description*: hjjk

Pre-processor Name*: jhjj

```
import com.avanseus.eventFileFormat.IPreprocessor;








return null;
```

1. Syntax error, insert "VariableDeclarators" to complete LocalVariableDeclaration
2. Syntax error, insert ";" to complete BlockStatements
3. hggg cannot be resolved

SamplePreprocessor
Testname
Testpppp
hhjhkjkk
hh
testfgfgf
jhjj
aaadesctest

Figure 15.3 - Pre Processor Screen with details of Error

To download the Saved Configurations, click the download icon ⤓.

To delete the Saved Configurations, click the delete icon 🗑 .

File Post-processor

CAN groups and ungroups incoming data for the subsequent process in the prediction generation cycle.

File Post-processor has two sections:

1. Splitting
2. Grouping

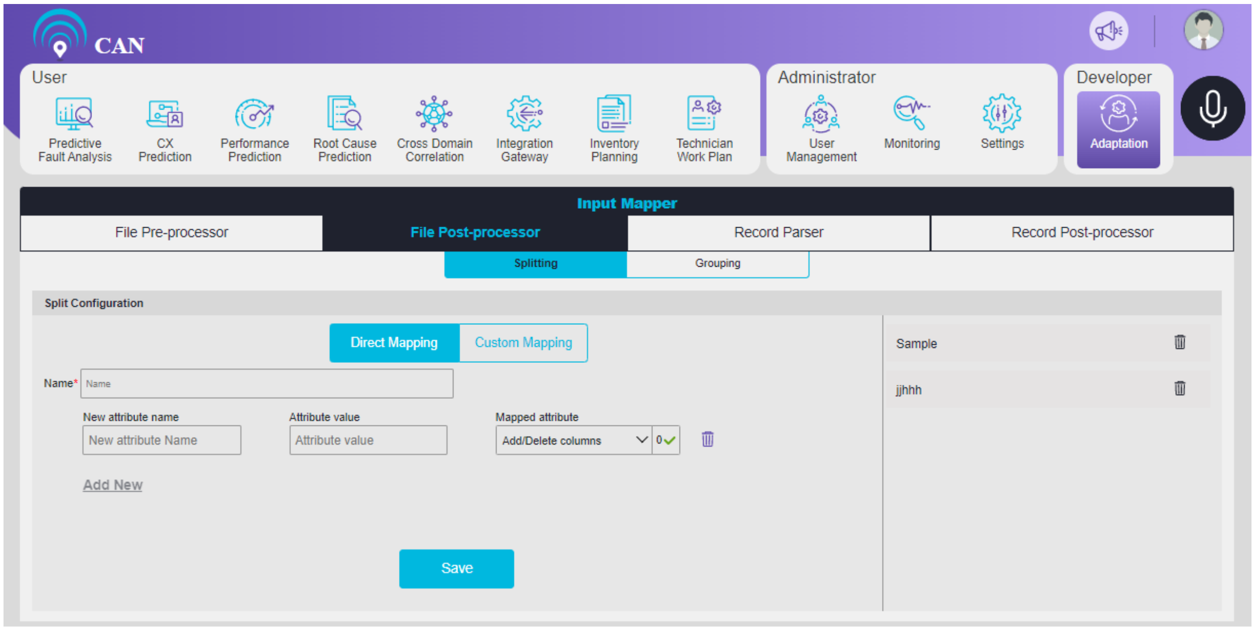


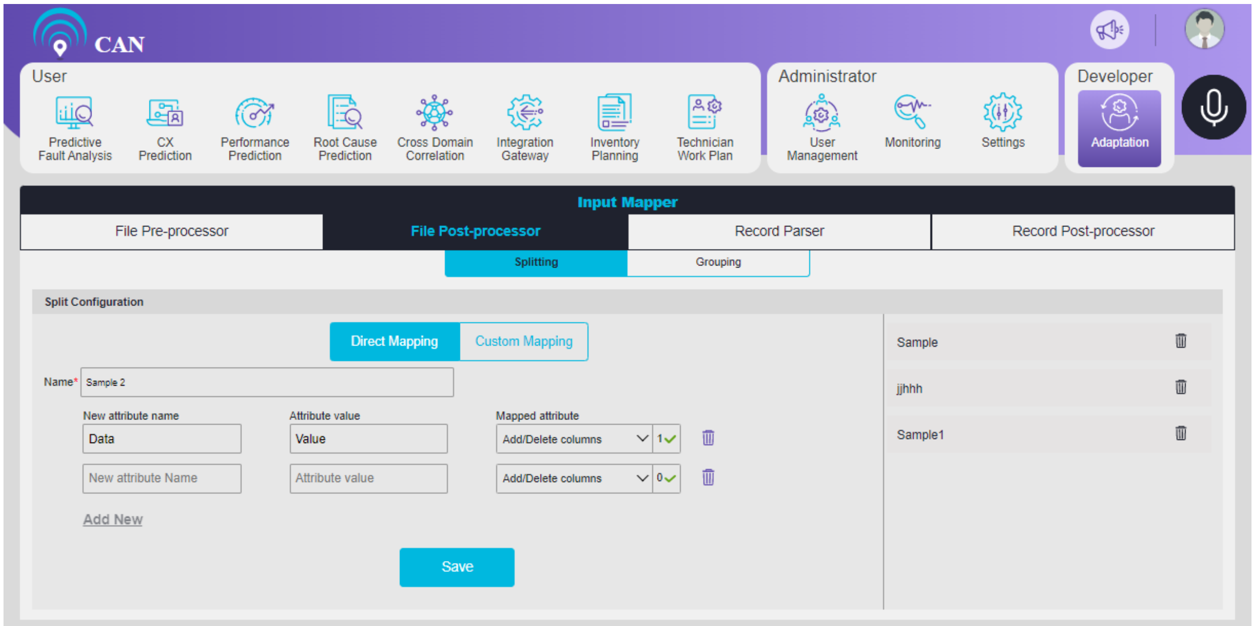
Figure 15.4 - File Post-processor Screen

Splitting:

This function convert single record into multiple records. Splitting is divided into two sections: **Direct Mapping** and **Custom Mapping**.

Direct Mapping: Mapped attribute header requires list of columns to be split. The splitting happens in a way that number of records added newly is equal to size of mapped attribute.

To add a new **Split Configuration**, enter the Name, New attribute name, Attribute value and Mapped attribute in the text box. Click **Add New** button to add new attribute. Click **Save** button to save the configuration. To delete an attribute, click 🗑icon.

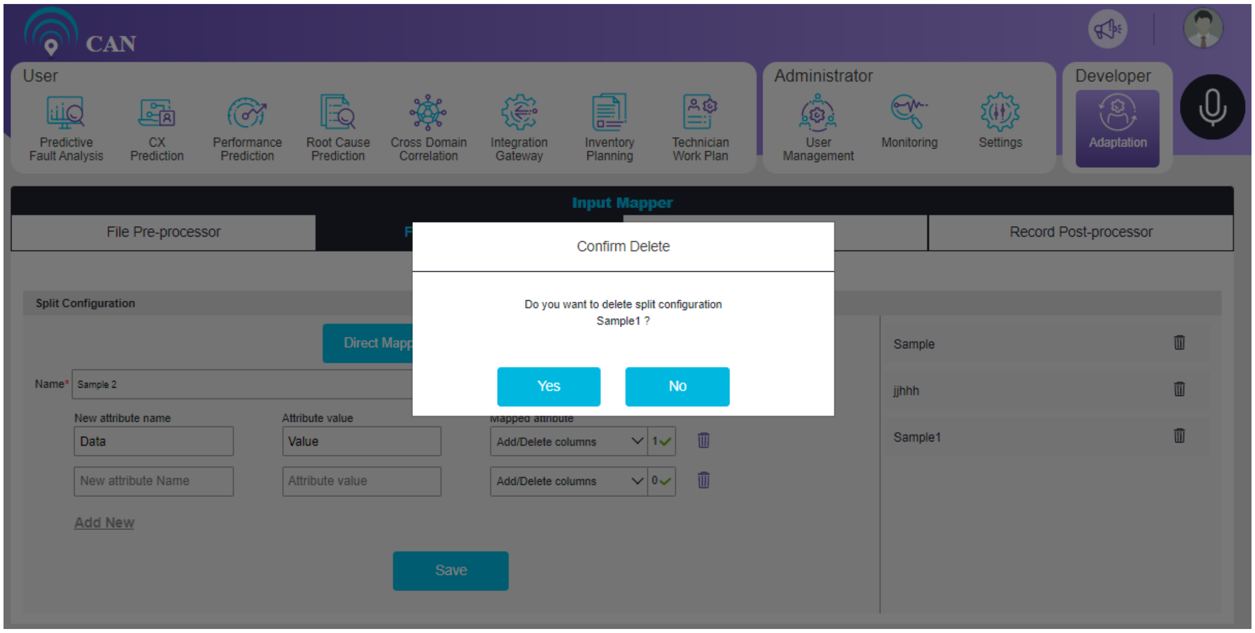


Name* Sample 2

New attribute name	Attribute value	Mapped attribute
Data	Value	Add/Delete columns 1

Figure 15.5 - Direct Mapping

Select the saved configuration from the right side of the screen. Click on 🗑 icon to delete a configuration. A dialogue box pops up. Click Yes to delete or No to retain the configuration.

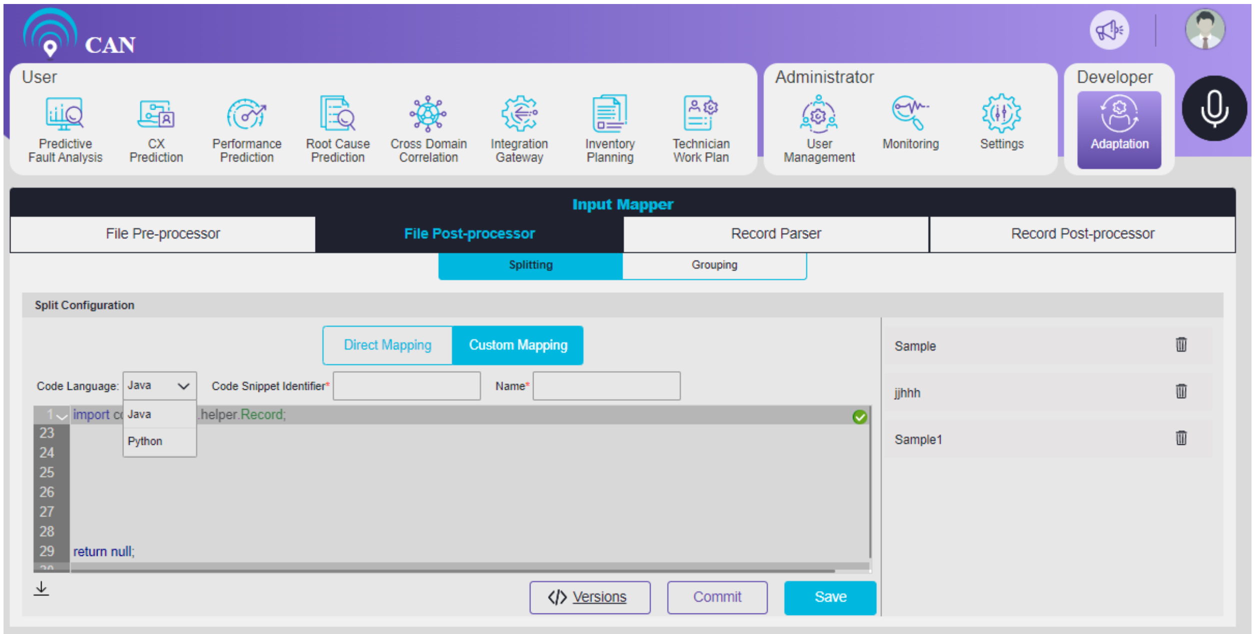


Confirm Delete

Do you want to delete split configuration Sample1 ?

Figure 15.6 - Delete Split Configuration

Custom Mapping: The custom mapping is used if single column cannot be used as split logic. Criteria that are more complex is configured by writing code in IDE. User can write and save Java or Python code. User can download the code by clicking on ⤓icon.



Code Language: Java

```
import c[...] helper.Record;




return null;
```

Figure 15.7 - Custom Mapping

Grouping:

Multiple records is grouped into single record using this screen.

To add a new **Group Configuration**, enter the Name, Attributes for group, Attributes for sort and Mapped attribute in the text box. Specify the Grouping Logic using the dropdown or code. Click **Add New** button to add new attribute. Click **Save** button to save the configuration. To delete an attribute, click 🗑 icon.

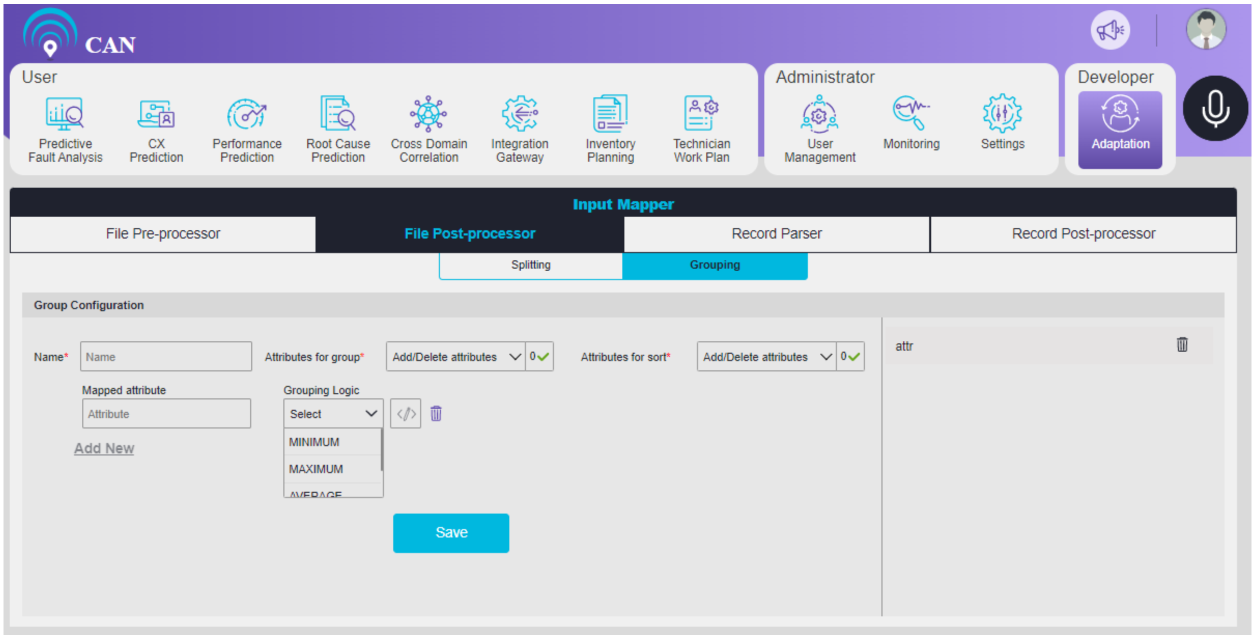
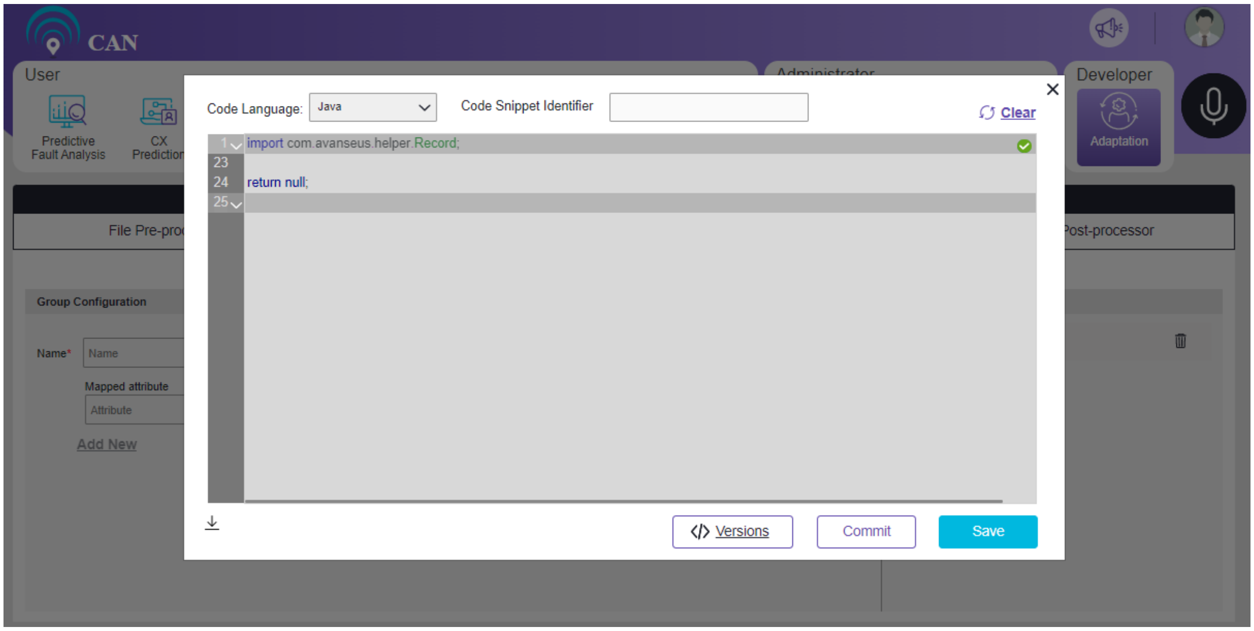


Figure 15.8 – Grouping Logic Dropdown

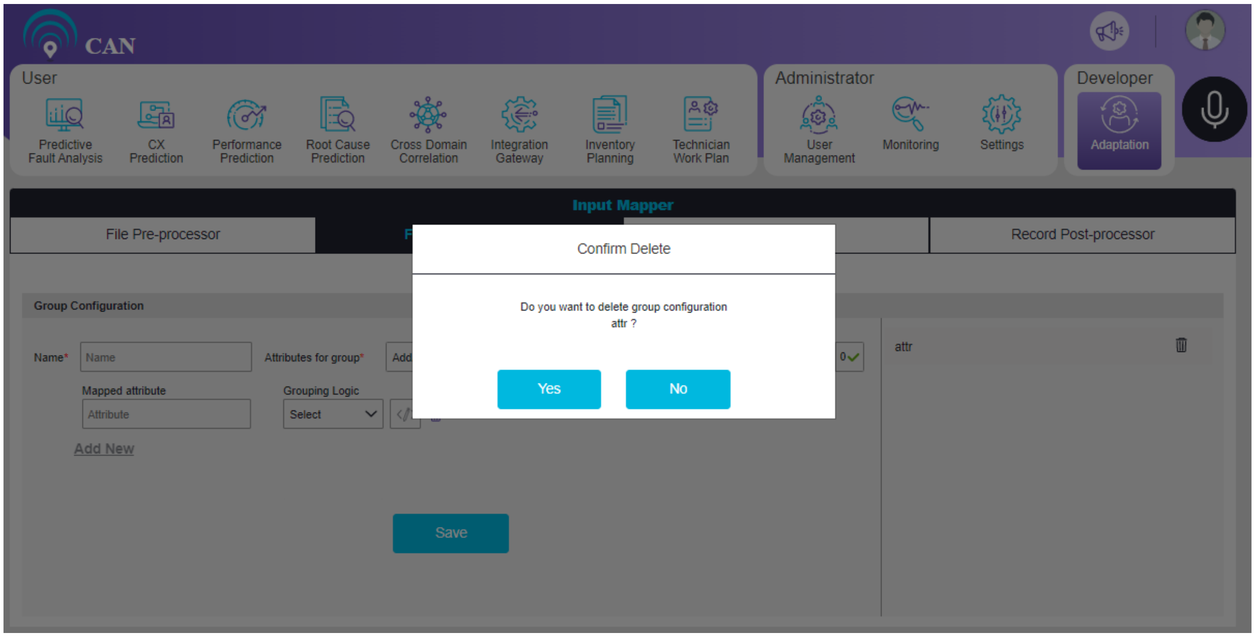


Code Language: Java

```
import com.avanseus.helper.Record;

return null;
```

Figure 15.9 - Grouping Logic

Select the saved configuration from the right side of the screen. Click on 🗑 icon to delete a configuration. A dialogue box pops up. Click Yes to delete or No to retain the configuration.



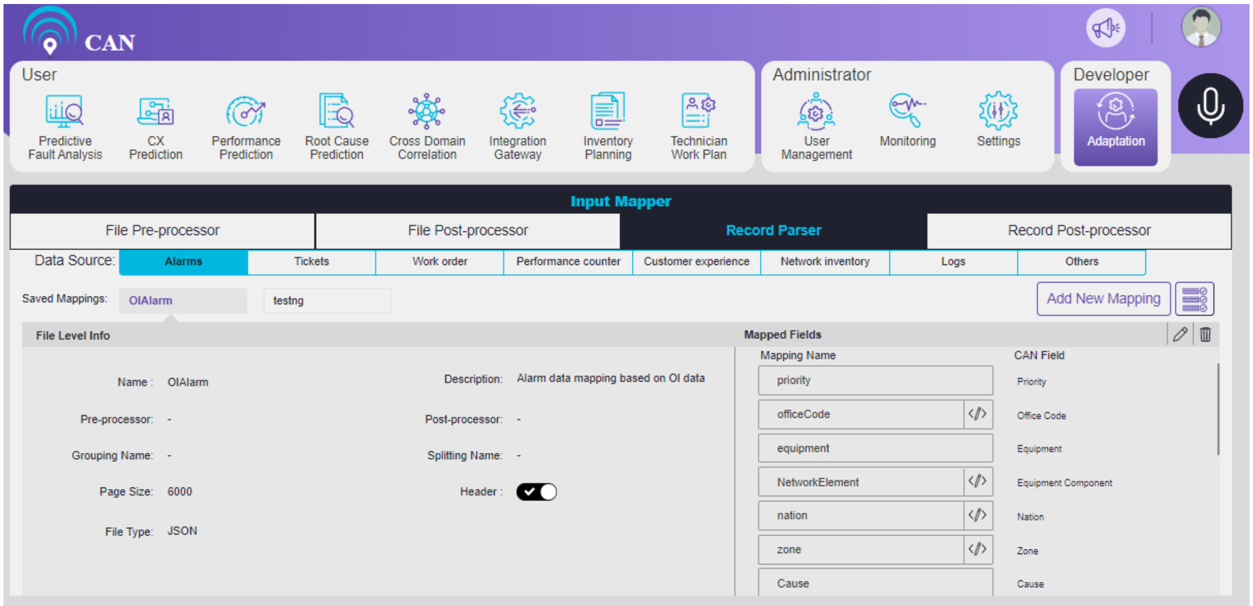
Do you want to delete group configuration attr ?

Figure 15.10 - Delete Group Configuration

Record 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. The parser code area accepts only the return type of field type that is being returned. These two data structures need to be in accord to generate the results. A client input data file should be synced with the CAN fields.

The data sources are Alarms, Tickets, Work order, Performance Counter, Customer experience, Network inventory, Logs and others.



Saved Mappings: OIAlarm testng

File Level Info

Name : OIAlarm

Description: Alarm data mapping based on OI data

Pre-processor: -

Post-processor: -

Grouping Name: -

Splitting Name: -

Page Size: 6000

Header : ✓

File Type: JSON

Mapped Fields

Mapping Name	CAN Field
priority	Priority
officeCode	Office Code
equipment	Equipment
NetworkElement	Equipment Component
nation	Nation
zone	Zone
Cause	Cause

Figure 15.11 - Record Parser Screen

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. Fields marked with * are mandatory fields.
3. The usual format of File Type is XLSX, DELIMTED, CUSTOMDELIMTER, JSON, XML and 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 write java/python code. This code is 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.
- In JSON file type, JSON key can be used for Mapping Name of parser, Mapped fields area and in IDE.
- In XML file type, Start tag (Use the tag as start), XML tag filter (Filter the tag from parsing) and XML attribute (Enable the attribute and use during parsing) are the parameters.

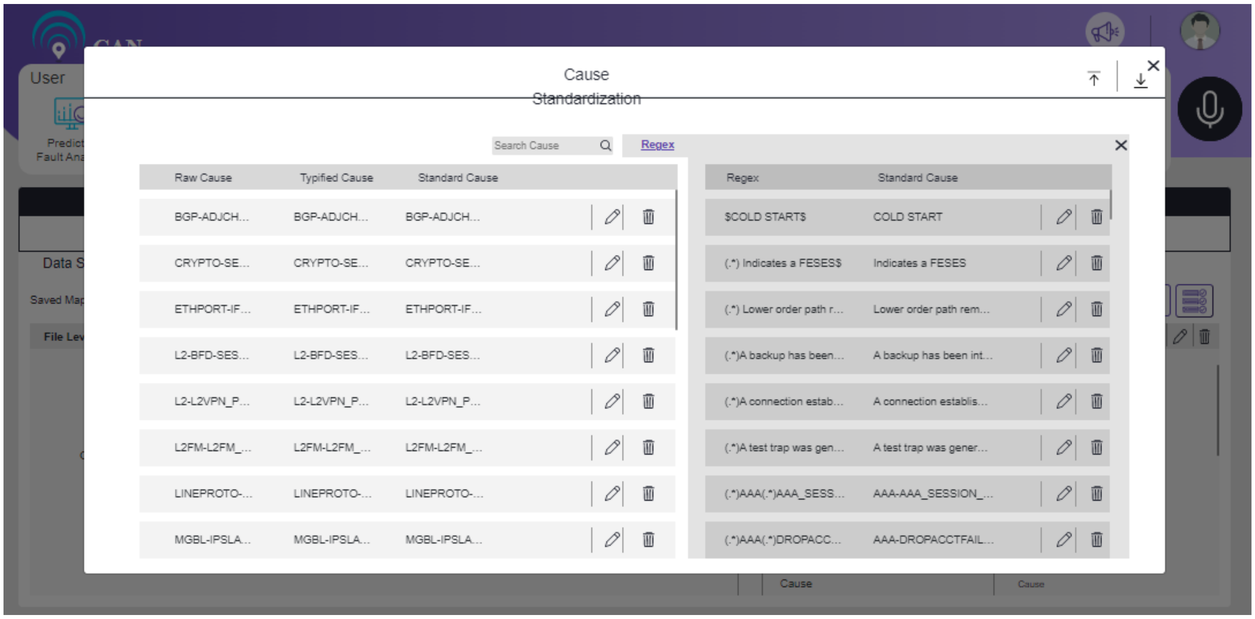
IMPORTANT: Refer the Input Mapper document for JSON and XML file type configuration.

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 CAN Field + 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.

Cause Standardization:

Alarm data that CAN processes is generally huge and diverse. Many times, the same causes are represented in different way though the underlying solution remains same. Cause standardization is converting such data into a standard format so that a better data set is created for accurate prediction.

In Alarms screen, on click of Cause Standardization Icon displays the **Cause Standardization table** as a Popup screen. In the Cause Standardization screen, on click of Regex displays the **Regex table**.

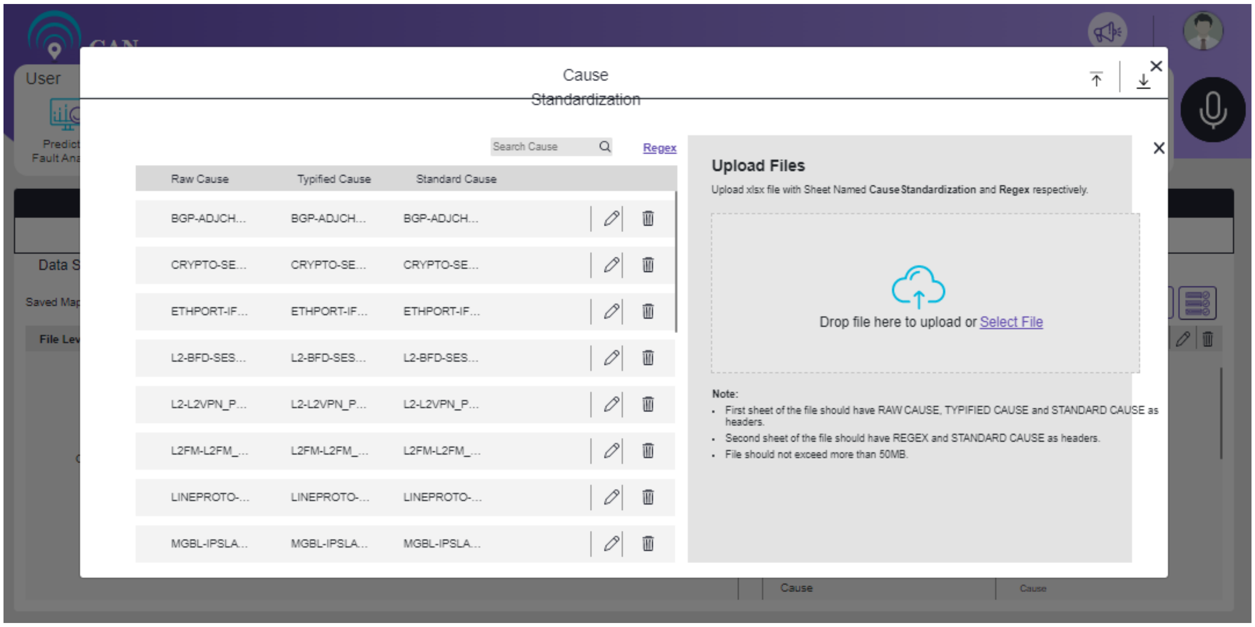


Raw Cause	Typified Cause	Standard Cause
BGP-ADJCH...	BGP-ADJCH...	BGP-ADJCH...
CRYPTO-SE...	CRYPTO-SE...	CRYPTO-SE...
ETHPORT-IF...	ETHPORT-IF...	ETHPORT-IF...
L2-BFD-SES...	L2-BFD-SES...	L2-BFD-SES...
L2-L2VPN_P...	L2-L2VPN_P...	L2-L2VPN_P...
L2FM-L2FM_...	L2FM-L2FM_...	L2FM-L2FM_...
LINEPROTO-...	LINEPROTO-...	LINEPROTO-...
MGBL-IPSLA...	MGBL-IPSLA...	MGBL-IPSLA...

Regex	Standard Cause
$COLD START$	COLD START
(.*) Indicates a FESES$	Indicates a FESES
(.*) Lower order path r...	Lower order path rem...
(.*)A backup has been...	A backup has been int...
(.*)A connection estab...	A connection establis...
(.*)A test trap was gen...	A test trap was gener...
(.*)AAA(.*)AAA_SESS...	AAA-AAA_SESSION_...
(.*)AAA(.*)DROPACC...	AAA-DROPACCTFAIL...

Figure 15.12 - Cause Standardization and Regex Table

User can click on the ↑ icon to upload xlsx file with Sheet Named **Cause Standardization** and **Regex** respectively.



Raw Cause	Typified Cause	Standard Cause
BGP-ADJCH...	BGP-ADJCH...	BGP-ADJCH...
CRYPTO-SE...	CRYPTO-SE...	CRYPTO-SE...
ETHPORT-IF...	ETHPORT-IF...	ETHPORT-IF...
L2-BFD-SES...	L2-BFD-SES...	L2-BFD-SES...
L2-L2VPN_P...	L2-L2VPN_P...	L2-L2VPN_P...
L2FM-L2FM_...	L2FM-L2FM_...	L2FM-L2FM_...
LINEPROTO-...	LINEPROTO-...	LINEPROTO-...
MGBL-IPSLA...	MGBL-IPSLA...	MGBL-IPSLA...

Upload xlsx file with Sheet Named **Cause Standardization** and **Regex** respectively.

Note:

- First sheet of the file should have RAW CAUSE, TYPIFIED CAUSE and STANDARD CAUSE as headers.
- Second sheet of the file should have REGEX and STANDARD CAUSE as headers.
- File should not exceed more than 50MB.

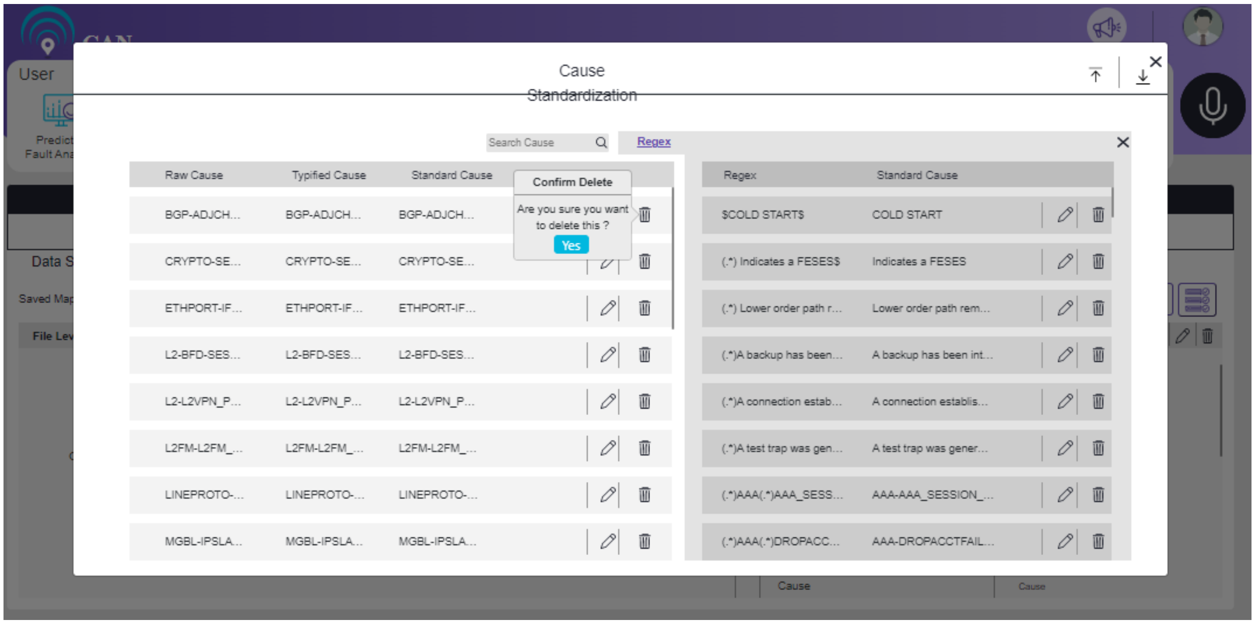
Figure 15.13 - Cause Standardization File Upload

NOTE:

- First sheet of the file should have RAW CAUSE, TYPIFIED CAUSE and STANDARD CAUSE as headers.
- Second sheet of the file should have REGEX and STANDARD CAUSE as headers.
- File should not exceed more than 50MB.

User can download the Cause Standardization and Regex by clicking the download ⤓ icon.

User can click on the edit icon ✎ to edit the causes in Cause Standardization table and Regex table. User has the option to Delete Raw cause and the associated Typified cause, Standard cause from Cause standardization table and Regex table.



Raw Cause	Typified Cause	Standard Cause
BGP-ADJCH...	BGP-ADJCH...	BGP-ADJCH...
CRYPTO-SE...	CRYPTO-SE...	CRYPTO-SE...
ETHPORT-IF...	ETHPORT-IF...	ETHPORT-IF...
L2-BFD-SES...	L2-BFD-SES...	L2-BFD-SES...
L2-L2VPN_P...	L2-L2VPN_P...	L2-L2VPN_P...
L2FM-L2FM_...	L2FM-L2FM_...	L2FM-L2FM_...
LINEPROTO-...	LINEPROTO-...	LINEPROTO-...
MGBL-IPSLA...	MGBL-IPSLA...	MGBL-IPSLA...

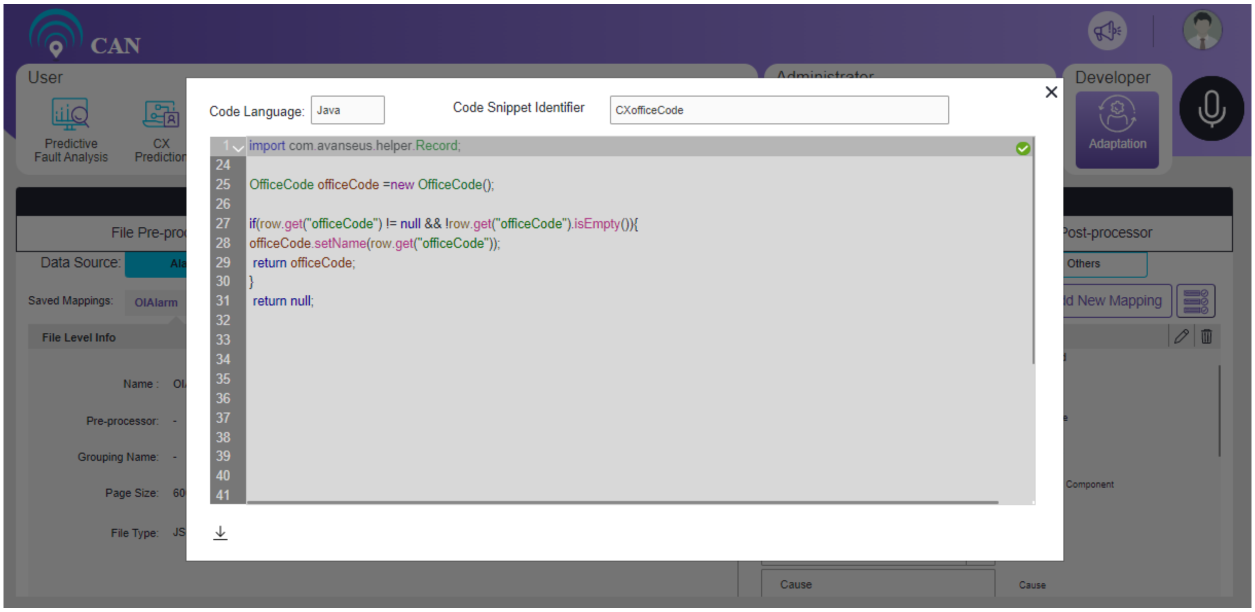
Regex	Standard Cause
$COLD START$	COLD START
(.*) Indicates a FESES$	Indicates a FESES
(.*) Lower order path r...	Lower order path rem...
(.*)A backup has been...	A backup has been int...
(.*)A connection estab...	A connection establis...
(.*)A test trap was gen...	A test trap was gener...
(.*)AAA(.*)AAA_SESS...	AAA-AAA_SESSION_...
(.*)AAA(.*)DROPACC...	AAA-DROPACCTFAIL...

Figure 15.14 - Delete Confirmation for Cause

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 be automatically 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 ⤓.



Data Source: Ala

Saved Mappings: OIAlarm

Name : OI

Pre-processor: -

Grouping Name: -

Page Size: 60

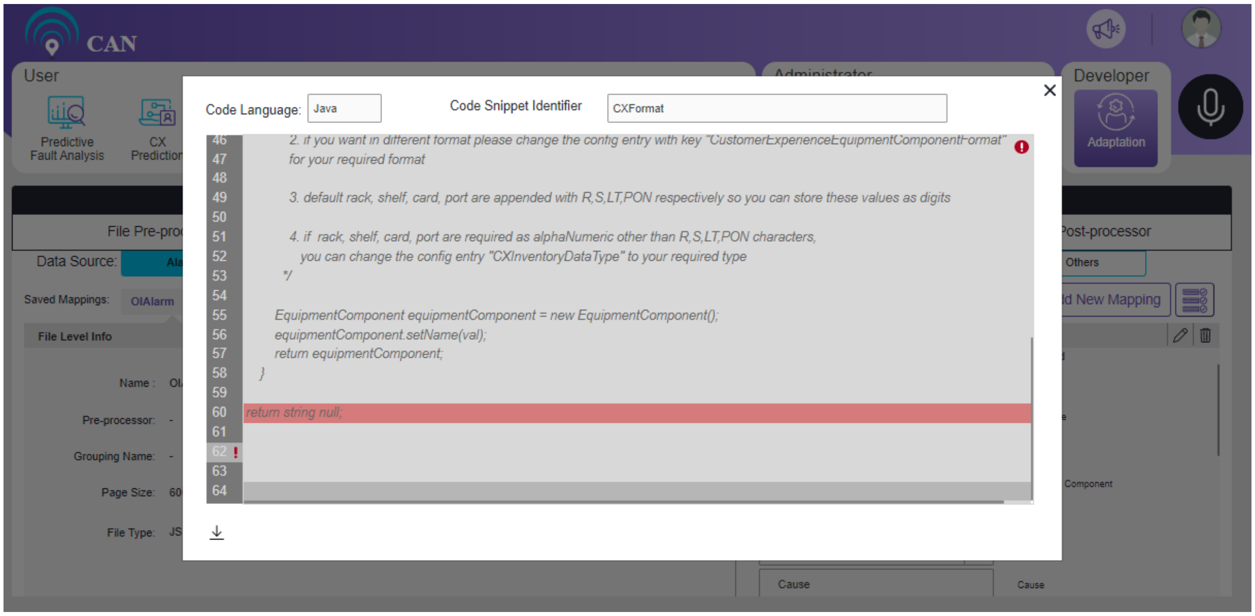
File Type: JS

Code Language: Java

Code Snippet Identifier CXofficeCode

```
import com.avanseus.helper.Record;

OfficeCode officeCode =new OfficeCode();

if(row.get("officeCode") != null && !row.get("officeCode").isEmpty()){
officeCode.setName(row.get("officeCode"));
 return officeCode;
}
 return null;
```

In case the code is not correct then the screen will show the exclamatory mark in red color. This represents error in the code. User need to delete the error in order to save the code.



Data Source: Ala

Saved Mappings: OIAlarm

Name : OI

Pre-processor: -

Grouping Name: -

Page Size: 60

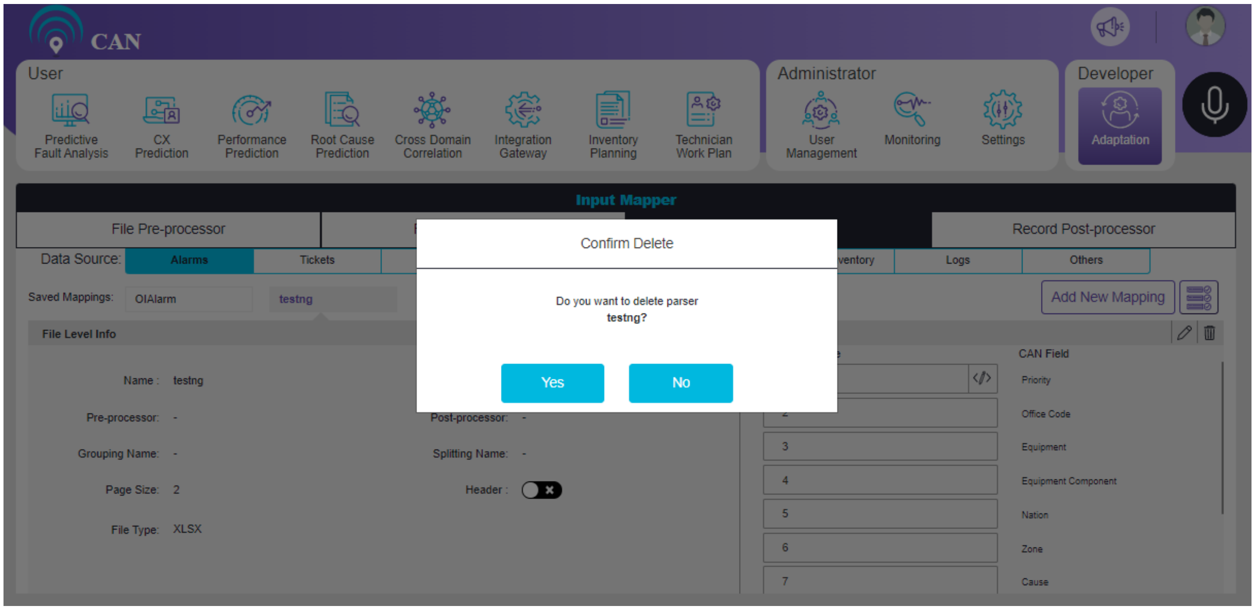
File Type: JS

Code Language: Java

Code Snippet Identifier CXFormat

```
       2. if you want in different format please change the config entry with key "CustomerExperienceEquipmentComponentFormat"
       for your required format

       3. default rack, shelf, card, port are appended with R,S,LT,PON respectively so you can store these values as digits

       4. if  rack, shelf, card, port are required as alphaNumeric other than R,S,LT,PON characters,
         you can change the config entry "CXInventoryDataType" to your required type
      */

     EquipmentComponent equipmentComponent = new EquipmentComponent();
     equipmentComponent.setName(val);
     return equipmentComponent;
  }

return string null;
```

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



Confirm Delete

Do you want to delete parser testng?

Yes No

Name : testng

Pre-processor: -

Grouping Name: -

Page Size: 2

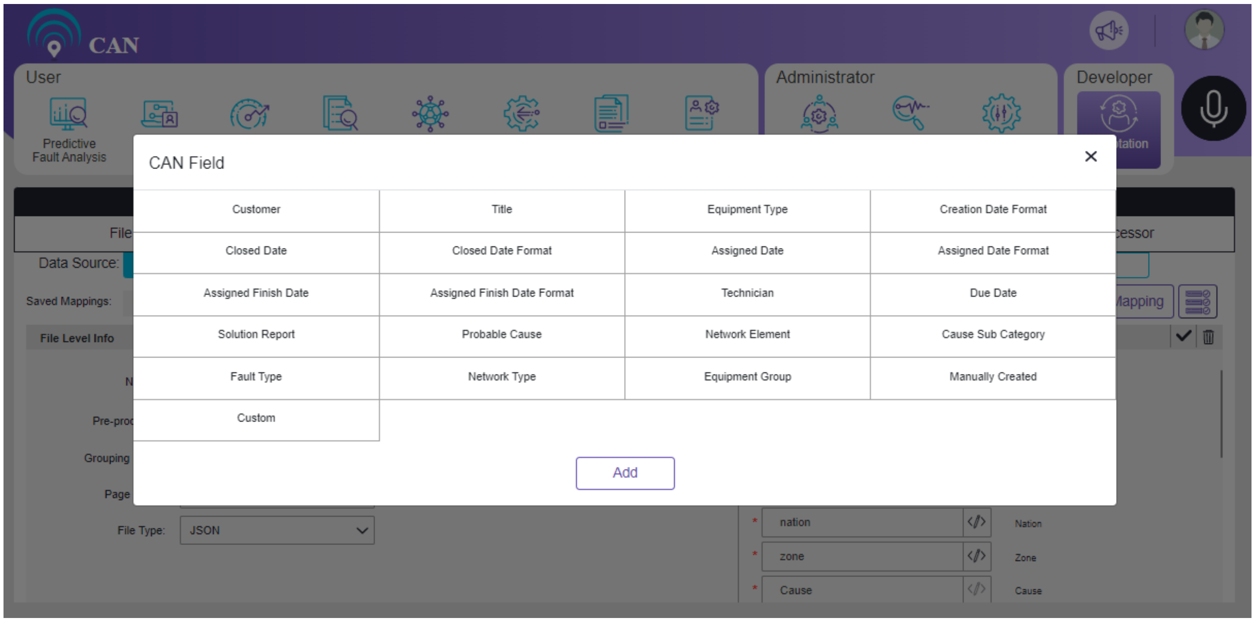
File Type: XLSX

Post-processor: -

Splitting Name: -

Header :

Figure 15.15 – Record Parser Screen to Delete the Configuration



CAN Field

Customer	Title	Equipment Type	Creation Date Format
Closed Date	Closed Date Format	Assigned Date	Assigned Date Format
Assigned Finish Date	Assigned Finish Date Format	Technician	Due Date
Solution Report	Probable Cause	Network Element	Cause Sub Category
Fault Type	Network Type	Equipment Group	Manually Created
Custom			

Add

nation

zone

Cause

Figure 15.16 - CAN Fields

Record Post-Processor

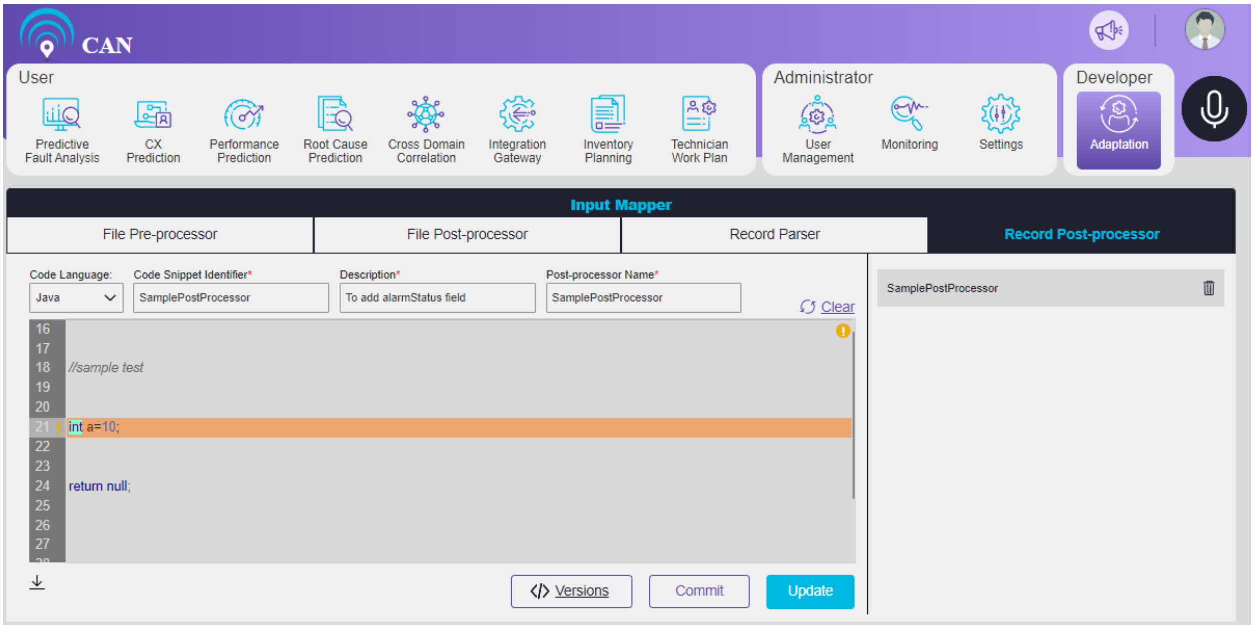
Post-processor modifies or discards the data after parsing and just before loading of the data.

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

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

By default, the Record 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.



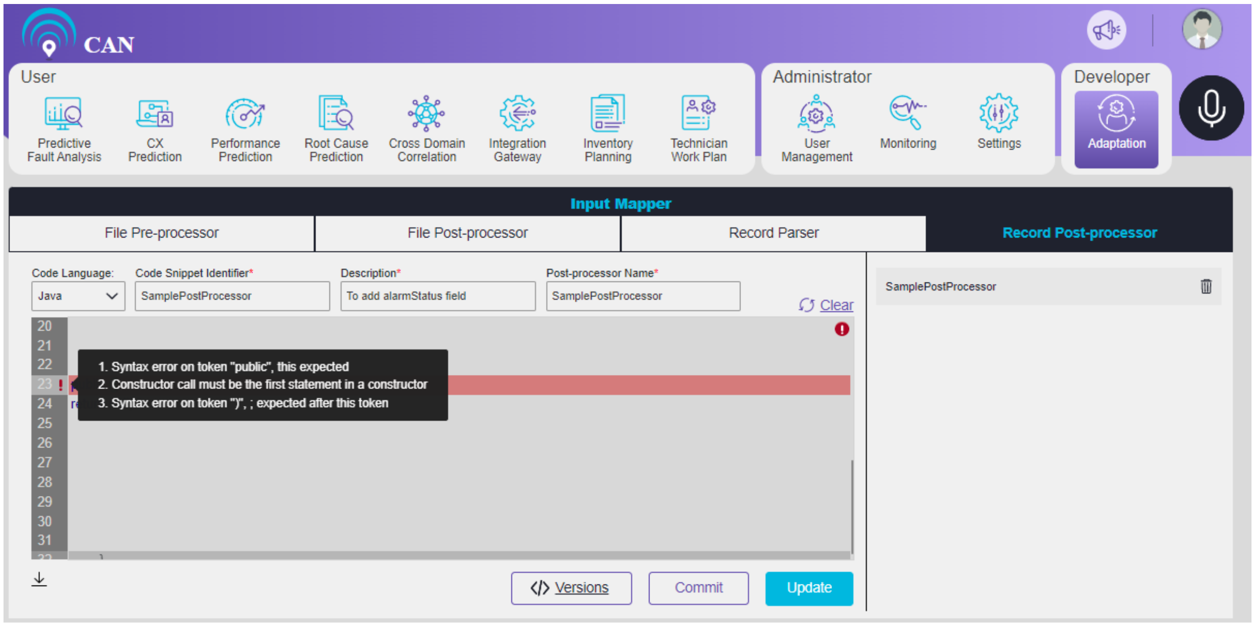
Code Language: Java
Code Snippet Identifier*: SamplePostProcessor
Description*: To add alarmStatus field
Post-processor Name*: SamplePostProcessor

```
//sample test

int a=10;


return null;
```

SamplePostProcessor

Figure 15.17 - 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.



Code Language: Java
Code Snippet Identifier*: SamplePostProcessor
Description*: To add alarmStatus field
Post-processor Name*: SamplePostProcessor

1. Syntax error on token "public", this expected
2. Constructor call must be the first statement in a constructor
3. Syntax error on token ")", ; expected after this token

SamplePostProcessor

Figure 15.18 – Record Post Processor Screen with details of Error in Code

To download the saved configurations, click the download icon ⤓.

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:

1. SFTP
2. FTP
3. GITHUB
4. EMAIL
5. CUSTOM
6. SECURE KAFKA
7. PROMETHEUS
8. 3GPP5G

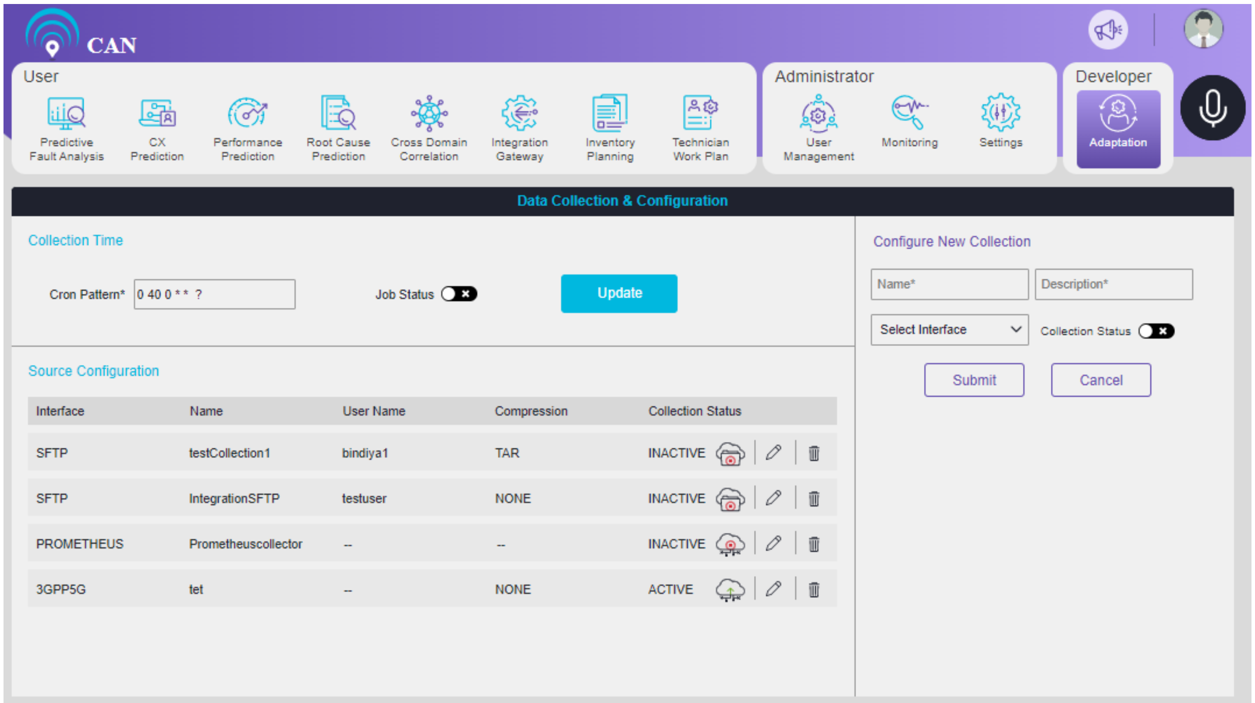
User can add, edit and delete a Data Collection Configuration and specify the active collection time cron for the next job.

The icons used to indicate the configurations are as follows:

1. The active file that perform batch processing (non Kafka) is represented by icon.
2. The inactive file that perform batch processing (non Kafka) is represented by icon.
3. The active file that perform stream processing (Kafka) is represented by icon.
4. 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 **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.



Data Collection & Configuration

Collection Time

Cron Pattern* 0 40 0 * * ?

Job Status

Update

Source Configuration

Interface	Name	User Name	Compression	Collection Status
SFTP	testCollection1	bindiya1	TAR	INACTIVE
SFTP	IntegrationSFTP	testuser	NONE	INACTIVE
PROMETHEUS	Prometheuscollector	--	--	INACTIVE
3GPP5G	tet	--	NONE	ACTIVE

Configure New Collection

Name*

Description*

Select Interface

Collection Status

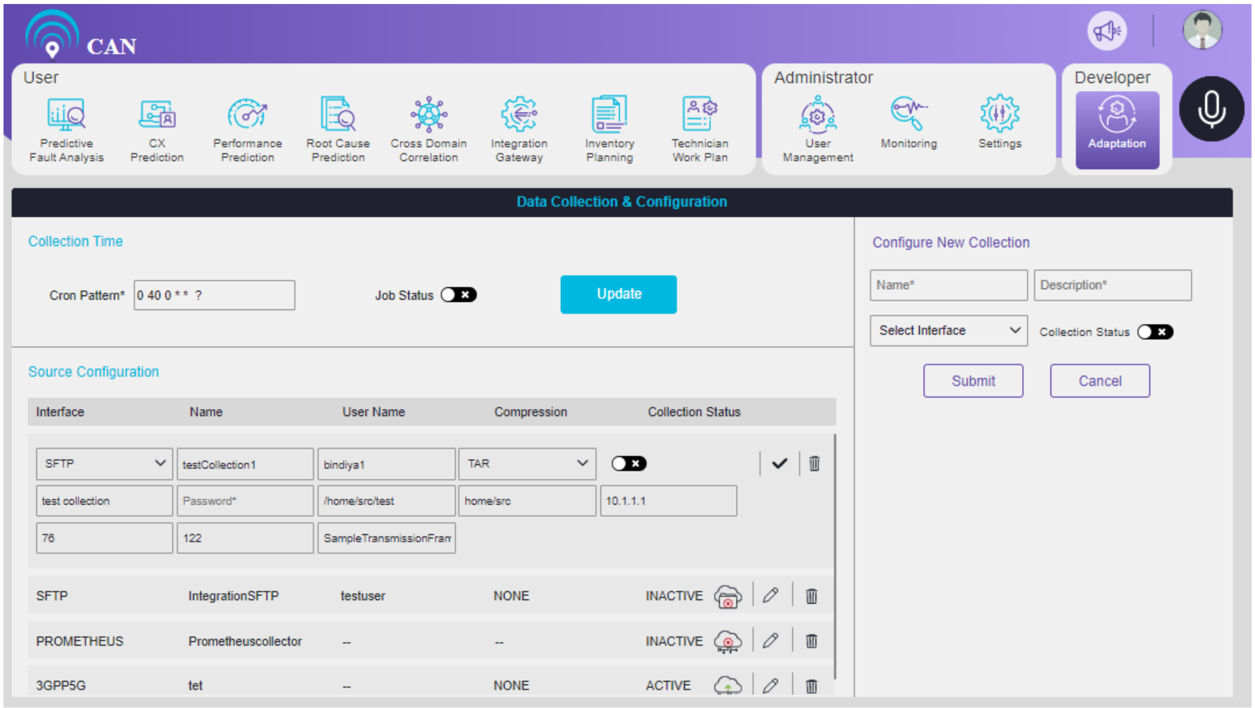
Submit

Cancel

Figure 15.19 - 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, Name, User Name, Compression and Collection Status 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 🗑 .



Collection Time

Cron Pattern* 0 40 0 * * ?

Job Status

Configure New Collection

Name*

Description*

Select Interface

Collection Status

Source Configuration

Interface	Name	User Name	Compression	Collection Status
SFTP	testCollection1	bindiya1	TAR	
test collection	Password*	/home/src/test	home/src	10.1.1.1
76	122	SampleTransmissionFram		
SFTP	IntegrationSFTP	testuser	NONE	INACTIVE
PROMETHEUS	Prometheuscollector	--	--	INACTIVE
3GPP5G	tet	--	NONE	ACTIVE

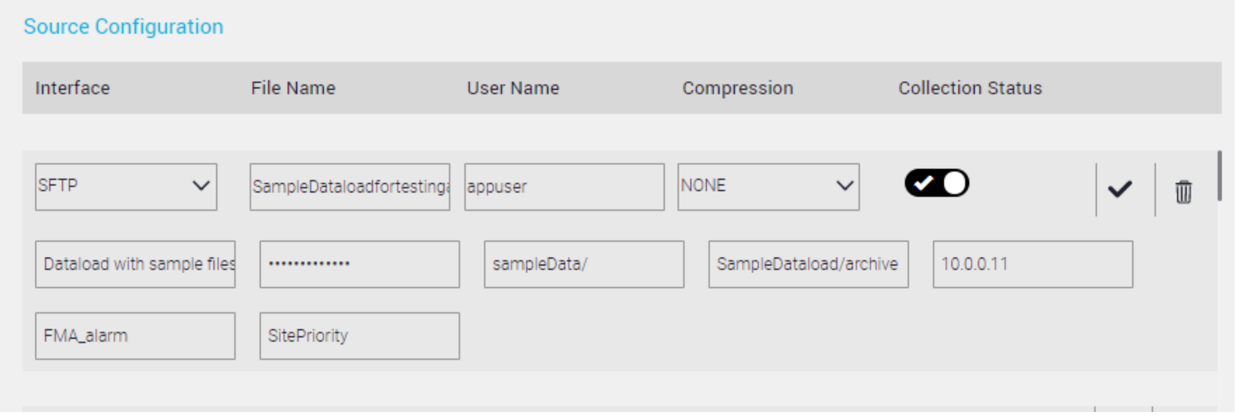
Figure 15.20 - Data Collection Configuration Edit Option

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, Z 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), port number (on which SFTP/FTP is running) and source archive folder path (relative path of archive folder on SFTP/FTP).



Source Configuration

Interface	File Name	User Name	Compression	Collection Status
SFTP	SampleDataloadfortesting	appuser	NONE	✓

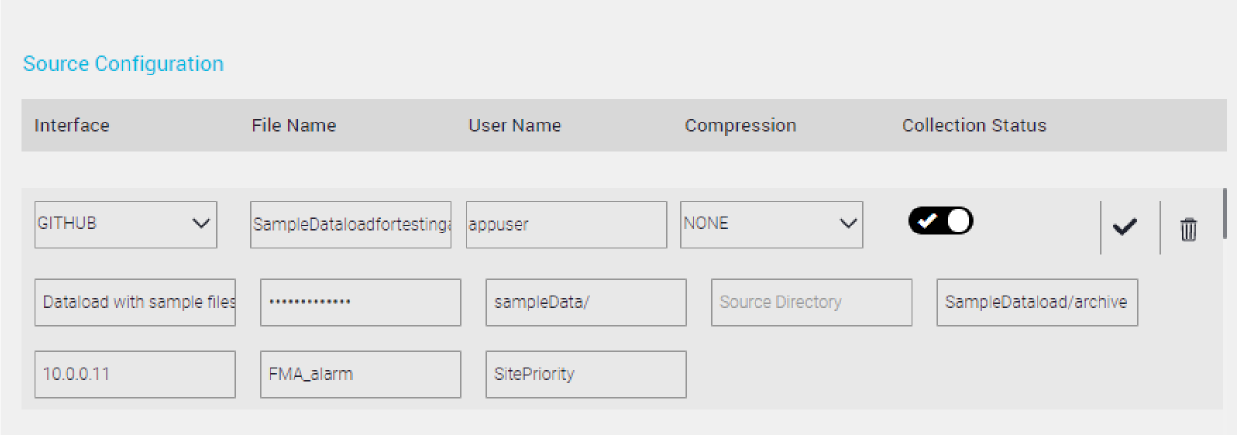
Dataload with sample files | ••••••••••••• | sampleData/ | SampleDataload/archive | 10.0.0.11

FMA_alarm | SitePriority

Figure 15.21 - 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 archival folder path (absolute path of archive folder on GITHUB) and source directory (location where git is cloned).



Source Configuration

Interface	File Name	User Name	Compression	Collection Status
GITHUB	SampleDataloadfortesting	appuser	NONE	✓

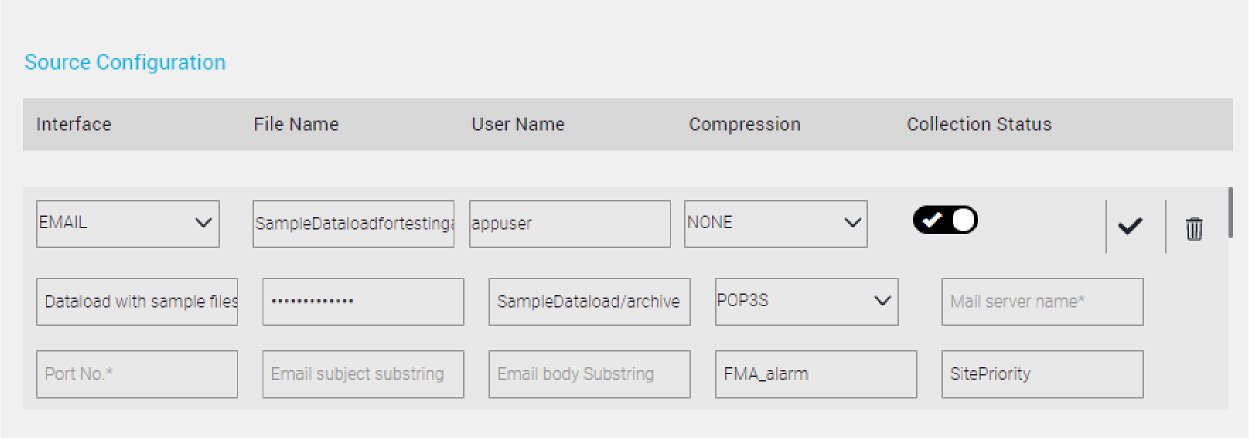
Dataload with sample files | ••••••••••••• | sampleData/ | Source Directory | SampleDataload/archive

10.0.0.11 | FMA_alarm | SitePriority

Figure 15.22 - 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) and Port number (email server port number). Instead of file name pattern, user must specify mail attachment (file) name pattern and search string for both email subject and body.



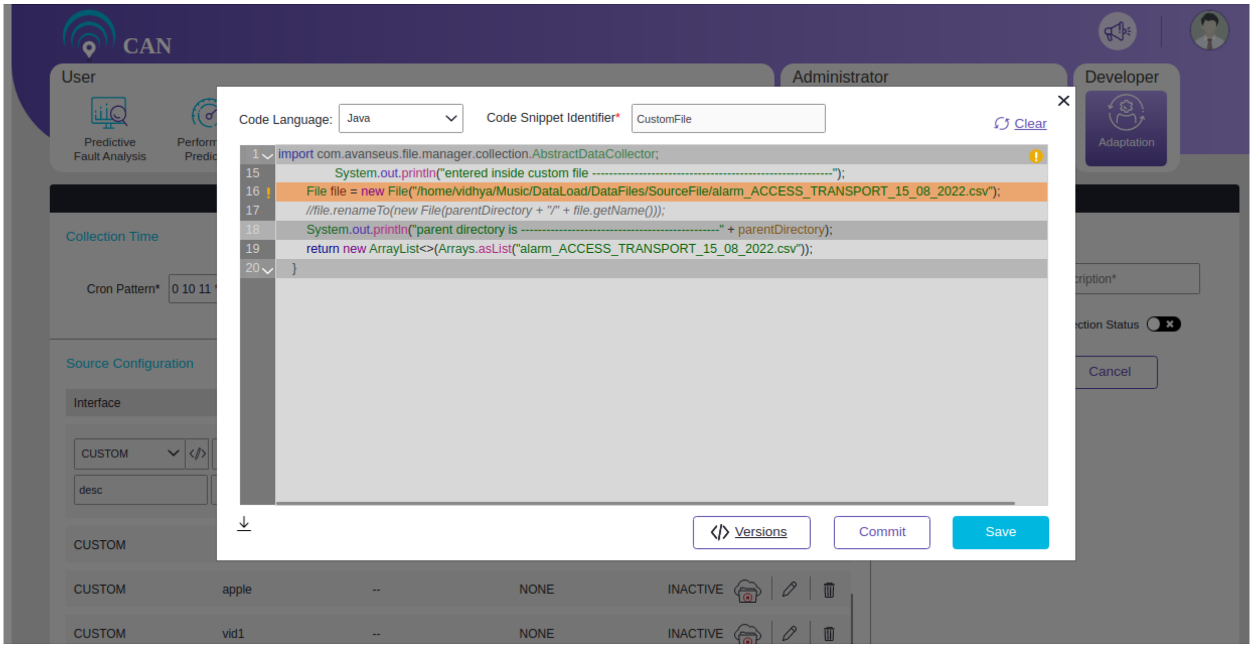
Source Configuration

Interface	File Name	User Name	Compression	Collection Status
EMAIL	SampleDataloadfortesting	appuser	NONE	✓
Dataload with sample files	•••••••••••••	SampleDataload/archive	POP3S	Mail server name*
Port No.*	Email subject substring	Email body Substring	FMA_alarm	SitePriority

Figure 15.23 - EMAIL Interface Configuration

CUSTOM

User can write code in Java or Python to specify a different data collection type apart from the listed interfaces.



Code Language: Java

Code Snippet Identifier* CustomFile

Clear

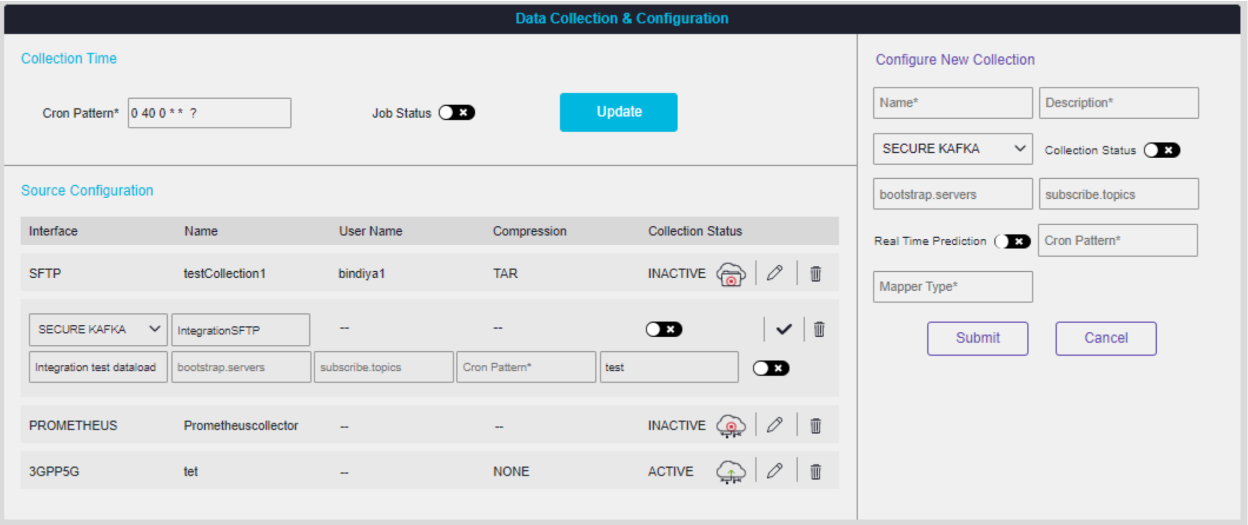
```
import com.avanseus.file.manager.collection.AbstractDataCollector;
            System.out.println("entered inside custom file ------------------------------------------------------------");
        File file = new File("/home/vidhya/Music/DataLoad/DataFiles/SourceFile/alarm_ACCESS_TRANSPORT_15_08_2022.csv");
        //file.renameTo(new File(parentDirectory + "/" + file.getName()));
        System.out.println("parent directory is -----------------------------------------------" + parentDirectory);
        return new ArrayList<>(Arrays.asList("alarm_ACCESS_TRANSPORT_15_08_2022.csv"));
    }
```

CUSTOM				
CUSTOM	apple	--	NONE	INACTIVE
CUSTOM	vid1	--	NONE	INACTIVE

Figure 15.24 - Custom Interface Configuration

SECURE KAFKA

In the Secure 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. User must specify cron for Real time prediction.



Data Collection & Configuration

Collection Time

Cron Pattern* 0 40 0 * * ?   Job Status   Update

Source Configuration

Interface	Name	User Name	Compression	Collection Status
SFTP	testCollection1	bindiya1	TAR	INACTIVE
SECURE KAFKA	IntegrationSFTP	--	--	
Integration test dataload	bootstrap.servers	subscribe.topics	Cron Pattern*	test
PROMETHEUS	Prometheuscollector	--	--	INACTIVE
3GPP5G	tet	--	NONE	ACTIVE

Configure New Collection

Name* | Description*

SECURE KAFKA | Collection Status

bootstrap.servers | subscribe.topics

Real Time Prediction | Cron Pattern*

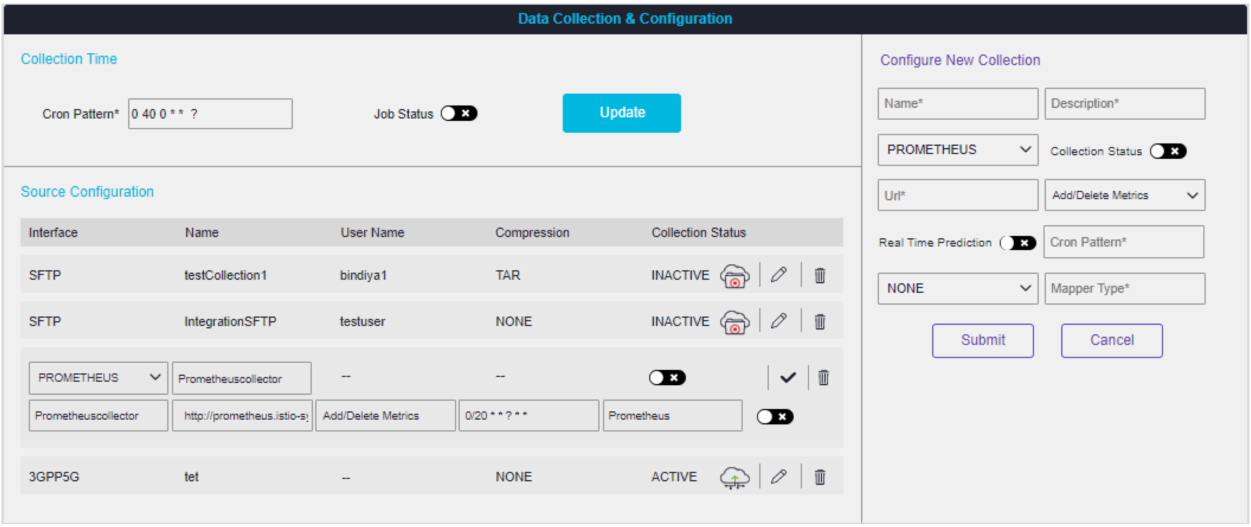
Mapper Type*

Submit   Cancel

Figure 15.25 – Secure Kafka Interface Configuration

PROMETHEUS

In the Prometheus interface, apart from above mentioned fields, user must specify Url (URL of Prometheus where data is extracted), Add/Delete metrics (select the required parameters from the list of metrics) and cron for Real time prediction.



Data Collection & Configuration

Collection Time

Cron Pattern* 0 40 0 * * ?   Job Status   Update

Source Configuration

Interface	Name	User Name	Compression	Collection Status
SFTP	testCollection1	bindiya1	TAR	INACTIVE
SFTP	IntegrationSFTP	testuser	NONE	INACTIVE
PROMETHEUS	Prometheuscollector	--	--	
Prometheuscollector	http://prometheus.istio-sy	Add/Delete Metrics	0/20 * * ? * *	Prometheus
3GPP5G	tet	--	NONE	ACTIVE

Configure New Collection

Name* | Description*

PROMETHEUS | Collection Status

Url* | Add/Delete Metrics

Real Time Prediction | Cron Pattern*

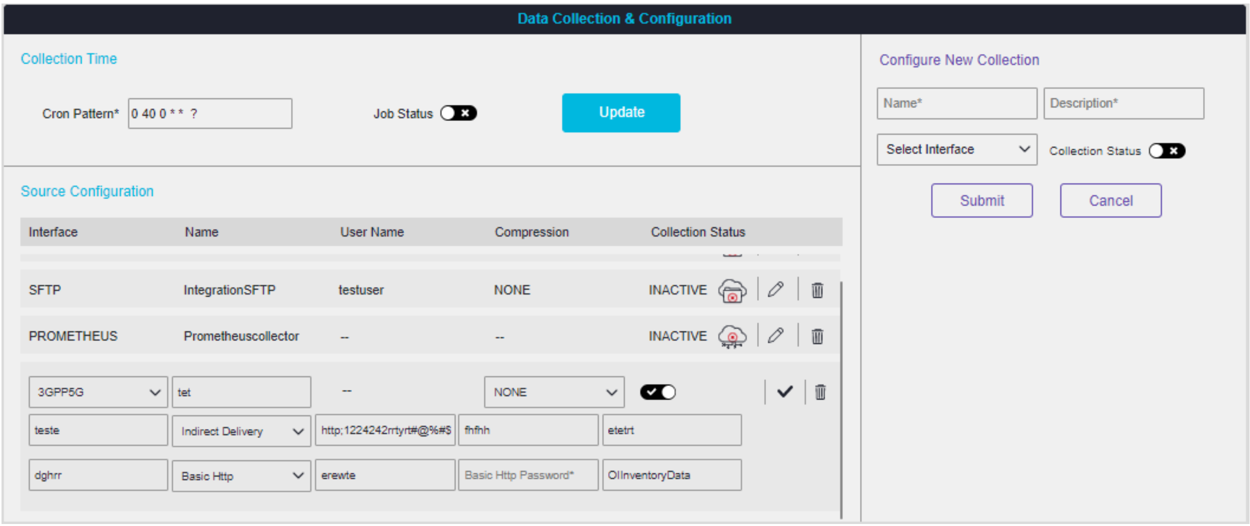
NONE | Mapper Type*

Submit   Cancel

Figure 15.26 - Prometheus Interface Configuration

3GPP5G

In the 3GPP5G interface, apart from above mentioned fields, user must specify configuration type (Direct delivery, Indirect delivery, Http server push), URL, Authentication type, Authentication username, Authentication password, Form parameters (payload of an HTTP request), Query parameters (query component in the URL), Complex query (logical combination of multiple query parameters) and Complex operation.


Data Collection & Configuration

Collection Time

Cron Pattern* 0 40 0 * * ?

Job Status

Source Configuration

Interface	Name	User Name	Compression	Collection Status
SFTP	IntegrationSFTP	testuser	NONE	INACTIVE
PROMETHEUS	Prometheuscollector	--	--	INACTIVE
3GPP5G	tet	--	NONE	

teste	Indirect Delivery	http;1224242rrtyrt#@%#$	fhfhh	etetrt
dghrr	Basic Http	erewte	Basic Http Password*	OIInventoryData

Configure New Collection

Name* Description*

Select Interface

Collection Status

Figure 15.27 - 3GPP5G Interface Configuration

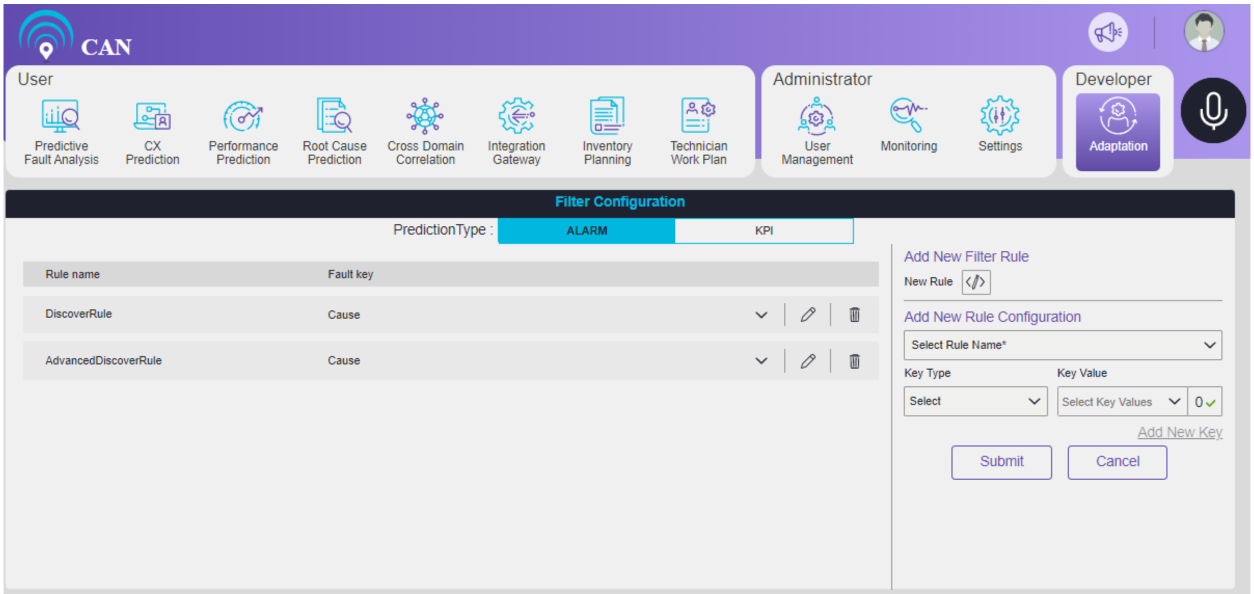
Filter Configuration

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:

1. Generation of initial set of predicted faults
2. Generation of final set of predicted faults.

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

ALARM



Filter Configuration

PredictionType : ALARM KPI

Rule name	Fault key
DiscoverRule	Cause
AdvancedDiscoverRule	Cause

Add New Filter Rule

New Rule

Add New Rule Configuration

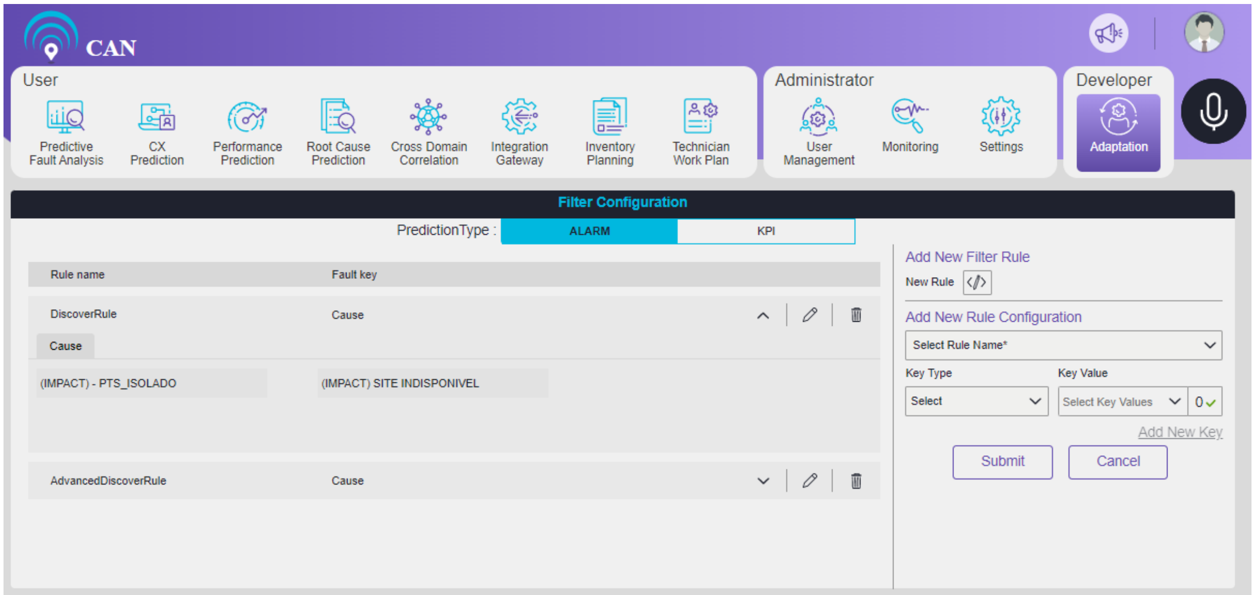
Select Rule Name*

Key Type: Select

Key Value: Select Key Values 0

Figure 15.28 - Filter Configuration Homepage

Click more icon ⌄ to view configuration details.



Filter Configuration

PredictionType : ALARM KPI

Rule name	Fault key
DiscoverRule	Cause
Cause	
(IMPACT) - PTS_ISOLADO	(IMPACT) SITE INDISPONIVEL
AdvancedDiscoverRule	Cause

Add New Filter Rule

New Rule

Add New Rule Configuration

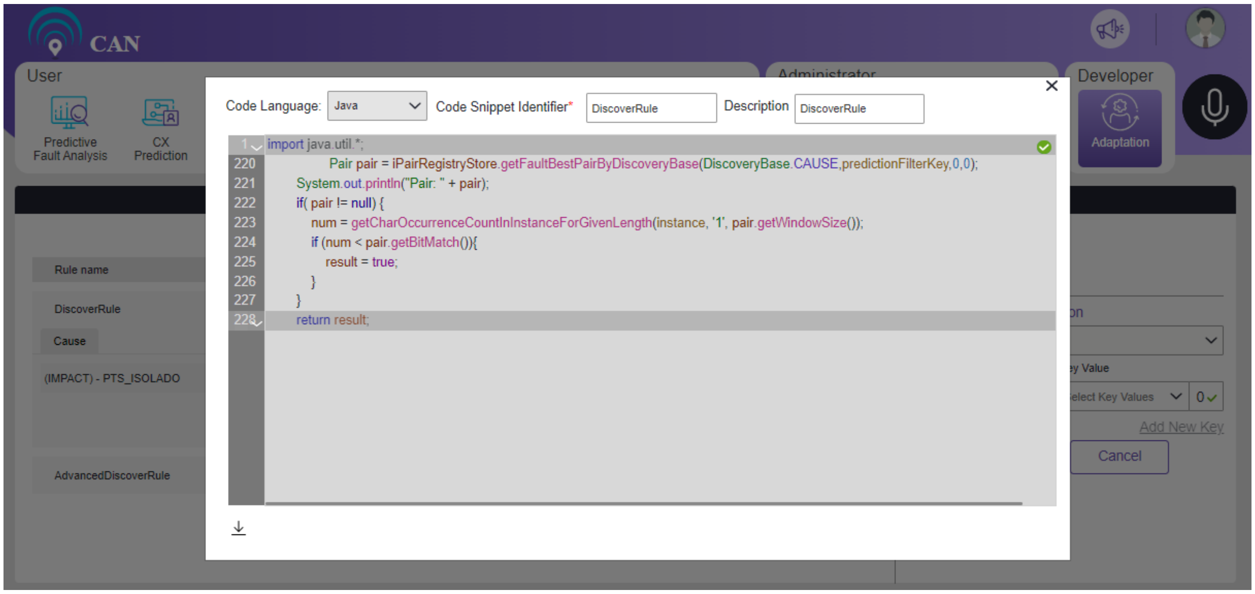
Select Rule Name*

Key Type: Select

Key Value: Select Key Values 0

Figure 15.29 - Configuration Details

Click on **Rule name** to view the rule code snippet. To download the rule, click the Download icon ⤓.



Code Language: Java

Code Snippet Identifier*: DiscoverRule

Description: DiscoverRule

```
import java.util.*;
            Pair pair = iPairRegistryStore.getFaultBestPairByDiscoveryBase(DiscoveryBase.CAUSE,predictionFilterKey,0,0);
        System.out.println("Pair: " + pair);
        if( pair != null) {
            num = getCharOccurrenceCountInInstanceForGivenLength(instance, '1', pair.getWindowSize());
            if (num < pair.getBitMatch()){
                result = true;
            }
        }
        return result;
```

Figure 15.30 - Rule Code Snippet

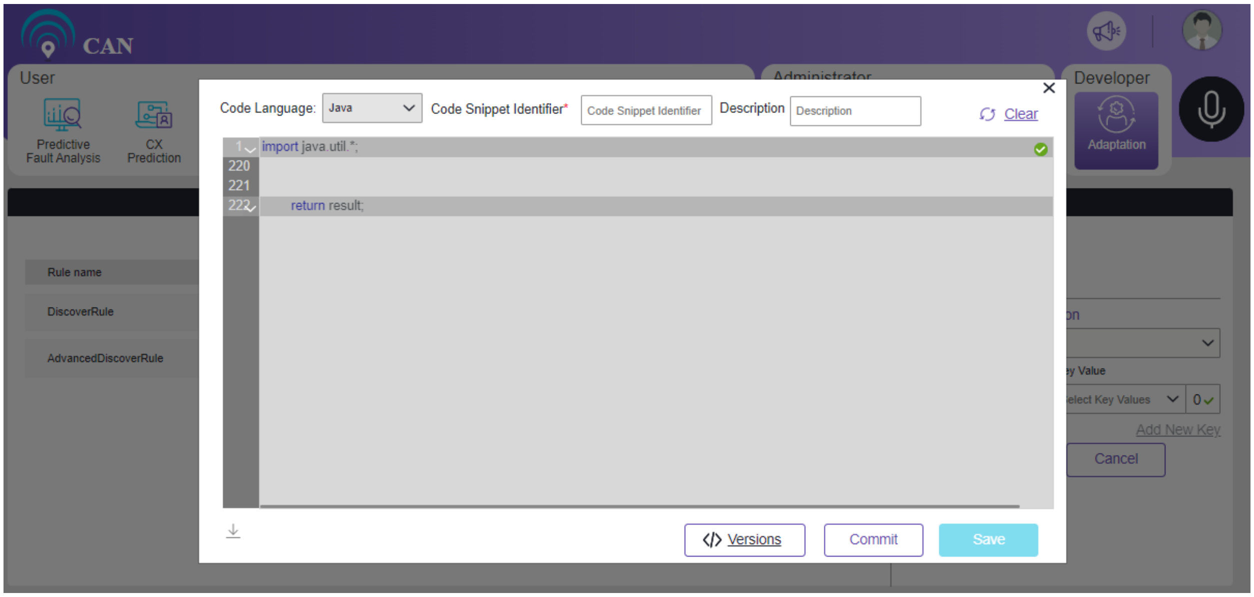
To Add New Filter Rule

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⤓.

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 be 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 do not want to add the New Rule.



```
import java.util.*;


    return result;
```

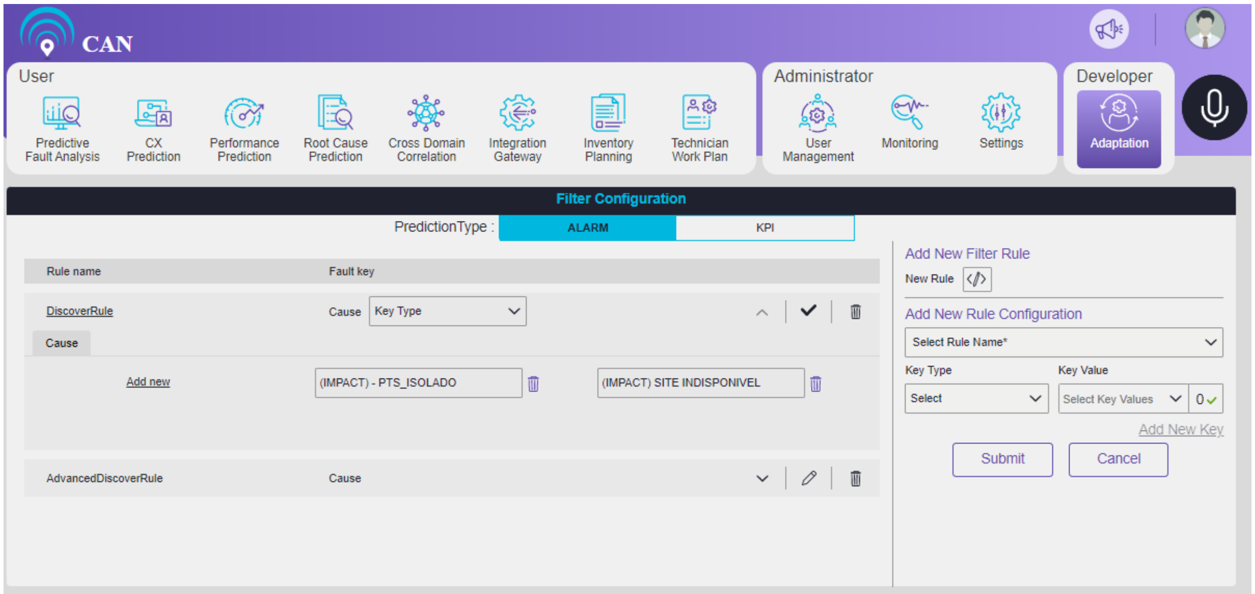
Figure 15.31 - Create Predicted Fault Filtration Rules

To Edit the Existing Rule Configuration

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.
3. Update the code and click **Update**.
4. User can click the clear option to delete the existing code.
5. User can also download the Rule java/python file. Click the **Download** icon ⤓ to download the Rule java/python file.
6. Click the **Close** button to close the screen.
7. Select the **Key Type** from the drop down to add the new fault key. User can add multiple Key types at a time.
8. Click **Add New option** to add new input box to select Key Value from the dropdown.

Note: After addition of New Option “Add New” option will be disabled. Once you select the Key Value from the drop down Add New option will re-enable.

9. Click the **Delete** icon to delete the Key Value.
10. Click the **Update** icon ✓ to save the changes.
11. Click the delete 🗑 icon to delete the existing Rule.



Filter Configuration

PredictionType : ALARM | KPI

Rule name	Fault key
DiscoverRule	Cause: Key Type
AdvancedDiscoverRule	Cause

Cause: Add new — (IMPACT) - PTS_ISOLADO — (IMPACT) SITE INDISPONIVEL

Add New Filter Rule

New Rule

Add New Rule Configuration

Select Rule Name*

Key Type: Select

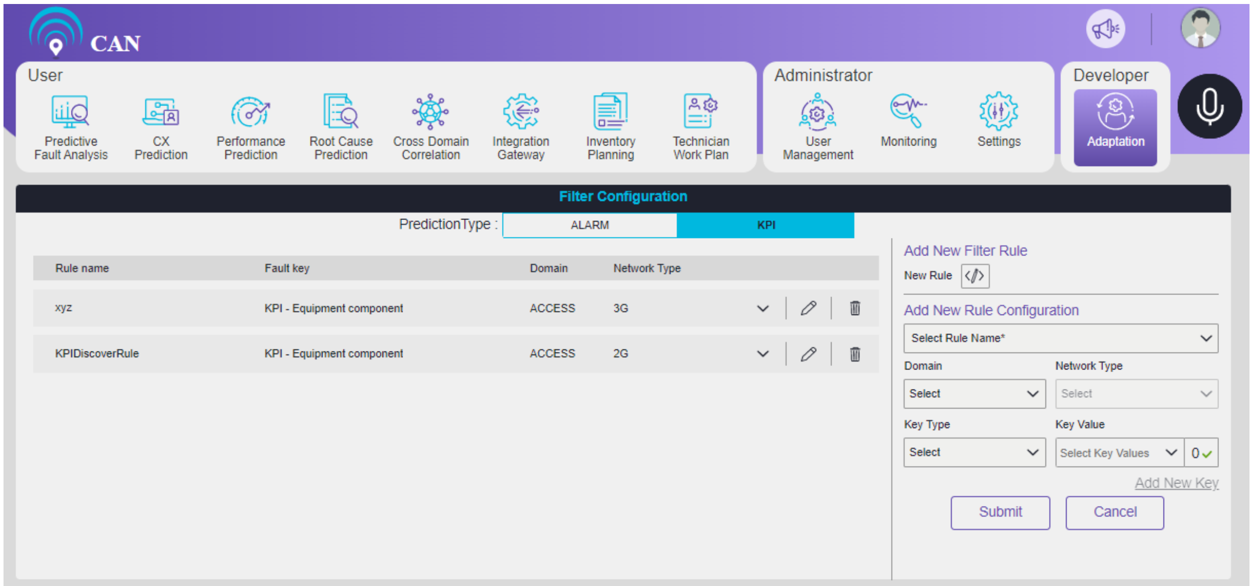
Key Value: Select Key Values 0

Add New Key

Submit Cancel

Figure 15.32 - Modifying Predicted Fault Filtration Rules for Alarm

KPI



Filter Configuration

PredictionType : ALARM | KPI

Rule name	Fault key	Domain	Network Type
xyz	KPI - Equipment component	ACCESS	3G
KPIDiscoverRule	KPI - Equipment component	ACCESS	2G

Add New Filter Rule

New Rule

Add New Rule Configuration

Select Rule Name*

Domain: Select

Network Type: Select

Key Type: Select

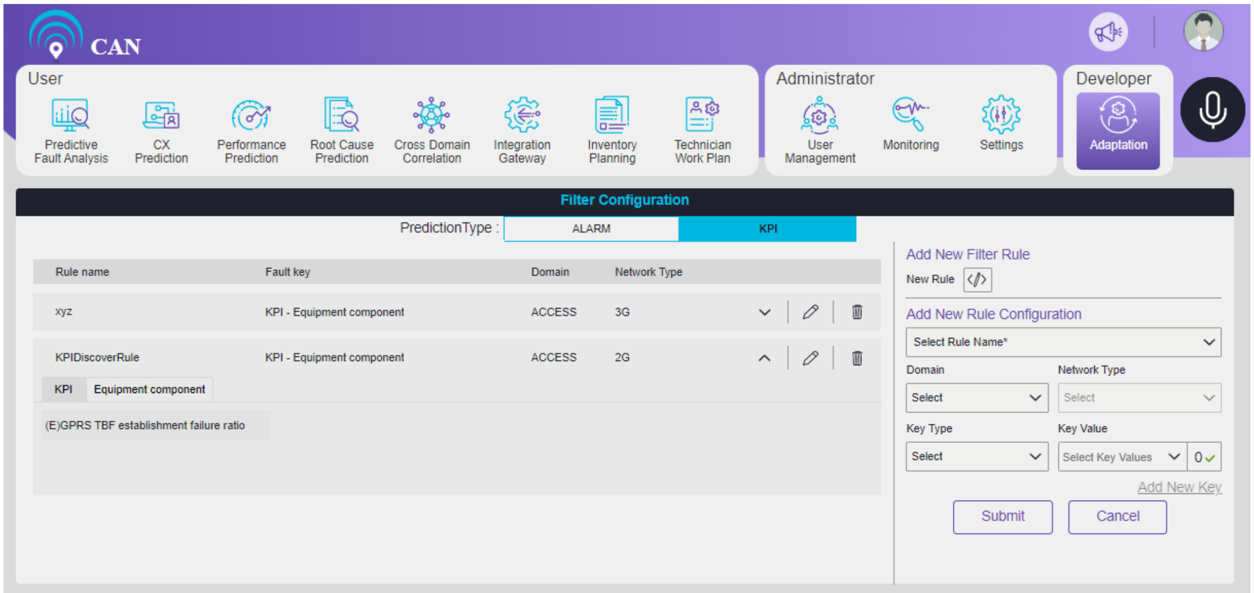
Key Value: Select Key Values 0

Add New Key

Submit Cancel

Figure 15.33 - Filter Configuration Homepage - KPI

Click more icon ⌄ to view configuration details.



PredictionType : ALARM | KPI

Rule name	Fault key	Domain	Network Type
xyz	KPI - Equipment component	ACCESS	3G
KPIDiscoverRule	KPI - Equipment component	ACCESS	2G

KPI | Equipment component

(E)GPRS TBF establishment failure ratio

Select Rule Name*

Domain: Select

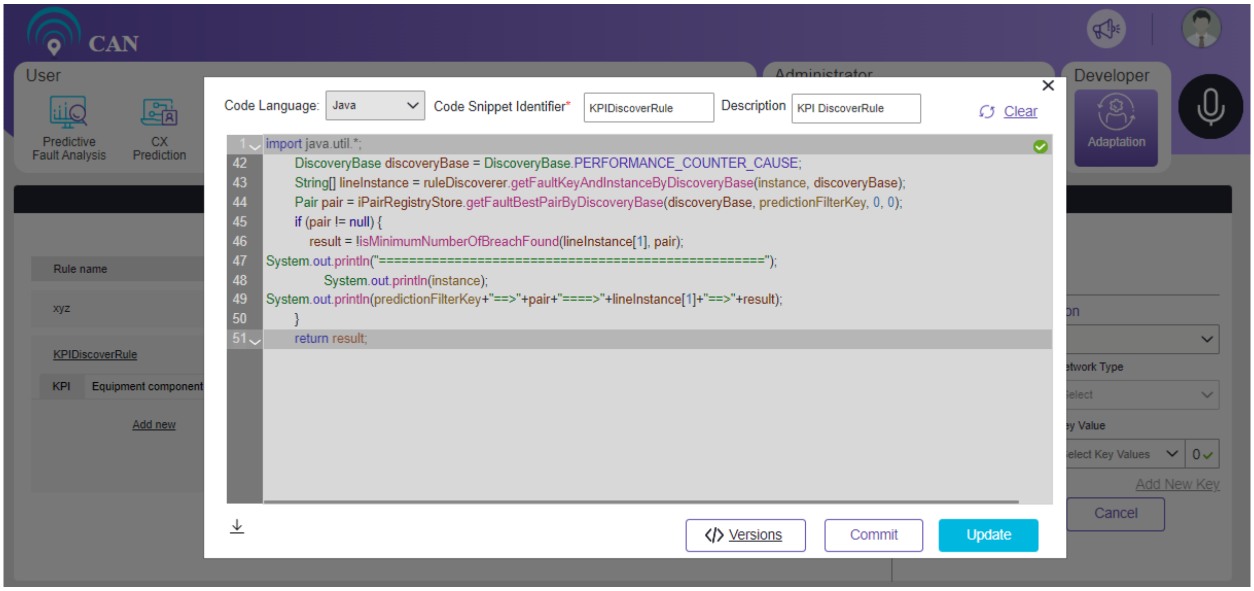
Network Type: Select

Key Type: Select

Key Value: Select Key Values 0

Figure 15.34 - KPI Configuration Details

Click on **Rule name** to view the rule code snippet. To download the rule, click the Download icon⤓.



Code Language: Java

Code Snippet Identifier*: KPIDiscoverRule

Description: KPI DiscoverRule

```
import java.util.*;
    DiscoveryBase discoveryBase = DiscoveryBase.PERFORMANCE_COUNTER_CAUSE;
    String[] lineInstance = ruleDiscoverer.getFaultKeyAndInstanceByDiscoveryBase(instance, discoveryBase);
    Pair pair = iPairRegistryStore.getFaultBestPairByDiscoveryBase(discoveryBase, predictionFilterKey, 0, 0);
    if (pair != null) {
      result = !isMinimumNumberOfBreachFound(lineInstance[1], pair);
System.out.println("=================================================");
        System.out.println(instance);
System.out.println(predictionFilterKey+"==>"+pair+"====>"+lineInstance[1]+"==>"+result);
    }
    return result;
```

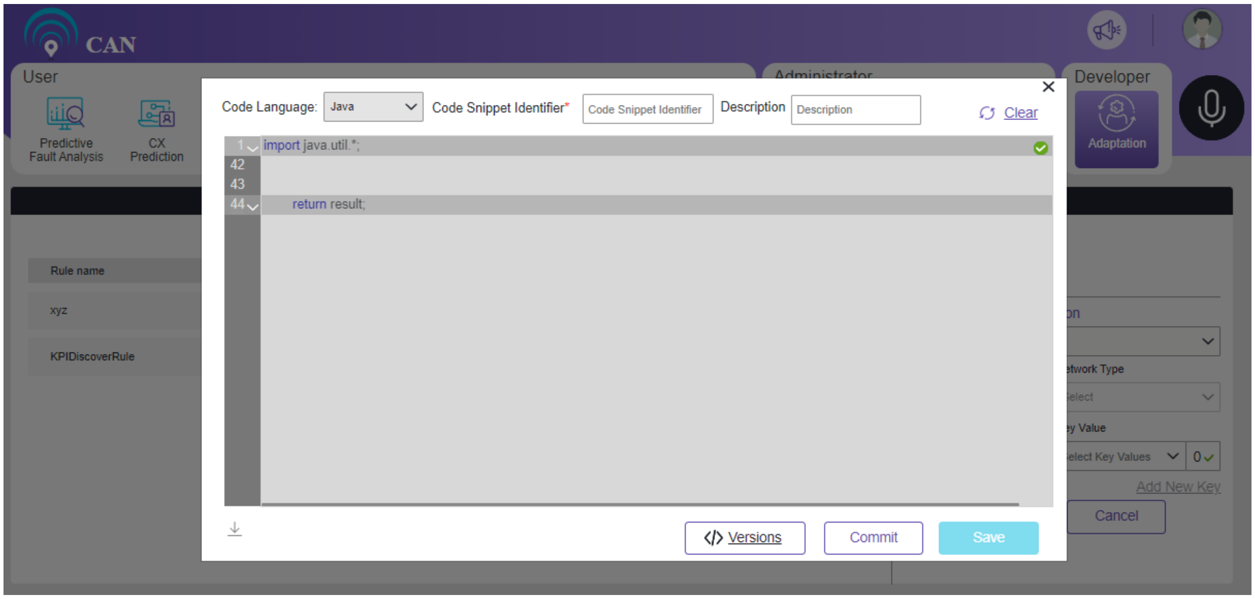
Figure 15.35 - Rule Code Snippet

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⤓.

To Add New Rule Configuration for Predicted Fault Filtration

1. Select the **Rule Name** from the drop down.
2. Select the **Domain** from the drop down.
3. Select the **Network Type** from the drop down.
4. Select the **Key type** from the drop down.
5. Select the **Key value** from the drop down.
6. After selection of Key value, **Add New Key** will be activated.
7. Click **Add New Key** to add multiple Key Type and Key Value.
8. Click **Submit** to add the New Rule for Filter Configuration.
9. Click **Cancel** if you do not want to add the New Rule.



Code Language: Java

Code Snippet Identifier*: Code Snippet Identifier

Description: Description

Select Key Values 0

```
import java.util.*;


    return result;
```

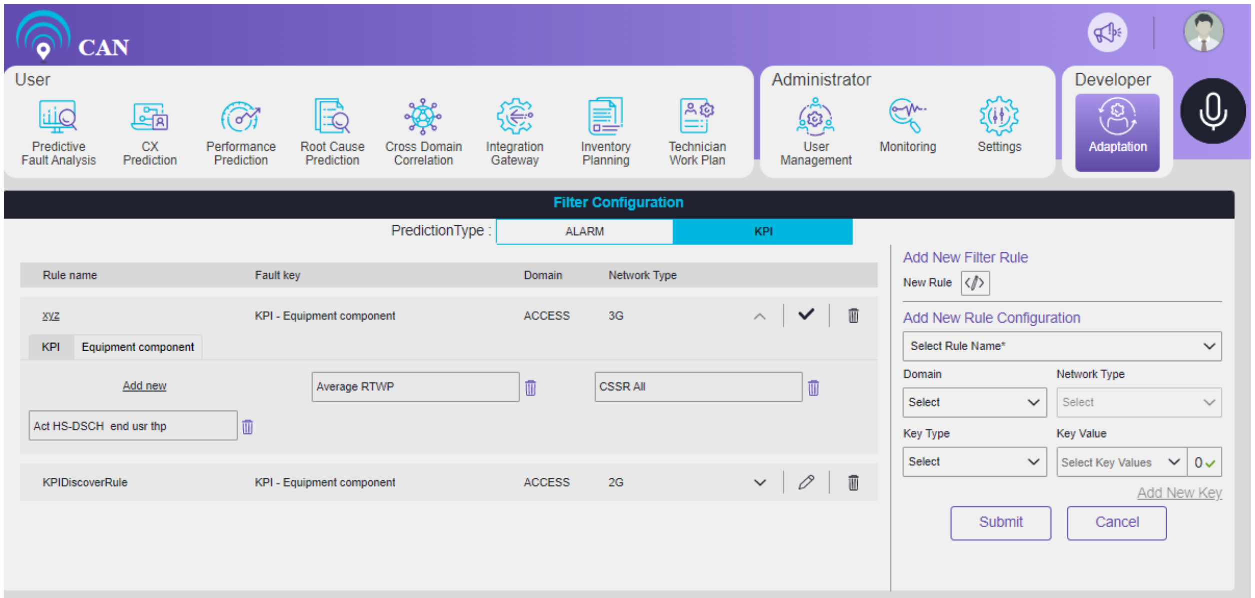
Figure 15.36 - Create Predicted Fault Filtration Rules for KPI

To Edit the Existing Rule Configuration

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.
3. Update the code and click **Update**.
4. User can click the clear option to delete the existing code.
5. User can also download the Rule java/python file. Click the **Download** icon ⤓ to download the Rule java/python file.
6. Click the **Close** button to close the screen.
7. Select the **Key Type** from the drop down to add the new fault key. User can add multiple Key types at a time.
8. Click **Add New option** to add new input box to select Key Value from the dropdown.

Note: After addition of New Option “Add New” option will be disabled. Once you select the Key Value from the drop down Add New option will re-enable.

9. Click the **Delete** icon to delete the Key Value.
10. Click the **Update** icon ✓ to save the changes.
11. Click the delete 🗑 icon to delete the existing Rule.



Filter Configuration

PredictionType : ALARM | KPI

Rule name	Fault key	Domain	Network Type
xyz	KPI - Equipment component	ACCESS	3G
KPIDiscoverRule	KPI - Equipment component	ACCESS	2G

KPI: Equipment component

Add new

Average RTWP

CSSR All

Act HS-DSCH end usr thp

Add New Filter Rule

New Rule

Add New Rule Configuration

Select Rule Name*

Domain: Select

Network Type: Select

Key Type: Select

Key Value: Select Key Values 0

Add New Key

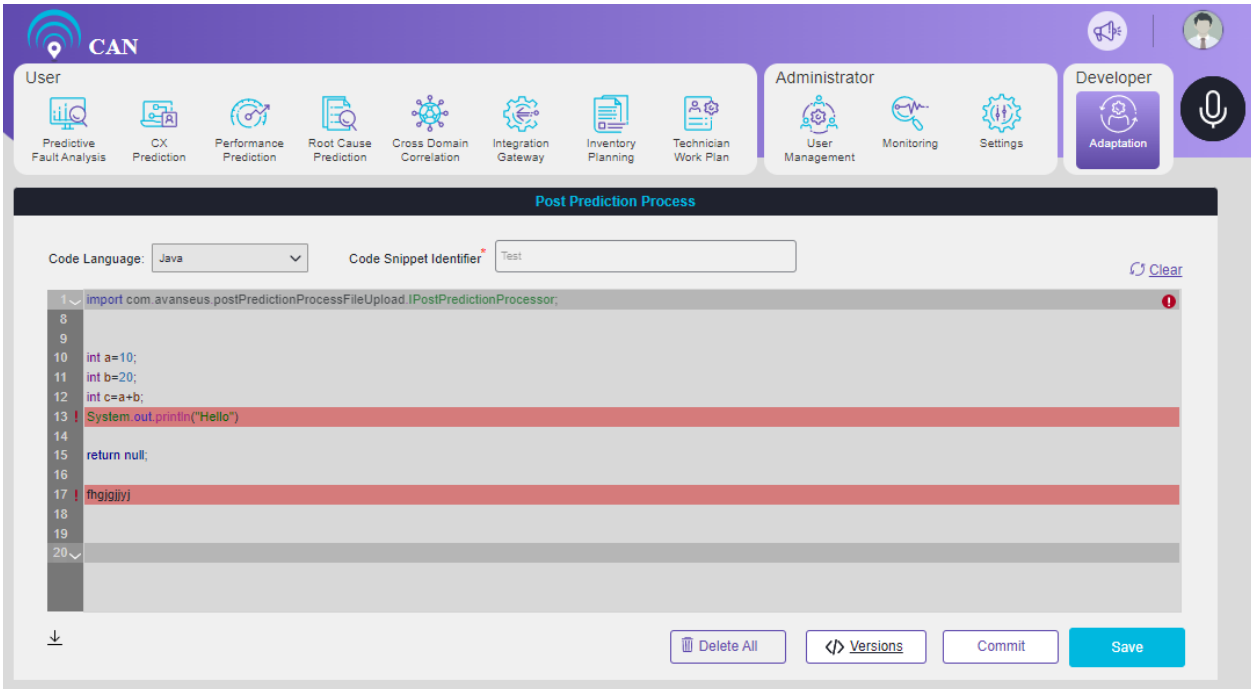
Submit | Cancel

Figure 15.37 - Modifying Predicted Fault Filtration Rules for KPI

Post Prediction Process

CAN supports IDE at the input data parsing stage before prediction. Users can use programming codes in java or python to customize the input data parsing. IDE can perform a variety of functions like write code, compile code, and debug code.

User needs to write a code to enrich predicted information with customized data. This file should implement **IPostPredictionProcess**.



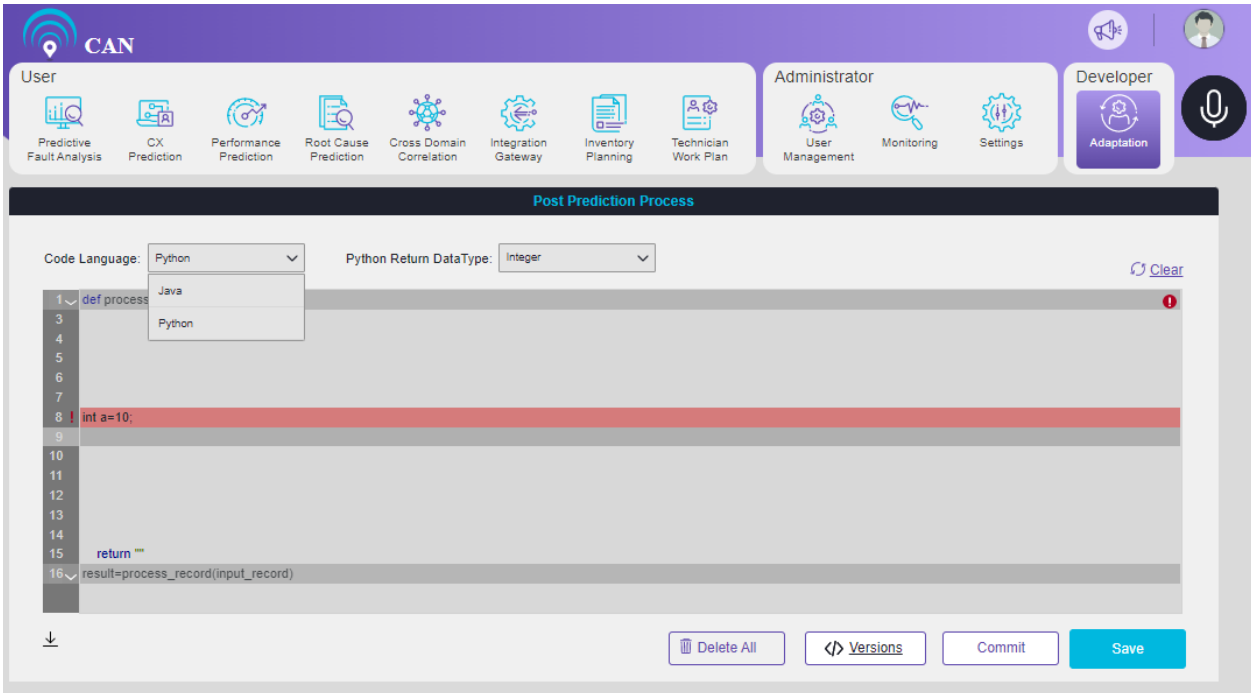
Code Language: Java

Code Snippet Identifier*: Test

```
import com.avanseus.postPredictionProcessFileUpload.IPostPredictionProcessor;


int a=10;
int b=20;
int c=a+b;
System.out.println("Hello")

return null;

fhgjgjjyj
```

Figure 15.38 - Post Prediction Process

User can write the java or python code. User can select the **Code Language** and **Return DataType** from the drop down.



Code Language: Python

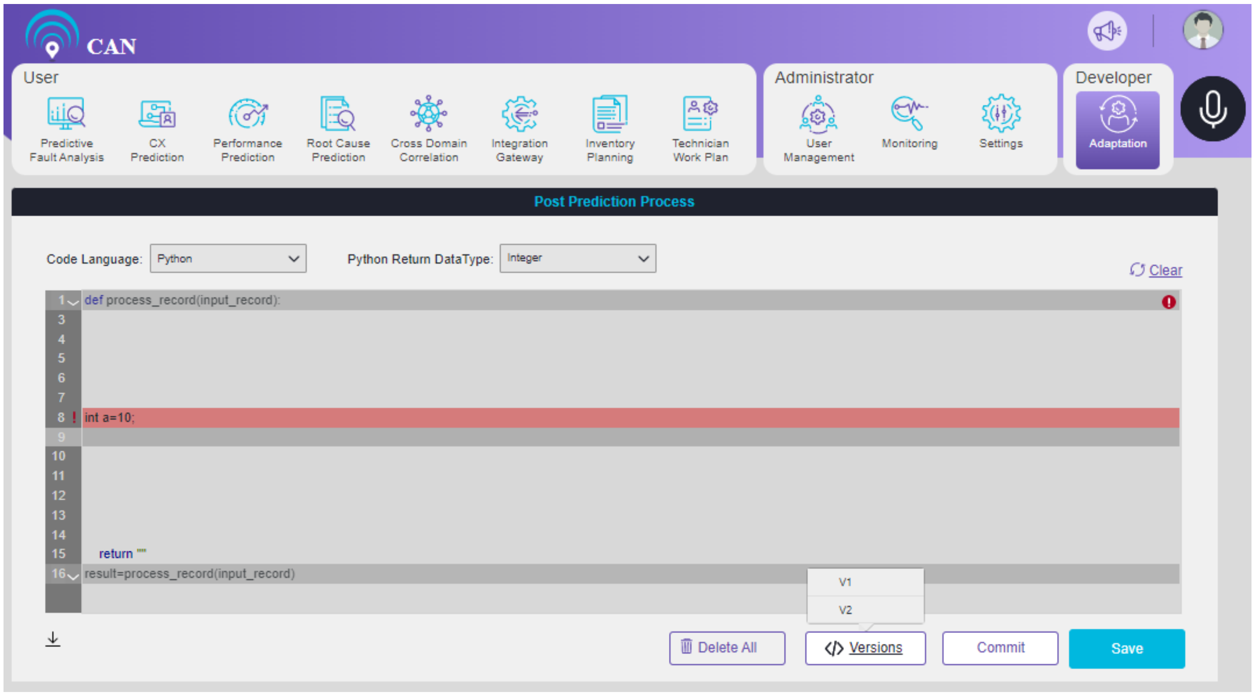
Python Return DataType: Integer

```
def process






int a=10;






    return ""
result=process_record(input_record)
```

Figure 15.39 – Code Language Selection

Click on **Commit** button to save this version of file.

User can write and save multiple versions of code and use them as and when required. To select the version, click on **Versions** button.



Code Language: Python

Python Return DataType: Integer

```
def process_record(input_record):






int a=10;






    return ""
result=process_record(input_record)
```

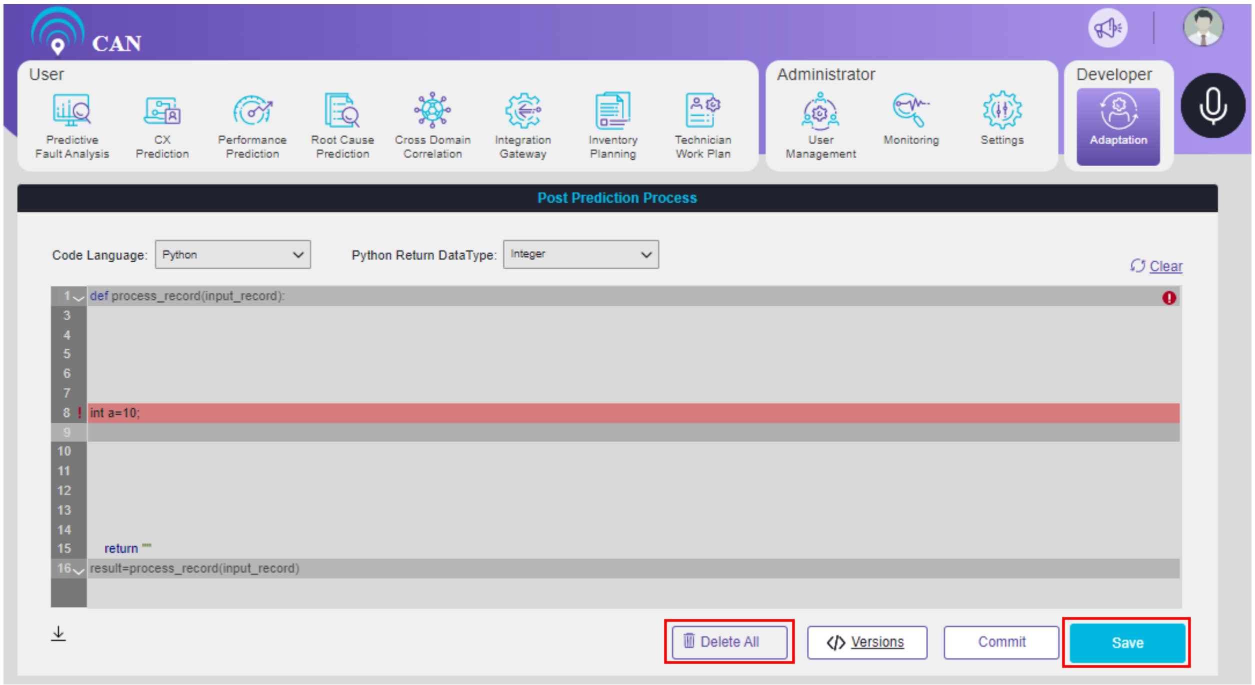
Figure 15.40 - Version Selection

User can **Save** a file, only if the code is error free.

User can download the java/python file. To download the file, click the download icon ⤓.

To delete a particular java/python file, click the clear icon Clear.

To delete all the versions of code, click on **Delete All** button.



Post Prediction Process

Code Language: Python

Python Return DataType: Integer

```
def process_record(input_record):



int a=10;





    return ""
result=process_record(input_record)
```

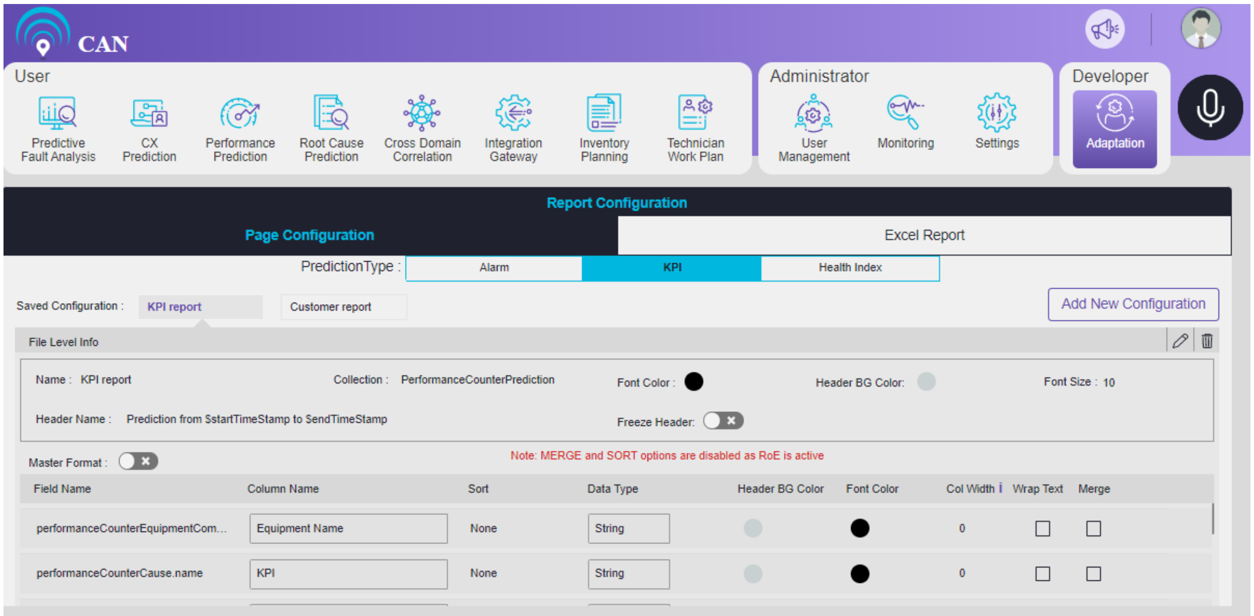
Figure 15.41 - File Delete/Save

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 two configurations under this:

1. Page Configuration
2. Excel Report



Report Configuration

PredictionType : KPI

Saved Configuration : KPI report | Customer report

File Level Info

Name : KPI report

Collection : PerformanceCounterPrediction

Font Color : ●

Header BG Color: ●

Font Size : 10

Header Name : Prediction from $startTimeStamp to $endTimeStamp

Freeze Header: ✖

Master Format : ✖

Note: MERGE and SORT options are disabled as RoE is active

Field Name	Column Name	Sort	Data Type	Header BG Color	Font Color	Col Width	Wrap Text	Merge
performanceCounterEquipmentCom...	Equipment Name	None	String	●	●	0	□	□
performanceCounterCause.name	KPI	None	String	●	●	0	□	□

Figure 15.42 - Existing Page Configuration

Page Configuration

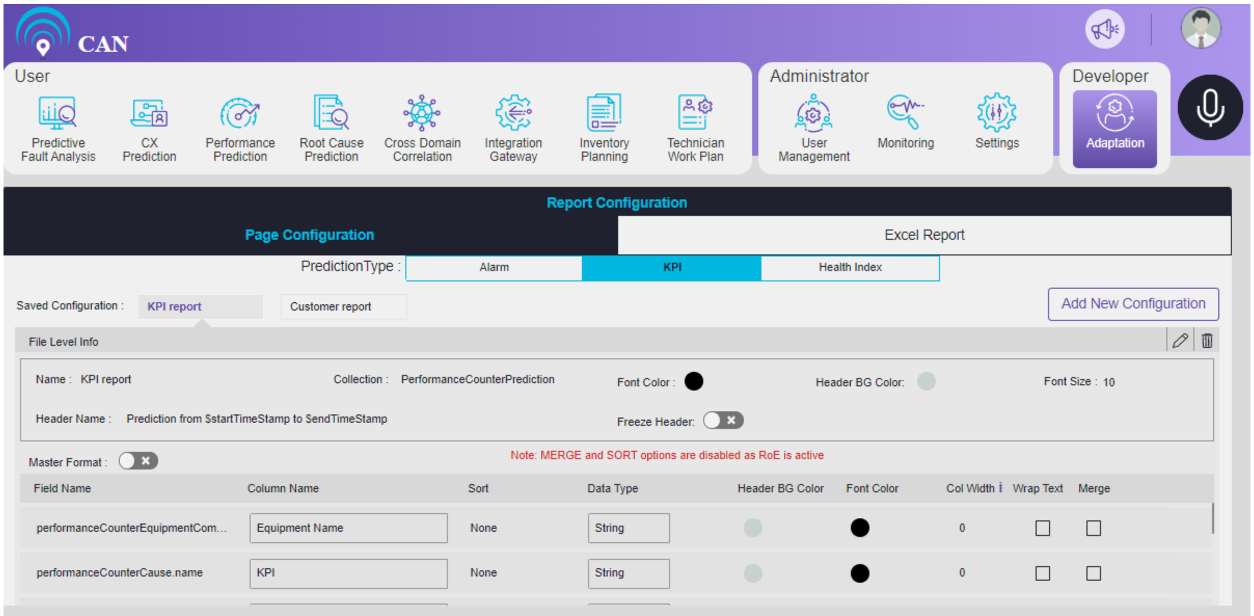
Page Configuration screen has configured all the Columns that are required to appear in every sheet of a prediction report and are customizable. It allows user to set excel sheet formats and excel sheet styles accordingly.

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.
5. 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
6. User can configure few other parameters to set each column of the prediction report. The parameters are as follows:
7. Field Name - Name of the field as it is in prediction result table i.e. Predicted Fault table as per CAN convention.
8. Column Name - Name of the column which user wishes to see in report.
9. Sort - Column values can be sorted as Ascending, Descending and None.
10. Data Type - Select the Data formats like String, Number, Percent, Complex and Drop down. If user selects the complex data type, Code Snippet popup (which is similar in functionality with respect to parser screen) appears.
11. Header BG Color - User can decide background color for column header.
12. Font Color - User can decide font color for column values.
13. Column Width - Sets width of column, here value 0 indicates auto resizing of column.
14. Wrap Text - If checked, text contents of each cell in that column will be wrapped.
15. Merge - Allows multiple adjacent cells to be combined into a single larger cell when values are similar.
16. Delete - User can delete a column.
17. 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.
18. 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.
19. If any of the pre-existing configuration is not required, click the delete icon🗑.



PredictionType : Alarm | KPI | Health Index

Saved Configuration : KPI report | Customer report

File Level Info

Name : KPI report   Collection : PerformanceCounterPrediction   Font Color : ●   Header BG Color: ●   Font Size : 10

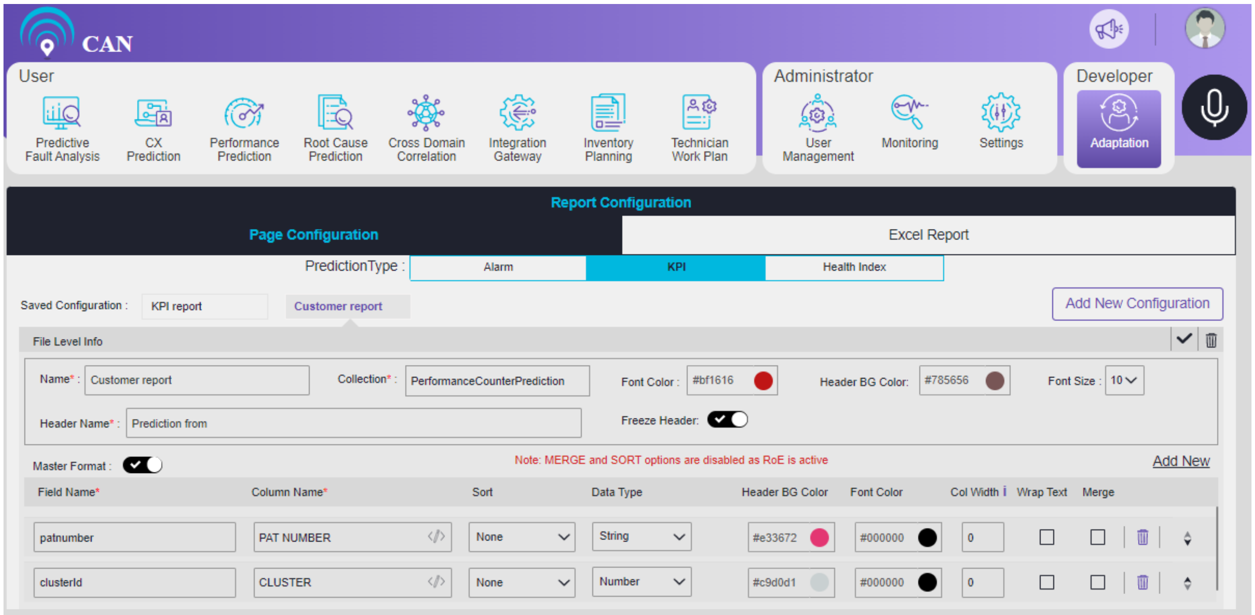
Header Name : Prediction from $startTimeStamp to $endTimeStamp   Freeze Header:

Master Format :

Note: MERGE and SORT options are disabled as RoE is active

Field Name	Column Name	Sort	Data Type	Header BG Color	Font Color	Col Width	Wrap Text	Merge
performanceCounterEquipmentCom...	Equipment Name	None	String	●	●	0	□	□
performanceCounterCause.name	KPI	None	String	●	●	0	□	□

Figure 15.43 - Existing Page Configuration



PredictionType : Alarm | KPI | Health Index

Saved Configuration : KPI report | Customer report

File Level Info

Name* : Customer report   Collection* : PerformanceCounterPrediction   Font Color : #bf1616 ●   Header BG Color: #785656 ●   Font Size : 10

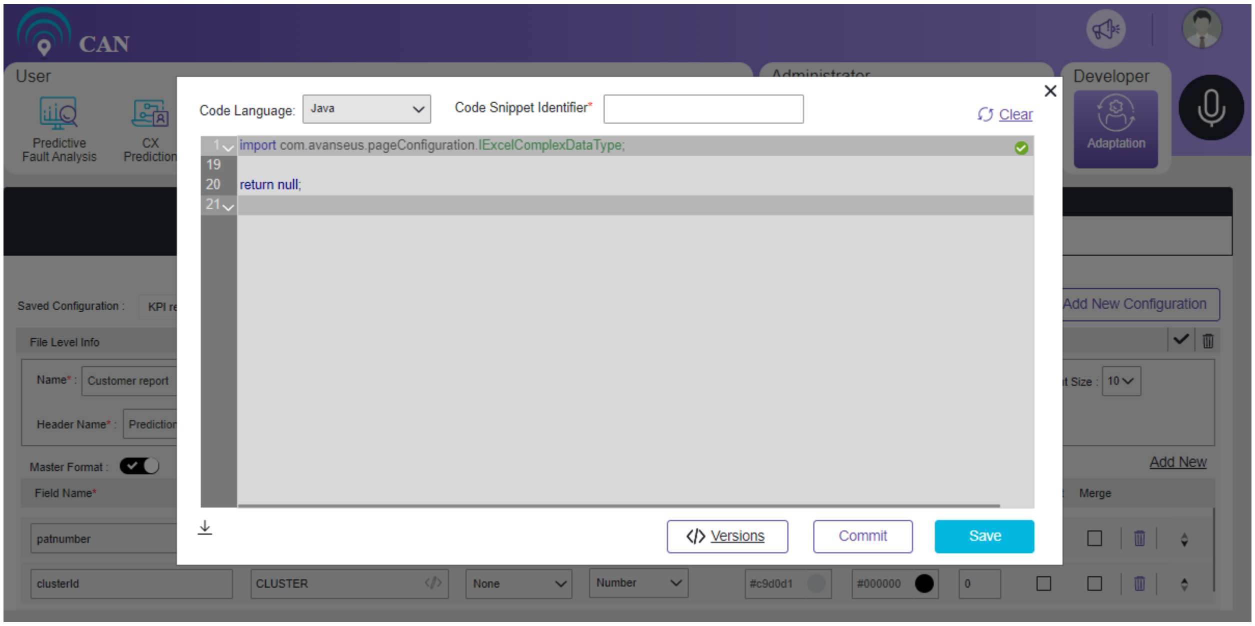
Header Name* : Prediction from   Freeze Header: ✓

Master Format : ✓

Note: MERGE and SORT options are disabled as RoE is active

Field Name*	Column Name*	Sort	Data Type	Header BG Color	Font Color	Col Width	Wrap Text	Merge
patnumber	PAT NUMBER	None	String	#e33672 ●	#000000 ●	0	□	□
clusterId	CLUSTER	None	Number	#c9d0d1 ●	#000000 ●	0	□	□

Figure 15.44 - Create New Page Configuration



Code Language: Java

Code Snippet Identifier*

```
import com.avanseus.pageConfiguration.IExcelComplexDataType;

return null;
```

Saved Configuration : KPI re

File Level Info

Name* : Customer report

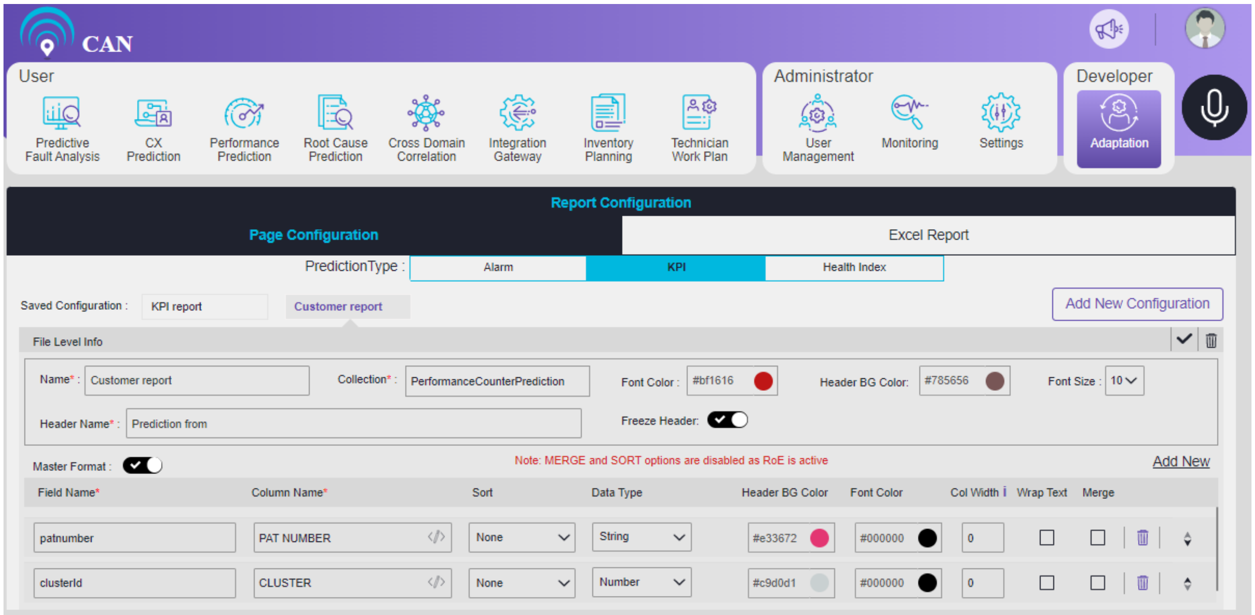
Header Name* : Prediction

Master Format :

Field Name*								Merge
patnumber								□
clusterId	CLUSTER	None	Number	#c9d0d1	#000000	0	□	□

Figure 15.45 - 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.



PredictionType : KPI

Saved Configuration : KPI report | Customer report

File Level Info

Name* : Customer report

Collection* : PerformanceCounterPrediction

Font Color : #bf1616

Header BG Color: #785656

Font Size : 10

Header Name* : Prediction from

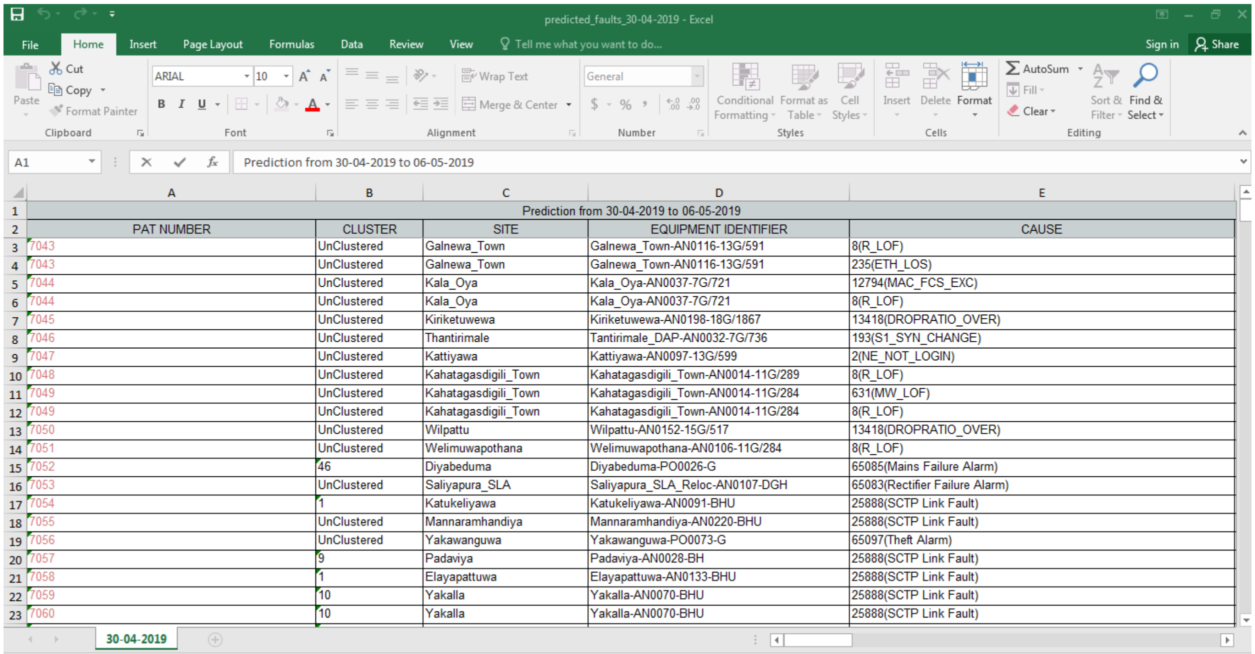
Freeze Header:

Master Format :

Note: MERGE and SORT options are disabled as RoE is active

Field Name*	Column Name*	Sort	Data Type	Header BG Color	Font Color	Col Width	Wrap Text	Merge
patnumber	PAT NUMBER	None	String	#e33672	#000000	0	□	□
clusterId	CLUSTER	None	Number	#c9d0d1	#000000	0	□	□

Figure 15.46 - Freeze Header Button



predicted_faults_30-04-2019 - Excel

A1 Prediction from 30-04-2019 to 06-05-2019

Prediction from 30-04-2019 to 06-05-2019

PAT NUMBER	CLUSTER	SITE	EQUIPMENT IDENTIFIER	CAUSE
7043	UnClustered	Galnewa_Town	Galnewa_Town-AN0116-13G/591	8(R_LOF)
7043	UnClustered	Galnewa_Town	Galnewa_Town-AN0116-13G/591	235(ETH_LOS)
7044	UnClustered	Kala_Oya	Kala_Oya-AN0037-7G/721	12794(MAC_FCS_EXC)
7044	UnClustered	Kala_Oya	Kala_Oya-AN0037-7G/721	8(R_LOF)
7045	UnClustered	Kiriketuwewa	Kiriketuwewa-AN0198-18G/1867	13418(DROPRATIO_OVER)
7046	UnClustered	Thantirimale	Tantirimale_DAP-AN0032-7G/736	193(S1_SYN_CHANGE)
7047	UnClustered	Kattiyawa	Kattiyawa-AN0097-13G/599	2(NE_NOT_LOGIN)
7048	UnClustered	Kahatagasdigili_Town	Kahatagasdigili_Town-AN0014-11G/289	8(R_LOF)
7049	UnClustered	Kahatagasdigili_Town	Kahatagasdigili_Town-AN0014-11G/284	631(MW_LOF)
7049	UnClustered	Kahatagasdigili_Town	Kahatagasdigili_Town-AN0014-11G/284	8(R_LOF)
7050	UnClustered	Wilpattu	Wilpattu-AN0152-15G/517	13418(DROPRATIO_OVER)
7051	UnClustered	Welimuwapothana	Welimuwapothana-AN0106-11G/284	8(R_LOF)
7052	46	Diyabeduma	Diyabeduma-PO0026-G	65085(Mains Failure Alarm)
7053	UnClustered	Saliyapura_SLA	Saliyapura_SLA_Reloc-AN0107-DGH	65083(Rectifier Failure Alarm)
7054	1	Katukeliyawa	Katukeliyawa-AN0091-BHU	25888(SCTP Link Fault)
7055	UnClustered	Mannaramhandiya	Mannaramhandiya-AN0220-BHU	25888(SCTP Link Fault)
7056	UnClustered	Yakawanguwa	Yakawanguwa-PO0073-G	65097(Theft Alarm)
7057	9	Padaviya	Padaviya-AN0028-BH	25888(SCTP Link Fault)
7058	1	Elayapattuwa	Elayapattuwa-AN0133-BHU	25888(SCTP Link Fault)
7059	10	Yakalla	Yakalla-AN0070-BHU	25888(SCTP Link Fault)
7060	10	Yakalla	Yakalla-AN0070-BHU	25888(SCTP Link Fault)

Figure 15.47 - 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.
4. 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

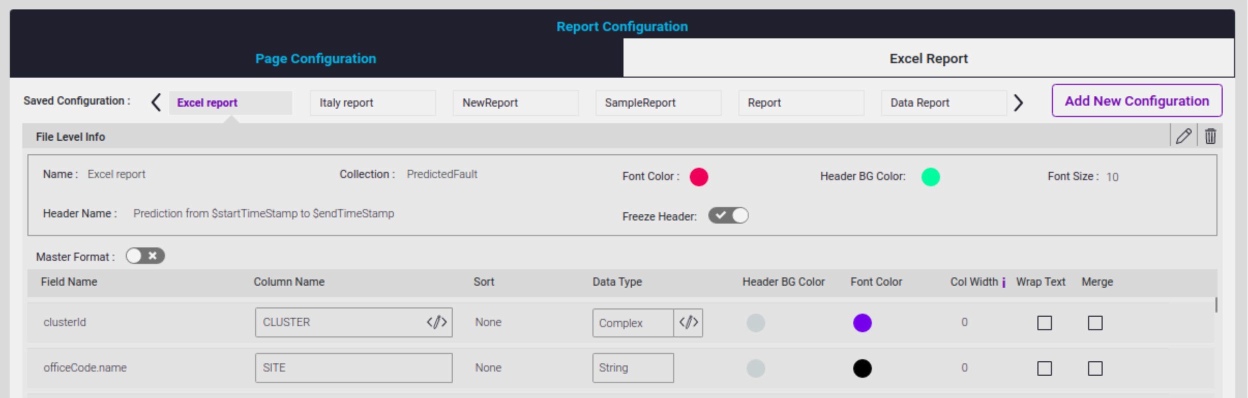
5. User can configure few other parameters to set each column of the prediction report The parameters are as follows:
6. Field Name - Name of the field as it is in prediction result table i.e. Predicted Fault table as per CAN convention.
7. Column Name - Name of the column which user wishes to see in report.
8. Sort - Column values can be sorted as Ascending, Descending and None.
9. Data Type - Select the Data formats like String, Number, Percent, Complex and Drop down. If user selects the complex data type, Code Snippet popup (which is similar in functionality with respect to parser screen) appears.
10. Header BG Color - User can decide background color for column header.
11. Font Color - User can decide font color for column values.
12. Column Width - Sets width of column, here value 0 indicates auto resizing of column.
13. Wrap Text - If checked, text contents of each cell in that column will be wrapped.

14. Merge - Allows multiple adjacent cells to be combined into a single larger cell when values are similar.
15. Delete - User can delete a column.
16. 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.
17. 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.



Saved Configuration : ‹ Excel report | Italy report | NewReport | SampleReport | Report | Data Report ›

Name : Excel report
Collection : PredictedFault
Font Color : ●
Header BG Color: ●
Font Size : 10
Header Name : Prediction from $startTimeStamp to $endTimeStamp
Freeze Header: ✓●
Master Format : ○✕

Field Name	Column Name	Sort	Data Type	Header BG Color	Font Color	Col Width i	Wrap Text	Merge
clusterId	CLUSTER	None	Complex	●	●	0	□	□
officeCode.name	SITE	None	String	●	●	0	□	□

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 of this screen, **'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 is not required, user can delete the existing configuration.

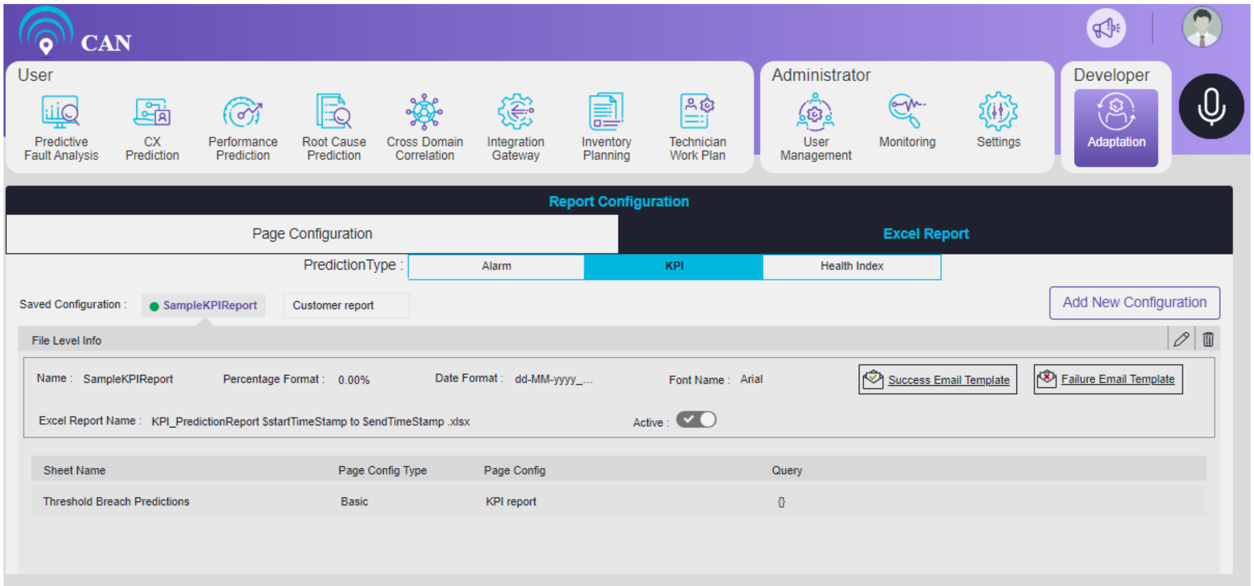
A switch to activate and deactivate excel report configuration is also available.

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, and 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.
   - Click the **Add New Mapping** button. User can also modify or delete the existing sheet configuration.
   - 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. Delete - User can delete a column.
     vi. 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.



PredictionType : Alarm | KPI | Health Index

Saved Configuration : ● SampleKPIReport | Customer report

File Level Info

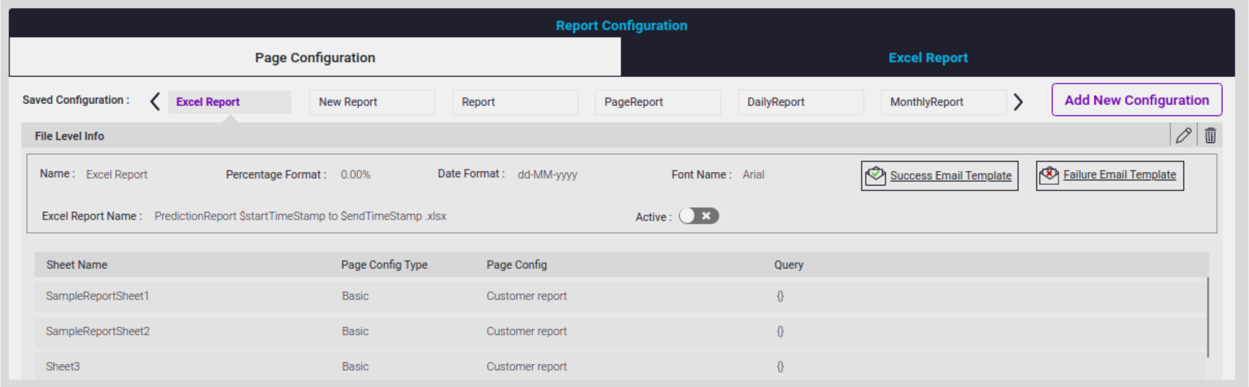
Name : SampleKPIReport   Percentage Format : 0.00%   Date Format : dd-MM-yyyy_...   Font Name : Arial

Excel Report Name : KPI_PredictionReport $startTimeStamp to $endTimeStamp .xlsx   Active : ✓

Sheet Name	Page Config Type	Page Config	Query
Threshold Breach Predictions	Basic	KPI report	{}

Figure 15.48 - 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.



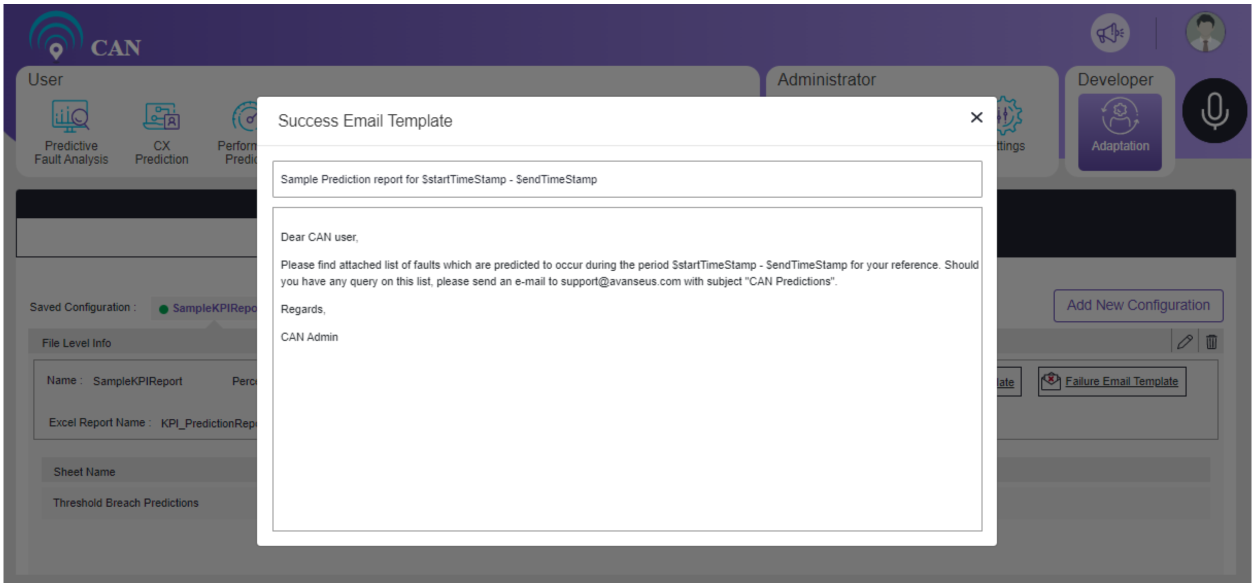
Saved Configuration : Excel Report | New Report | Report | PageReport | DailyReport | MonthlyReport

File Level Info

Name : Excel Report
Percentage Format : 0.00%
Date Format : dd-MM-yyyy
Font Name : Arial
Success Email Template
Failure Email Template

Excel Report Name : PredictionReport $startTimeStamp to $endTimeStamp .xlsx
Active :

Sheet Name	Page Config Type	Page Config	Query
SampleReportSheet1	Basic	Customer report	{}
SampleReportSheet2	Basic	Customer report	{}
Sheet3	Basic	Customer report	{}



Saved Configuration : SampleKPIRepo

File Level Info

Name : SampleKPIReport

Excel Report Name : KPI_PredictionRepo

Sheet Name

Threshold Breach Predictions

Success Email Template

Sample Prediction report for $startTimeStamp - $endTimeStamp

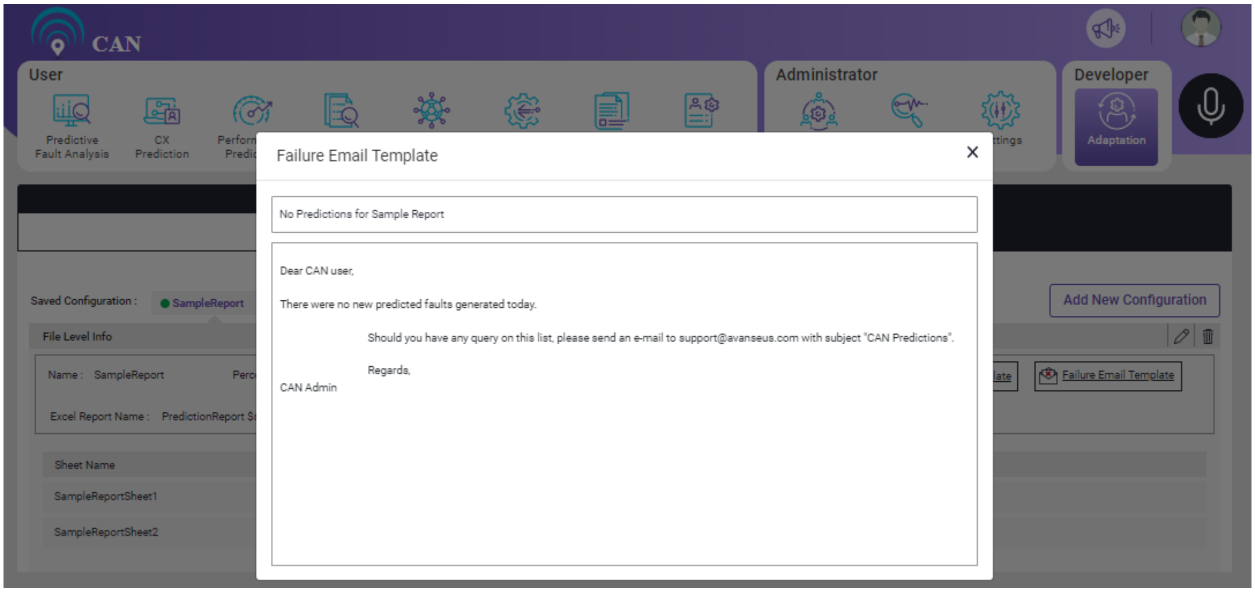
Dear CAN user,

Please find attached list of faults which are predicted to occur during the period $startTimeStamp - $endTimeStamp for your reference. Should you have any query on this list, please send an e-mail to support@avanseus.com with subject "CAN Predictions".

Regards,

CAN Admin

Figure 15.49 - Success Email Template



Failure Email Template

No Predictions for Sample Report

Dear CAN user,

There were no new predicted faults generated today.

Should you have any query on this list, please send an e-mail to support@avanseus.com with subject "CAN Predictions".

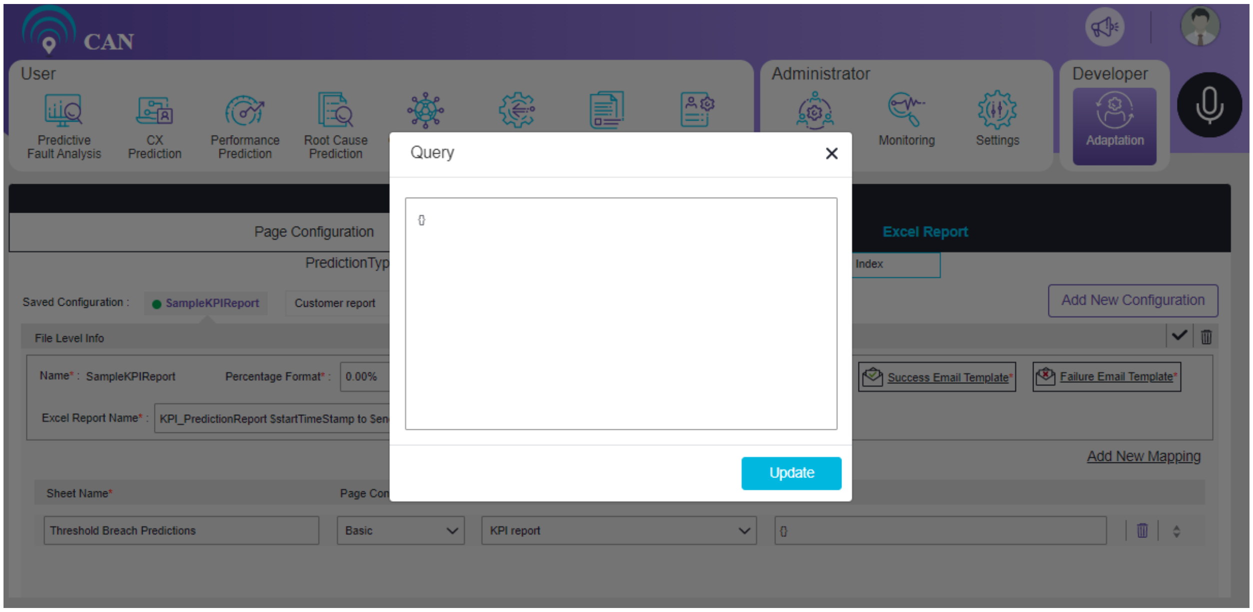
Regards,

CAN Admin

Figure 15.50 - Failure Email Template

To Create a New Configuration

1. Click the **Add New Configuration** button.
2. Write the Configuration Name, Percentage Format, and 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.
   - 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.



Query

{}

PredictionTyp

Saved Configuration : SampleKPIReport | Customer report

File Level Info

Name* : SampleKPIReport | Percentage Format* : 0.00%

Excel Report Name* : KPI_PredictionReport $startTimeStamp to $en

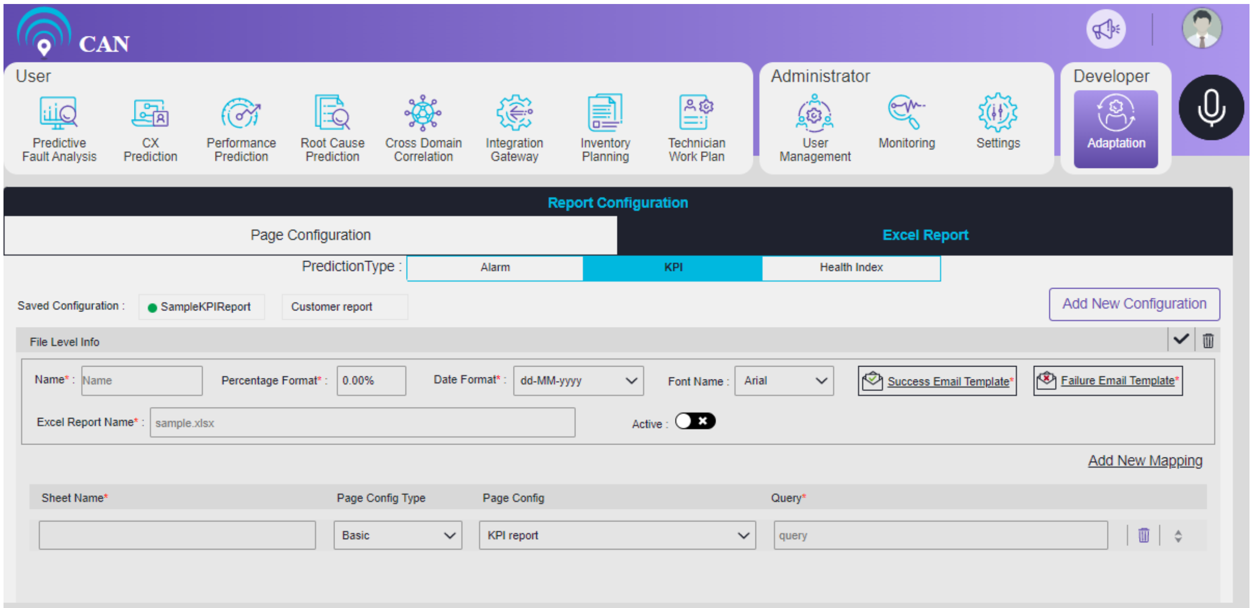
Sheet Name*	Page Con		
Threshold Breach Predictions	Basic	KPI report	{}

Figure 15.51 - Query Snippet

v. Delete - User can delete a column.

vi. 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, the changes will not reflect in the Excel Report Configuration Page.



PredictionType : Alarm | KPI | Health Index

Saved Configuration : SampleKPIReport | Customer report

File Level Info

Name* : Name | Percentage Format* : 0.00% | Date Format* : dd-MM-yyyy | Font Name : Arial

Excel Report Name* : sample.xlsx | Active :

Sheet Name*	Page Config Type	Page Config	Query*
	Basic	KPI report	query

Figure 15.52 - Create New Excel Report Configuration

Alarm Inclusions/Exclusions

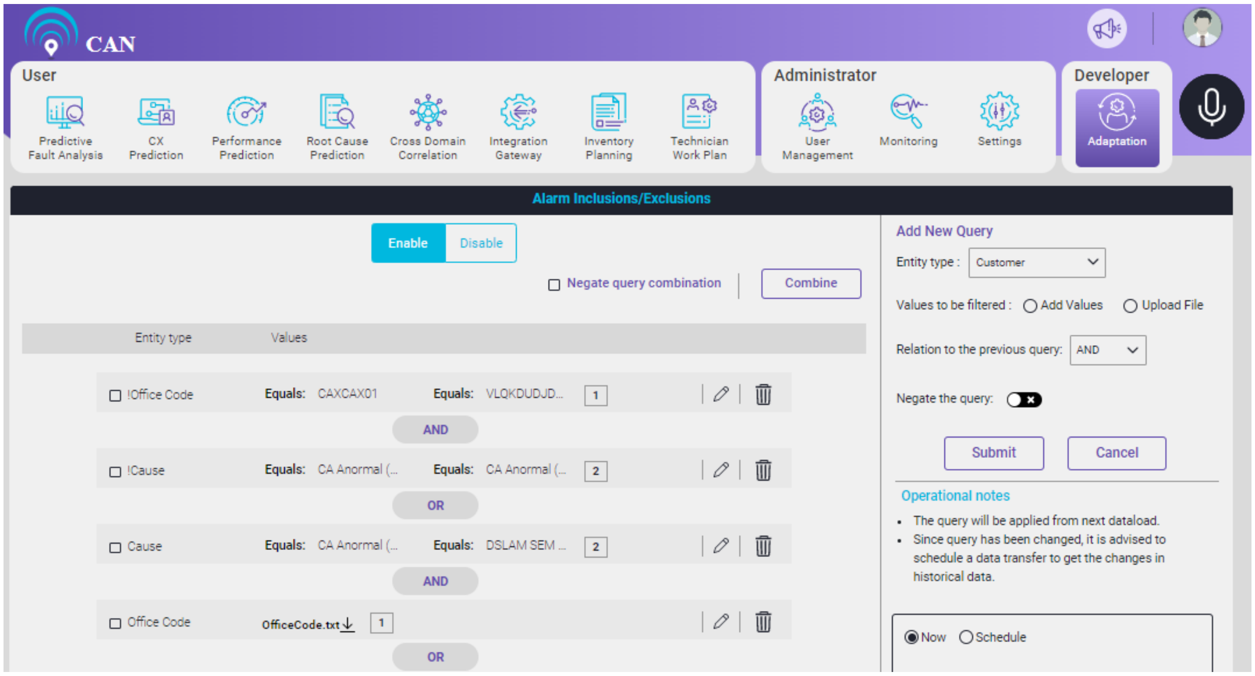
This screen is to save an Inclusion and Exclusion rule. User can transfer the data between **Alarm** and **Alarm_all** Table based on the rule.

After the transfer of the data:

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

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

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



□ Negate query combination

Entity type	Values			
□ !Office Code	Equals: CAXCAX01	Equals: VLQKDUDJD...	1	
AND				
□ !Cause	Equals: CA Anormal (...	Equals: CA Anormal (...	2	
OR				
□ Cause	Equals: CA Anormal (...	Equals: DSLAM SEM ...	2	
AND				
□ Office Code	OfficeCode.txt		1	
OR				

Add New Query

Entity type : Customer

Values to be filtered : ○ Add Values ○ Upload File

Relation to the previous query: AND

Negate the query:

Operational notes

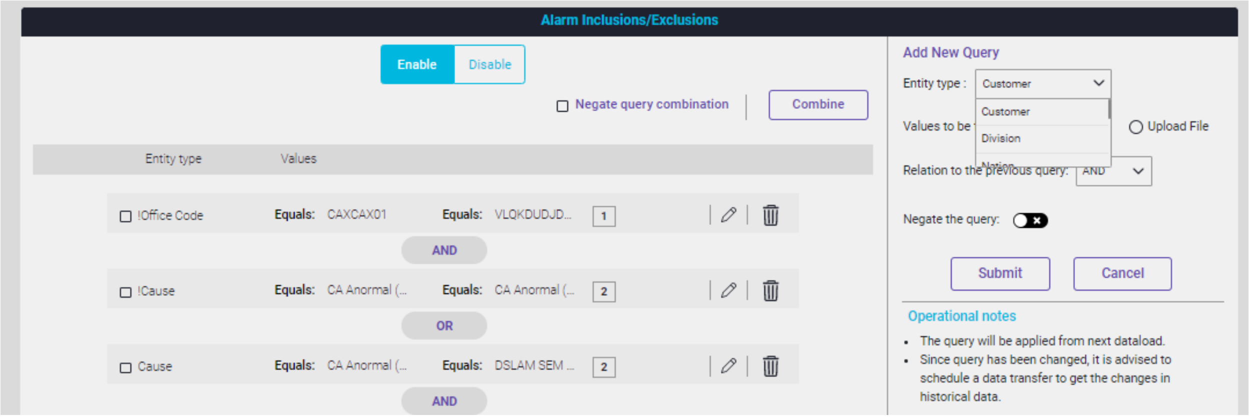
- The query will be applied from next dataload.
- Since query has been changed, it is advised to schedule a data transfer to get the changes in historical data.

● Now ○ Schedule

Figure 15.53 - Alarm Inclusion/Exclusion Toggle Switch

To Add New Query for the Alarm Inclusion/Exclusion

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



□ Negate query combination

Entity type	Values			
□ !Office Code	Equals: CAXCAX01	Equals: VLQKDUDJD...	1	
AND				
□ !Cause	Equals: CA Anormal (...	Equals: CA Anormal (...	2	
OR				
□ Cause	Equals: CA Anormal (...	Equals: DSLAM SEM ...	2	
AND				

Add New Query

Entity type : Customer

Values to be ○ Upload File

Relation to the previous query: AND

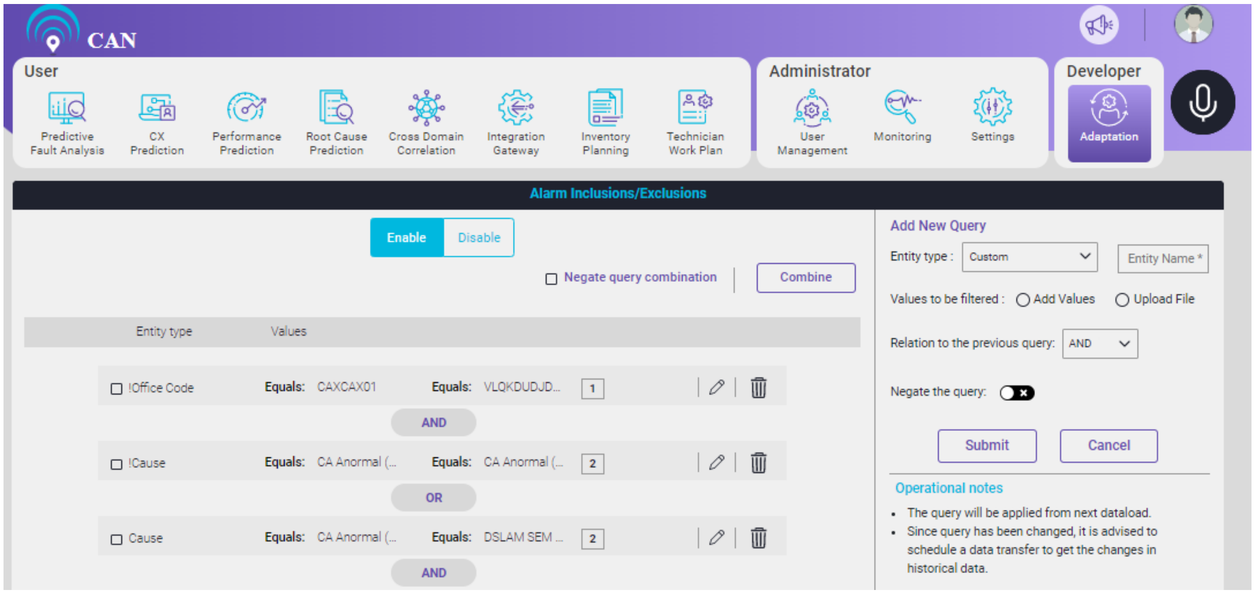
Negate the query:

Operational notes

- 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.

Figure 15.54 - 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.



Add New Query

Entity type : Custom | Entity Name *

Values to be filtered : ○ Add Values ○ Upload File

Relation to the previous query: AND

Negate the query:

Entity type	Values				
□ !Office Code	Equals: CAXCAX01	Equals: VLQKDUDJD...	1		
	AND				
□ !Cause	Equals: CA Anormal (...	Equals: CA Anormal (...	2		
	OR				
□ Cause	Equals: CA Anormal (...	Equals: DSLAM SEM ...	2		
	AND				

Operational notes

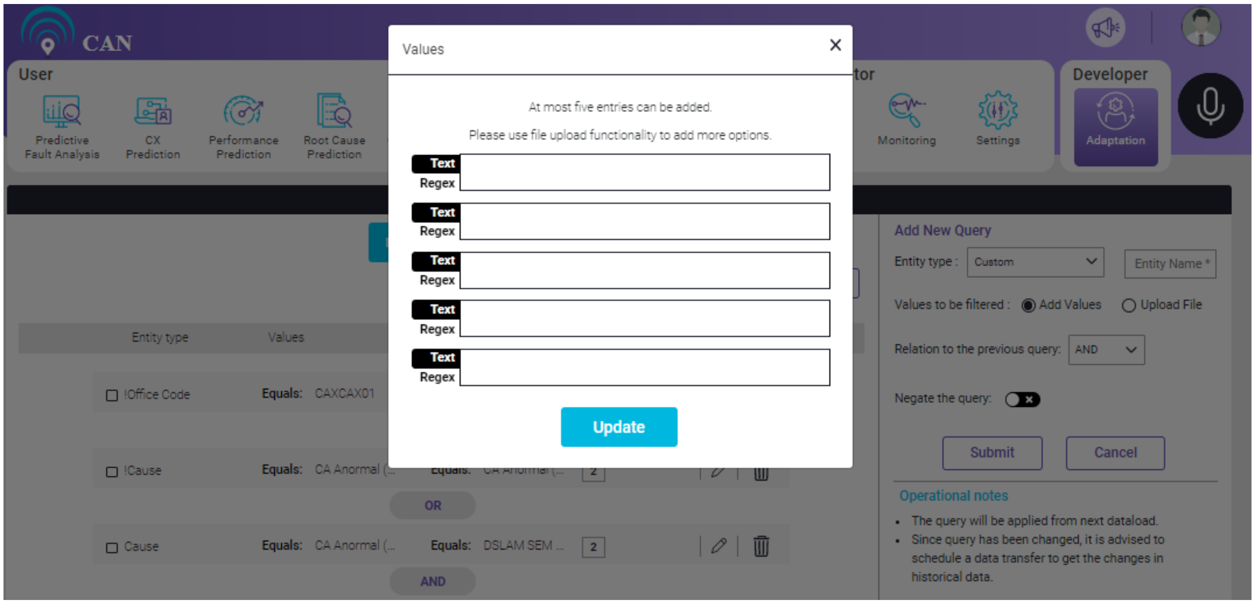
- The query will be applied from next dataload.
- Since query has been changed, it is advised to schedule a data transfer to get the changes in historical data.

Figure 15.55 - Alarm Inclusions/Exclusions Custom Entity Type

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.



At most five entries can be added.

Please use file upload functionality to add more options.

Add New Query

Entity type : Custom | Entity Name *

Values to be filtered : ● Add Values ○ Upload File

Relation to the previous query: AND

Negate the query:

Operational notes

- 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.

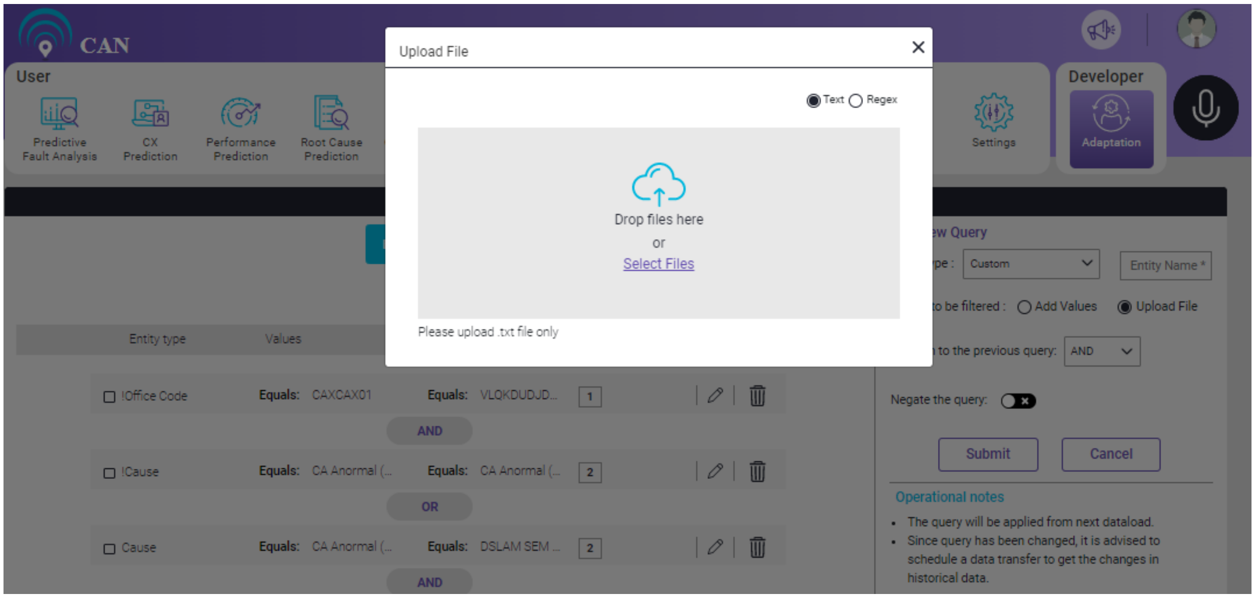
Figure 15.56 – Add Values

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.



Upload File

● Text ○ Regex

Drop files here

or

Select Files

Please upload .txt file only

□ !Office Code	Equals:	CAXCAX01	Equals:	VLQKDUDJD...	1
□ !Cause	Equals:	CA Anormal (...	Equals:	CA Anormal (...	2
□ Cause	Equals:	CA Anormal (...	Equals:	DSLAM SEM ...	2

...w Query

...pe : Custom Entity Name *

...to be filtered : ○ Add Values ● Upload File

...to the previous query: AND

Negate the query:

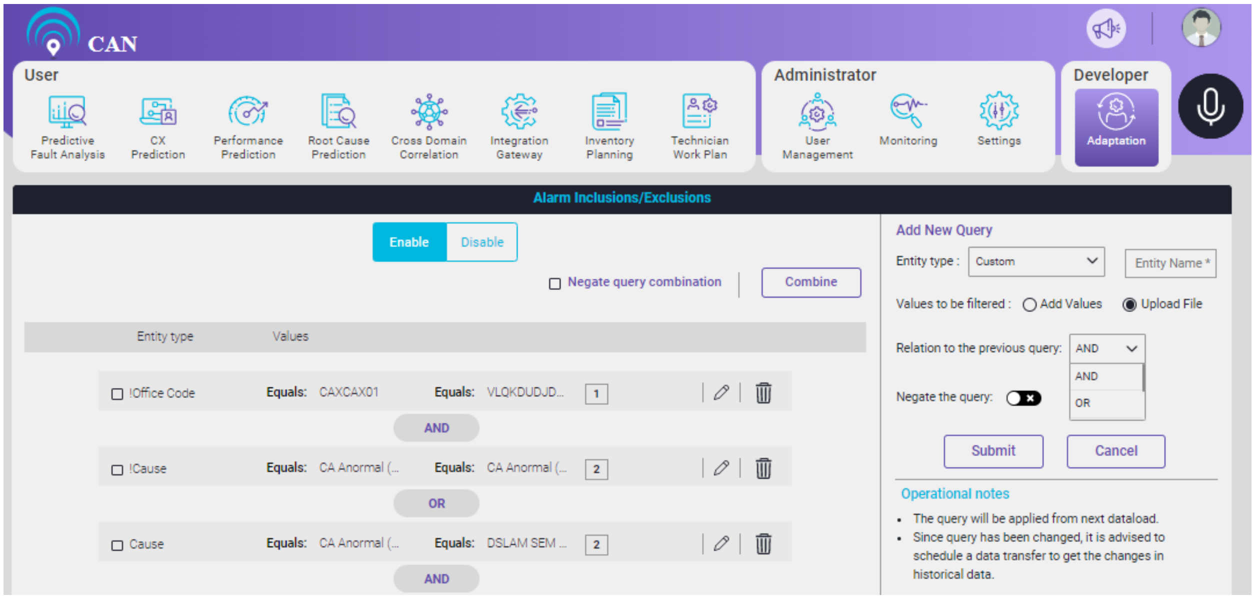
Operational notes

- 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.

Figure 15.57 - 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.



□ Negate query combination

Entity type	Values			
□ !Office Code	Equals: CAXCAX01	Equals: VLQKDUDJD...	1	
AND				
□ !Cause	Equals: CA Anormal (...	Equals: CA Anormal (...	2	
OR				
□ Cause	Equals: CA Anormal (...	Equals: DSLAM SEM ...	2	
AND				

Add New Query

Entity type : Custom | Entity Name *

Values to be filtered : ○ Add Values ● Upload File

Relation to the previous query: AND (AND, OR)

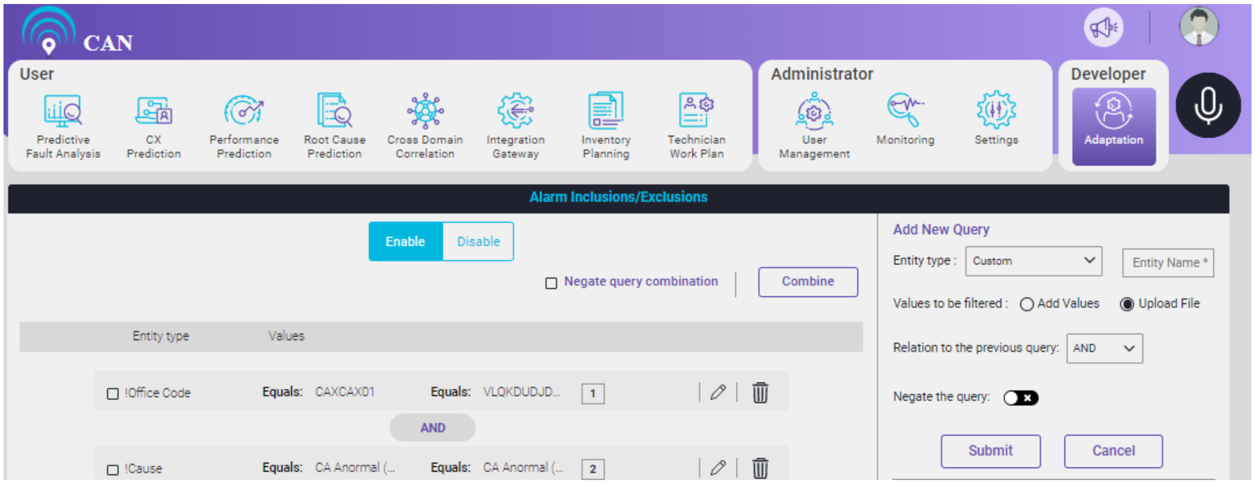
Negate the query:

Operational notes

- 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.

Figure 15.58 - Relation to the previous query

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



□ Negate query combination

Entity type	Values			
□ !Office Code	Equals: CAXCAX01	Equals: VLQKDUDJD...	1	
AND				
□ !Cause	Equals: CA Anormal (...	Equals: CA Anormal (...	2	

Add New Query

Entity type : Custom | Entity Name *

Values to be filtered : ○ Add Values ● Upload File

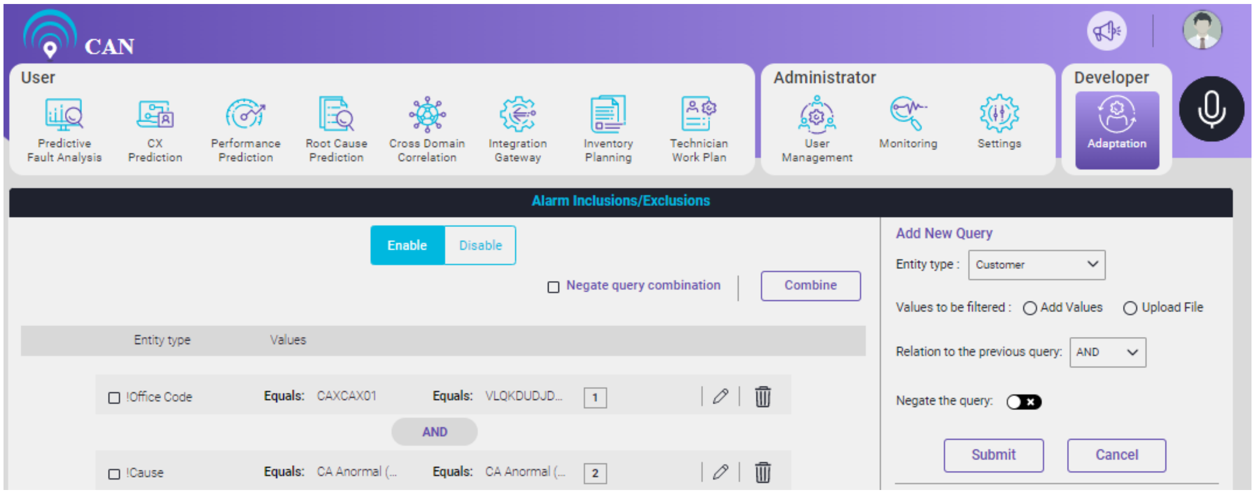
Relation to the previous query: AND

Negate the query:

Figure 15.59 - Negate the query

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

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



□ Negate query combination

Entity type	Values				
□ !Office Code	Equals:	CAXCAX01	Equals:	VLQKDUDJD...	1
AND					
□ !Cause	Equals:	CA Anormal (...	Equals:	CA Anormal (...	2

Add New Query

Entity type : Customer

Values to be filtered : ○ Add Values ○ Upload File

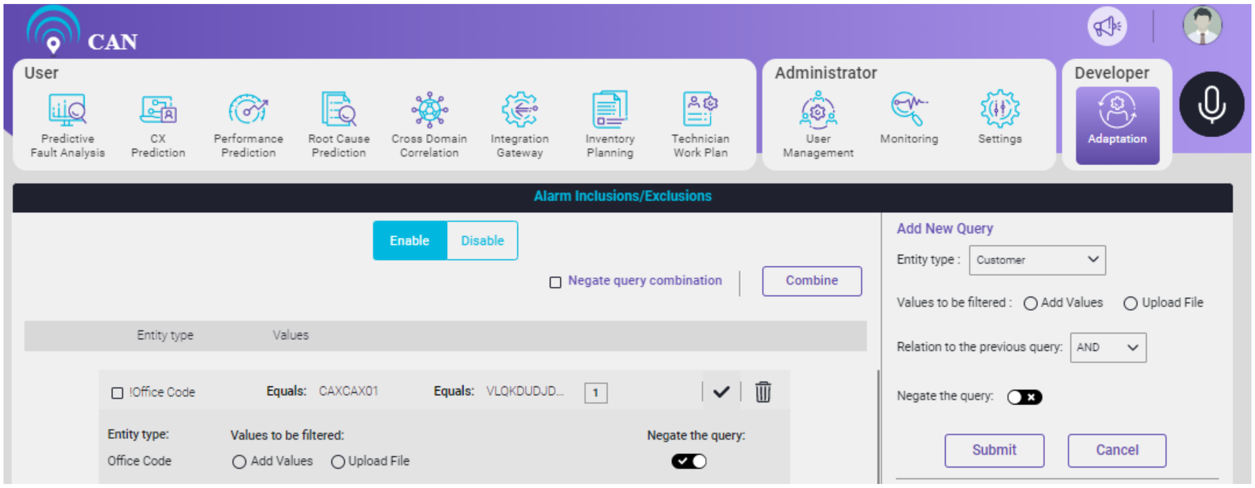
Relation to the previous query: AND

Negate the query: ✗

Figure 15.60 - Add New Query

Edit:

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



□ Negate query combination

Entity type	Values				
□ !Office Code	Equals:	CAXCAX01	Equals:	VLQKDUDJD...	1

Entity type: Office Code

Values to be filtered: ○ Add Values ○ Upload File

Negate the query: ✓

Add New Query

Entity type : Customer

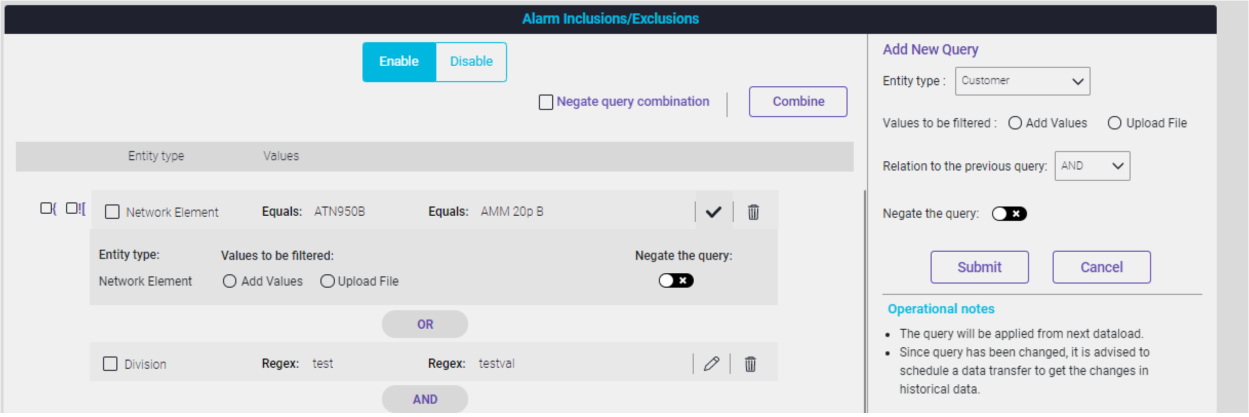
Values to be filtered : ○ Add Values ○ Upload File

Relation to the previous query: AND

Negate the query: ✗

Figure 15.61 - Edit Query

To save the changes, click the save icon ✓.

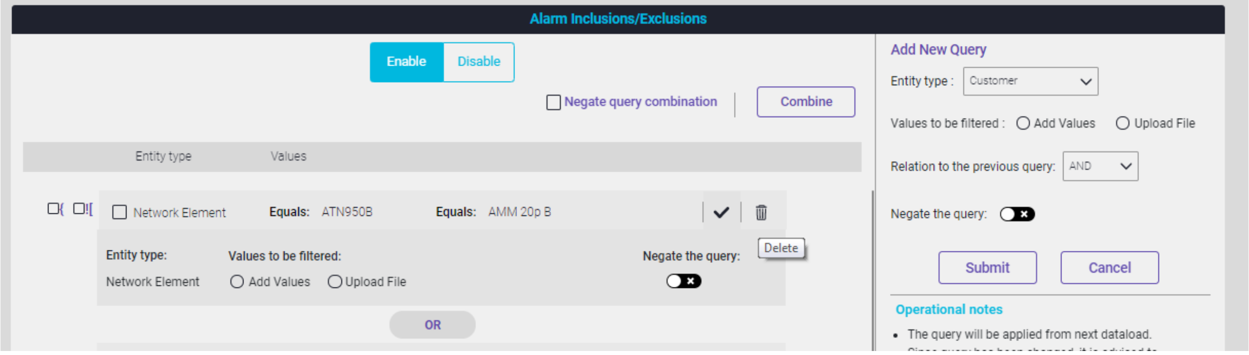


- The query will be applied from next dataload.
- Since query has been changed, it is advised to schedule a data transfer to get the changes in historical data.

Figure 15.62 - Save Icon

Delete:

To delete a query, click the delete icon 🗑.

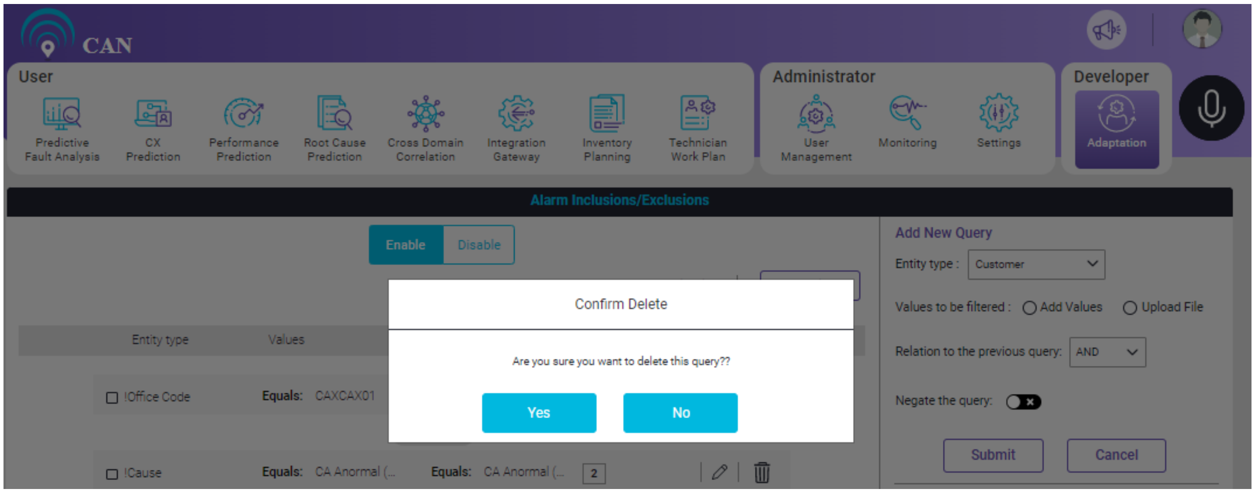


- The query will be applied from next dataload.

Figure 15.63 - Delete a sub query

A dialog box will appear.

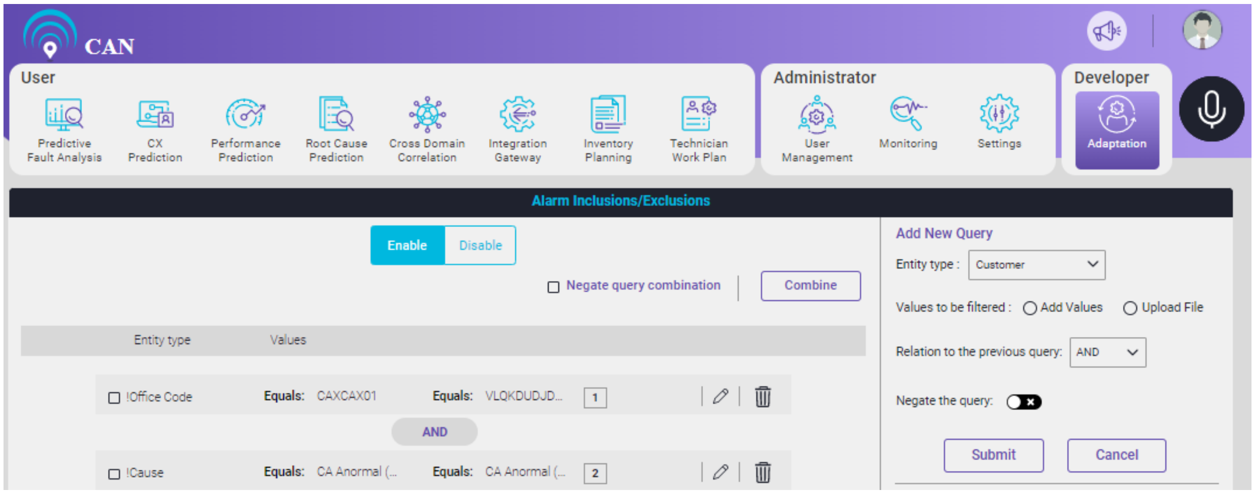
To confirm the deletion, click **Yes**, otherwise click **No**.



Are you sure you want to delete this query??

Figure 15.64 - Deletion Confirmation Message

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



□ Negate query combination

Entity type	Values				
□ !Office Code	Equals:	CAXCAX01	Equals:	VLQKDUDJD...	1
AND					
□ !Cause	Equals:	CA Anormal (...	Equals:	CA Anormal (...	2

Entity type : Customer

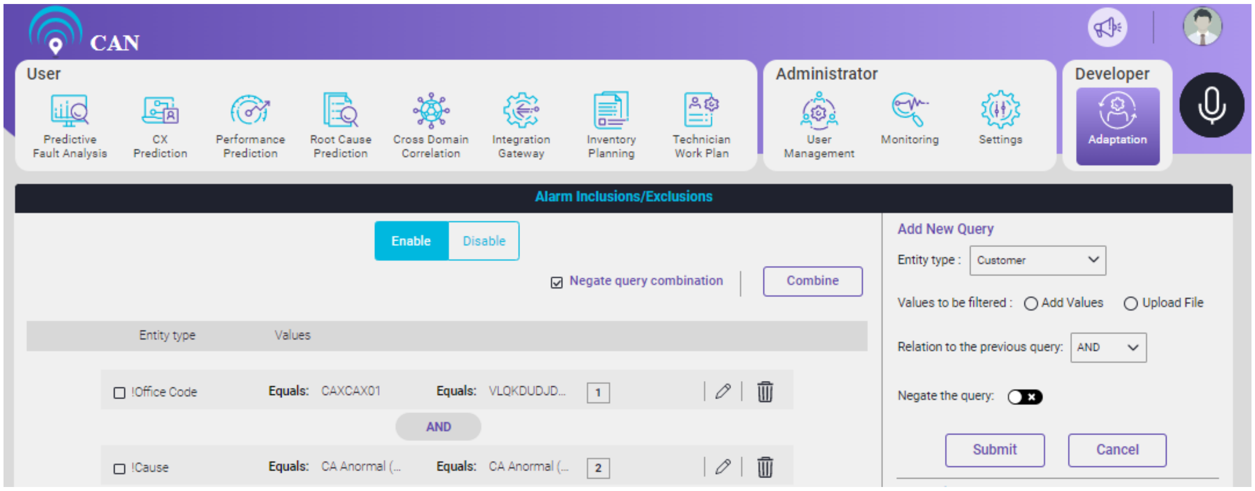
Values to be filtered : ○ Add Values ○ Upload File

Relation to the previous query: AND

Negate the query:

Figure 15.65 - Combination of Queries

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



☑ Negate query combination

Entity type	Values				
□ !Office Code	Equals:	CAXCAX01	Equals:	VLQKDUDJD...	1
AND					
□ !Cause	Equals:	CA Anormal (...	Equals:	CA Anormal (...	2

Entity type : Customer

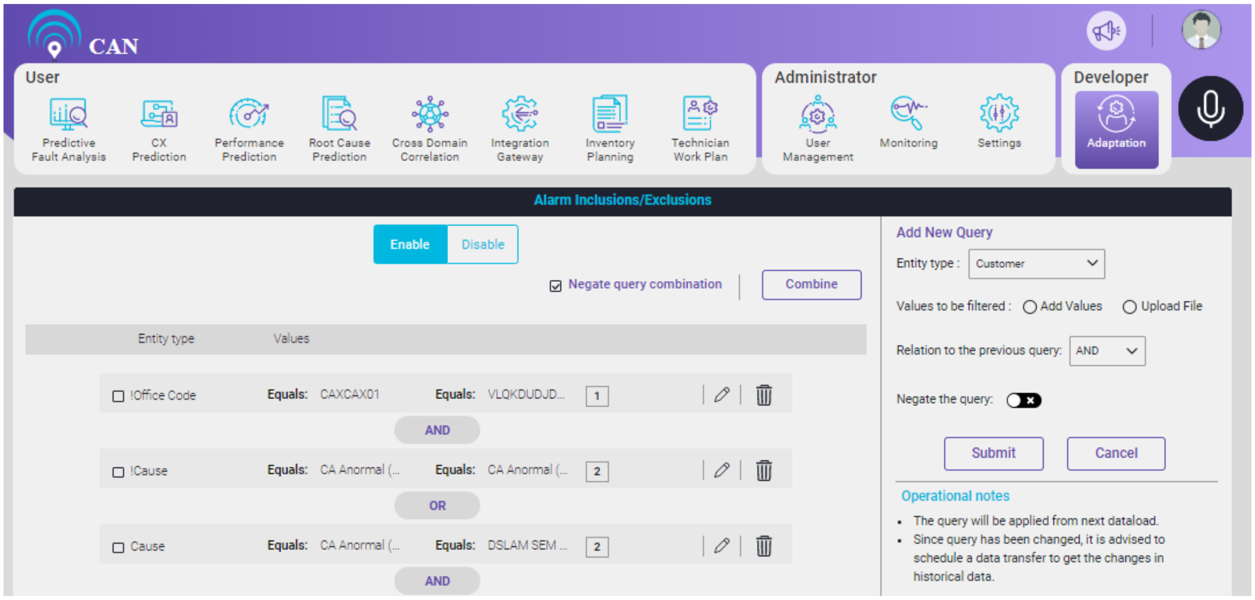
Values to be filtered : ○ Add Values ○ Upload File

Relation to the previous query: AND

Negate the query:

Figure 15.66 - 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.



☑ Negate query combination

Entity type	Values		
□ !Office Code	Equals: CAXCAX01	Equals: VLQKDUDJD...	1
□ !Cause	Equals: CA Anormal (...	Equals: CA Anormal (...	2
□ Cause	Equals: CA Anormal (...	Equals: DSLAM SEM ...	2

Add New Query

Entity type : Customer

Values to be filtered : ○ Add Values ○ Upload File

Relation to the previous query: AND

Negate the query:

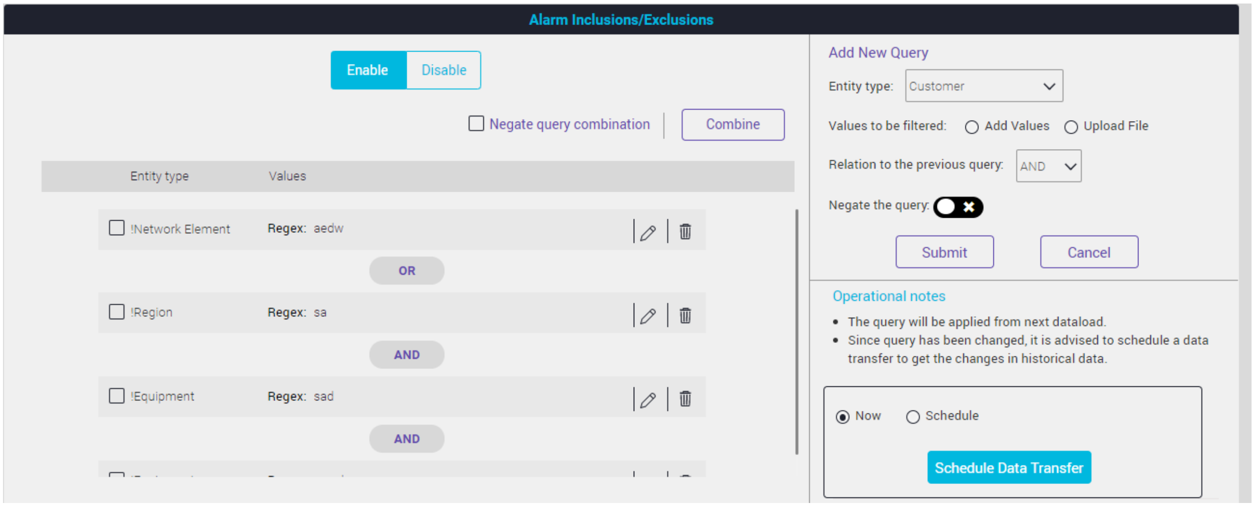
Operational notes

- 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.

Figure 15.67 - Operational Notes

To Schedule a Job:

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



□ Negate query combination

Entity type	Values
□ !Network Element	Regex: aedw
□ !Region	Regex: sa
□ !Equipment	Regex: sad

Add New Query

Entity type: Customer

Values to be filtered: ○ Add Values ○ Upload File

Relation to the previous query: AND

Negate the query:

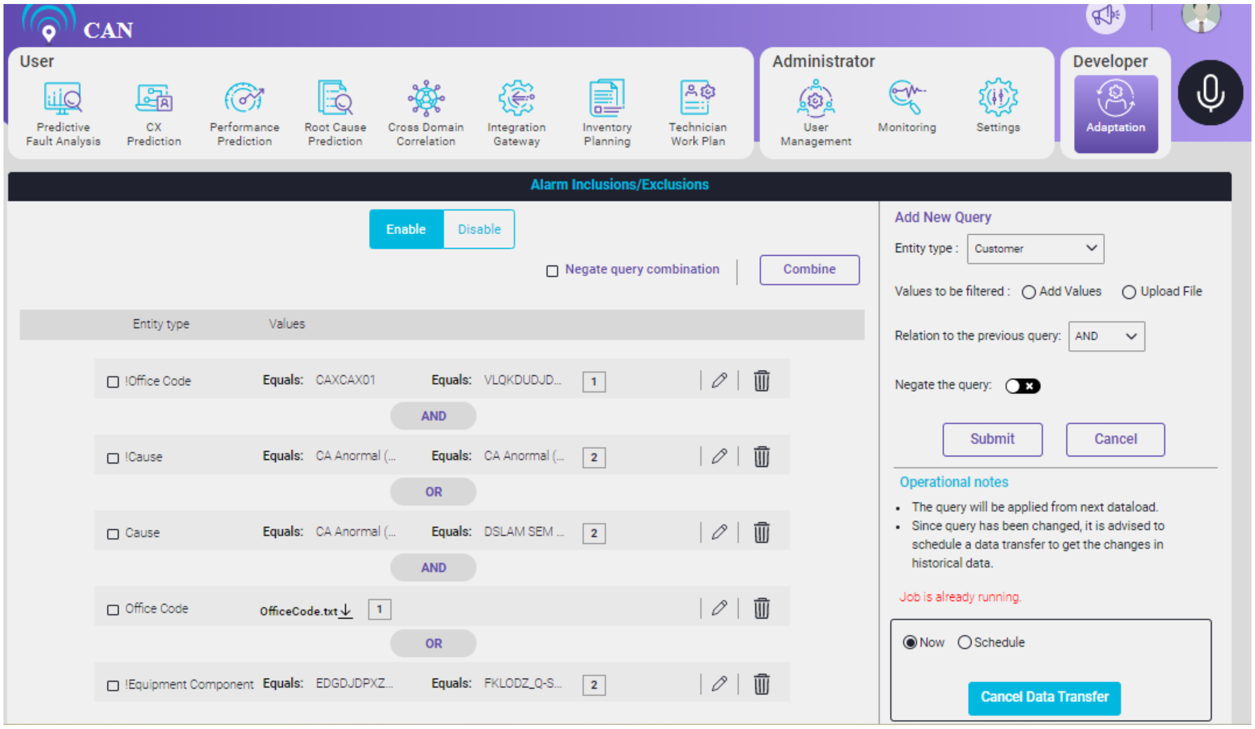
Operational notes

- 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.

● Now ○ Schedule

Figure 15.68 - 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 data load.
   - 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.



Alarm Inclusions/Exclusions

□ Negate query combination

Entity type	Values				
□ !Office Code	Equals:	CAXCAX01	Equals:	VLQKDUDJD...	1
AND					
□ !Cause	Equals:	CA Anormal (...	Equals:	CA Anormal (...	2
OR					
□ Cause	Equals:	CA Anormal (...	Equals:	DSLAM SEM ...	2
AND					
□ Office Code	OfficeCode.txt				1
OR					
□ !Equipment Component	Equals:	EDGDJDPXZ...	Equals:	FKLODZ_Q-S...	2

Add New Query

Entity type : Customer

Values to be filtered : ○ Add Values ○ Upload File

Relation to the previous query: AND

Negate the query:

Operational notes

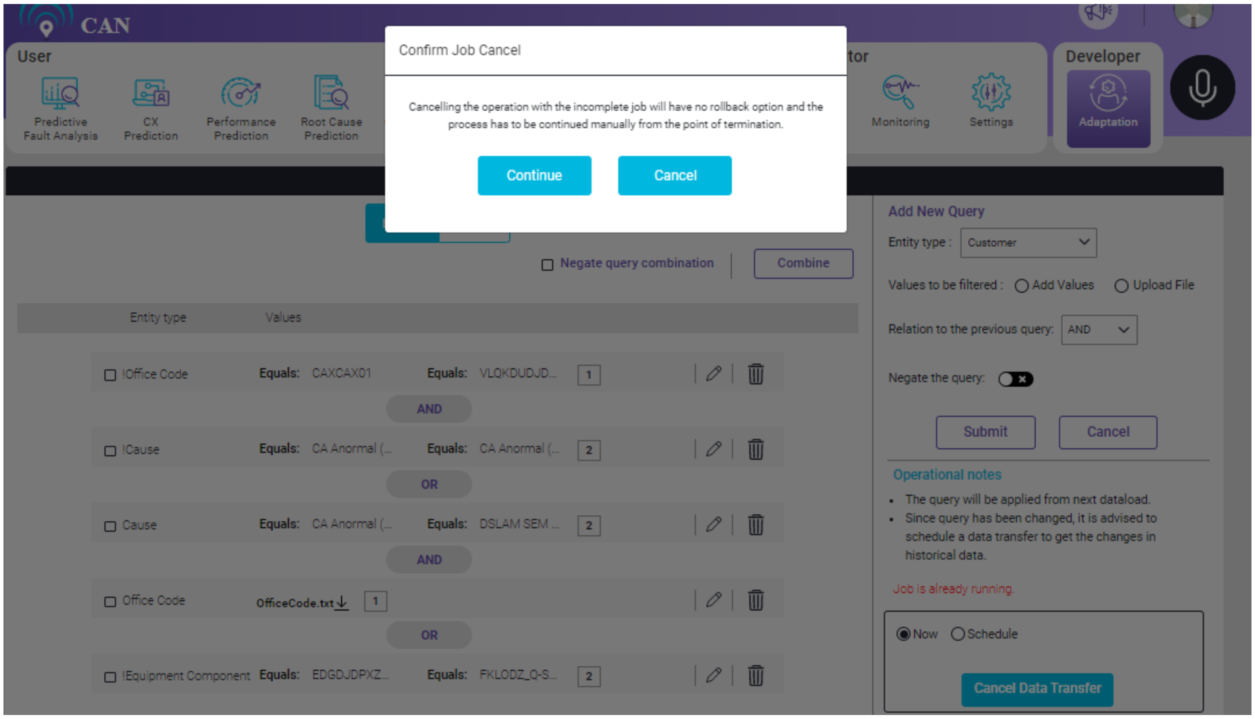
- The query will be applied from next dataload.
- Since query has been changed, it is advised to schedule a data transfer to get the changes in historical data.

Job is already running.

● Now ○ Schedule

Figure 15.69 - 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.



Confirm Job Cancel

Cancelling the operation with the incomplete job will have no rollback option and the process has to be continued manually from the point of termination.

Entity type		Values			
□ !Office Code	Equals:	CAXCAX01	Equals:	VLQKDUDJD...	1
□ !Cause	Equals:	CA Anormal (...	Equals:	CA Anormal (...	2
□ Cause	Equals:	CA Anormal (...	Equals:	DSLAM SEM ...	2
□ Office Code		OfficeCode.txt			1
□ !Equipment Component	Equals:	EDGDJDPXZ...	Equals:	FKLODZ_Q-S...	2

Add New Query

Entity type : Customer

Values to be filtered : ○ Add Values ○ Upload File

Relation to the previous query: AND

Negate the query:

Operational notes

- 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.

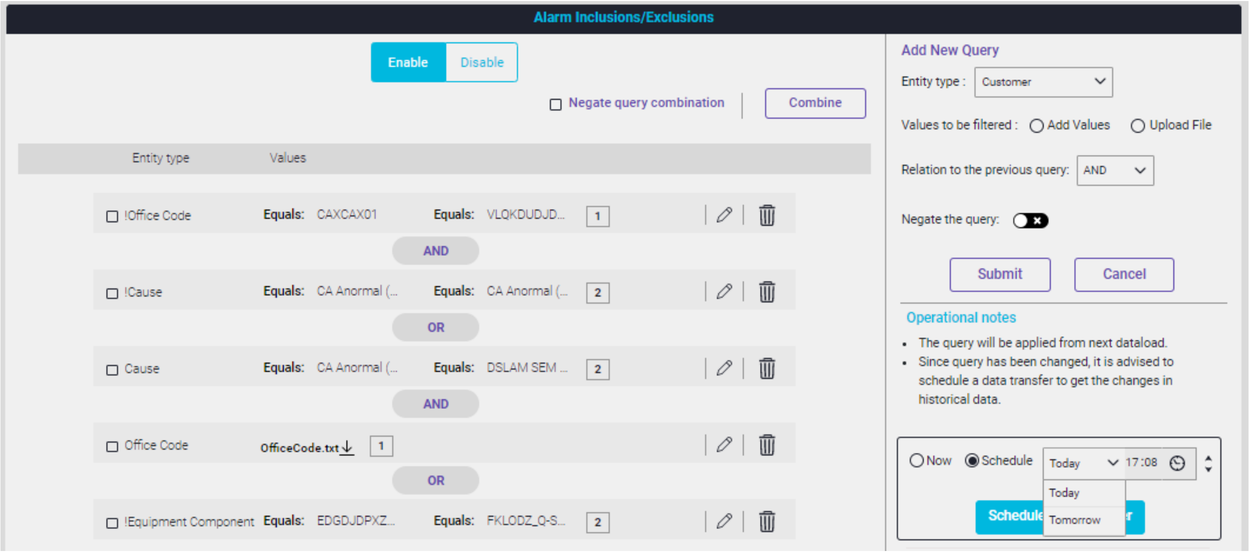
Job is already running.

● Now ○ Schedule

Figure 15.70 - Cancel data transfer confirmation

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.



Entity type		Values			
□ !Office Code	Equals:	CAXCAX01	Equals:	VLQKDUDJD...	1
□ !Cause	Equals:	CA Anormal (...	Equals:	CA Anormal (...	2
□ Cause	Equals:	CA Anormal (...	Equals:	DSLAM SEM ...	2
□ Office Code		OfficeCode.txt			1
□ !Equipment Component	Equals:	EDGDJDPXZ...	Equals:	FKLODZ_Q-S...	2

Add New Query

Entity type : Customer

Values to be filtered : ○ Add Values ○ Upload File

Relation to the previous query: AND

Negate the query:

Operational notes

- 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.

○ Now ● Schedule Today 17:08

Figure 15.71 - Job Scheduler

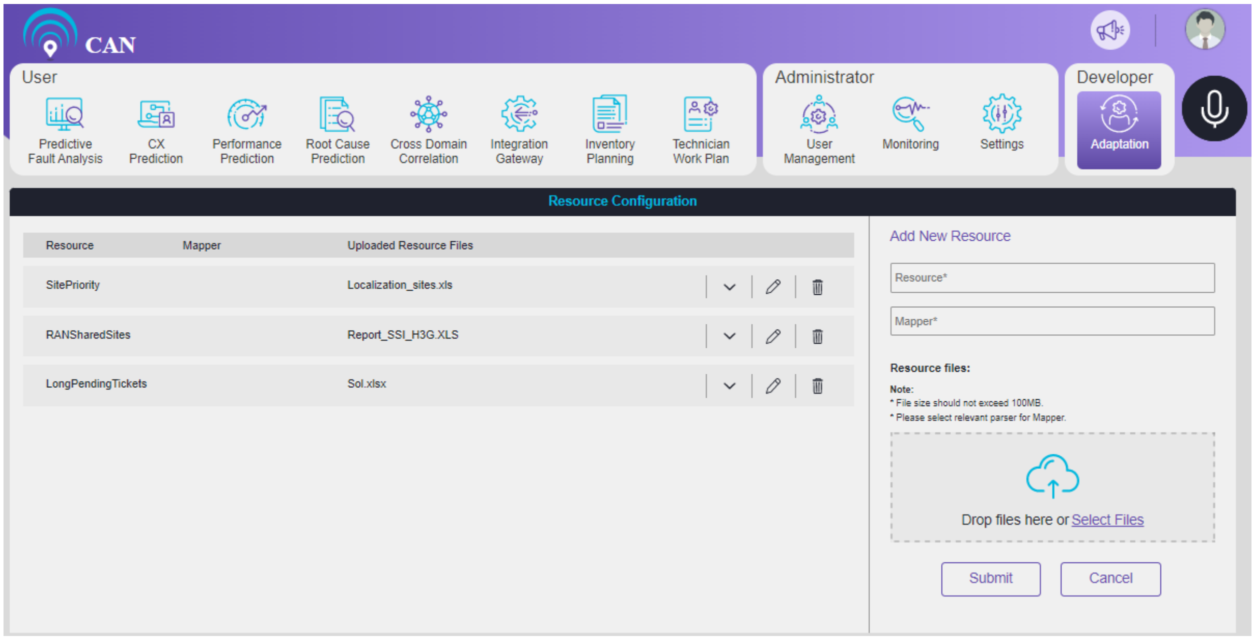
Resource Configuration

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 (*Example:* 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.



Resource Configuration

Resource	Mapper	Uploaded Resource Files
SitePriority		Localization_sites.xls
RANSharedSites		Report_SSI_H3G.XLS
LongPendingTickets		Sol.xlsx

Add New Resource

Resource*

Mapper*

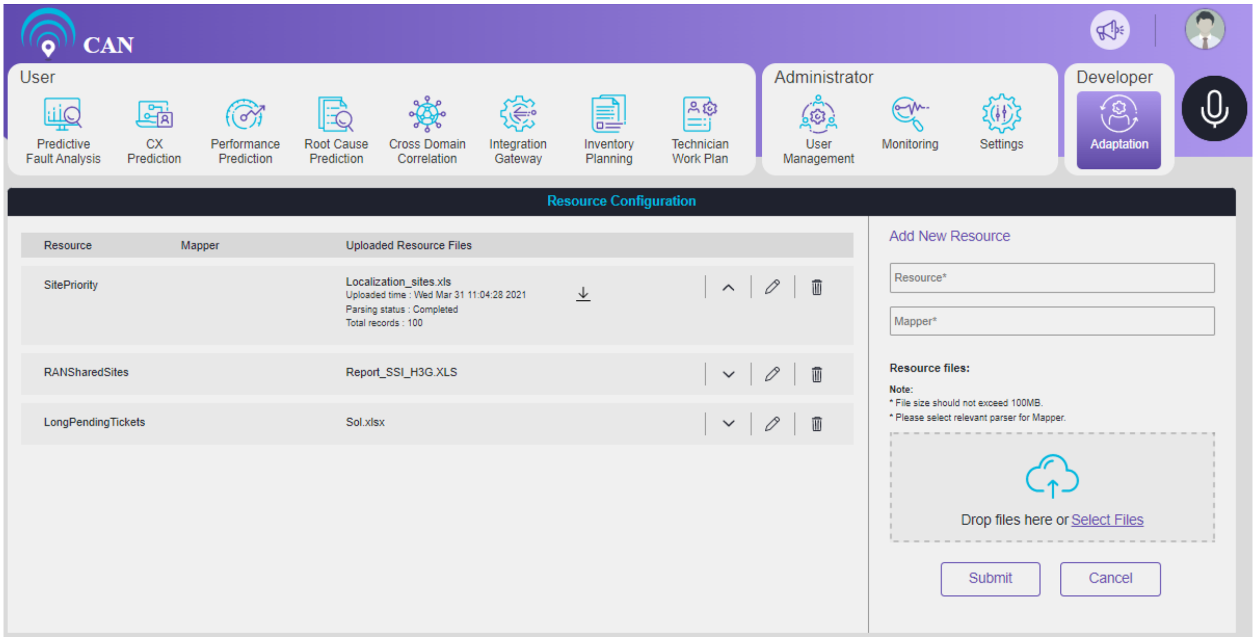
Resource files:

Note:
* File size should not exceed 100MB.
* Please select relevant parser for Mapper.

Drop files here or Select Files

Figure 15.72 - Resource Configuration Screen

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



Resource	Mapper	Uploaded Resource Files
SitePriority		Localization_sites.xls Uploaded time : Wed Mar 31 11:04:28 2021 Parsing status : Completed Total records : 100
RANSharedSites		Report_SSI_H3G.XLS
LongPendingTickets		Sol.xlsx

Add New Resource

Resource*

Mapper*

Resource files:

Note:
* File size should not exceed 100MB.
* Please select relevant parser for Mapper.

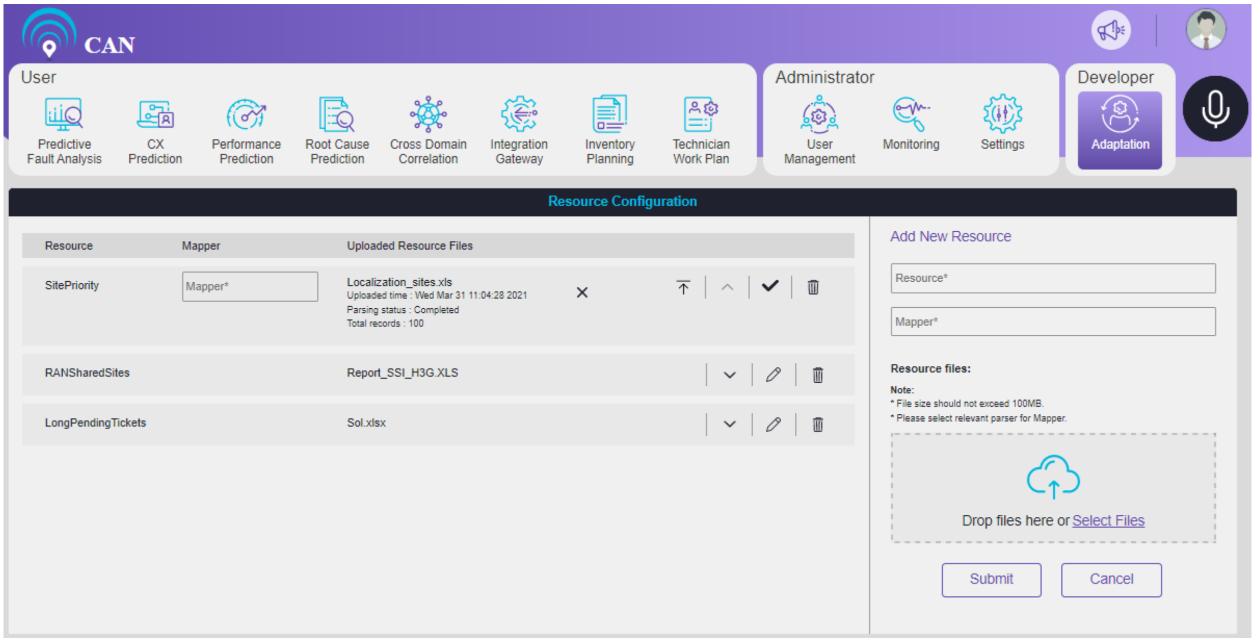
Drop files here or Select Files

Submit Cancel

Figure 15.73 - Resource Configuration Details

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 🗑.



Resource	Mapper	Uploaded Resource Files
SitePriority	Mapper*	Localization_sites.xls Uploaded time : Wed Mar 31 11:04:28 2021 Parsing status : Completed Total records : 100
RANSharedSites		Report_SSI_H3G.XLS
LongPendingTickets		Sol.xlsx

Add New Resource

Resource*

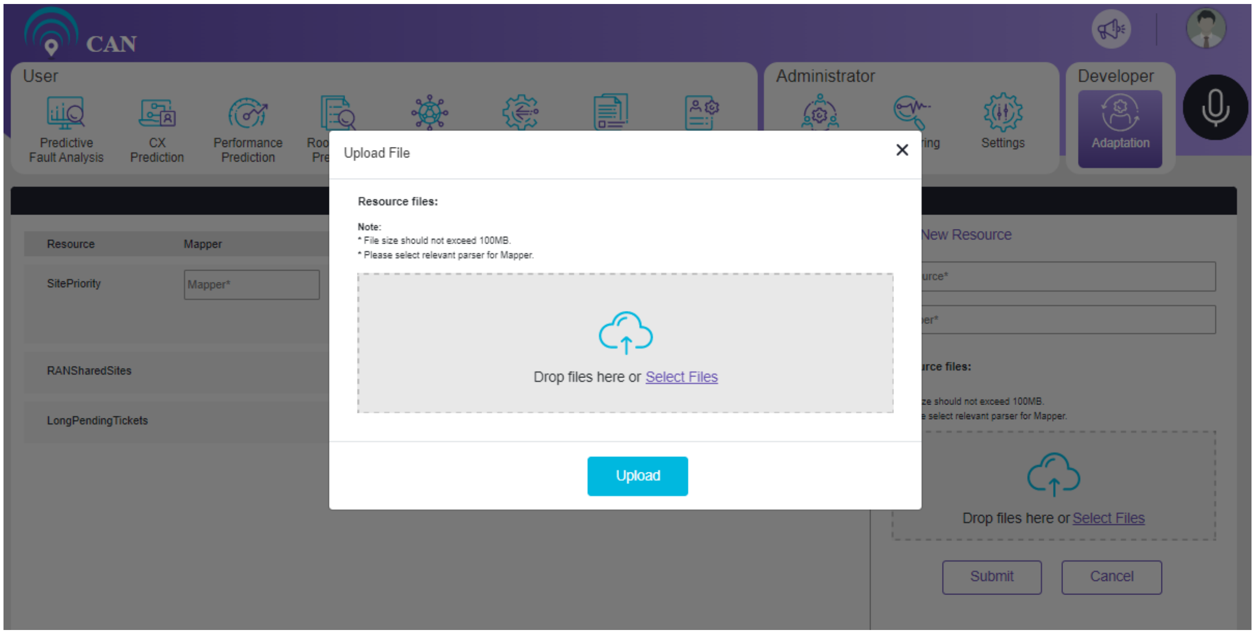
Mapper*

Resource files:

Note:
* File size should not exceed 100MB.
* Please select relevant parser for Mapper.

Drop files here or Select Files

Figure 15.74 - Edit Existing Resource Files



Upload File

Resource files:

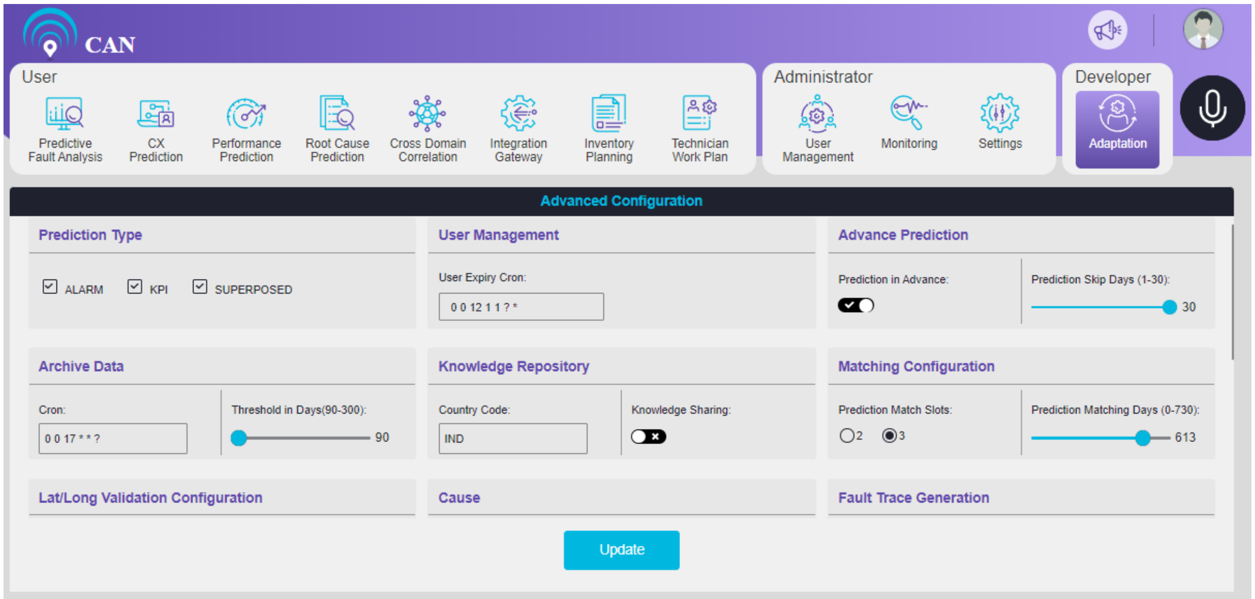
Note:
* File size should not exceed 100MB.
* Please select relevant parser for Mapper.

Drop files here or Select Files

Figure 15.75 - Upload Resource Files

Advanced Configuration

Developers use this screen to configure Prediction Algorithm settings and General settings.



Advanced Configuration

Prediction Type

☑ ALARM ☑ KPI ☑ SUPERPOSED

User Management

User Expiry Cron: 0 0 12 1 1 ? *

Advance Prediction

Prediction in Advance: ✓

Prediction Skip Days (1-30): 30

Archive Data

Cron: 0 0 17 * * ?

Threshold in Days(90-300): 90

Knowledge Repository

Country Code: IND

Knowledge Sharing: ✗

Matching Configuration

Prediction Match Slots: ○2 ●3

Prediction Matching Days (0-730): 613

Lat/Long Validation Configuration

Cause

Fault Trace Generation

Update

Figure 15.76 - Advanced Configuration

Advanced Configuration includes the following:

Prediction Type

- The data type to define the type of prediction to be done. The three data types are ALARM, KPI and SUPERPOSED.

User Management

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

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 does not fall under this set threshold will be moved to Archival table.

Cause

- Category - User can configure the category as per the requirement. User have the option to Add or Delete the Cause category. INFRA, CONFIGURATION and HARDWARE category are set as default.

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.

Lat/Long Validation Configuration

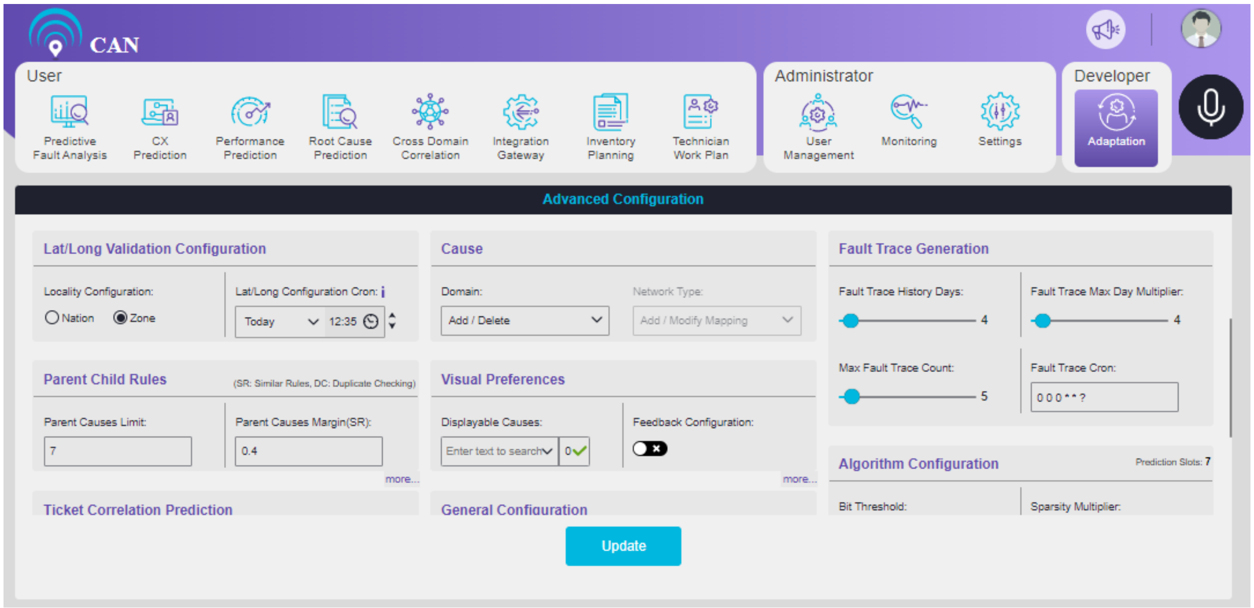
- Locality Configuration - The level at which the Lat/Long should be validated. The 2 locality types are Nation and Zone.
- Lat/Long Configuration Cron - Schedule the job for validation, 10 minutes from the time update button is clicked. Configure job for Today or Tomorrow.

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.

Fault Trace Generation

- Fault Trace History Days - Number of days to go back during an iteration to find fault traces.
- Fault Trace Max Day Multiplier - A multiplier that increases the horizon of days in history to go back to find fault traces.
- Max Fault Trace Count - The max number of faults in a fault trace.
- Fault Trace Cron - Cron trigger to schedule job to calculate fault traces.



Advanced Configuration

Lat/Long Validation Configuration

Locality Configuration: ○ Nation ● Zone

Lat/Long Configuration Cron: Today 12:35

Cause

Domain: Add / Delete

Network Type: Add / Modify Mapping

Fault Trace Generation

Fault Trace History Days: 4

Fault Trace Max Day Multiplier: 4

Max Fault Trace Count: 5

Fault Trace Cron: 0 0 0 * * ?

Parent Child Rules (SR: Similar Rules, DC: Duplicate Checking)

Parent Causes Limit: 7

Parent Causes Margin(SR): 0.4

more...

Visual Preferences

Displayable Causes: Enter text to search 0

Feedback Configuration:

more...

Algorithm Configuration Prediction Slots: 7

Bit Threshold:

Sparsity Multiplier:

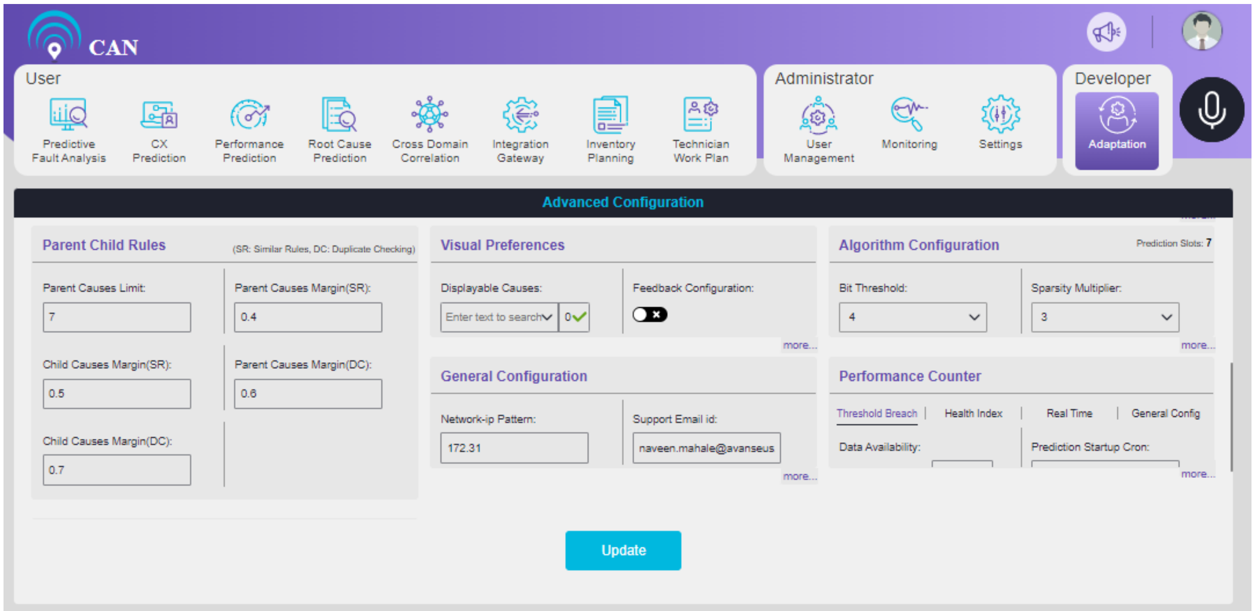
Ticket Correlation Prediction

General Configuration

Figure 15.77 - Fault Trace Generation

Parent Child Rules

- Parent Causes Limit - Maximum number of parent cause that can be input during the rule configuration.
- Parent Causes Margin (SR) - Minimum margin for checking the parent cause similarity percentage among other rules.
- Child Causes Margin (SR) - Minimum margin for checking the child cause similarity percentage among other rules.
- Parent Causes Margin (DC) - When the similarity percentage is more than the margin, parent cause is specified as duplicate.
- Child Causes Margin (DC) - When the similarity percentage is more than the margin, child cause is specified as duplicate.



Parent Child Rules (SR: Similar Rules, DC: Duplicate Checking)

Parent Causes Limit: 7

Parent Causes Margin(SR): 0.4

Child Causes Margin(SR): 0.5

Parent Causes Margin(DC): 0.6

Child Causes Margin(DC): 0.7

Visual Preferences

Displayable Causes: Enter text to search 0✓

Feedback Configuration:

General Configuration

Network-ip Pattern: 172.31

Support Email id: naveen.mahale@avanseus

Algorithm Configuration

Prediction Slots: 7

Bit Threshold: 4

Sparsity Multiplier: 3

Performance Counter

Threshold Breach | Health Index | Real Time | General Config

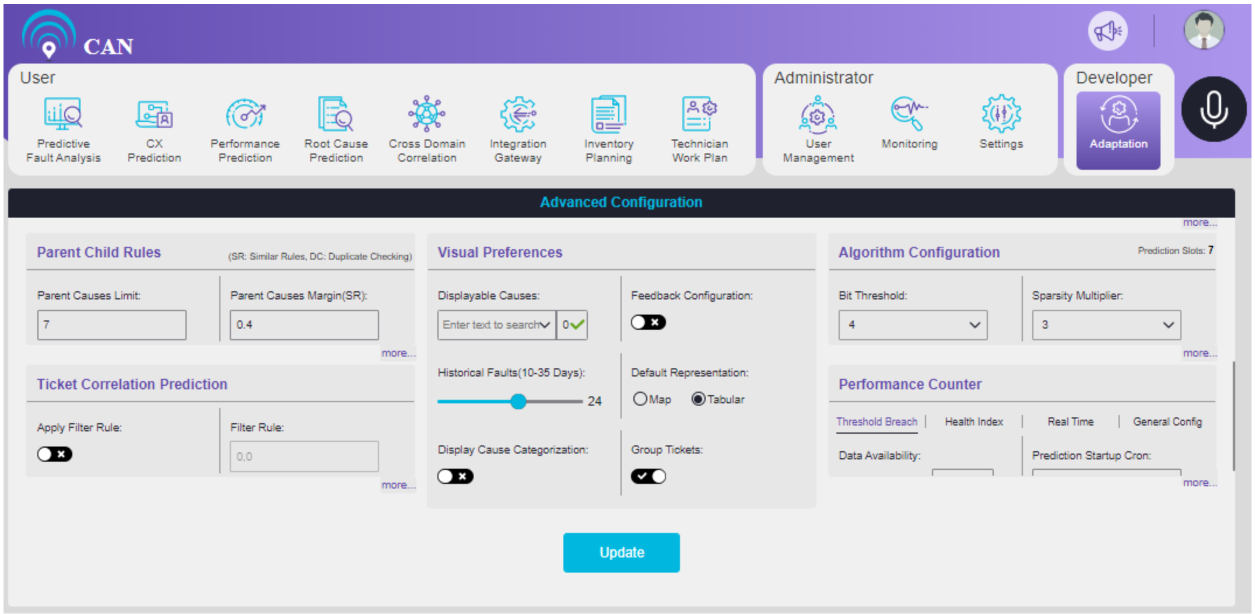
Data Availability:

Prediction Startup Cron:

Figure 15.78 - Parent Child Rules

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, enable or disable the toggle button to categorize the top faults.
- Group Tickets - Click the toggle button to YES, to group the alarms in Failure Analysis.



Parent Child Rules (SR: Similar Rules, DC: Duplicate Checking)

Parent Causes Limit: 7

Parent Causes Margin(SR): 0.4

Ticket Correlation Prediction

Apply Filter Rule: ○✕

Filter Rule: 0.0

Visual Preferences

Displayable Causes: Enter text to search 0 ✓

Feedback Configuration: ○✕

Historical Faults(10-35 Days): 24

Default Representation: ○ Map ● Tabular

Display Cause Categorization: ○✕

Group Tickets: ✓○

Algorithm Configuration — Prediction Slots: 7

Bit Threshold: 4

Sparsity Multiplier: 3

Performance Counter

Threshold Breach | Health Index | Real Time | General Config

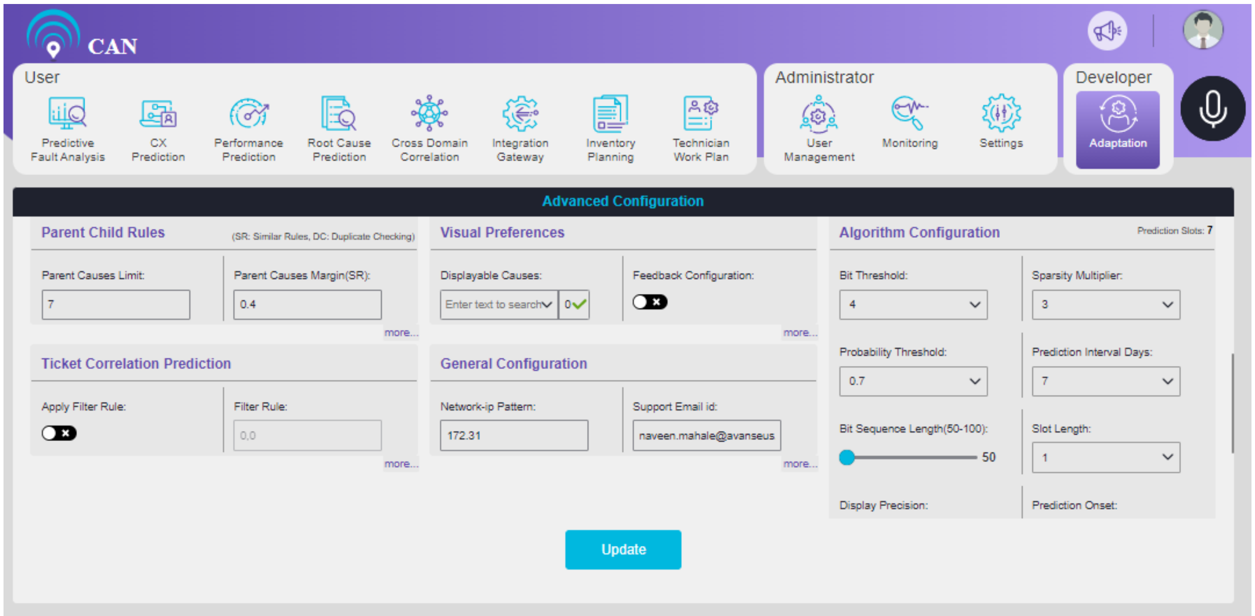
Data Availability:

Prediction Startup Cron:

Figure 15.79 - Visual Preferences

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.



Advanced Configuration

Parent Child Rules (SR: Similar Rules, DC: Duplicate Checking)

Parent Causes Limit: 7

Parent Causes Margin(SR): 0.4

more...

Visual Preferences

Displayable Causes: Enter text to search 0 ✓

Feedback Configuration: ☒

more...

Algorithm Configuration — Prediction Slots: 7

Bit Threshold: 4

Sparsity Multiplier: 3

Probability Threshold: 0.7

Prediction Interval Days: 7

Bit Sequence Length(50-100): 50

Slot Length: 1

Display Precision:

Prediction Onset:

Ticket Correlation Prediction

Apply Filter Rule: ☒

Filter Rule: 0,0

more...

General Configuration

Network-ip Pattern: 172.31

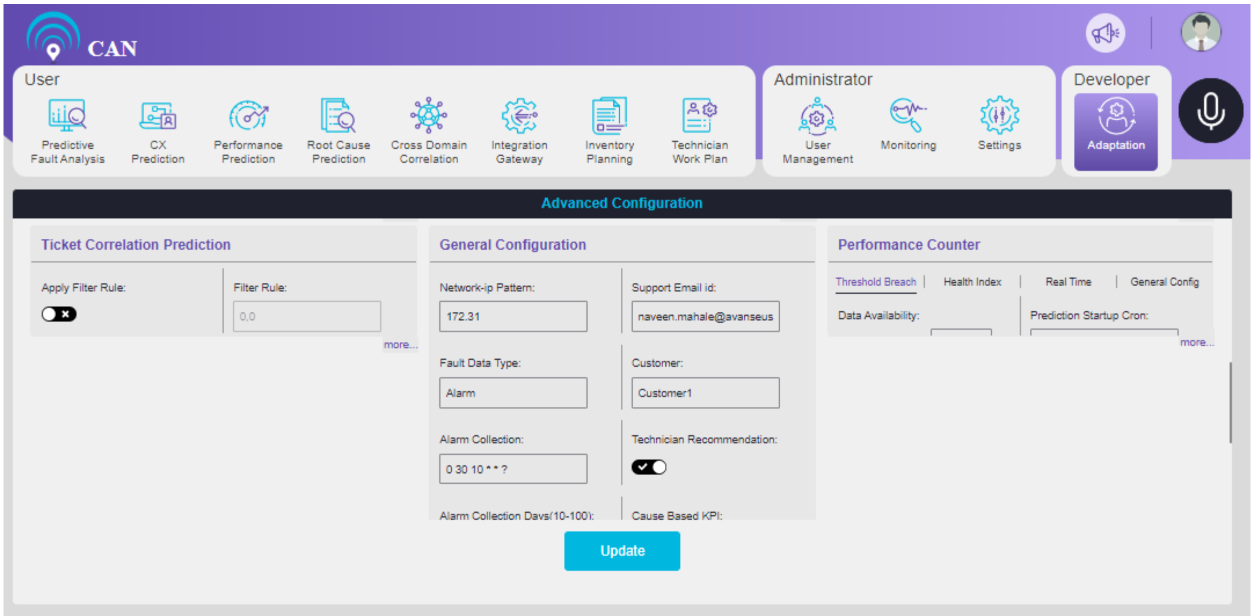
Support Email id: naveen.mahale@avanseus

more...

Figure 15.80 - Algorithm Configuration

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.
- Technician Recommendation - Decides whether a technician should be recommended.
- Alarm collection days - Number of days of data to be maintained for rendering UI.
- Prediction job - Cron to initiate data collection and prediction.
- 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 date format - It decides the date format.



Advanced Configuration

Ticket Correlation Prediction

Apply Filter Rule: ○✕

Filter Rule: 0.0

more...

General Configuration

Network-ip Pattern: 172.31

Support Email id: naveen.mahale@avanseus

Fault Data Type: Alarm

Customer: Customer1

Alarm Collection: 0 30 10 * * ?

Technician Recommendation: ✓●

Alarm Collection Days(10-100):

Cause Based KPI:

Performance Counter

Threshold Breach | Health Index | Real Time | General Config

Data Availability:

Prediction Startup Cron:

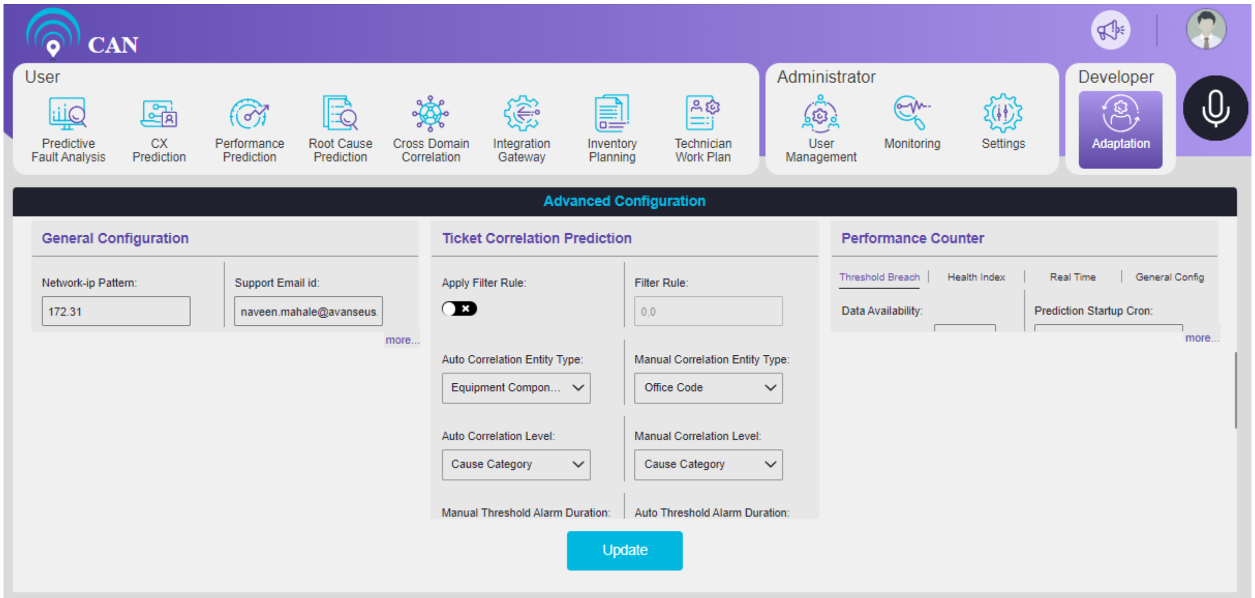
more...

Update

Figure 15.81 - General Configuration

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.
- Auto Correlation Entity Type: The device type/entity type at which we should run auto ticket correlation. For example, Equipment component, Office code.
- Manual Correlation Entity Type: the device type/entity type at which we should run manual ticket correlation.
- Auto Correlation Level: The cause group type at which we should auto run correlation.
- Manual Correlation Level: The cause group type at which we should run correlation manually.
- Manual Threshold Alarm Duration - This is the alarm duration to be considered during the Manual Ticket Correlation Prediction. User can slide the slider to set the duration of the alarm (0-30) minutes.
- Auto Threshold Alarm Duration - This is the alarm duration to be considered during the Auto Ticket Correlation Prediction. User can slide the slider to set the duration of the alarm (0-2) 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 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.
- Sparsity multiplier - Multiplier to go back more in history as part of variable horizon.
- Manual Ticket Correlation Level - It correlates the alarms and tickets. The Correlation level for Manual Ticket Correlation prediction.
- Threshold Probability - Probable threshold of the fault occurrence.



Advanced Configuration

General Configuration

Network-ip Pattern: 172.31

Support Email id: naveen.mahale@avanseus.

more...

Ticket Correlation Prediction

Apply Filter Rule: ✕

Filter Rule: 0,0

Auto Correlation Entity Type: Equipment Compon...

Manual Correlation Entity Type: Office Code

Auto Correlation Level: Cause Category

Manual Correlation Level: Cause Category

Manual Threshold Alarm Duration:

Auto Threshold Alarm Duration:

Performance Counter

Threshold Breach | Health Index | Real Time | General Config

Data Availability:

Prediction Startup Cron:

more...

Figure 15.82 - Ticket Correlation Prediction

Performance Counter

- Data Availability - Frequency of data availability in performance counter data.
- Prediction Interval - The period for which prediction is made e.g. 6 days.
- 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.
- Default Representation - Default view of the performance prediction tab.
- Default Domain - User has an option to select the default domain to be displayed on the performance prediction screen.
- Default Network Type - User has an option to select the default network type according to the domain.

Parameters specific to Threshold Breach, Health Index and Real Time are as follows:

Threshold Breach

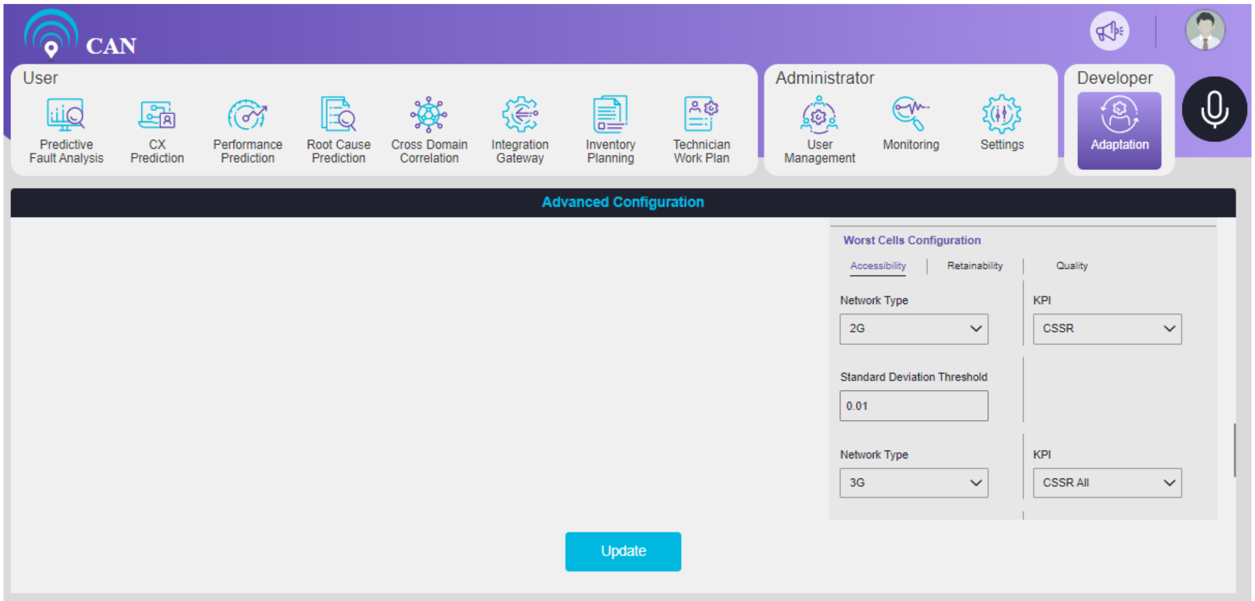
- Prediction Startup Cron - Schedule the job to start the prediction.
- Worst Cells Limit - Displays the maximum number of worst cells on the performance prediction screen.

Worst Cells Configuration

Accessibility / Retainability / Quality

Worst Cell is defined for Threshold Breach using the Accessibility, Retainability and Quality parameters. It is applicable only for ACCESS domain.

- Network Type - User can select the Network Type from the dropdown.
- KPI - For each network type, a KPI is defined.
- Standard Deviation Threshold - When the value goes below the specified threshold, that KPI is considered as worst cell.
- Add New Configuration - This is used to add a new configuration for every Network Type.



Worst Cells Configuration

Accessibility | Retainability | Quality

Network Type: 2G

KPI: CSSR

Standard Deviation Threshold: 0.01

Network Type: 3G

KPI: CSSR All

Figure 15.83 - Worst Cells Configuration

Health Index

- Prediction Startup Cron - Schedule the job to start the prediction.
- Critical Level - The health of the equipment component has degraded.
- Warning Level - The health of an equipment component is degrading, so client has to take the necessary action.

Real Time

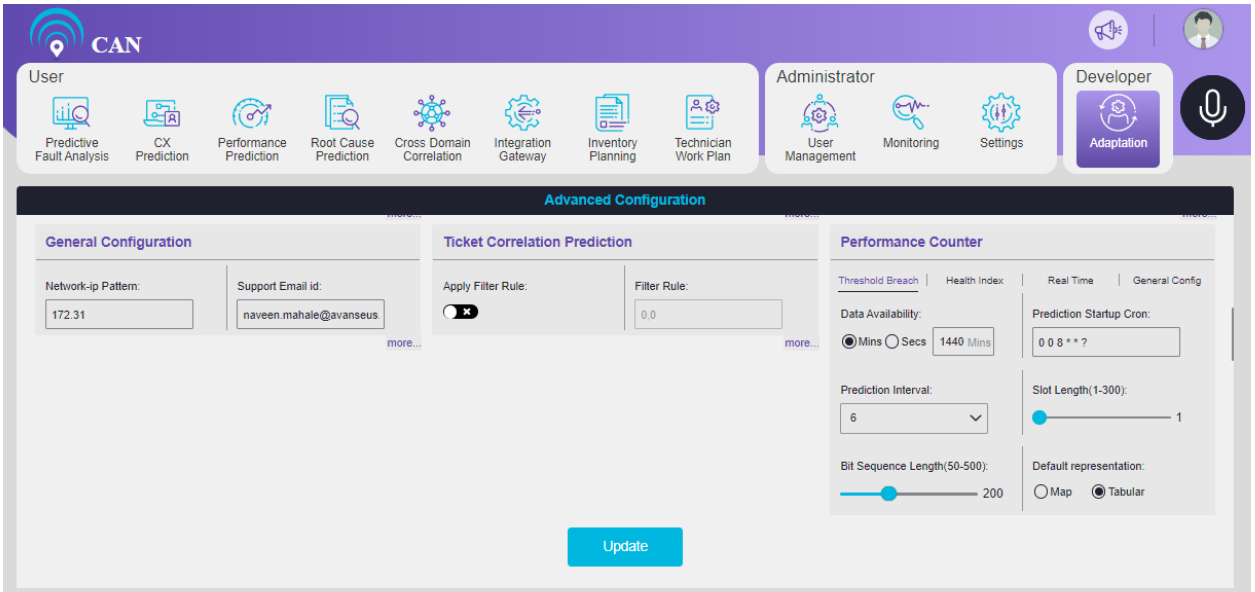
- Cron: Schedule the job to retrieve real time predictions.

Archive Data

- Prediction Threshold Slots - Maximum number of slots to keep the data and remove the older data from Prediction table.
- Threshold Slots - Maximum number of slots to keep the data and remove the older data from Performance Counter table.
- Cron - Schedule the job for archiving the data.

General Config

- Domain - User has a drop down to Add or Delete the domain. Domain value should be CORE or TRANSPORT, ACCESS, E2E, WIRED-LINE or as per the customer data.
- Network Type - User has a drop down to Add or Delete the Network Type. The Network Type will depend on the domain. **Network Type** should be relevant to domain and it should be unique across all the domains.



General Configuration

Network-ip Pattern: 172.31

Support Email id: naveen.mahale@avanseus.

Ticket Correlation Prediction

Apply Filter Rule: ✕

Filter Rule: 0,0

Performance Counter

Data Availability: ● Mins ○ Secs 1440 Mins

Prediction Startup Cron: 0 0 8 * * ?

Prediction Interval: 6

Slot Length(1-300): 1

Bit Sequence Length(50-500): 200

Default representation: ○ Map ● Tabular

Figure 15.84 - Performance Counter

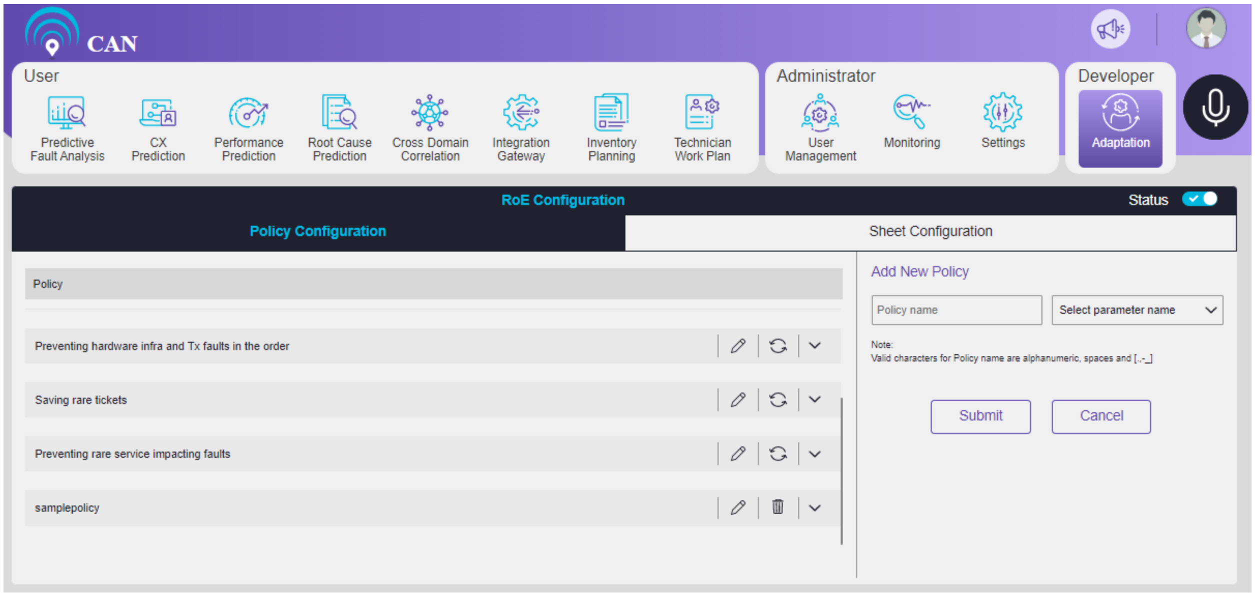
RoE Configuration

Return on Effort (RoE) index based prediction shortlisting is a way of selecting a particular subset of predicted faults that 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 two tabs:

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



Preventing hardware infra and Tx faults in the order

Saving rare tickets

Preventing rare service impacting faults

samplepolicy

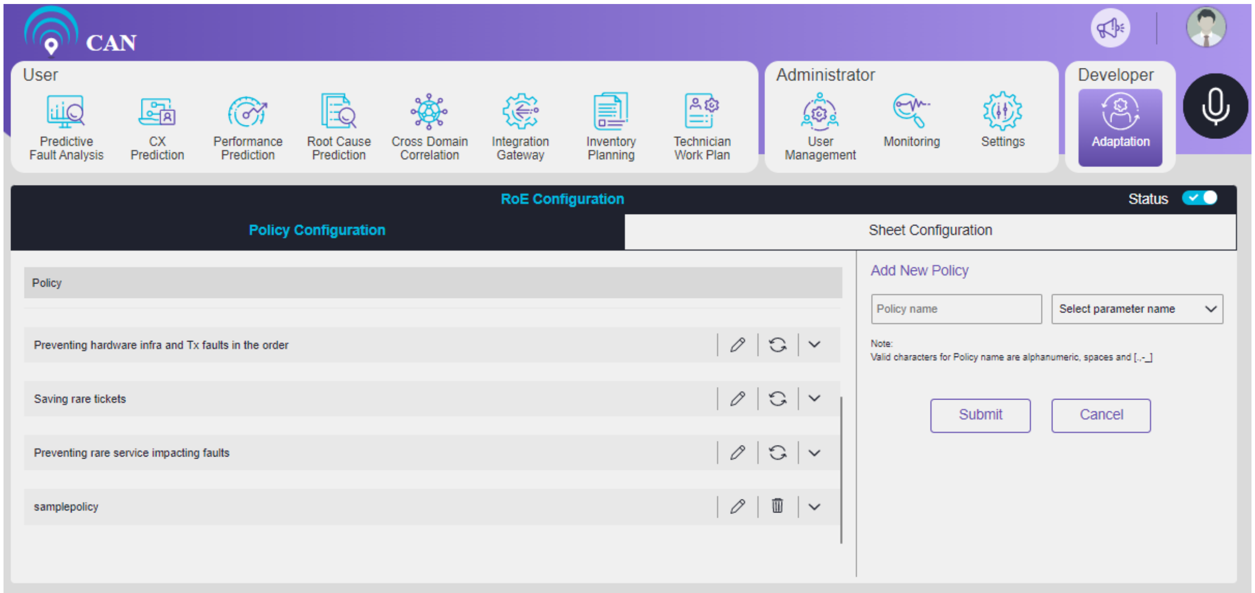
Note:
Valid characters for Policy name are alphanumeric, spaces and [.-_]

Figure 15.85 - 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.



Preventing hardware infra and Tx faults in the order

Saving rare tickets

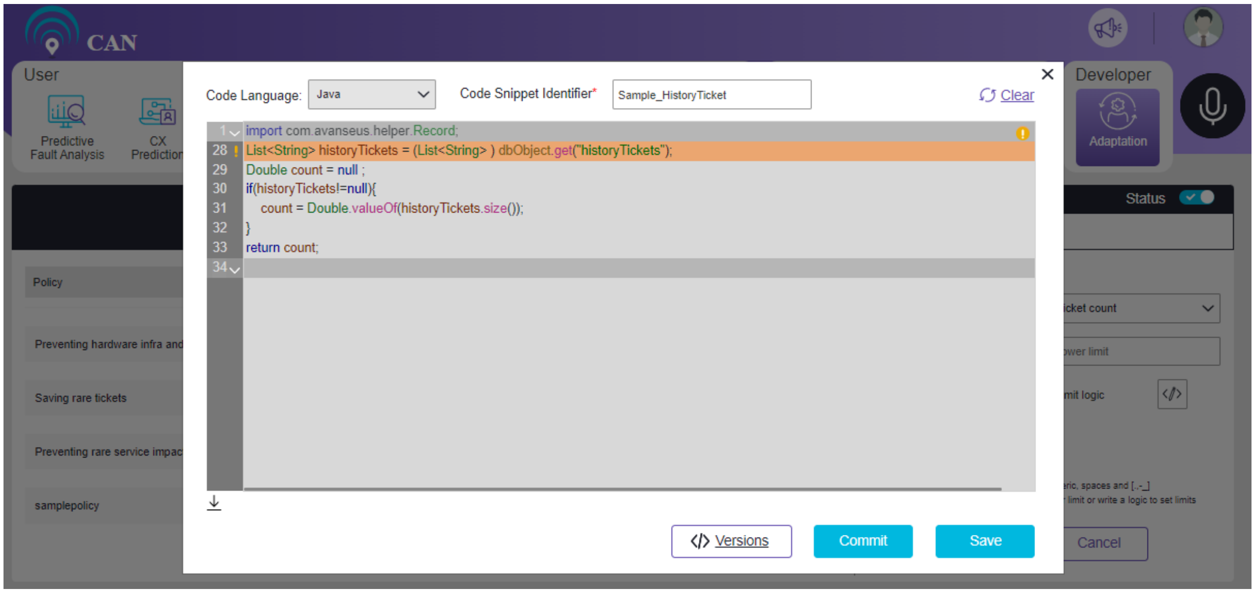
Preventing rare service impacting faults

samplepolicy

Note:
Valid characters for Policy name are alphanumeric, spaces and [.-_]

Figure 15.86 – Add New Policy in Policy Configuration

3. Click the Parameter value icon </>.



Code Language: Java

Code Snippet Identifier* Sample_HistoryTicket

```
import com.avanseus.helper.Record;
List<String> historyTickets = (List<String> ) dbObject.get("historyTickets");
Double count = null ;
if(historyTickets!=null){
    count = Double.valueOf(historyTickets.size());
}
return count;
```

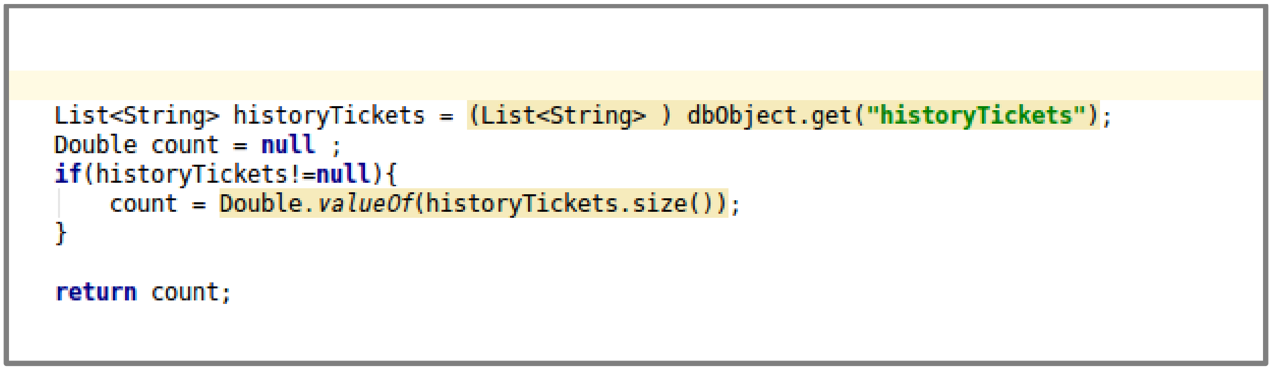
Figure 15.87 - Code Snippet for Parameter Value

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 impact** 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 15.88 - Logic to Fetch Number of Tickets

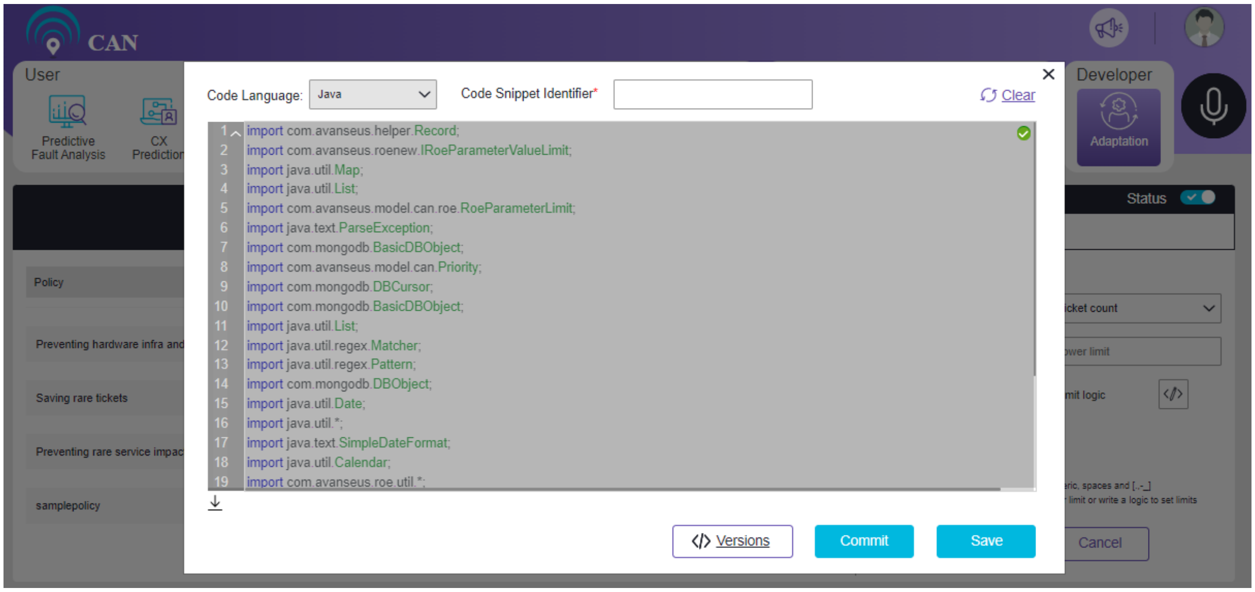
Note: The java code will implement IRoeParameterValue interface that provides “dbObject” as parameter.

This implementation needs code snippet. It does not 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.



Code Language: Java

Code Snippet Identifier*

```java
import com.avanseus.helper.Record;
import com.avanseus.roenew.IRoeParameterValueLimit;
import java.util.Map;
import java.util.List;
import com.avanseus.model.can.roe.RoeParameterLimit;
import java.text.ParseException;
import com.mongodb.BasicDBObject;
import com.avanseus.model.can.Priority;
import com.mongodb.DBCursor;
import com.mongodb.BasicDBObject;
import java.util.List;
import java.util.regex.Matcher;
import java.util.regex.Pattern;
import com.mongodb.DBObject;
import java.util.Date;
import java.util.*;
import java.text.SimpleDateFormat;
import java.util.Calendar;
import com.avanseus.roe.util.*;
```

Figure 15.89 - 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 that provides predictedFaultCursor as parameter and expects RoeParameterLimit as return type.

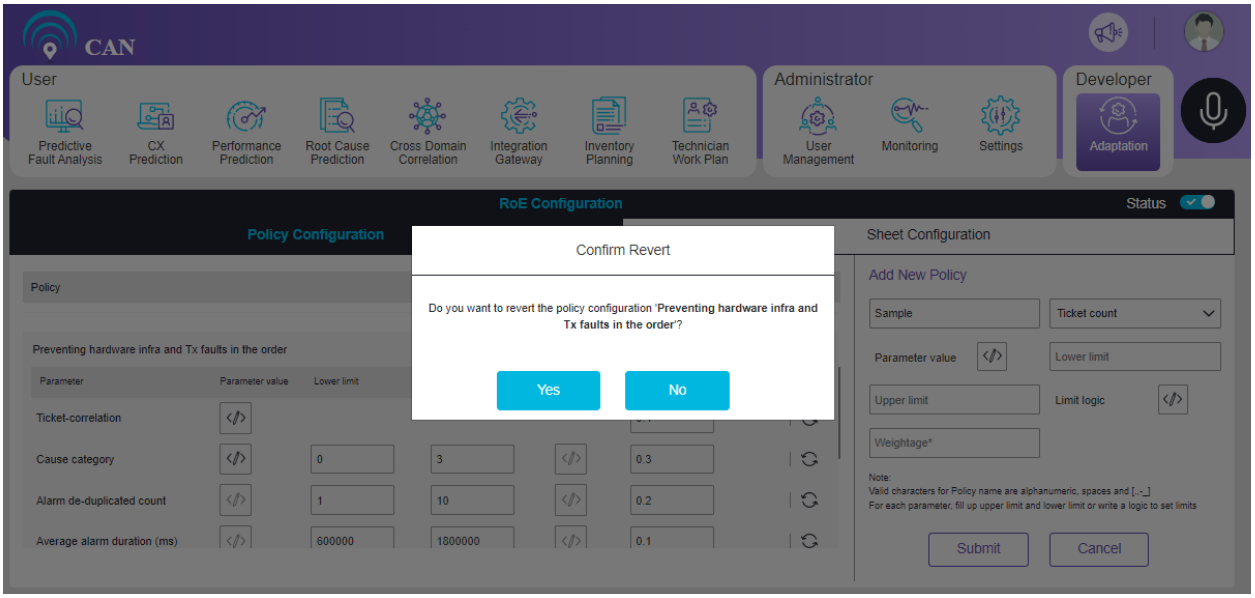
```
RoeParameterLimit roeParameterLimit = new RoeParameterLimit();
roeParameterLimit.setLowerLimit(0.0);
roeParameterLimit.setUpperLimit(4.0);
return roeParameterLimit;
```

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, and 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.



Confirm Revert

Do you want to revert the policy configuration '**Preventing hardware infra and Tx faults in the order**'?

Yes No

Policy

Preventing hardware infra and Tx faults in the order

Parameter	Parameter value	Lower limit			
Ticket-correlation	</>				
Cause category	</>	0	3	</>	0.3
Alarm de-duplicated count	</>	1	10	</>	0.2
Average alarm duration (ms)	</>	600000	1800000	</>	0.1

Add New Policy

Sample Ticket count

Parameter value </> Lower limit

Upper limit Limit logic </>

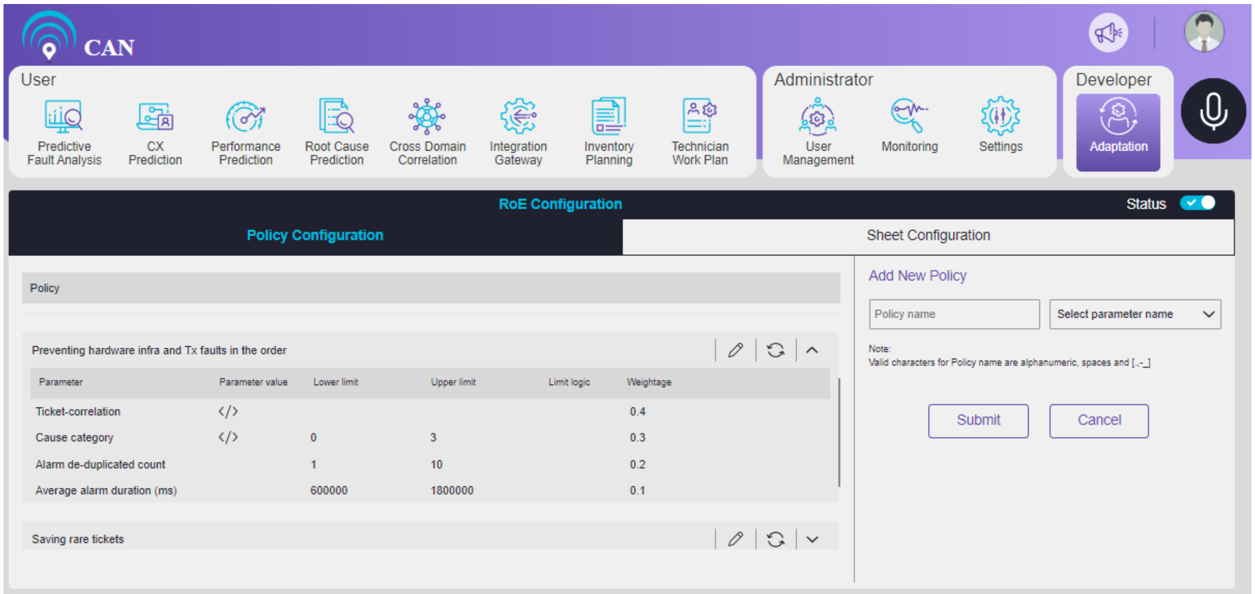
Weightage*

Note:
Valid characters for Policy name are alphanumeric, spaces and [.,-_]
For each parameter, fill up upper limit and lower limit or write a logic to set limits

Submit Cancel

Figure 15.90 - Revert Confirmation Message

5. User can click on ⌄ icon to view the details of the configured policy.



Policy

Preventing hardware infra and Tx faults in the order

Parameter	Parameter value	Lower limit	Upper limit	Limit logic	Weightage
Ticket-correlation	</>				0.4
Cause category	</>	0	3		0.3
Alarm de-duplicated count		1	10		0.2
Average alarm duration (ms)		600000	1800000		0.1

Saving rare tickets

Add New Policy

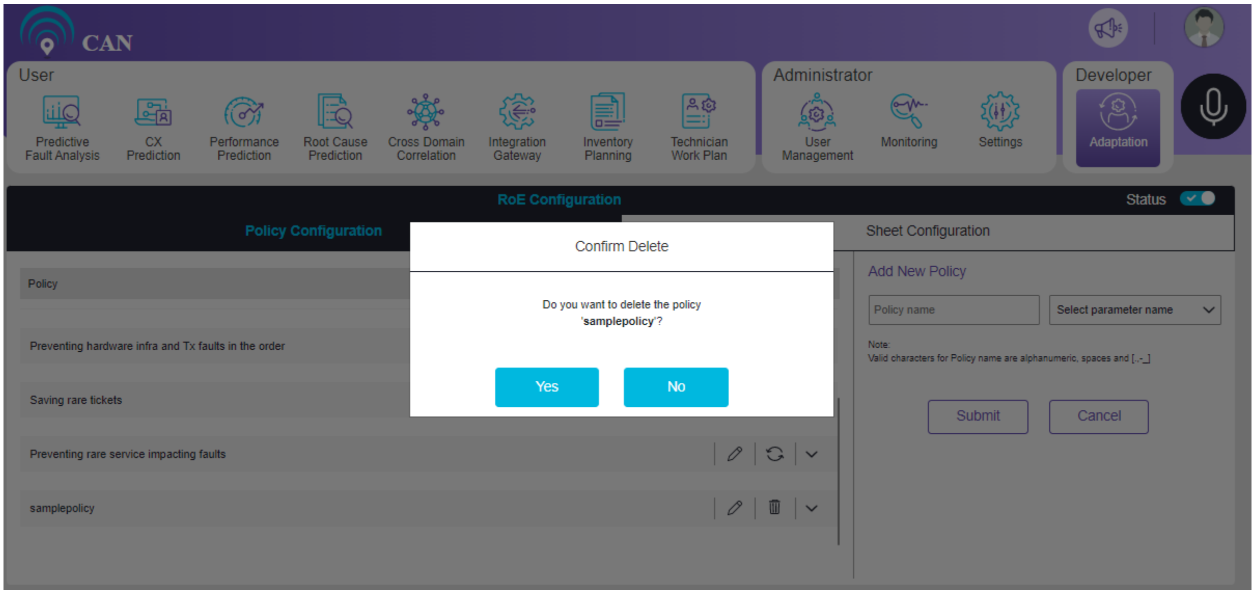
Policy name Select parameter name

Note:
Valid characters for Policy name are alphanumeric, spaces and [.,-_]

Submit Cancel

Figure 15.91 – Policy Details

6. User can use the delete icon 🗑 to delete the particular parameter row in the user added New Policy.
7. Click **Yes** button to delete the newly Added New Policy. Click **No** if you do not want to delete.



Policy

Preventing hardware infra and Tx faults in the order

Saving rare tickets

Preventing rare service impacting faults

samplepolicy

Confirm Delete

Do you want to delete the policy 'samplepolicy'?

Add New Policy

Policy name | Select parameter name

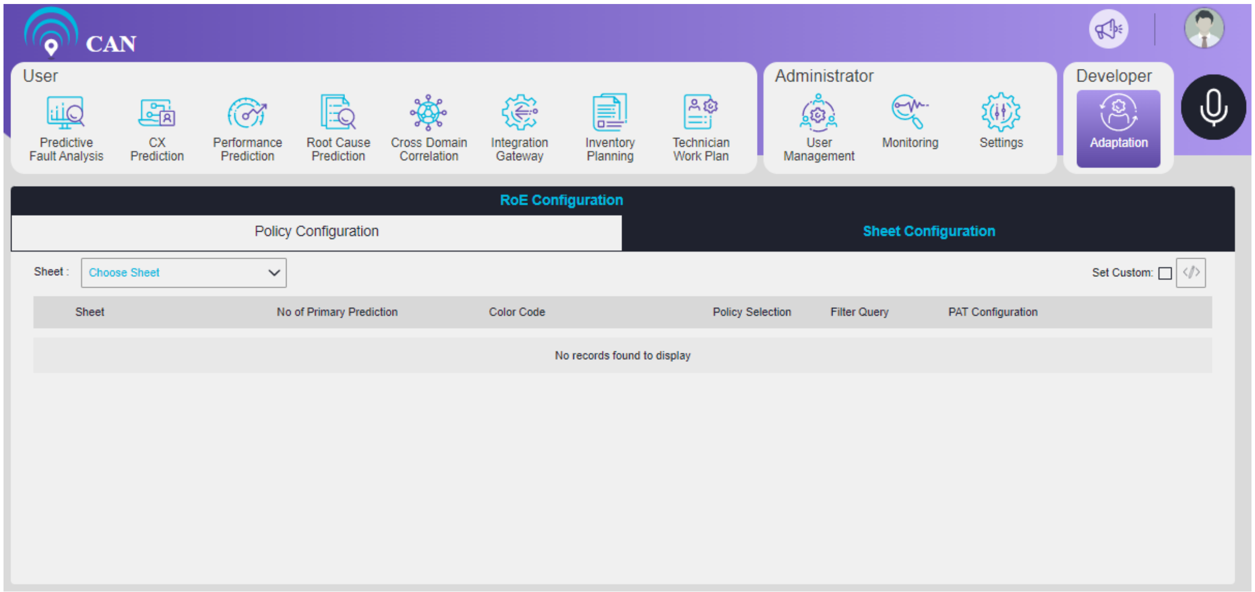
Note:
Valid characters for Policy name are alphanumeric, spaces and [.-_]

Figure 15.92 - Delete Confirmation Message

To enable/disable RoE, use the toggle button ✓.

Sheet Configuration

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



Sheet : Choose Sheet

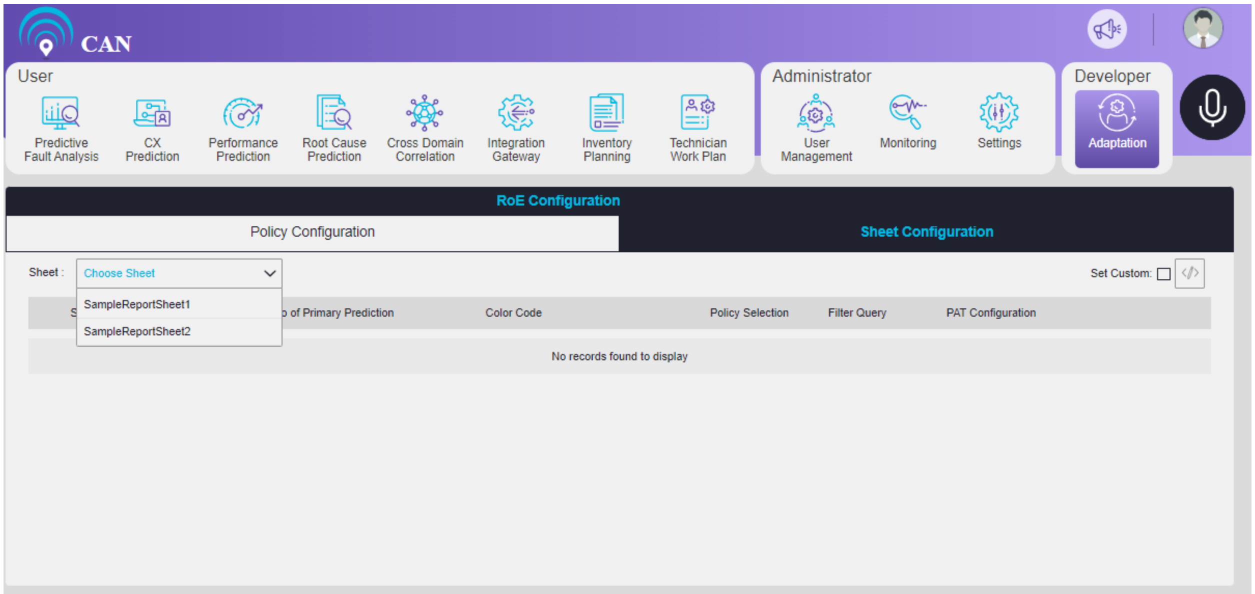
Set Custom: □

Sheet	No of Primary Prediction	Color Code	Policy Selection	Filter Query	PAT Configuration

No records found to display

Figure 15.93 - 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.



Sheet : Choose Sheet

SampleReportSheet1
SampleReportSheet2

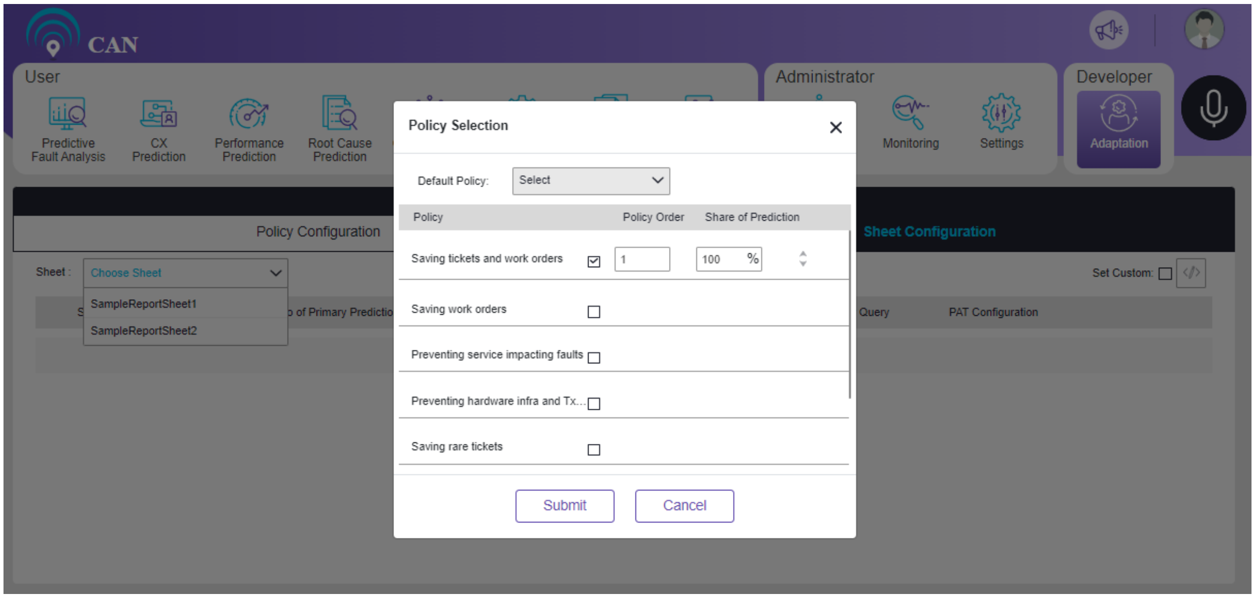
Set Custom: □

S	of Primary Prediction	Color Code	Policy Selection	Filter Query	PAT Configuration

No records found to display

Figure 15.94 - 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** (such that sum of them equals 100)**.**



Policy Selection ✕

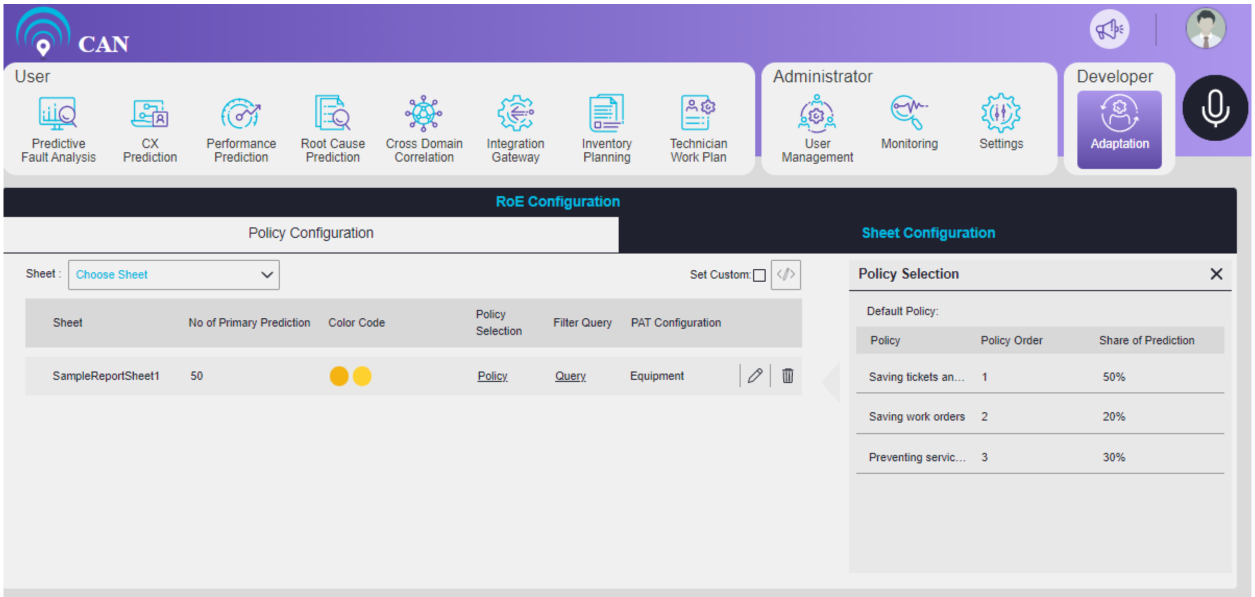
Default Policy: Select

Policy		Policy Order	Share of Prediction
Saving tickets and work orders	☑	1	100 %
Saving work orders	□		
Preventing service impacting faults	□		
Preventing hardware infra and Tx...	□		
Saving rare tickets	□		

Submit Cancel

Figure 15.95 - Policy Selection

User can see the details of the Policy Selection. To see the details, under **Policy Selection**, click **<u>Policy</u>**.



Sheet	No of Primary Prediction	Color Code	Policy Selection	Filter Query	PAT Configuration
SampleReportSheet1	50	●●	Policy	Query	Equipment

Policy Selection ✕

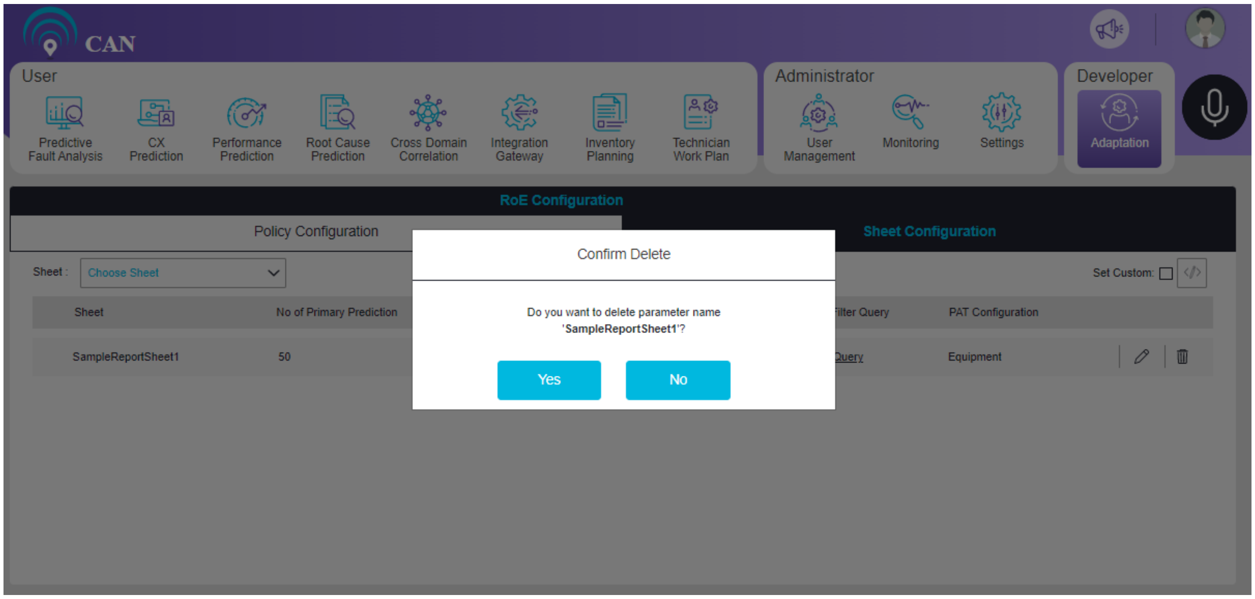
Default Policy:

Policy	Policy Order	Share of Prediction
Saving tickets an...	1	50%
Saving work orders	2	20%
Preventing servic...	3	30%

Figure 15.96 - 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.



Confirm Delete

Do you want to delete parameter name 'SampleReportSheet1'?

Yes No

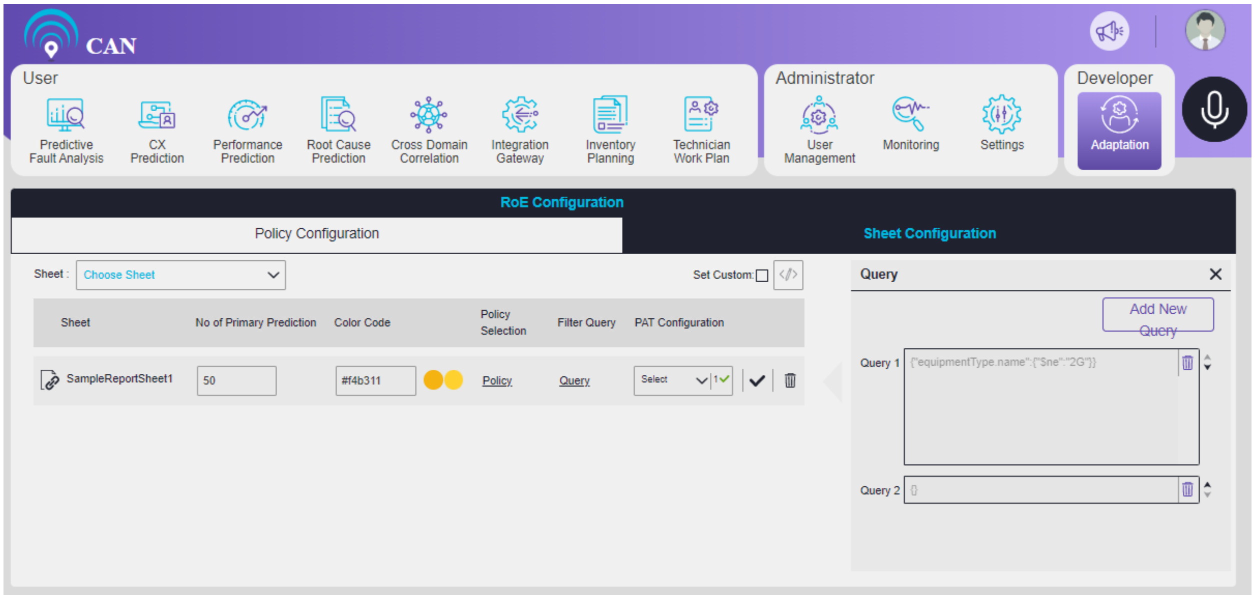
Figure 15.97 - Delete the Configuration for SampleSheet1

Configurations provided in this tab are:

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

4. PAT Configuration: PAT is a unique and predictive ticket identifier that is required to track the predictions.

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



Sheet	No of Primary Prediction	Color Code	Policy Selection	Filter Query	PAT Configuration
SampleReportSheet1	50	#f4b311 ●●	Policy	Query	Select

Query 1 {"equipmentType.name":{"$ne":"2G"}}

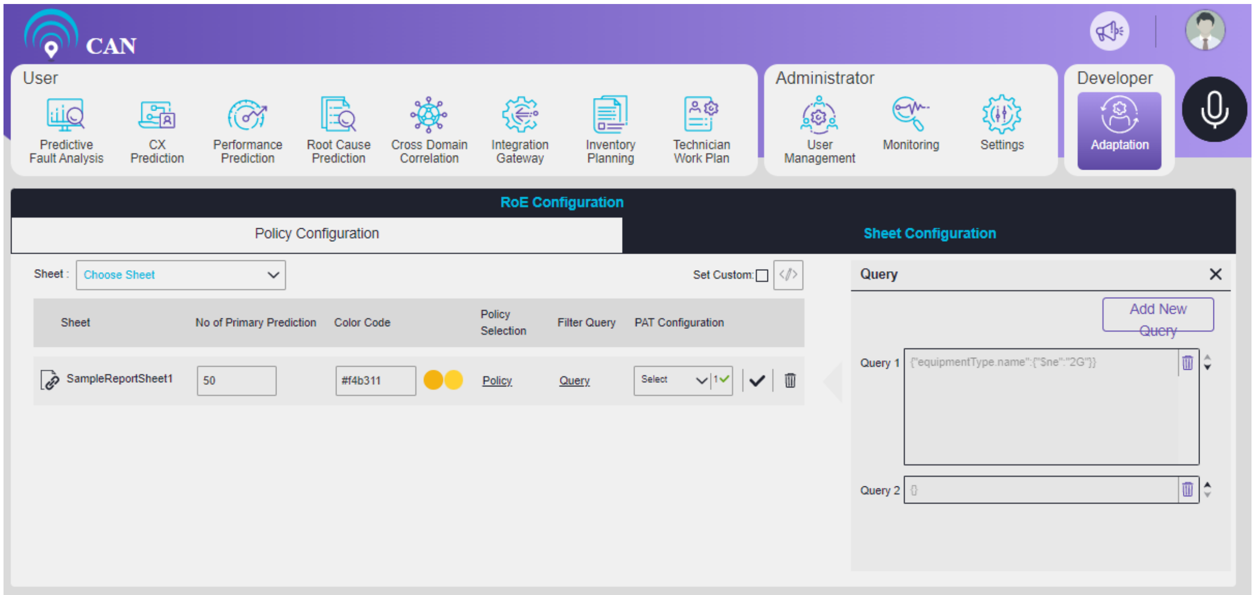
Query 2 {}

Figure 15.98 - 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.



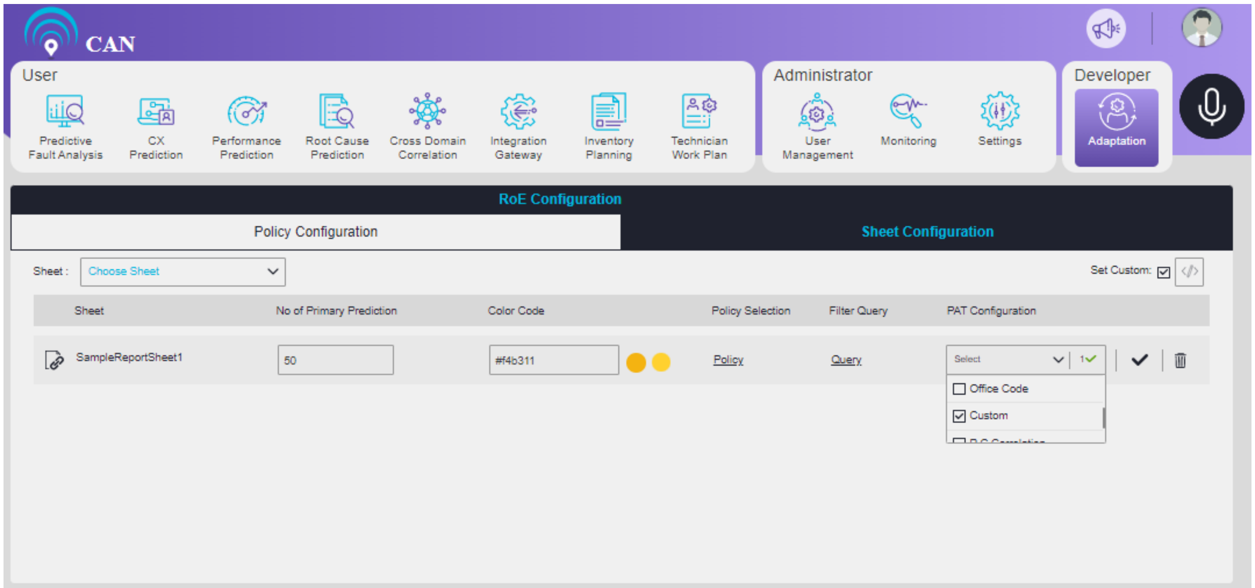
Sheet	No of Primary Prediction	Color Code	Policy Selection	Filter Query	PAT Configuration
SampleReportSheet1	50	#f4b311 ●●	Policy	Query	Select

Query 1 {"equipmentType.name":{"$ne":"2G"}}

Query 2 {}

Figure 15.99 - Pop up to Write Query in json Format

User can select one or multiple PAT configuration from the drop down. PAT is configured at the generation level based on the customer requirement. If **Custom** is selected, the grouping logic to perform PAT generation is based on custom logic that user has written in IDE. Checkbox is used to enable or disable its usage in ROE sheet configuration.



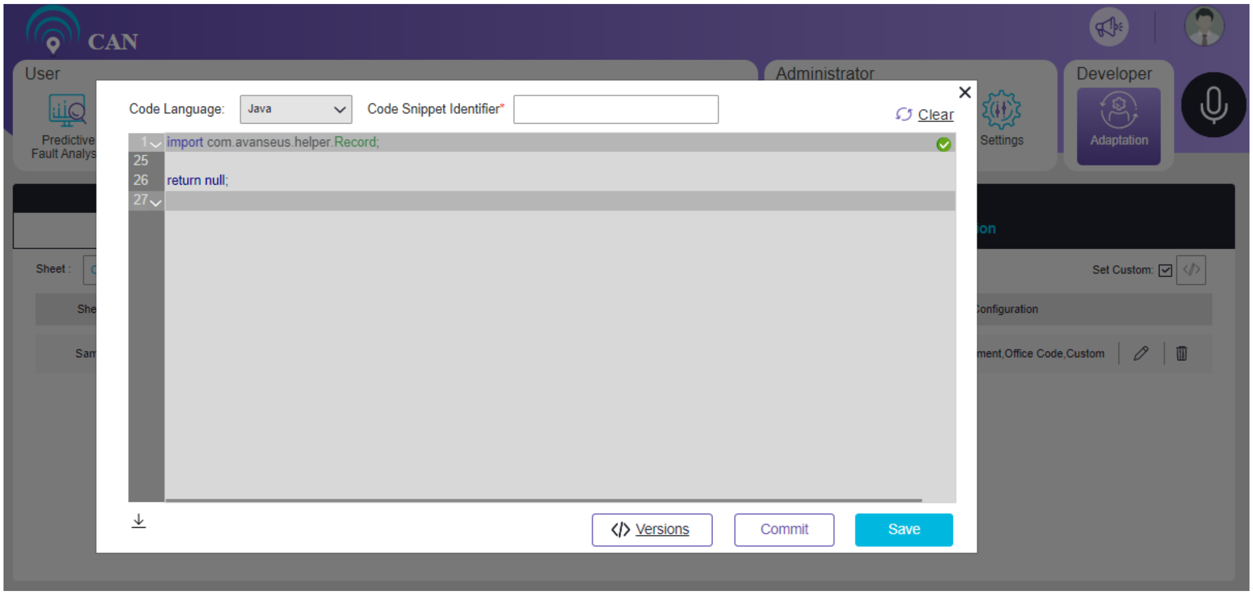
Sheet : Choose Sheet

Set Custom: ☑

Sheet	No of Primary Prediction	Color Code	Policy Selection	Filter Query	PAT Configuration
SampleReportSheet1	50	#f4b311	Policy	Query	Select 1✓

☐ Office Code
☑ Custom
☐ P C Correlation

Figure 15.100 - PAT Configuration Selection



Code Language: Java

Code Snippet Identifier*

```
import com.avanseus.helper.Record;

return null;
```

Figure 15.101 - Custom PAT Configuration IDE

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.

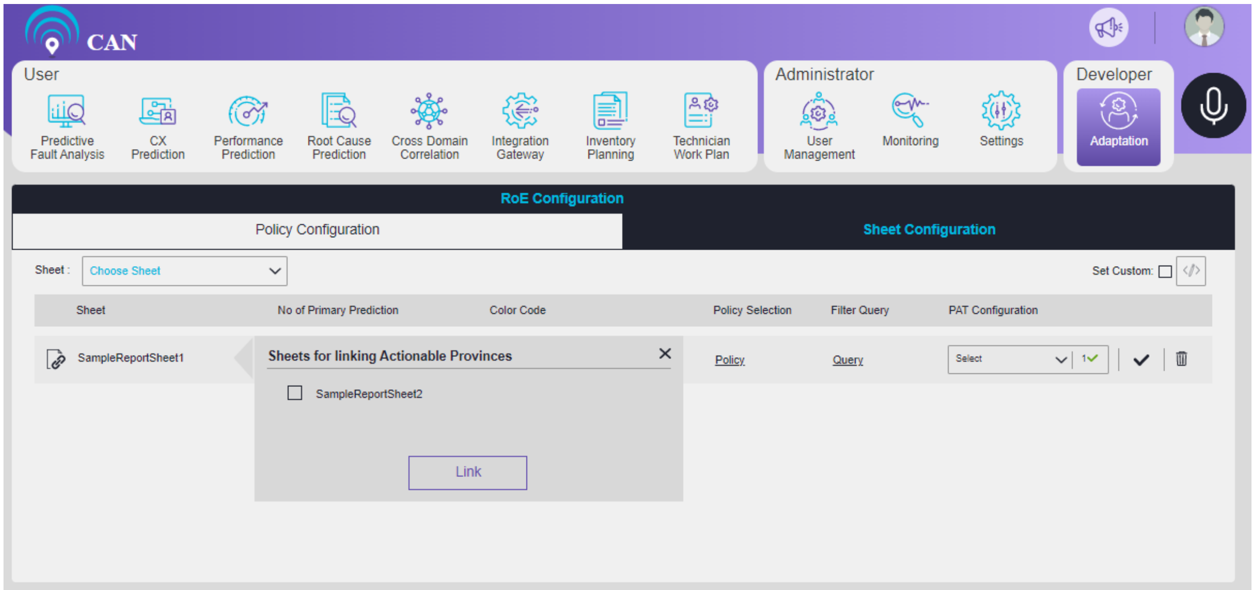


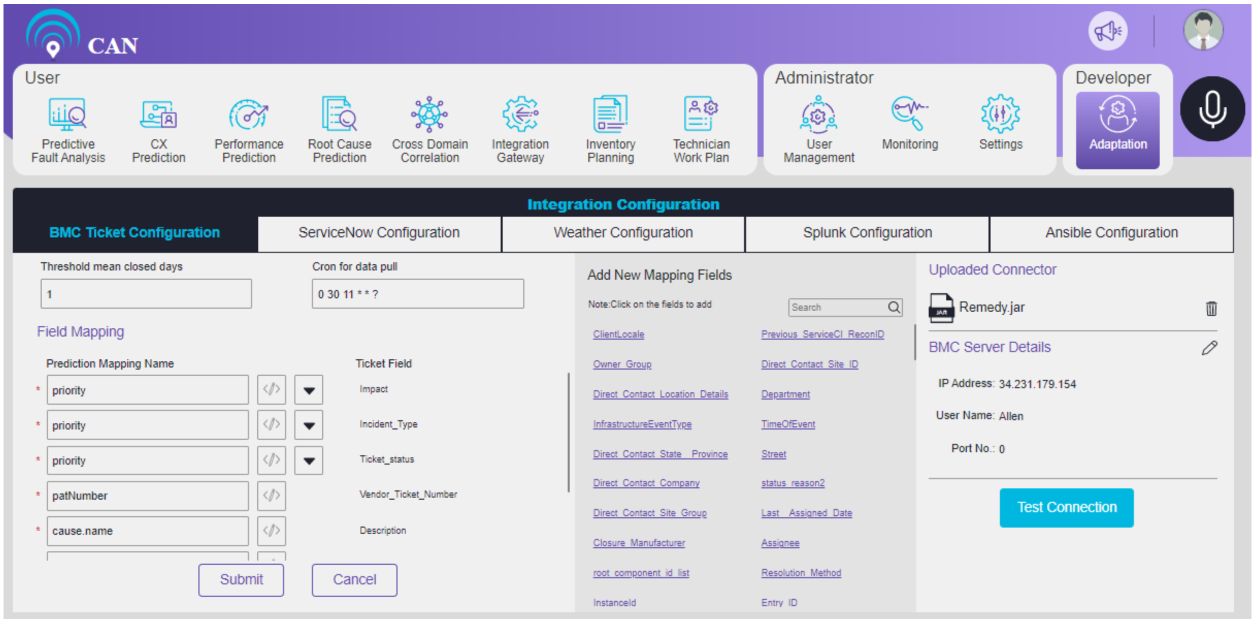
Figure 15.102 - Linked sheets

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

Integration Configuration

Integration Configuration has five tabs:

1. BMC Ticket Configuration
2. ServiceNow Configuration
3. Weather Configuration
4. Splunk Configuration
5. Ansible Configuration



Threshold mean closed days: 1

Cron for data pull: 0 30 11 * * ?

Field Mapping

Prediction Mapping Name	Ticket Field
* priority	Impact
* priority	Incident_Type
* priority	Ticket_status
* patNumber	Vendor_Ticket_Number
* cause.name	Description

Add New Mapping Fields

Note:Click on the fields to add

ClientLocale	Previous_ServiceCI_ReconID
Owner_Group	Direct_Contact_Site_ID
Direct_Contact_Location_Details	Department
InfrastructureEventType	TimeOfEvent
Direct_Contact_State__Province	Street
Direct_Contact_Company	status_reason2
Direct_Contact_Site_Group	Last__Assigned_Date
Closure_Manufacturer	Assignee
root_component_id_list	Resolution_Method
InstanceId	Entry_ID

Uploaded Connector

Remedy.jar

BMC Server Details

IP Address: 34.231.179.154

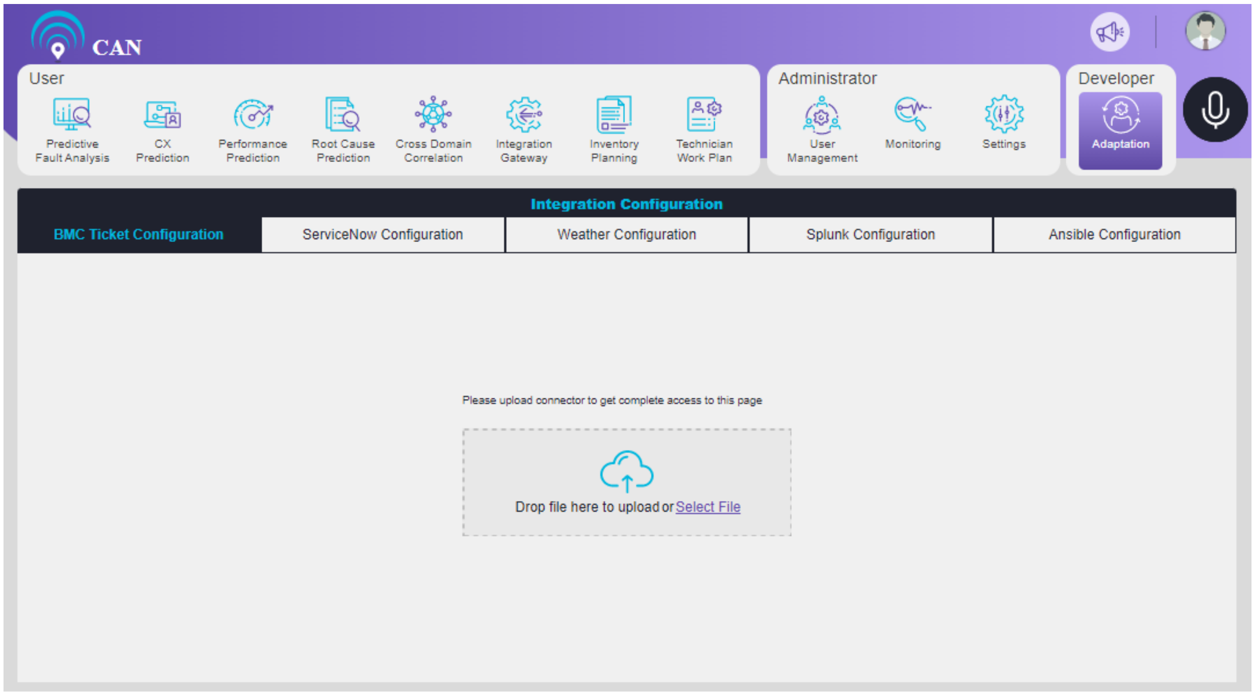
User Name: Allen

Port No.: 0

Figure 15.103 - Integration Configuration Screen

BMC Ticket Configuration

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



Please upload connector to get complete access to this page

Drop file here to upload or Select File

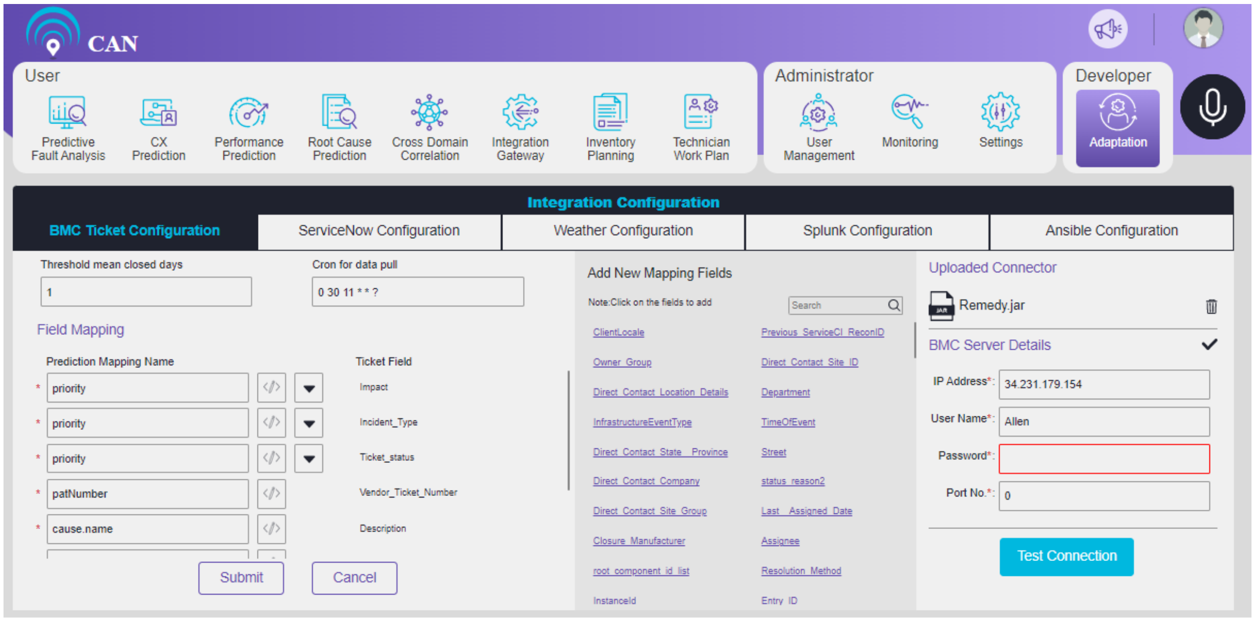
Figure 15.104 - BMC Ticket Configuration Screen

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.



Threshold mean closed days: 1

Cron for data pull: 0 30 11 * * ?

Prediction Mapping Name	Ticket Field
priority	Impact
priority	Incident_Type
priority	Ticket_status
patNumber	Vendor_Ticket_Number
cause.name	Description

IP Address*: 34.231.179.154

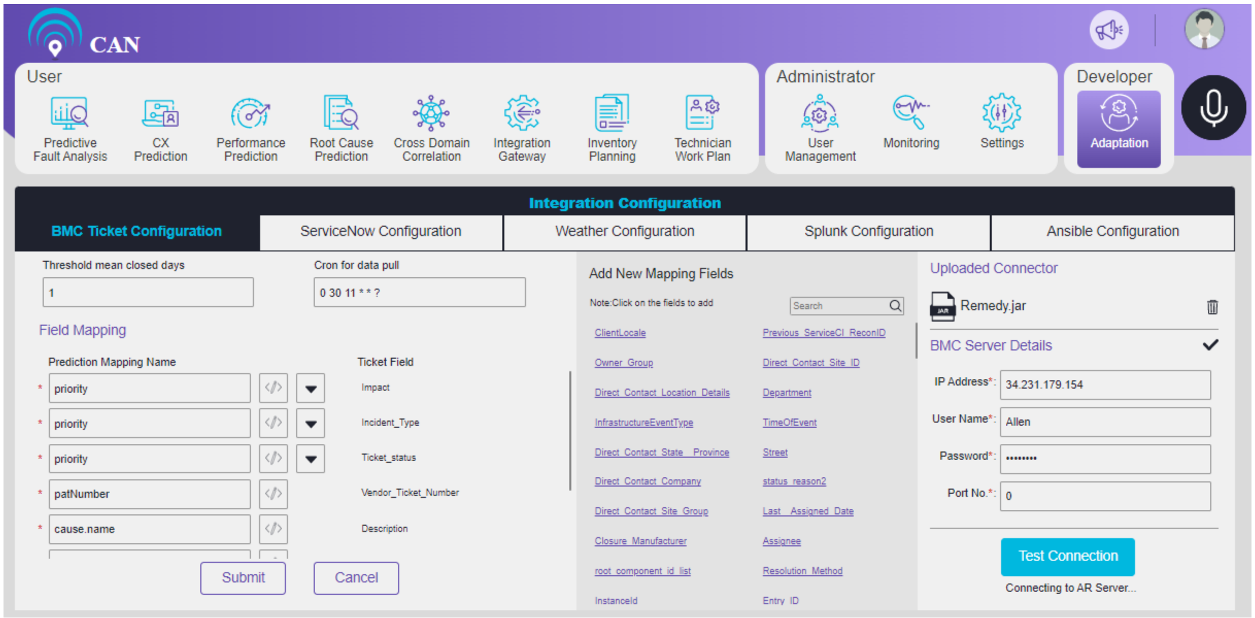
User Name*: Allen

Password*:

Port No.*: 0

Figure 15.105 - BMC Server Details

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



Threshold mean closed days: 1

Cron for data pull: 0 30 11 * * ?

Prediction Mapping Name	Ticket Field
priority	Impact
priority	Incident_Type
priority	Ticket_status
patNumber	Vendor_Ticket_Number
cause.name	Description

IP Address*: 34.231.179.154

User Name*: Allen

Password*: ••••••••

Port No.*: 0

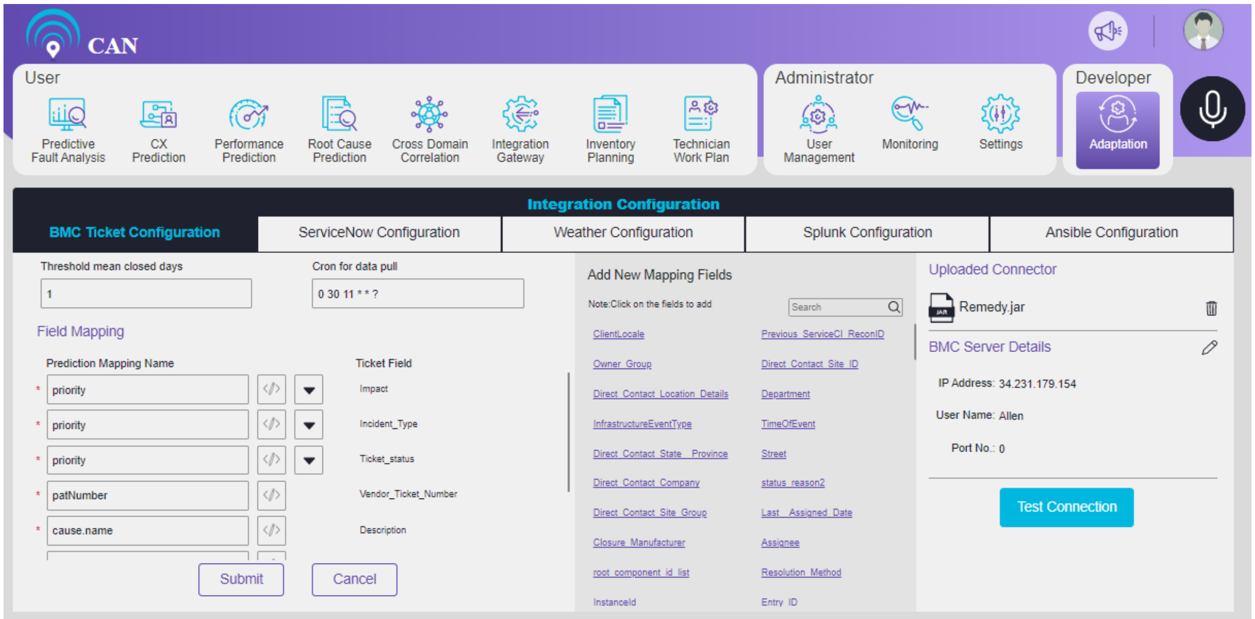
Connecting to AR Server...

Figure 15.106 - 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.



Threshold mean closed days: 1

Cron for data pull: 0 30 11 * * ?

Field Mapping

Prediction Mapping Name	Ticket Field
* priority	Impact
* priority	Incident_Type
* priority	Ticket_status
* patNumber	Vendor_Ticket_Number
* cause.name	Description

Add New Mapping Fields

Note:Click on the fields to add

Search

ClientLocale	Previous_ServiceCI_ReconID
Owner_Group	Direct_Contact_Site_ID
Direct_Contact_Location_Details	Department
InfrastructureEventType	TimeOfEvent
Direct_Contact_State__Province	Street
Direct_Contact_Company	status_reason2
Direct_Contact_Site_Group	Last__Assigned_Date
Closure_Manufacturer	Assignee
root_component_id_list	Resolution_Method
InstanceId	Entry_ID

Uploaded Connector

Remedy.jar

BMC Server Details

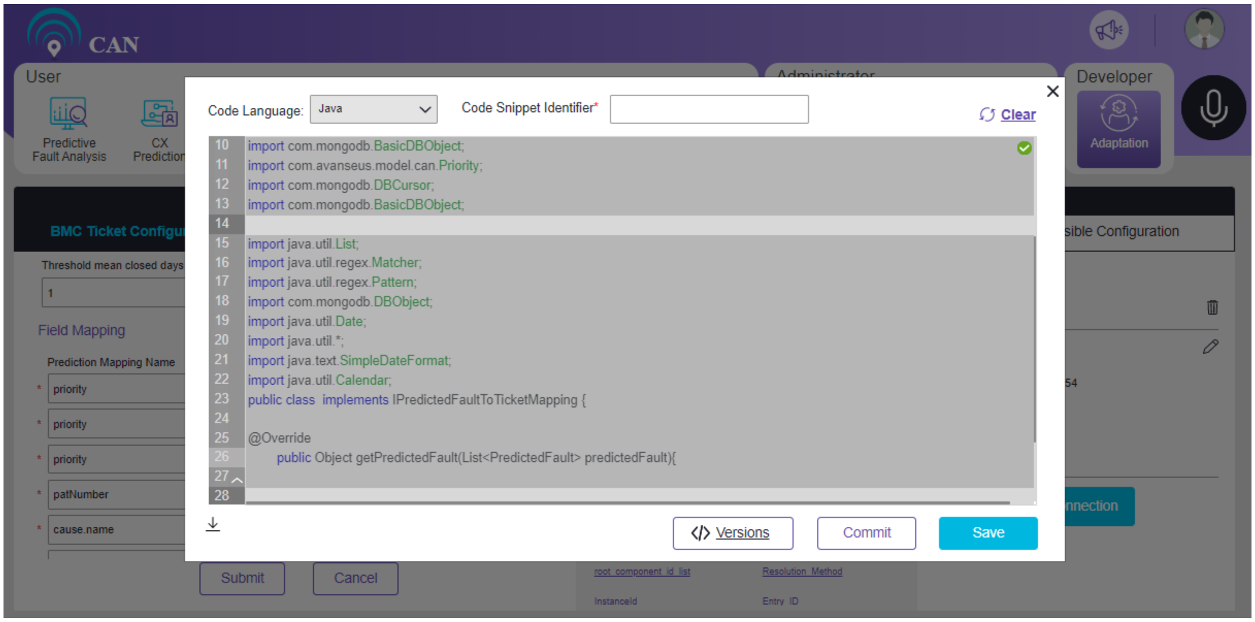
IP Address: 34.231.179.154

User Name: Allen

Port No.: 0

Figure 15.107 - BMC Ticket Configuration Screen

Click the icon </> to edit the mapping codes. User can see the saved configuration. User can write the corresponding java or python mapping code in the text area. It will automatically be compiled. Click the **Save** button to save the code. Click the **</>Versions** button to select the required version of code.



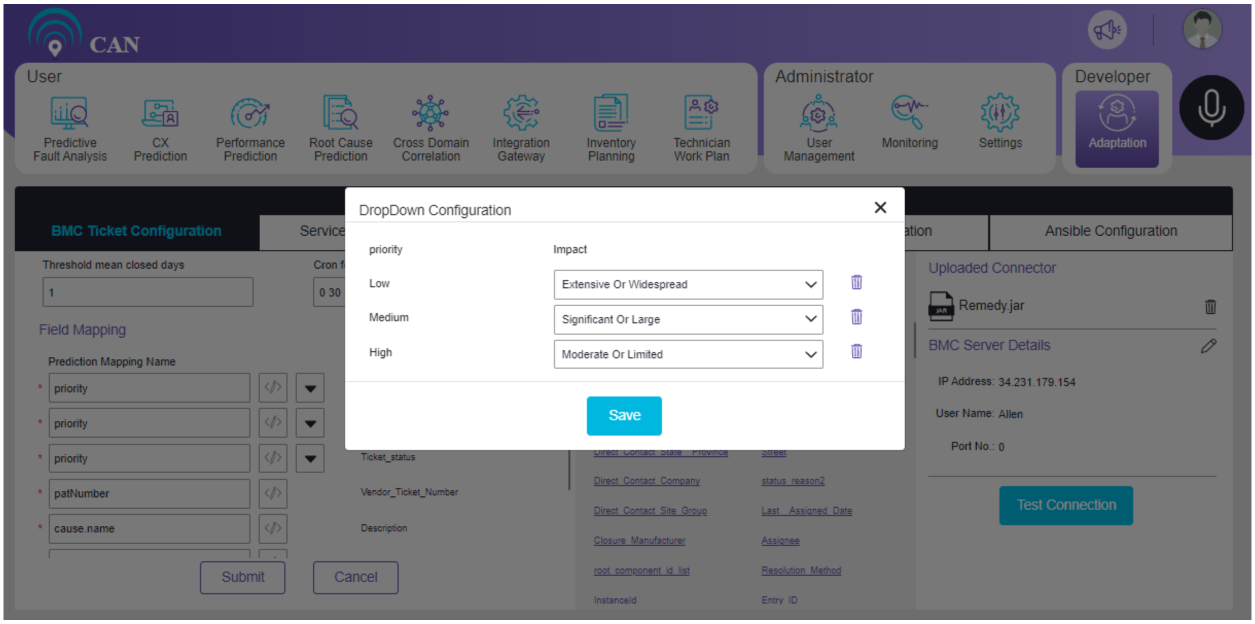
Code Language: Java

Code Snippet Identifier*

```
import com.mongodb.BasicDBObject;
import com.avanseus.model.can.Priority;
import com.mongodb.DBCursor;
import com.mongodb.BasicDBObject;

import java.util.List;
import java.util.regex.Matcher;
import java.util.regex.Pattern;
import com.mongodb.DBObject;
import java.util.Date;
import java.util.*;
import java.text.SimpleDateFormat;
import java.util.Calendar;
public class  implements IPredictedFaultToTicketMapping {

@Override
     public Object getPredictedFault(List<PredictedFault> predictedFault){
```

Figure 15.108 - 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.



DropDown Configuration

priority	Impact
Low	Extensive Or Widespread
Medium	Significant Or Large
High	Moderate Or Limited

Save

Threshold mean closed days: 1

Cron f: 0 30

Prediction Mapping Name: priority, priority, priority, patNumber, cause.name

Ticket_status

Vendor_Ticket_Number

Description

Direct_Contact_State_Province, Street, Direct_Contact_Company, status_reason2, Direct_Contact_Site_Group, Last_Assigned_Date, Closure_Manufacturer, Assignee, root_component_id_list, Resolution_Method, InstanceId, Entry_ID

Uploaded Connector: Remedy.jar

BMC Server Details

IP Address: 34.231.179.154

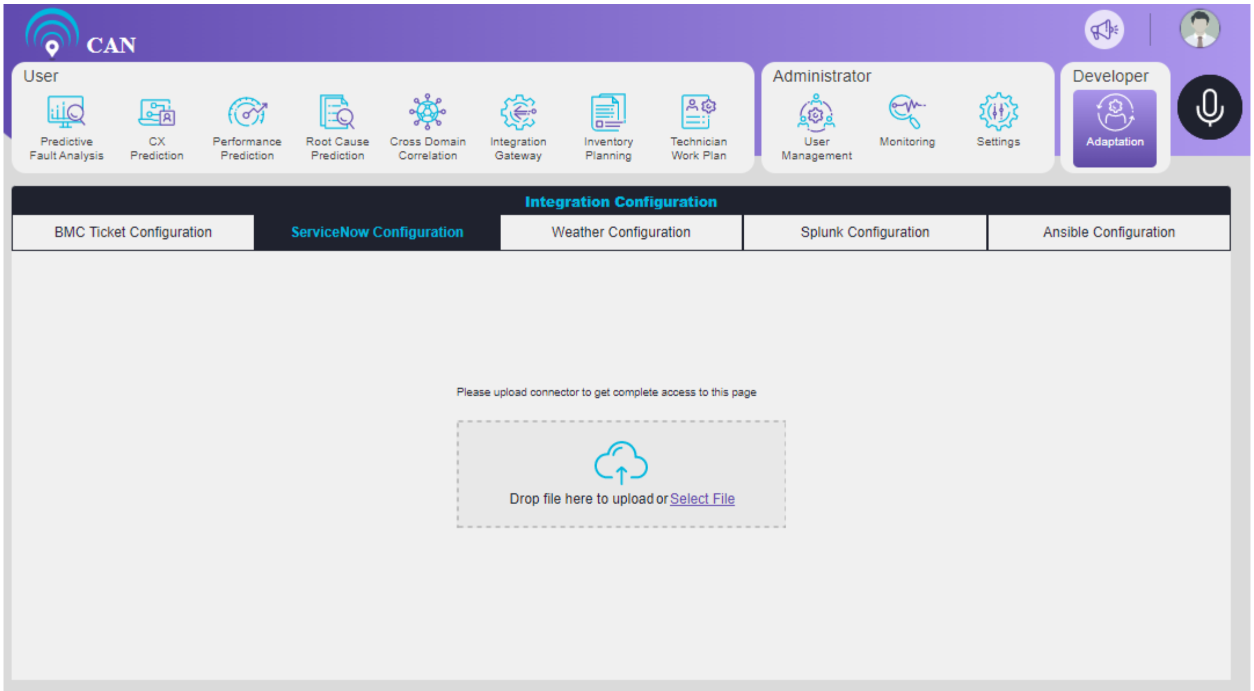
User Name: Allen

Port No.: 0

Figure 15.109 - Dropdown Configuration Screen

ServiceNow Configuration

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



Please upload connector to get complete access to this page

Drop file here to upload or Select File

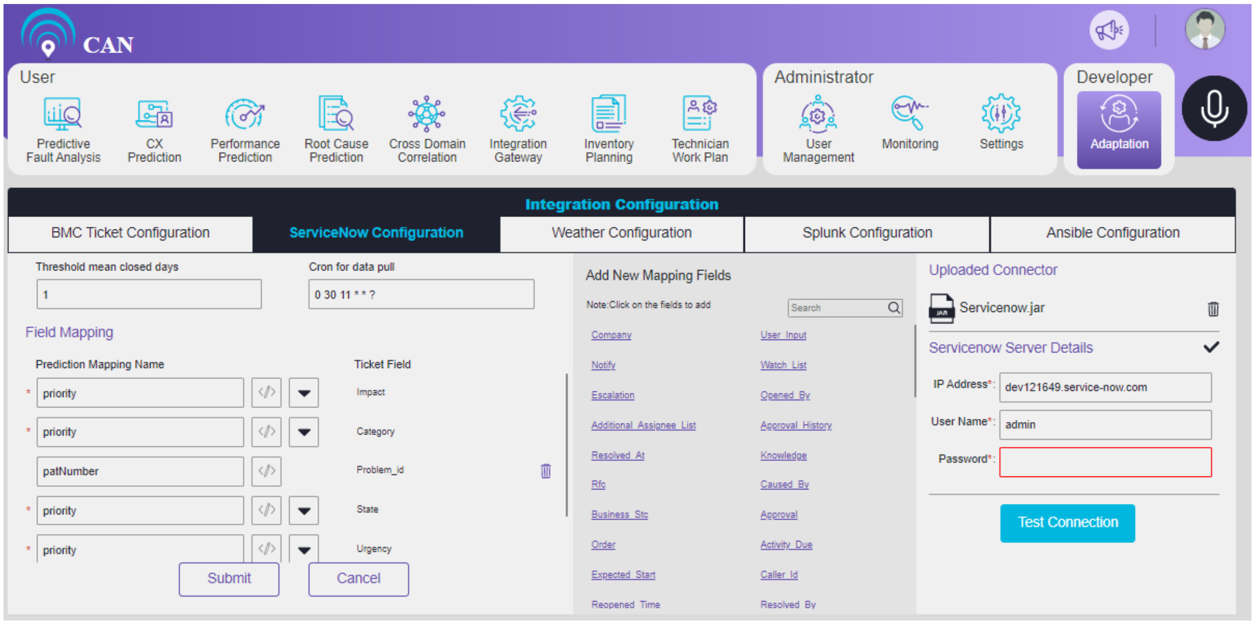
Figure 15.110 - ServiceNow Configuration Screen

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 ServiceNow Configuration

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



Threshold mean closed days: 1

Cron for data pull: 0 30 11 * * ?

Prediction Mapping Name	Ticket Field
* priority	Impact
* priority	Category
patNumber	Problem_id
* priority	State
* priority	Urgency

Servicenow.jar

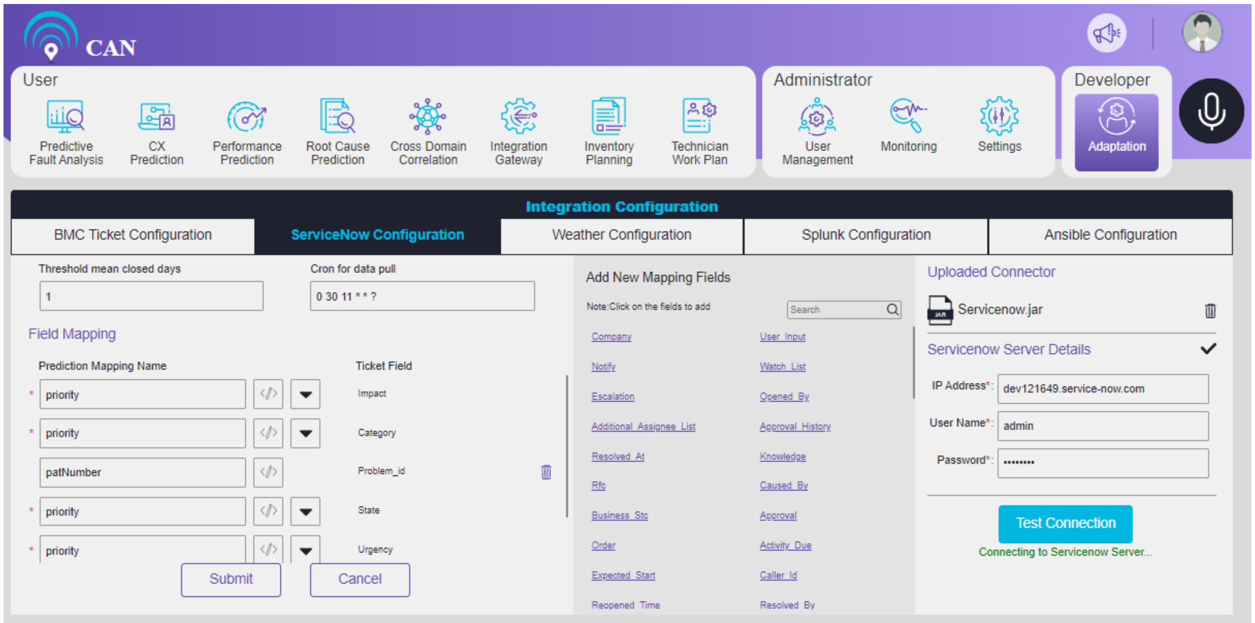
IP Address*: dev121649.service-now.com

User Name*: admin

Password*:

Figure 15.111 - ServiceNow Server Details

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



Threshold mean closed days: 1

Cron for data pull: 0 30 11 * * ?

Field Mapping

Prediction Mapping Name	Ticket Field
* priority	Impact
* priority	Category
patNumber	Problem_id
* priority	State
* priority	Urgency

Add New Mapping Fields

Note:Click on the fields to add

Company	User_Input
Notify	Watch_List
Escalation	Opened_By
Additional_Assignee_List	Approval_History
Resolved_At	Knowledge
Rfc	Caused_By
Business_Stc	Approval
Order	Activity_Due
Expected_Start	Caller_Id
Reopened_Time	Resolved_By

Uploaded Connector

Servicenow.jar

Servicenow Server Details ✓

IP Address*: dev121649.service-now.com

User Name*: admin

Password*: ••••••••

Connecting to Servicenow Server...

Figure 15.112 - ServiceNow Test Connection

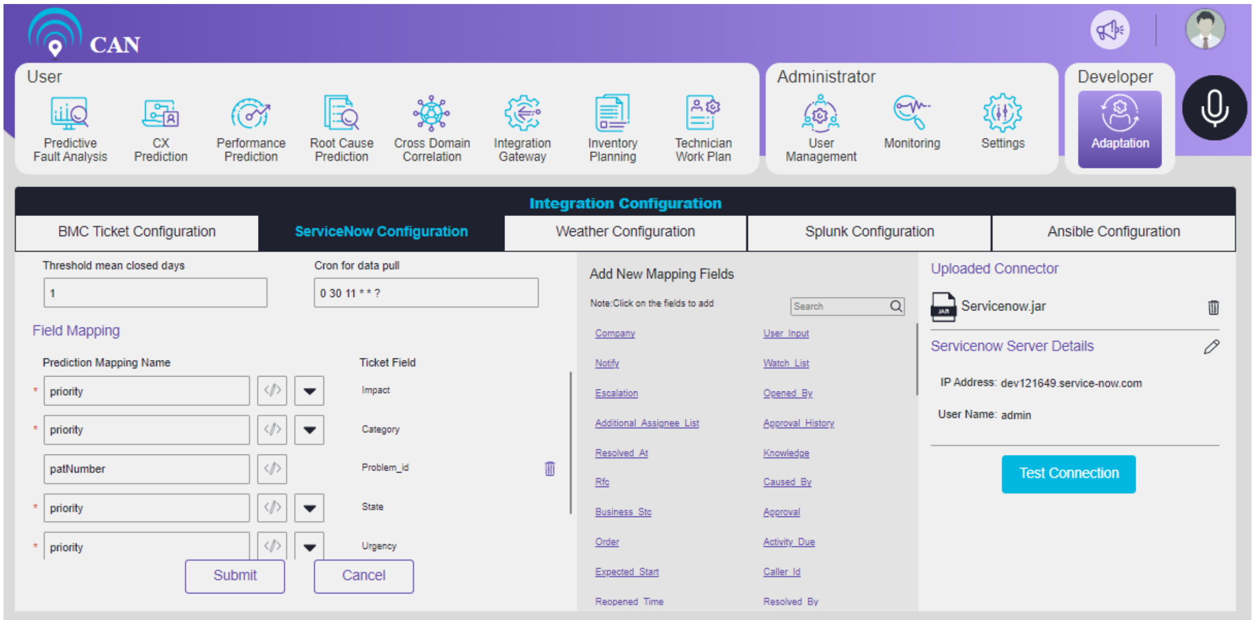
In **ServiceNow** configuration, we map the prediction fields to ServiceNow.

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**.



Threshold mean closed days: 1

Cron for data pull: 0 30 11 * * ?

Field Mapping

Prediction Mapping Name	Ticket Field
* priority	Impact
* priority	Category
patNumber	Problem_id
* priority	State
* priority	Urgency

Add New Mapping Fields

Note:Click on the fields to add

Company	User_Input
Notify	Watch_List
Escalation	Opened_By
Additional_Assignee_List	Approval_History
Resolved_At	Knowledge
Rfc	Caused_By
Business_Stc	Approval
Order	Activity_Due
Expected_Start	Caller_Id
Reopened_Time	Resolved_By

Uploaded Connector

Servicenow.jar

Servicenow Server Details

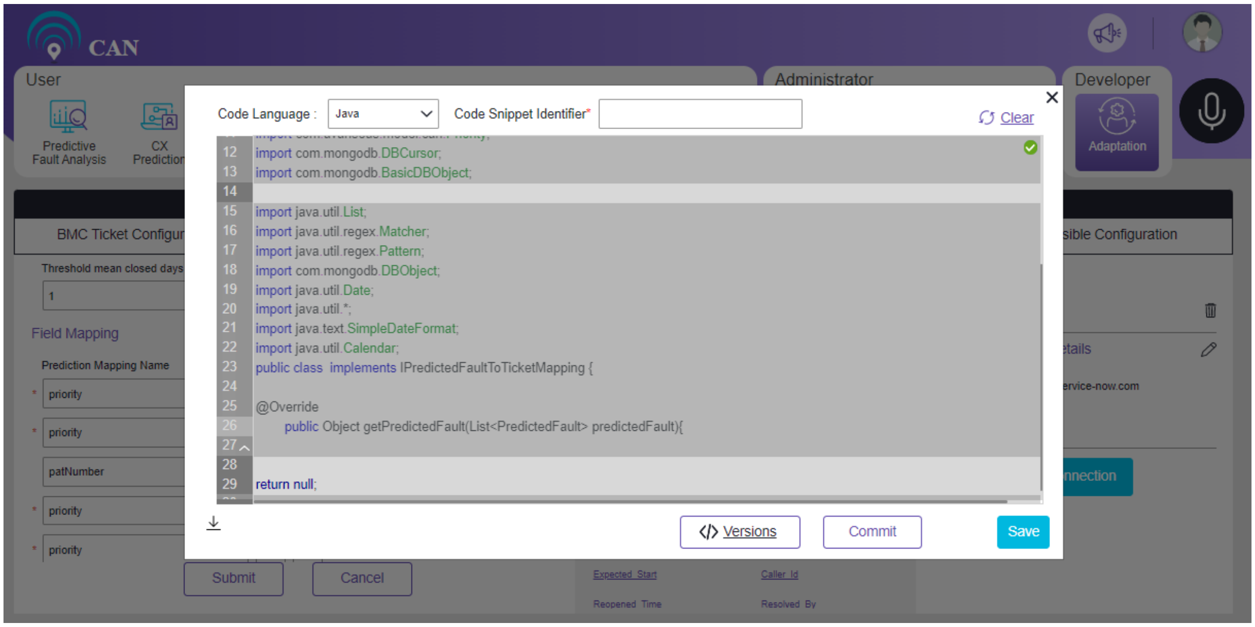
IP Address: dev121649.service-now.com

User Name: admin

Figure 15.113 - 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 or python mapping code in the text area. It will be automatically compiled. Click the **Save** button to save the code. Click the **</>Versions** button to select the required version of code.



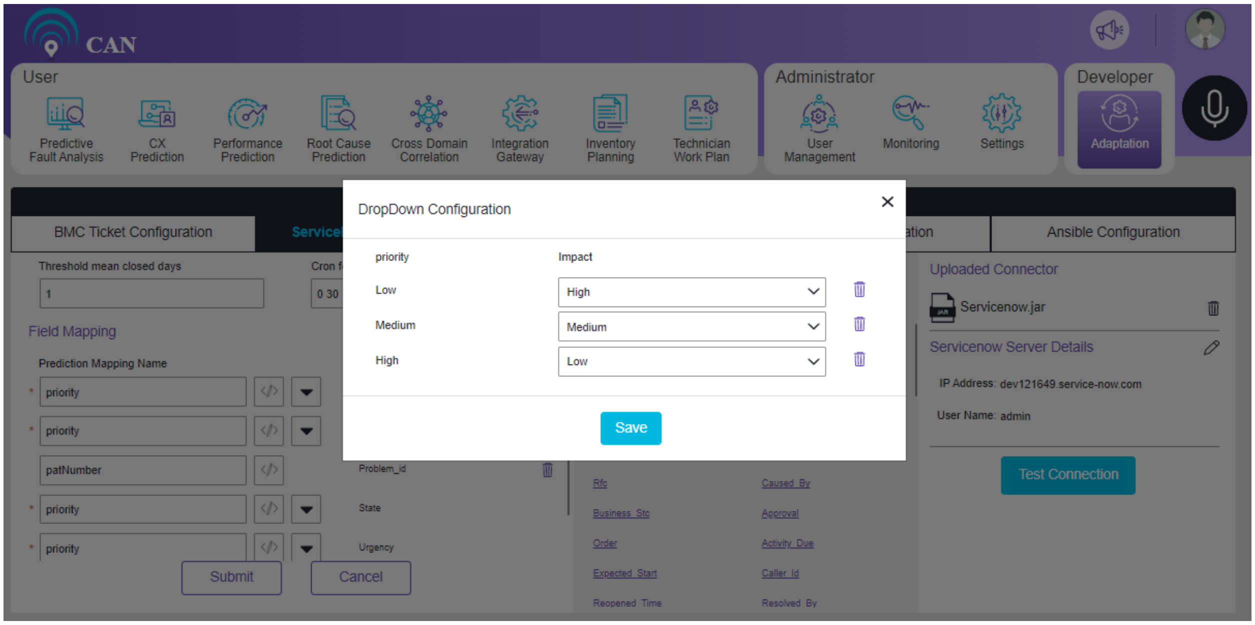
Code Language : Java

Code Snippet Identifier*

```
import com.mongodb.DBCursor;
import com.mongodb.BasicDBObject;

import java.util.List;
import java.util.regex.Matcher;
import java.util.regex.Pattern;
import com.mongodb.DBObject;
import java.util.Date;
import java.util.*;
import java.text.SimpleDateFormat;
import java.util.Calendar;
public class  implements IPredictedFaultToTicketMapping {

@Override
      public Object getPredictedFault(List<PredictedFault> predictedFault){


return null;
```

Figure 15.114 - 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.



DropDown Configuration

priority	Impact
Low	High
Medium	Medium
High	Low

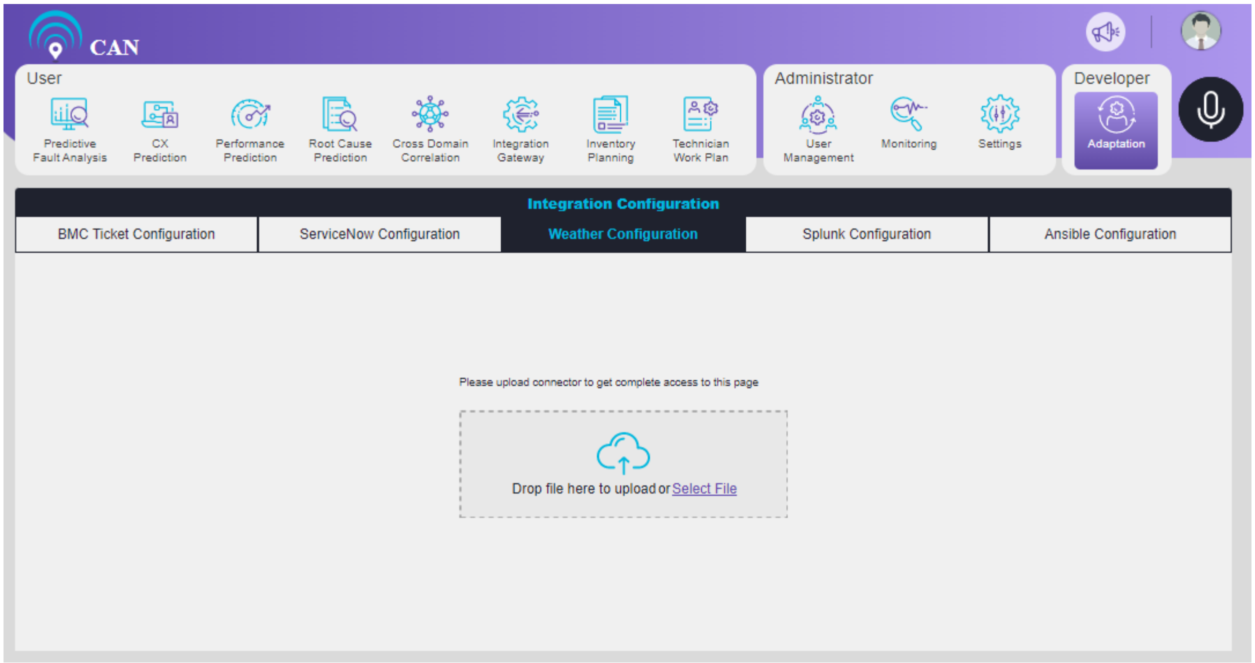
IP Address: dev121649.service-now.com

User Name: admin

Figure 15.115 - Dropdown Configuration Screen

Weather Configuration

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



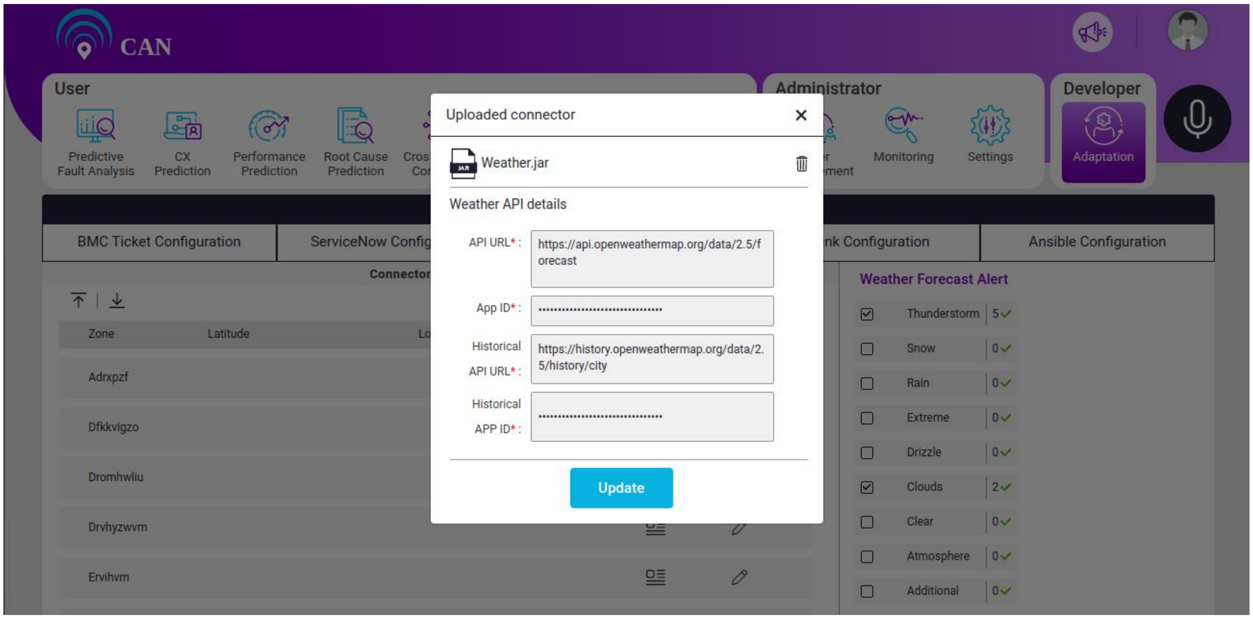
Please upload connector to get complete access to this page

Figure 15.116 - 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.
4. Write the Historical API URL details "https://history.openweathermap.org/data/2.5/history/city" in the Historical API URL field.
5. Write the Historical APP ID in the Historical APP ID field.
6. Click the **Save Details** button.
7. Click the Update button to update all the existing Weather API details.



Uploaded connector ×

Weather.jar

Weather API details

API URL* : https://api.openweathermap.org/data/2.5/forecast

App ID* : ••••••••••••••••••••••••••••••

Historical API URL* : https://history.openweathermap.org/data/2.5/history/city

Historical APP ID* : ••••••••••••••••••••••••••••••

Update

Zone	Latitude
Adrxpzf	
Dfkkvigzo	
Dromhwliu	
Drvhyzwvm	
Ervihvm	

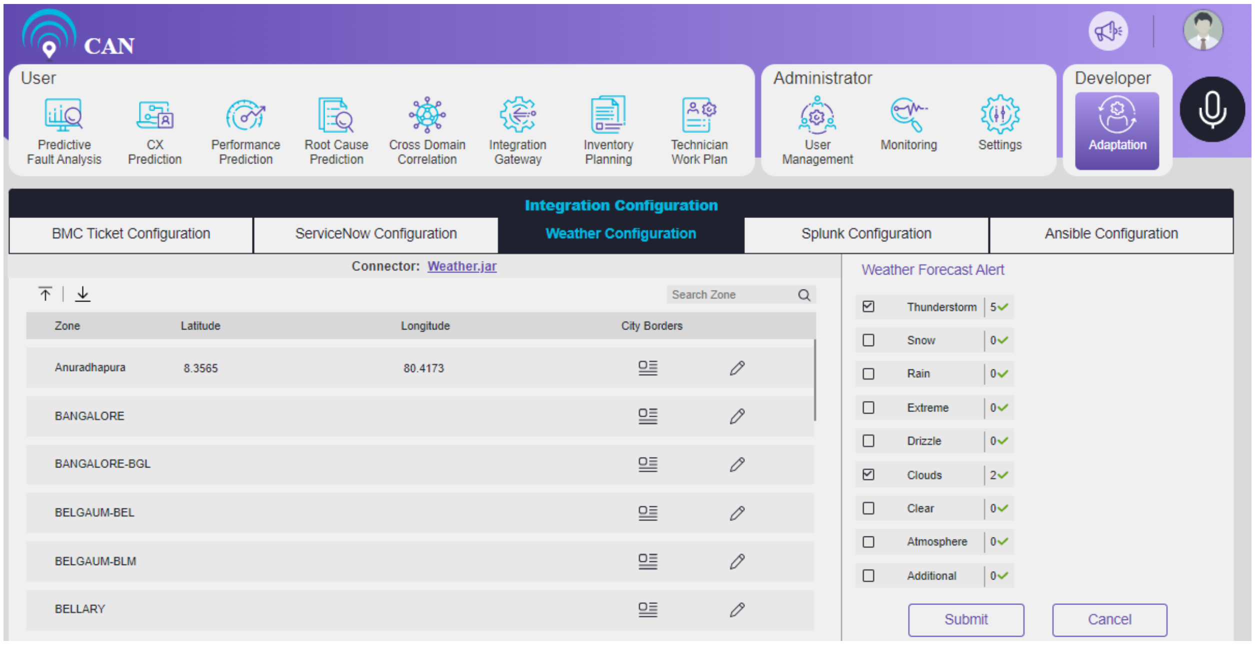
Weather Forecast Alert

☑	Thunderstorm	5✓
☐	Snow	0✓
☐	Rain	0✓
☐	Extreme	0✓
☐	Drizzle	0✓
☑	Clouds	2✓
☐	Clear	0✓
☐	Atmosphere	0✓
☐	Additional	0✓

Figure 15.117 - Weather API Login Page

The Weather Integration screen will display the following components:

- Zone
- Latitude
- Longitude
- City Borders



Connector: Weather.jar

Zone	Latitude	Longitude	City Borders
Anuradhapura	8.3565	80.4173	
BANGALORE			
BANGALORE-BGL			
BELGAUM-BEL			
BELGAUM-BLM			
BELLARY			

Weather Forecast Alert

☑	Thunderstorm	5✓
☐	Snow	0✓
☐	Rain	0✓
☐	Extreme	0✓
☐	Drizzle	0✓
☑	Clouds	2✓
☐	Clear	0✓
☐	Atmosphere	0✓
☐	Additional	0✓

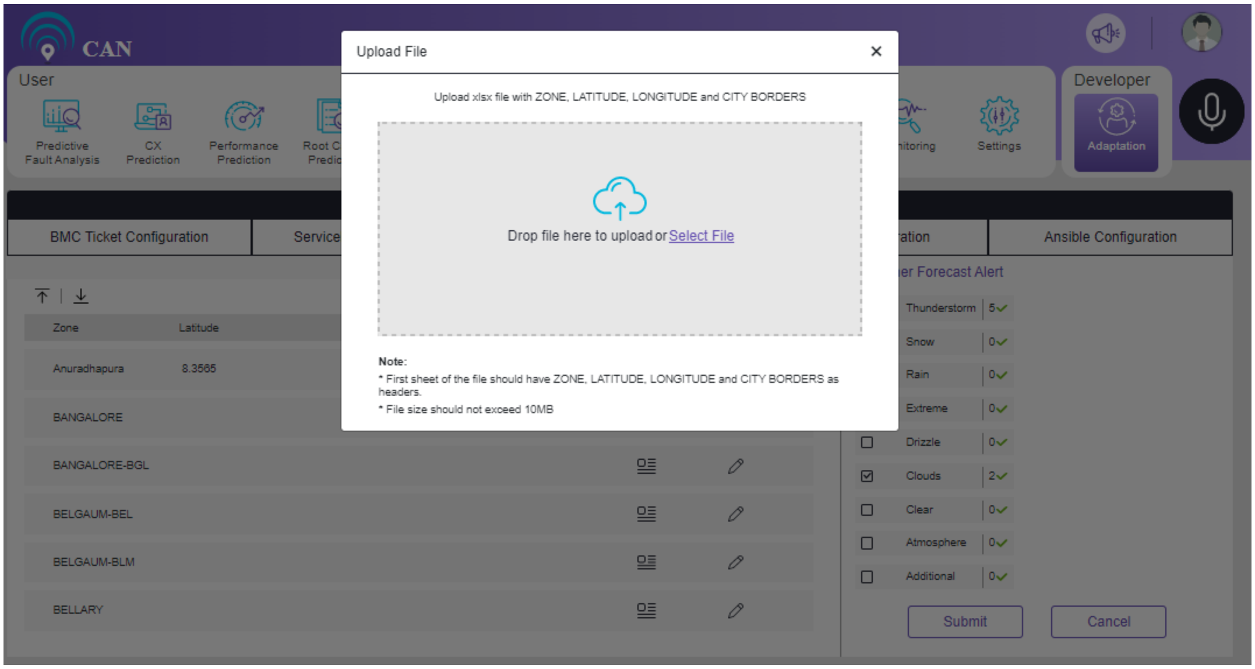
Submit Cancel

Figure 15.118 - 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 information.

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



Upload File

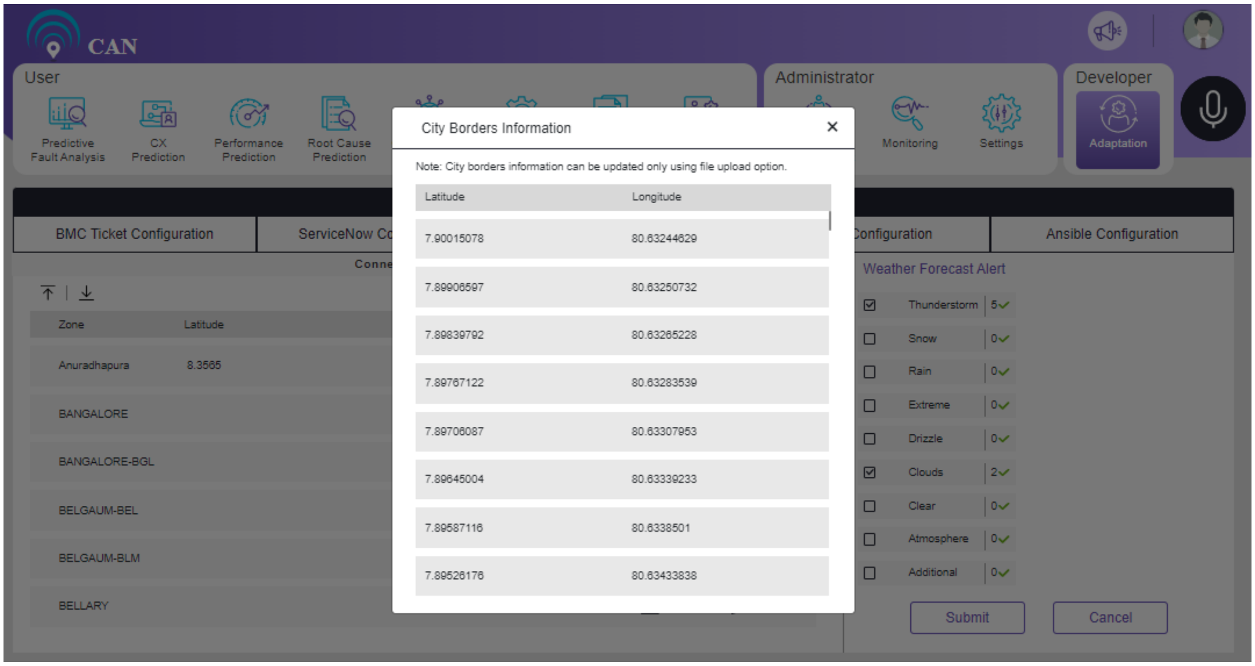
Upload xlsx file with ZONE, LATITUDE, LONGITUDE and CITY BORDERS

Drop file here to upload or Select File

Note:
- First sheet of the file should have ZONE, LATITUDE, LONGITUDE and CITY BORDERS as headers.
- File size should not exceed 10MB

Figure 15.119 - Weather Integration File Upload

Click the city borders icon ☰ to view the city border information.



City Borders Information

Note: City borders information can be updated only using file upload option.

Latitude	Longitude
7.90015078	80.63244629
7.89906597	80.63250732
7.89839792	80.63265228
7.89767122	80.63283539
7.89706087	80.63307953
7.89645004	80.63339233
7.89587116	80.6338501
7.89526176	80.63433838

Figure 15.120 - City Border Information

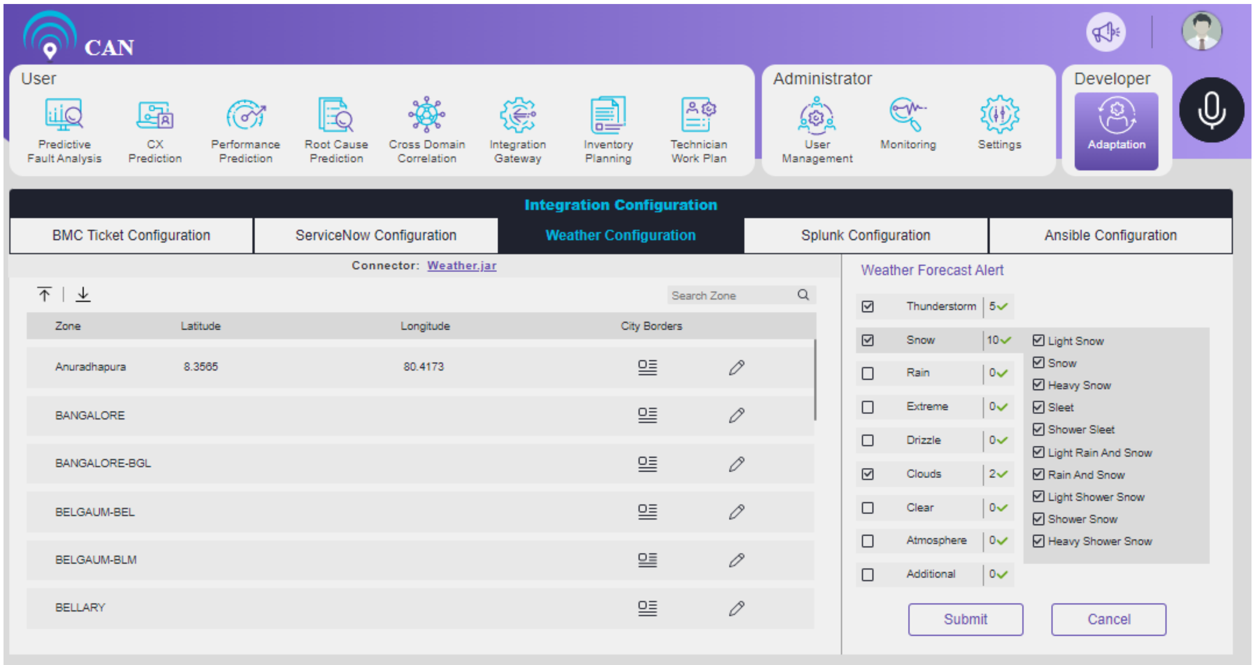
Click the download icon ⤓ to get the zone details.

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 the requirement.

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

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



Connector: Weather.jar

Zone	Latitude	Longitude	City Borders
Anuradhapura	8.3565	80.4173	
BANGALORE			
BANGALORE-BGL			
BELGAUM-BEL			
BELGAUM-BLM			
BELLARY			

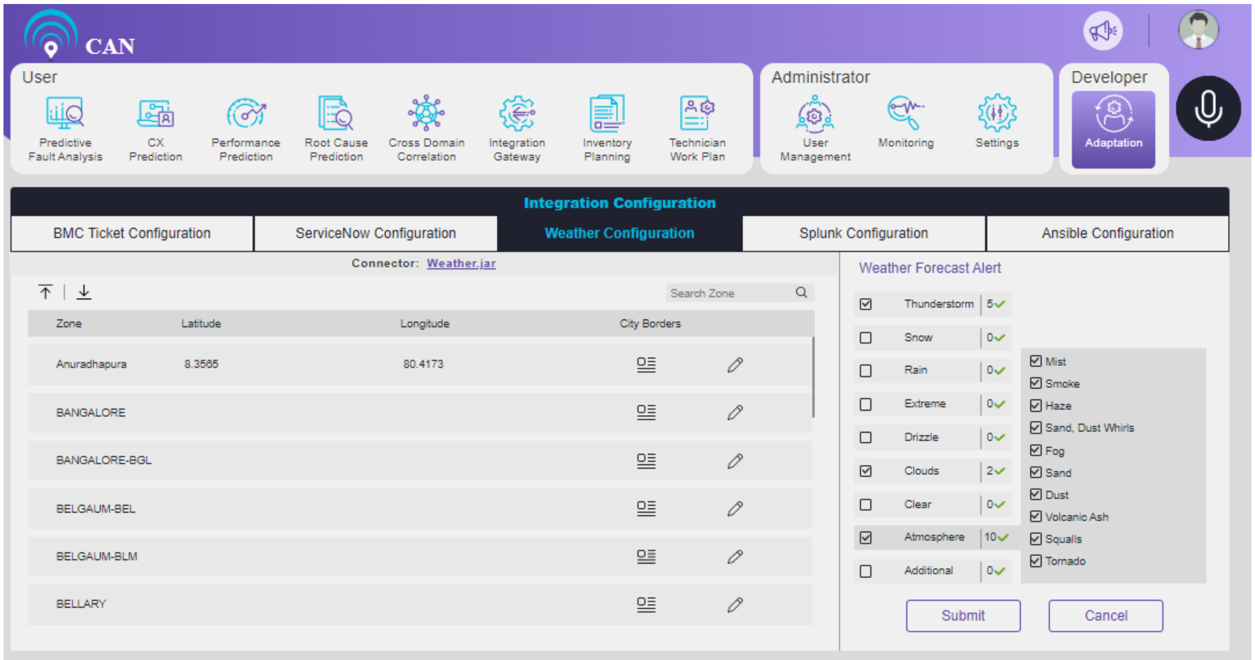
Weather Forecast Alert

☑ Thunderstorm 5 ✓
☑ Snow 10 ✓
☐ Rain 0 ✓
☐ Extreme 0 ✓
☐ Drizzle 0 ✓
☑ Clouds 2 ✓
☐ Clear 0 ✓
☐ Atmosphere 0 ✓
☐ Additional 0 ✓

☑ Light Snow
☑ Snow
☑ Heavy Snow
☑ Sleet
☑ Shower Sleet
☑ Light Rain And Snow
☑ Rain And Snow
☑ Light Shower Snow
☑ Shower Snow
☑ Heavy Shower Snow

Figure 15.121 - Weather Forecast Alerts

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



Connector: Weather.jar

Zone	Latitude	Longitude	City Borders
Anuradhapura	8.3565	80.4173	
BANGALORE			
BANGALORE-BGL			
BELGAUM-BEL			
BELGAUM-BLM			
BELLARY			

Weather Forecast Alert

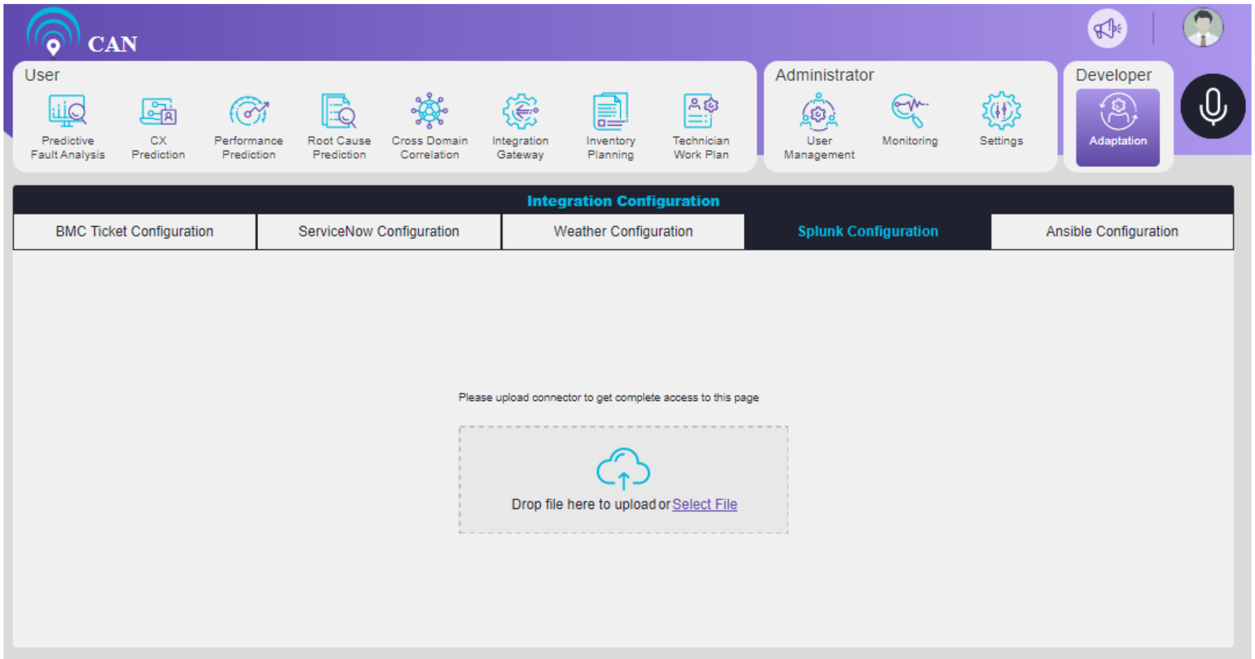
- ☑ Thunderstorm 5
- □ Snow 0
- □ Rain 0
- □ Extreme 0
- □ Drizzle 0
- ☑ Clouds 2
- □ Clear 0
- ☑ Atmosphere 10
- □ Additional 0

- ☑ Mist
- ☑ Smoke
- ☑ Haze
- ☑ Sand, Dust Whirls
- ☑ Fog
- ☑ Sand
- ☑ Dust
- ☑ Volcanic Ash
- ☑ Squalls
- ☑ Tornado

Figure 15.122 - Weather Forecast Alerts (Subfields)

Splunk Configuration

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



Please upload connector to get complete access to this page

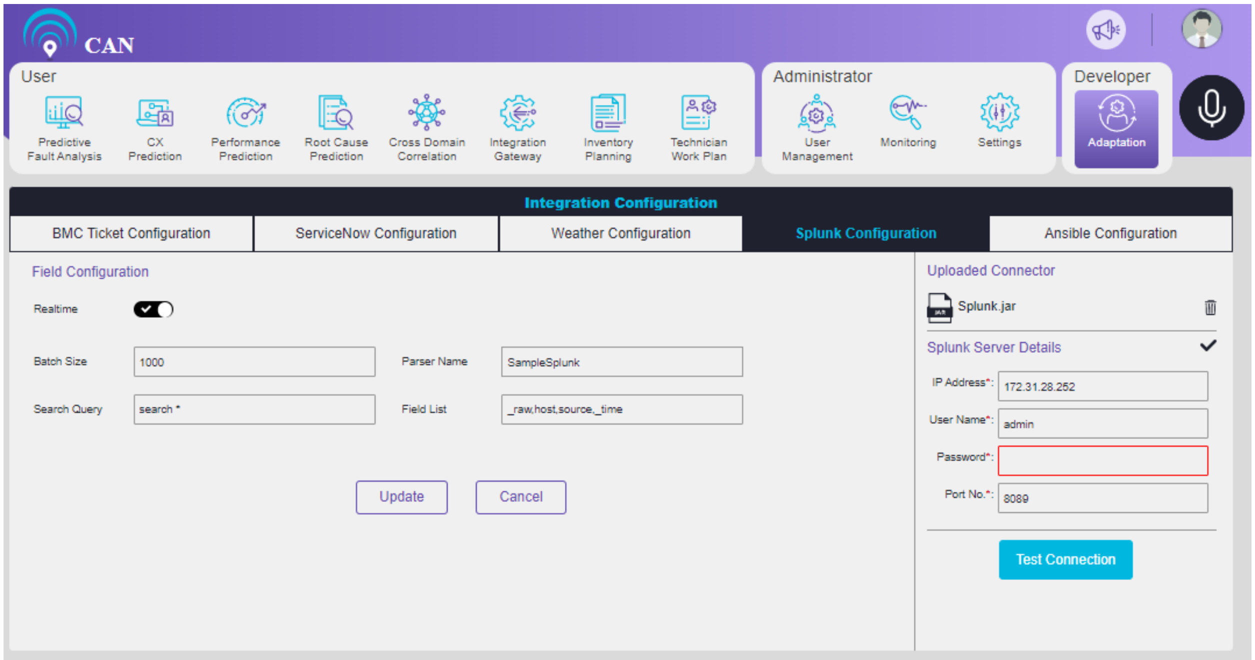
Figure 15.123 - Splunk Configuration Screen

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.



Integration Configuration

BMC Ticket Configuration | ServiceNow Configuration | Weather Configuration | Splunk Configuration | Ansible Configuration

Field Configuration

Realtime ✓

Batch Size: 1000
Parser Name: SampleSplunk
Search Query: search *
Field List: _raw,host,source,_time

Update Cancel

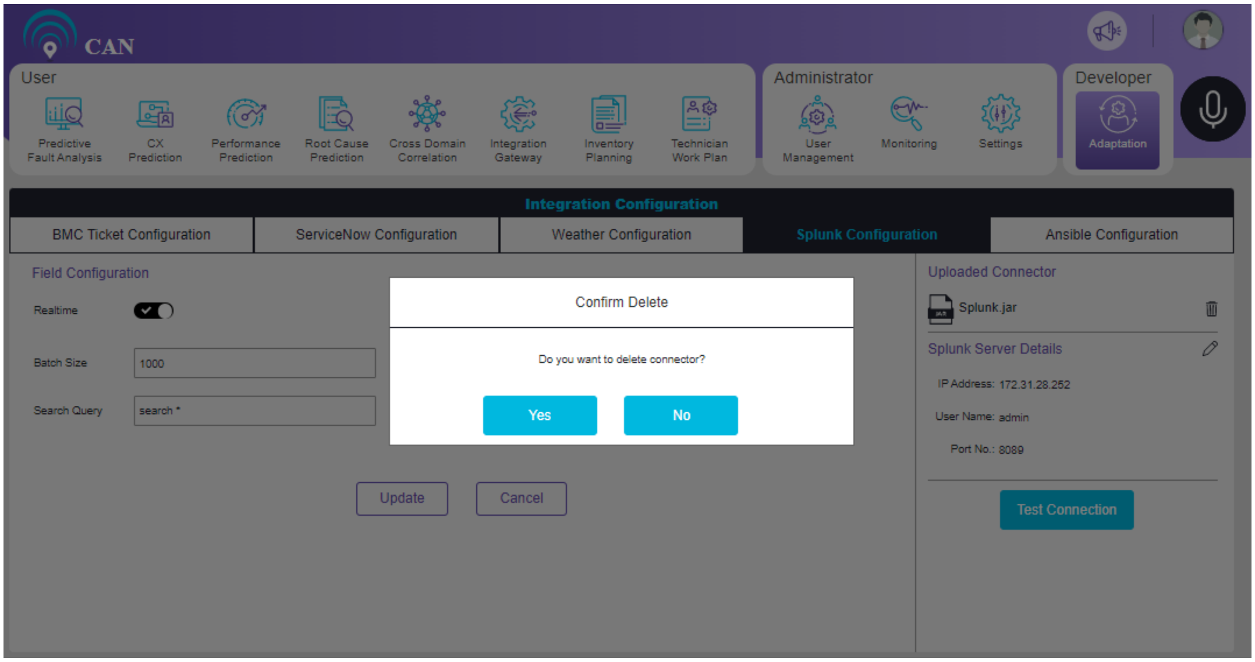
Uploaded Connector
Splunk.jar 🗑

Splunk Server Details ✓
IP Address*: 172.31.28.252
User Name*: admin
Password*:
Port No.*: 8089

Test Connection

Figure 15.124 - Splunk Server Details

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



Field Configuration

Realtime ✓

Batch Size: 1000

Search Query: search *

Confirm Delete

Do you want to delete connector?

Uploaded Connector

Splunk.jar

Splunk Server Details

IP Address: 172.31.28.252

User Name: admin

Port No.: 8089

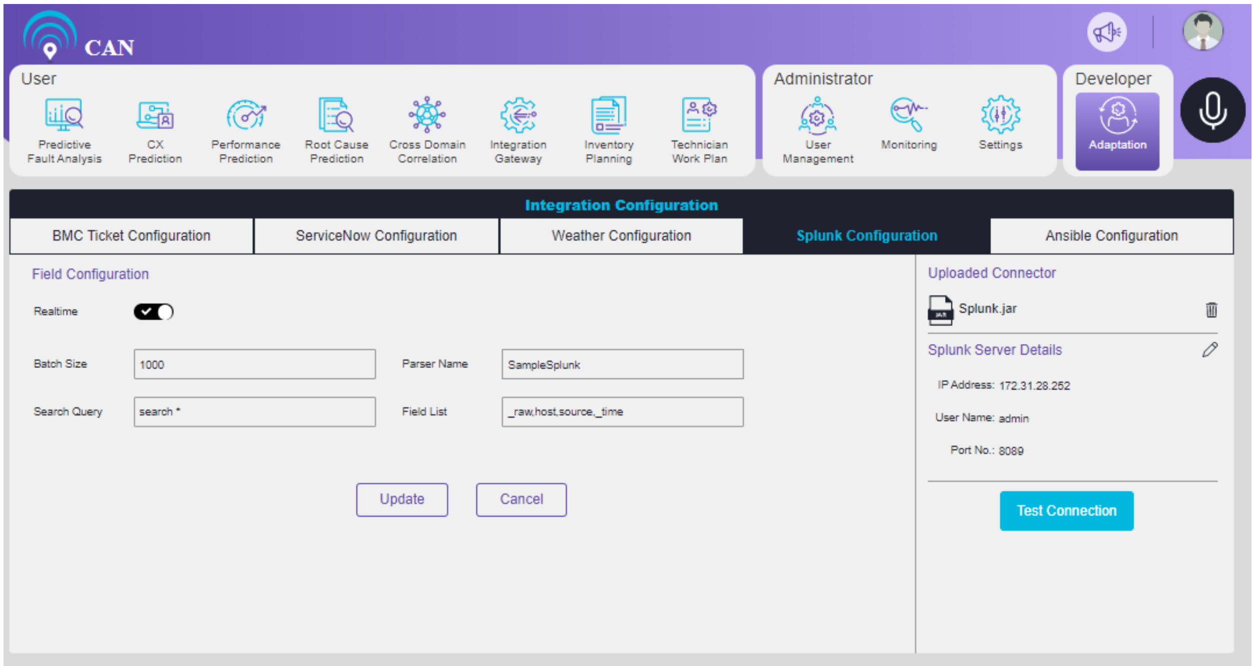
Figure 15.125 - Splunk Uploaded Controller

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.



Field Configuration

Realtime ✓

Batch Size: 1000

Parser Name: SampleSplunk

Search Query: search *

Field List: _raw,host,source,_time

Uploaded Connector

Splunk.jar

Splunk Server Details

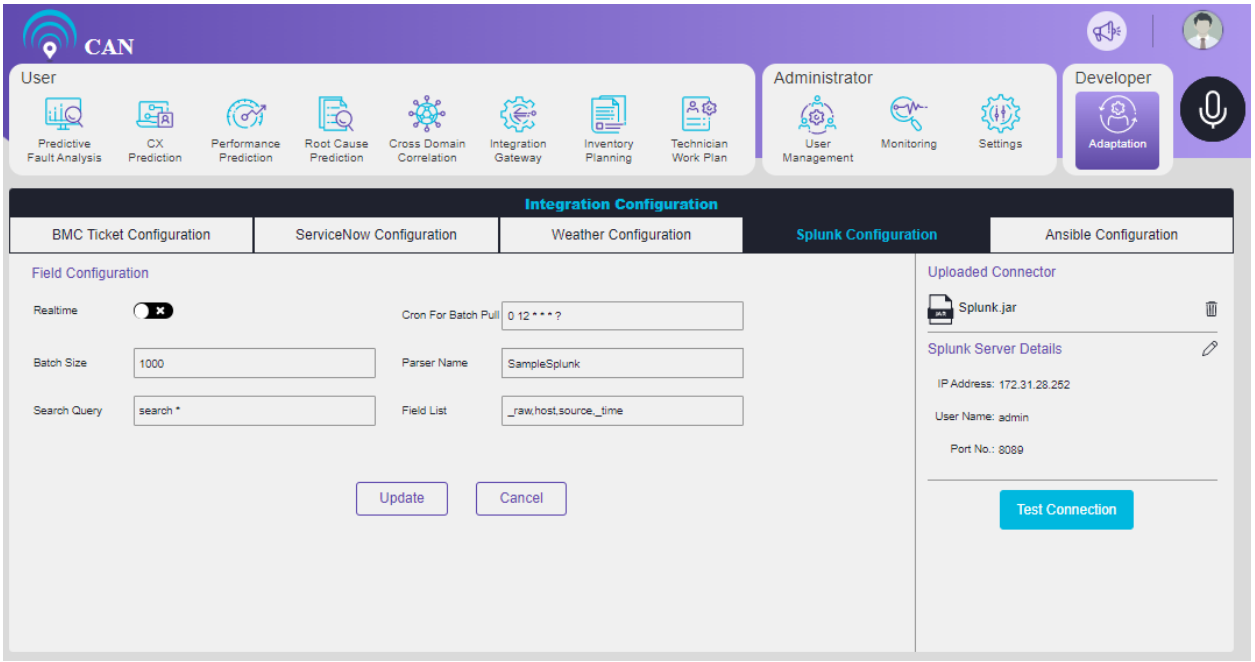
IP Address: 172.31.28.252

User Name: admin

Port No.: 8089

Figure 15.126 - 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).



Realtime

Cron For Batch Pull: 0 12 * * * ?

Batch Size: 1000

Parser Name: SampleSplunk

Search Query: search *

Field List: _raw,host,source,_time

Splunk.jar

IP Address: 172.31.28.252

User Name: admin

Port No.: 8089

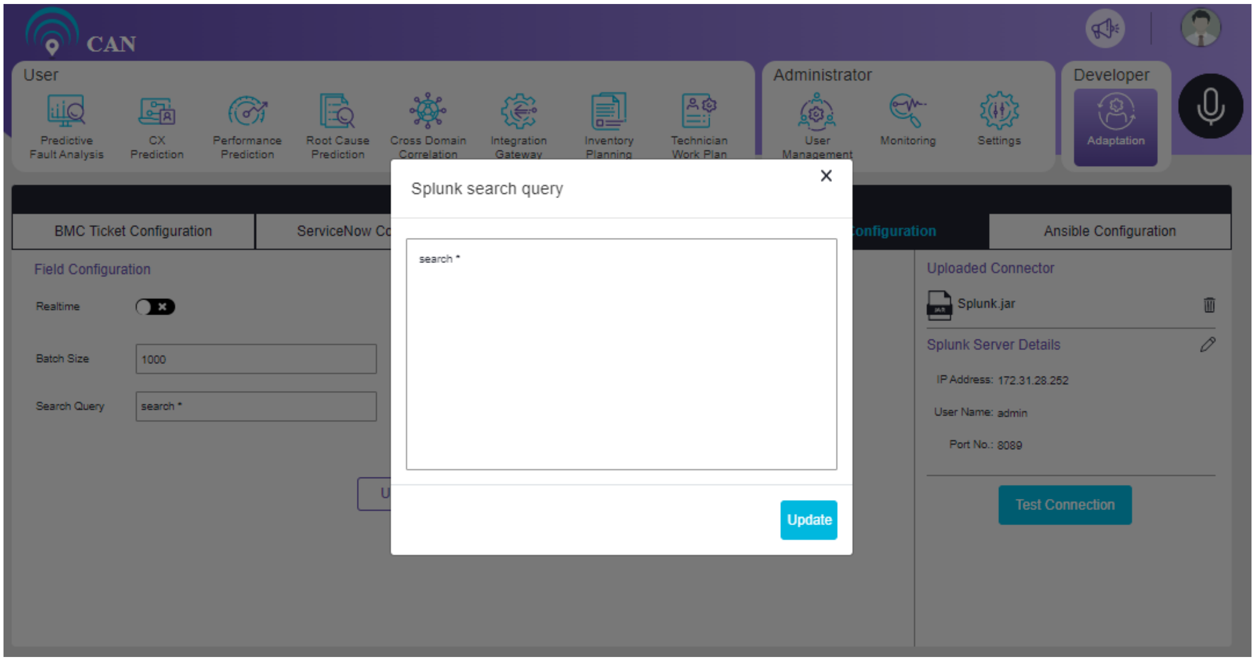
Figure 15.127 - Field Configuration – Cron for Batch Pull

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-defined values in the backend.

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

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



Splunk search query ×

search *

Realtime ✕

Batch Size 1000

Search Query search *

Splunk.jar

IP Address: 172.31.28.252

User Name: admin

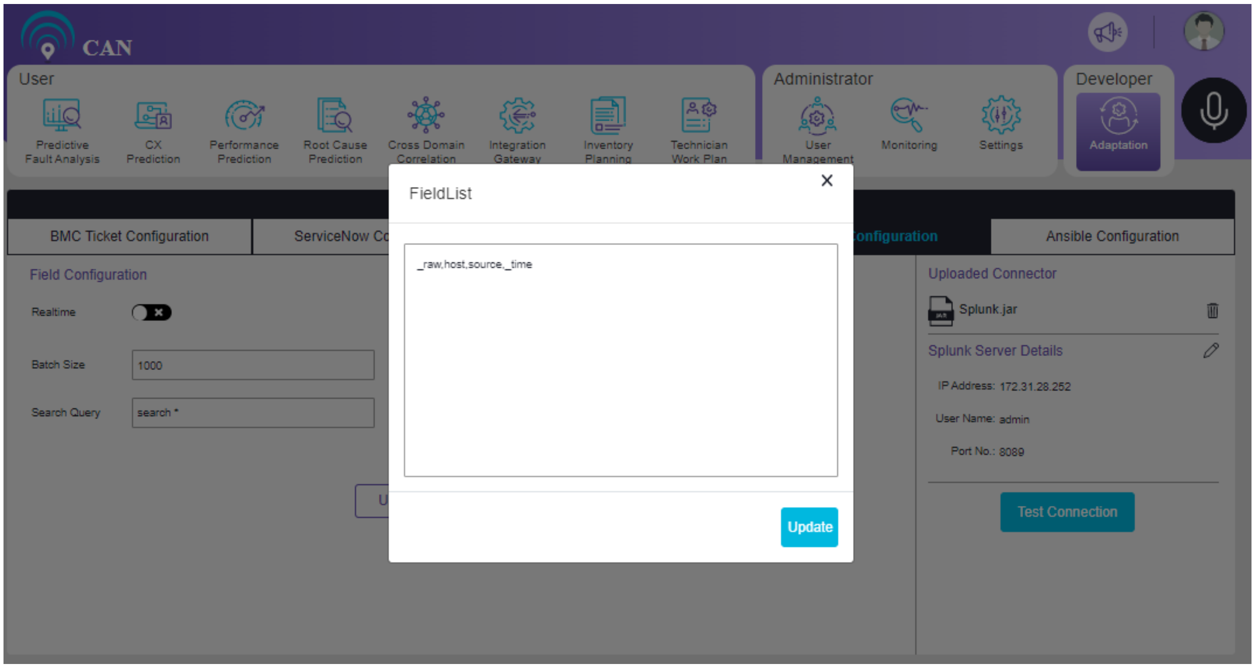
Port No.: 8089

Figure 15.128 - 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.

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



FieldList ×

_raw,host,source,_time

Realtime ✕

Batch Size 1000

Search Query search *

Splunk.jar

IP Address: 172.31.28.252

User Name: admin

Port No.: 8089

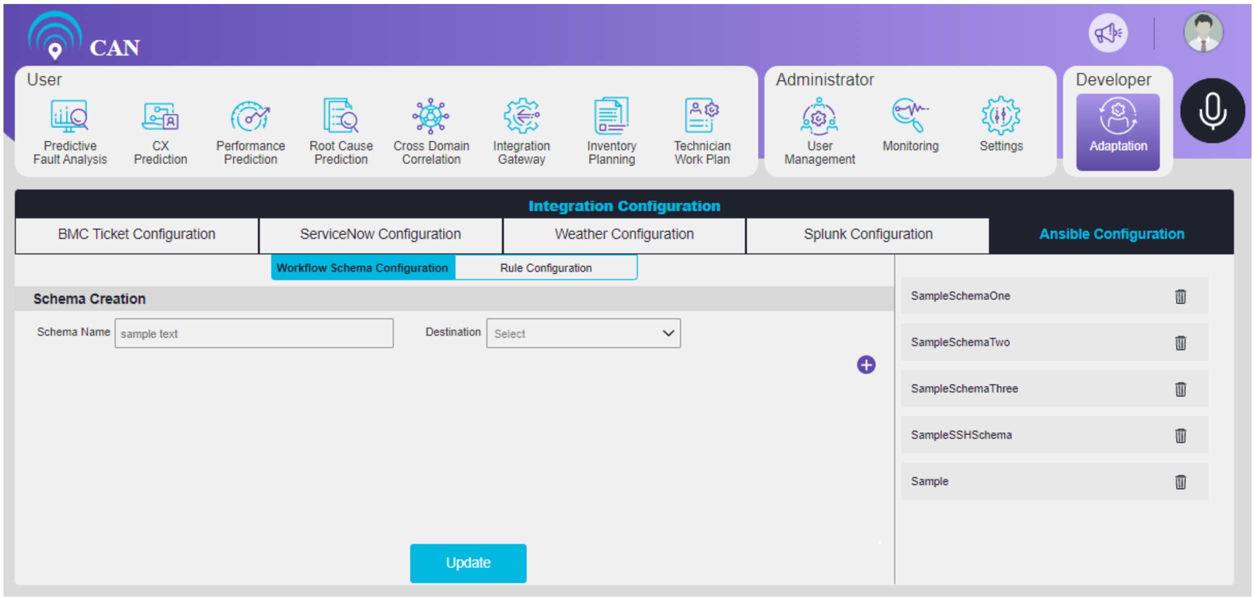
Figure 15.129 - Splunk Field List

Ansible Configuration

Ansible is an automation tool that provisions configuration management, application deployment, orchestration, and many other processes. It is a plug and play activation system where a set of commands having a workflow is defined. It runs on various interfaces. SSH is the widely used interface.

Ansible Configuration has two tabs:

1. Workflow Schema Configuration
2. Rule Configuration



Schema Creation

Schema Name: sample text

Destination: Select

SampleSchemaOne

SampleSchemaTwo

SampleSchemaThree

SampleSSHSchema

Sample

Figure 15.130 - Ansible Configuration

Workflow Schema Configuration

In workflow configuration, user can create multiple jobs and each job has multiple tasks.

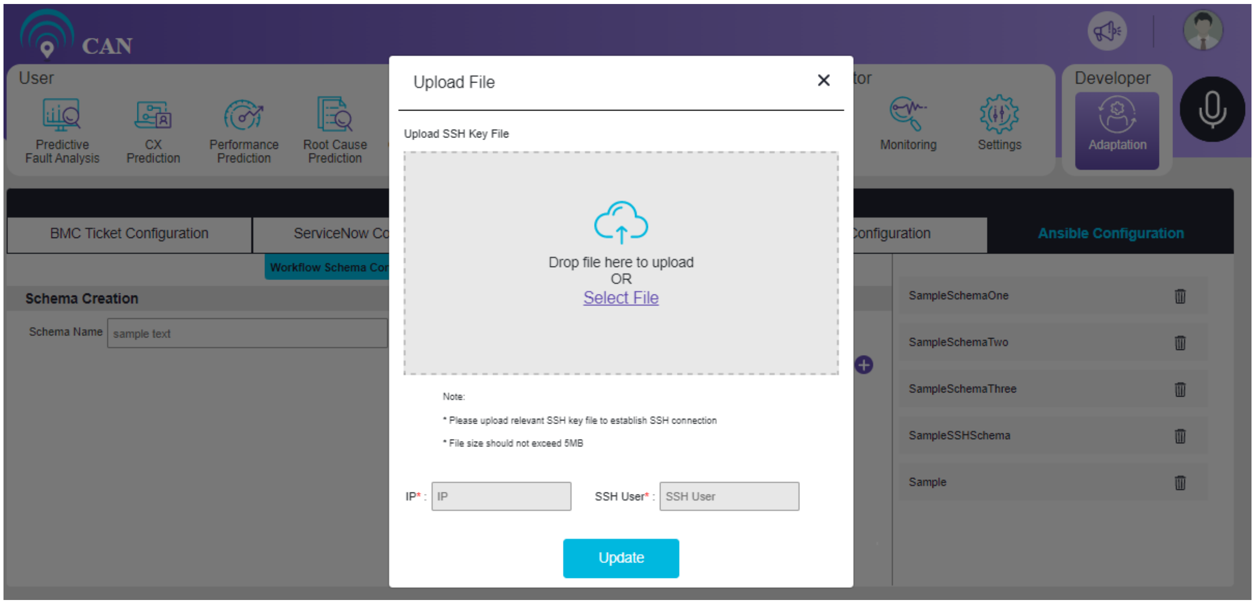
Schema Creation

1. Enter a **Schema Name** in the text box.
2. Select the **Destination** from the dropdown (SSH and Local).
3. Provision of **Local** destination is for trial task execution.
4. For **SSH** interface:
5. SSH certificate key file must be uploaded to establish SSH connection during run time.

Note:

***File size should not exceed 5MB.**

***IP and SSH User fields are mandatory.**



Upload File ×

Upload SSH Key File

Drop file here to upload
OR
Select File

Note:

* Please upload relevant SSH key file to establish SSH connection

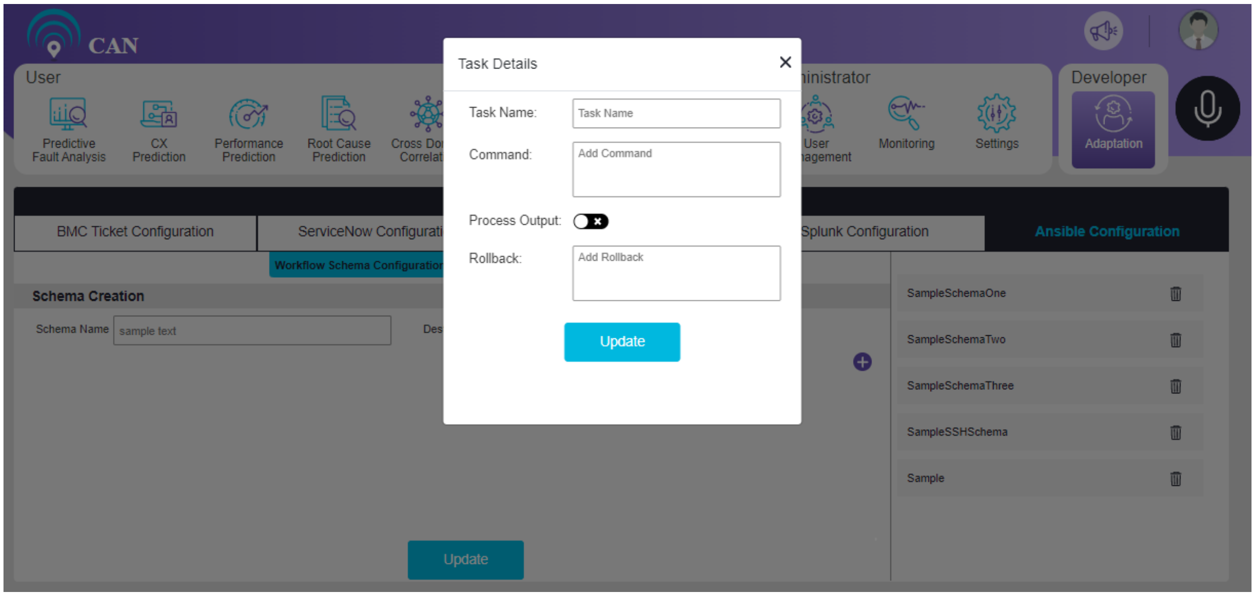
* File size should not exceed 5MB

IP* : IP SSH User* : SSH User

Update

Figure 15.131 - Upload SSH Key File

6. Destination IP (**IP**) and SSH username (**SSH User**) must be specified.
7. Click the **Update** to upload the file.
8. Click on **Add Task** icon ⊕ to add the first task.
9. Provide **Task Details.** It includes Task Name, Command, Process Output and Roll Back fields.



Task Details ×

Task Name: Task Name

Command: Add Command

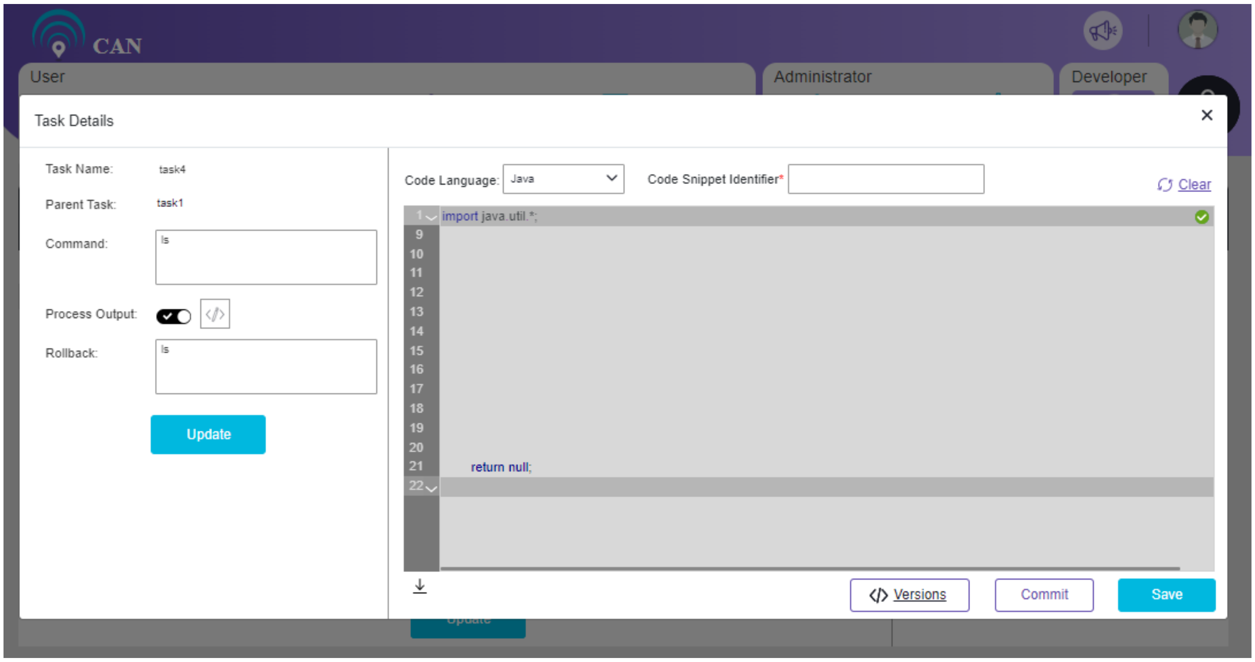
Process Output:

Rollback: Add Rollback

Update

Figure 15.132 - First Task Creation

10. Click the **Process Output** toggle switch to ON. User can write code to process the output in Java or Python language.



Task Name: task4

Parent Task: task1

Command: ls

Process Output: ✓

Rollback: ls

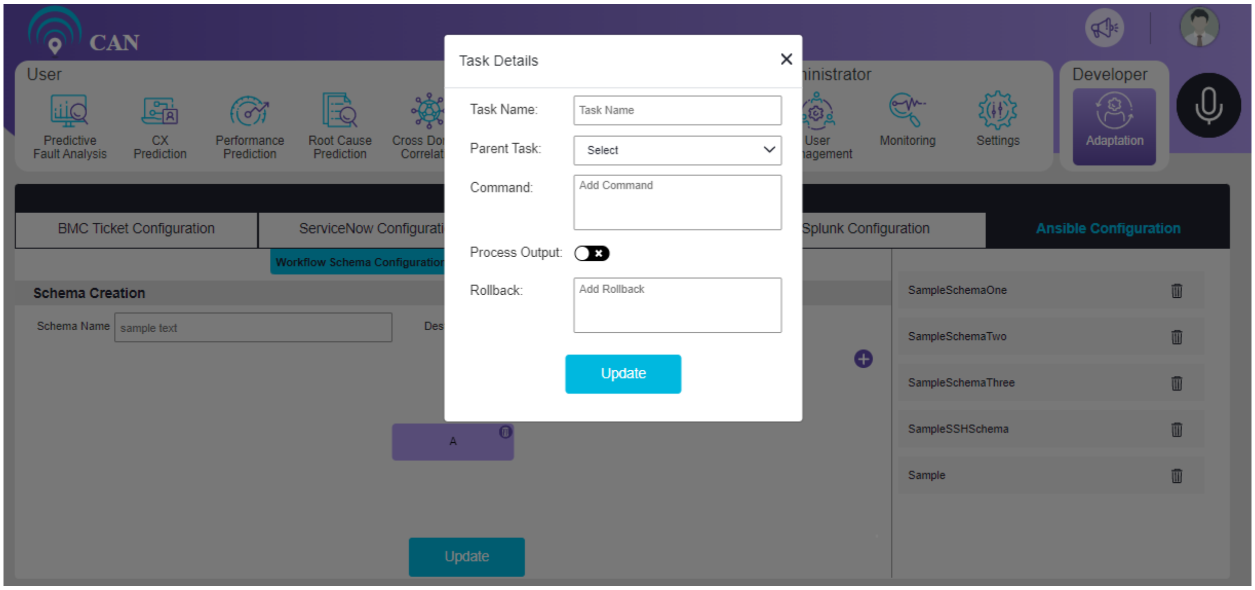
Code Language: Java

Code Snippet Identifier*

```
import java.util.*;



        return null;
```

Figure 15.133 - Process Output IDE

11. Click **Update** to save the details.
12. User can create multiple tasks by clicking the ⊕ icon.
13. The subsequent tasks will have **Parent Task** field.



Schema Name: sample text

Task Name: Task Name

Parent Task: Select

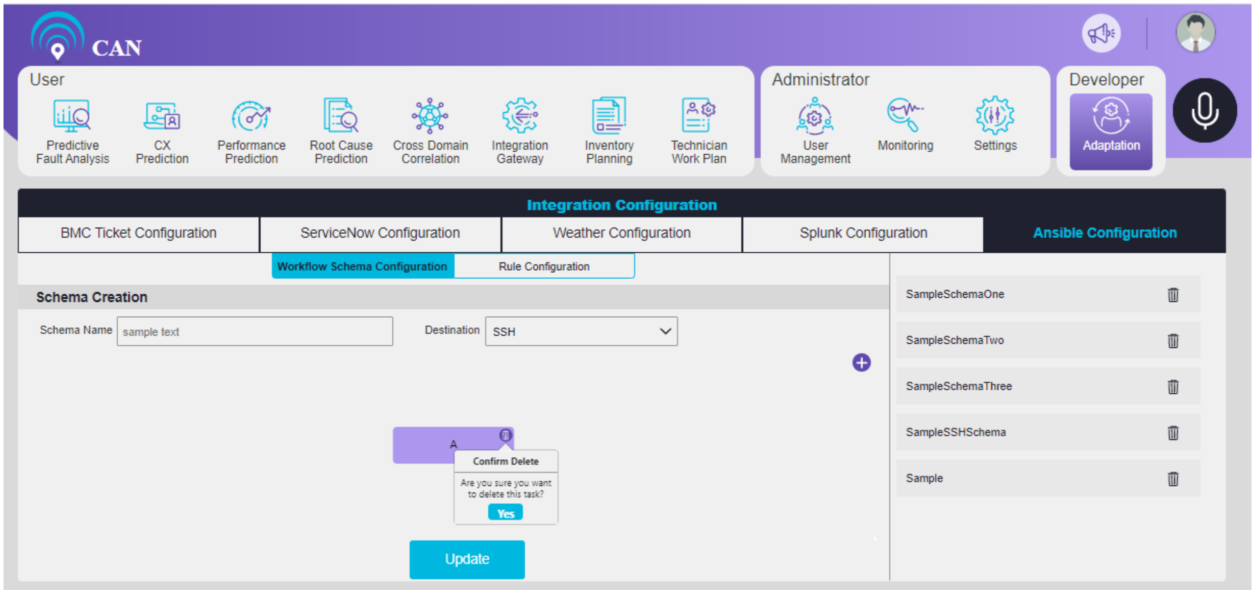
Command: Add Command

Process Output: ✗

Rollback: Add Rollback

Figure 15.134 - Subsequent Task Creation

14. Delete a task by clicking the **Delete Task** icon🗑.
15. Click **Yes** to delete the task.



Schema Name: sample text

Destination: SSH

Confirm Delete

Are you sure you want to delete this task?

Yes

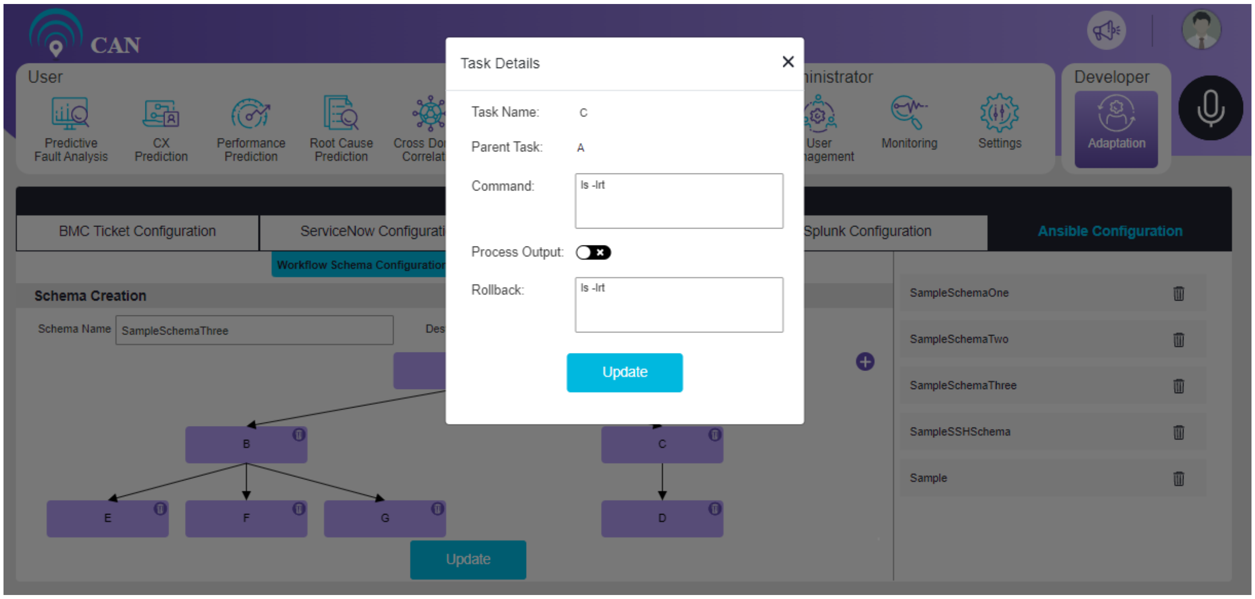
SampleSchemaOne
SampleSchemaTwo
SampleSchemaThree
SampleSSHSchema
Sample

Figure 15.135 - Delete Task

16. Click **Update** to save the Schema.

To Edit Schema

1. Click any saved schema on the right side of the screen.
2. The selected schema is displayed.
3. Click ⊕ icon to add additional task. Repeat **Schema Creation** steps.
4. Click an existing task to view the details of the task.



Schema Name: SampleSchemaThree

Task Details

Task Name: C

Parent Task: A

Command: ls -lrt

Process Output: ☒

Rollback: ls -lrt

Update

SampleSchemaOne
SampleSchemaTwo
SampleSchemaThree
SampleSSHSchema
Sample

Figure 15.136 - Task Details

5. Modify the task details and click **Update** to save the changes.
6. Delete a task by clicking the 🗑 icon.
7. The child tasks of that particular task are deleted as well.

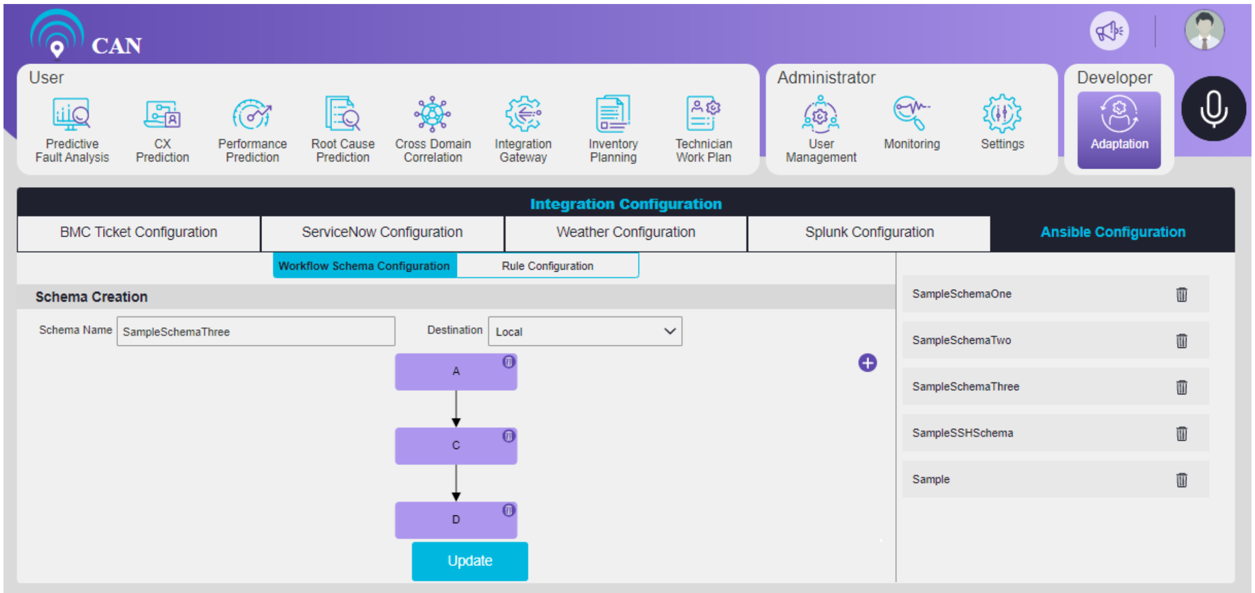
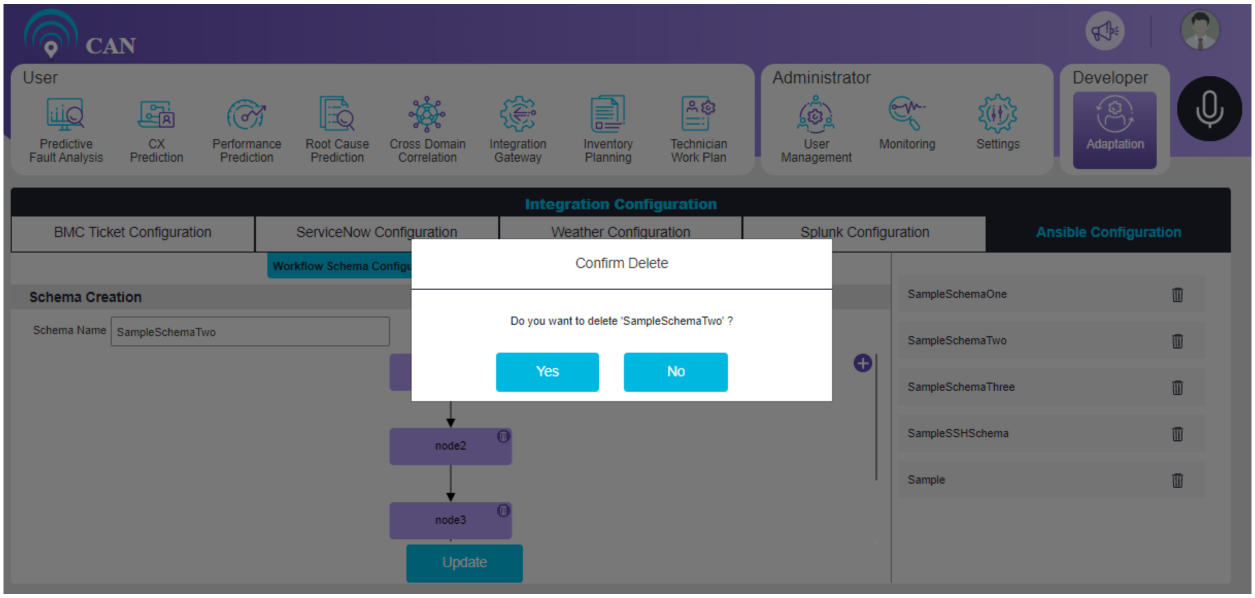


Figure 15.137 - Parent-Child Task Deletion

8. Click **Update** to save the changes.
9. Click on the Delete icon 🗑 to delete a workflow schema.



Confirm Delete

Do you want to delete 'SampleSchemaTwo' ?

Yes No

Figure 15.138 - Delete Schema

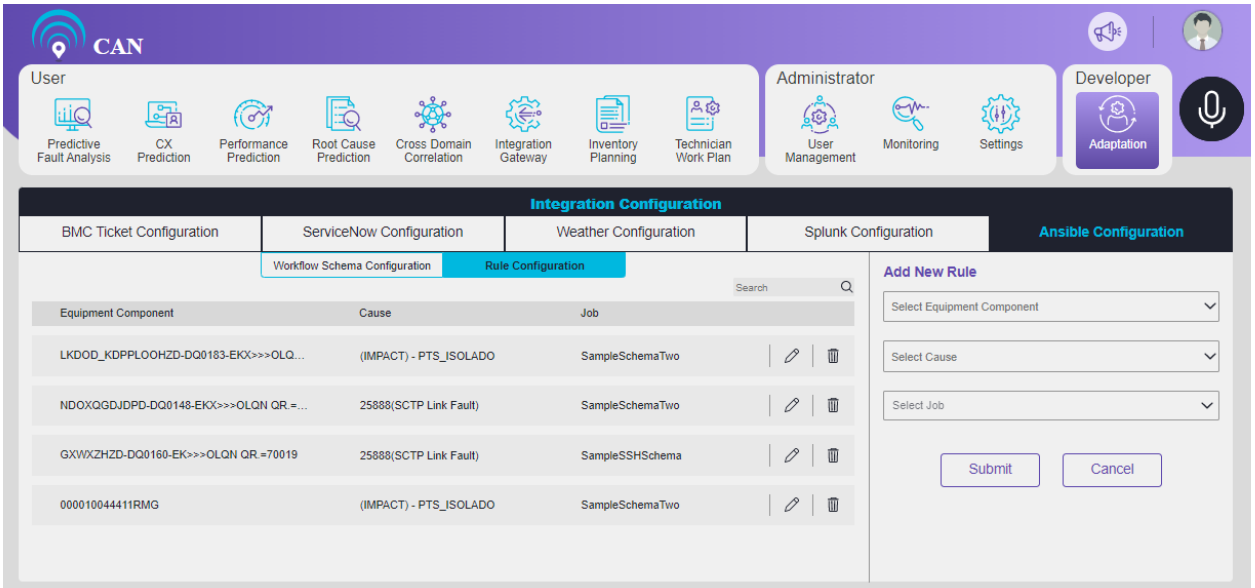
Rule Configuration

Rule configuration includes mapping between equipment, cause and job configuration.

To Add New Rule

To create a rule configuration, the workflow created is linked with equipment component & cause combination.

1. Select **Equipment Component** from the dropdown.
2. Select **Cause** from the dropdown.
3. Select **Job** from the dropdown.
4. Click **Submit** to create a new rule.



Equipment Component	Cause	Job
LKDOD_KDPPLOOHZD-DQ0183-EKX>>>OLQ...	(IMPACT) - PTS_ISOLADO	SampleSchemaTwo
NDOXQGDJDPD-DQ0148-EKX>>>OLQN QR.=...	25888(SCTP Link Fault)	SampleSchemaTwo
GXWXZHZD-DQ0160-EK>>>OLQN QR.=70019	25888(SCTP Link Fault)	SampleSSHSchema
000010044411RMG	(IMPACT) - PTS_ISOLADO	SampleSchemaTwo

Add New Rule

Select Equipment Component

Select Cause

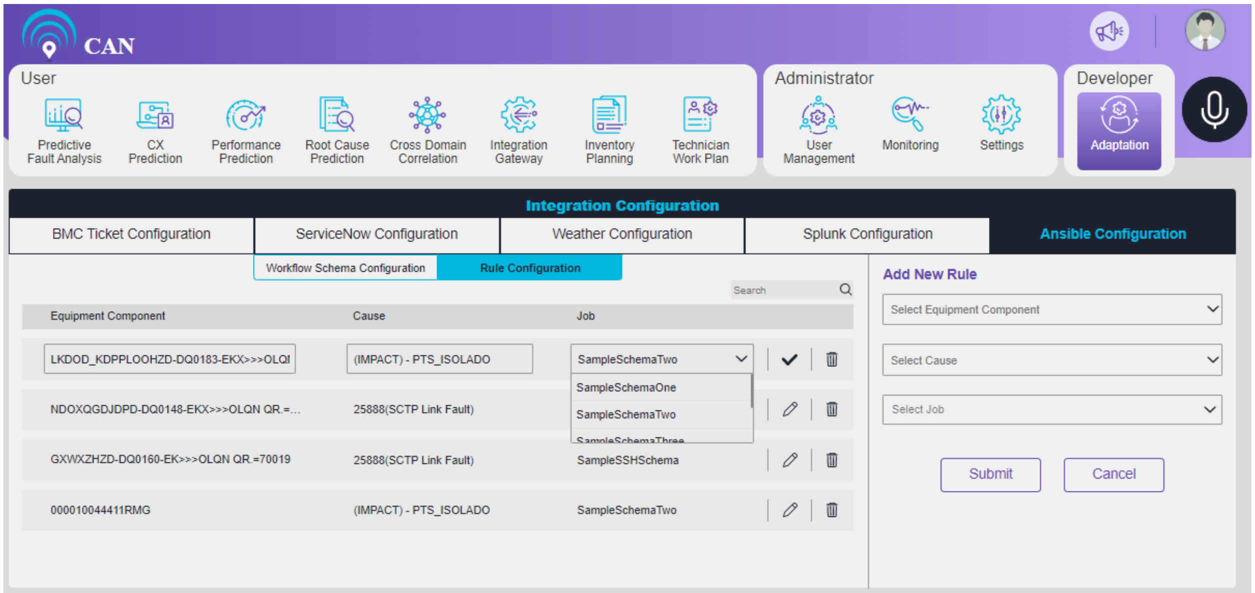
Select Job

Submit Cancel

Figure 15.139 - Add New Rule

To Edit Rule Configuration

1. Click the Edit icon✎.
2. Clear the Equipment Component or Cause data.
3. Select new **Equipment Component** or **Cause** from the dropdown.
4. Select **Job** from the dropdown.
5. Click the Update icon✓ to save the changes to the configuration.
6. Click the Delete icon🗑 to delete a configuration.
7. User can Search a configuration based on **Equipment Component** or **Cause**.



Equipment Component	Cause	Job
LKDOD_KDPPLOOHZD-DQ0183-EKX>>>OLQI	(IMPACT) - PTS_ISOLADO	SampleSchemaTwo SampleSchemaOne SampleSchemaTwo SampleSchemaThree
NDOXQGDJDPD-DQ0148-EKX>>>OLQN QR.=...	25888(SCTP Link Fault)	
GXWXZHZD-DQ0160-EK>>>OLQN QR.=70019	25888(SCTP Link Fault)	SampleSSHSchema
000010044411RMG	(IMPACT) - PTS_ISOLADO	SampleSchemaTwo

Figure 15.140 - Edit Rule Configuration

Topology Stitching Configuration

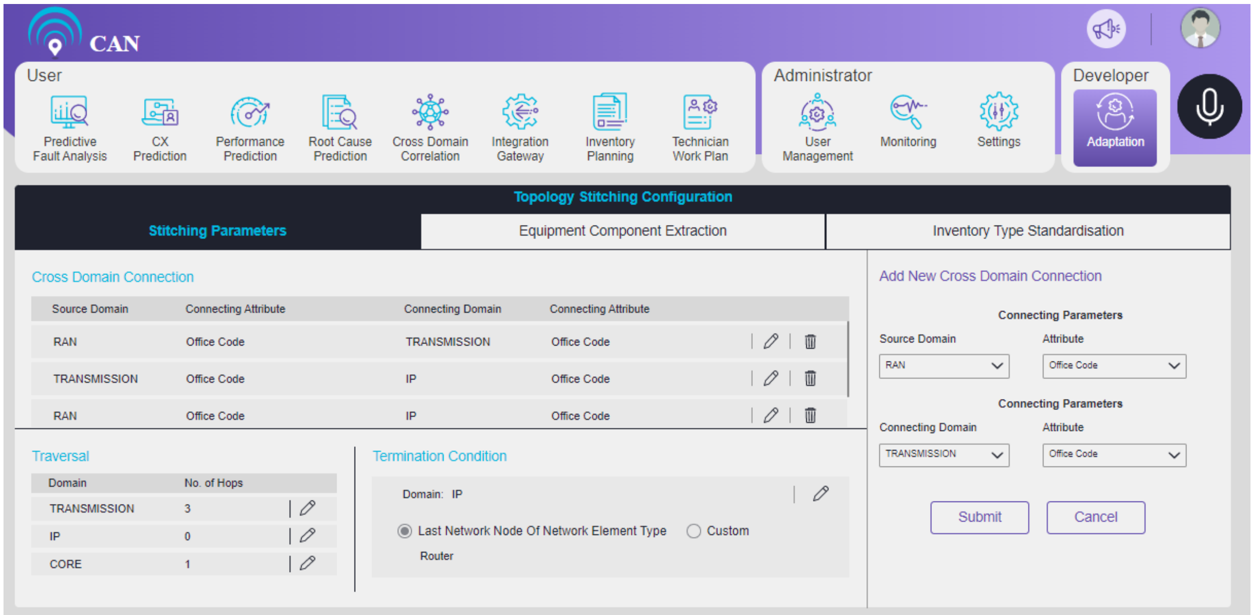
Topology Stitching is a method to discover topological connections across multiple domains and display the same, based on the inventory data. It is helpful in discovering the paths.

Topology Stitching has three tabs:

1. Stitching Parameters
2. Equipment Component Extraction
3. Inventory Type Standardisation

Stitching Parameters

Stitching parameters establish cross-domain connection (RAN, Transmission, IP and Core). Connection traverse from RAN → Transmission → IP → Core (if provided) and RAN → IP → Core (if provided).



Cross Domain Connection

Source Domain	Connecting Attribute	Connecting Domain	Connecting Attribute
RAN	Office Code	TRANSMISSION	Office Code
TRANSMISSION	Office Code	IP	Office Code
RAN	Office Code	IP	Office Code

Traversal

Domain	No. of Hops
TRANSMISSION	3
IP	0
CORE	1

Termination Condition

Domain: IP

● Last Network Node Of Network Element Type ○ Custom

Router

Add New Cross Domain Connection

Connecting Parameters

Source Domain: RAN

Attribute: Office Code

Connecting Parameters

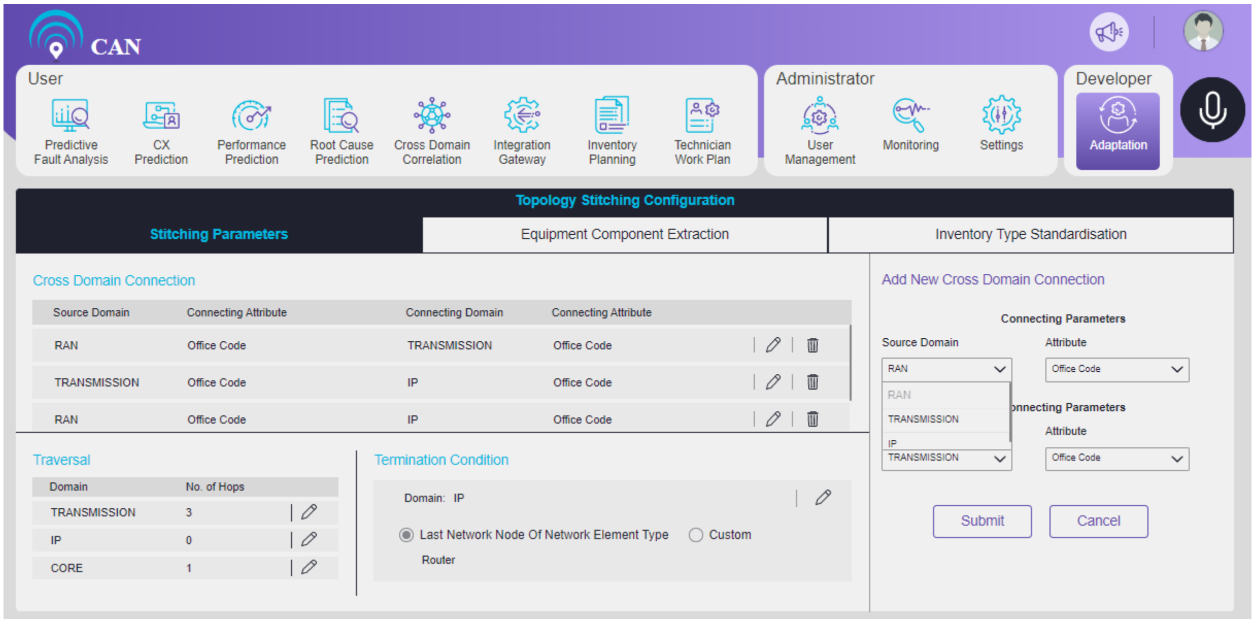
Connecting Domain: TRANSMISSION

Attribute: Office Code

Figure 15.141 - Stitching Parameters

To Add New Cross Domain Connection

1. Select the **Source Domain** from the dropdown (RAN, Transmission, and IP). By default, RAN is selected.
2. Select the **Attribute** of the source domain from the dropdown. CAN provides two options: Office Code and MAC Address. By default, Office Code is selected.
3. Select the Connecting Domain from the dropdown (Transmission, IP and Core).
4. Select the **Attribute** of the source domain from the dropdown. CAN provides two options: Office Code and MAC Address. By default, Office Code is selected.
5. Click **Submit** to add a new cross-domain connection.



Cross Domain Connection

Source Domain	Connecting Attribute	Connecting Domain	Connecting Attribute
RAN	Office Code	TRANSMISSION	Office Code
TRANSMISSION	Office Code	IP	Office Code
RAN	Office Code	IP	Office Code

Traversal

Domain	No. of Hops
TRANSMISSION	3
IP	0
CORE	1

Termination Condition

Domain: IP

● Last Network Node Of Network Element Type ○ Custom

Router

Add New Cross Domain Connection

Connecting Parameters

Source Domain: RAN
Attribute: Office Code

RAN
TRANSMISSION
IP

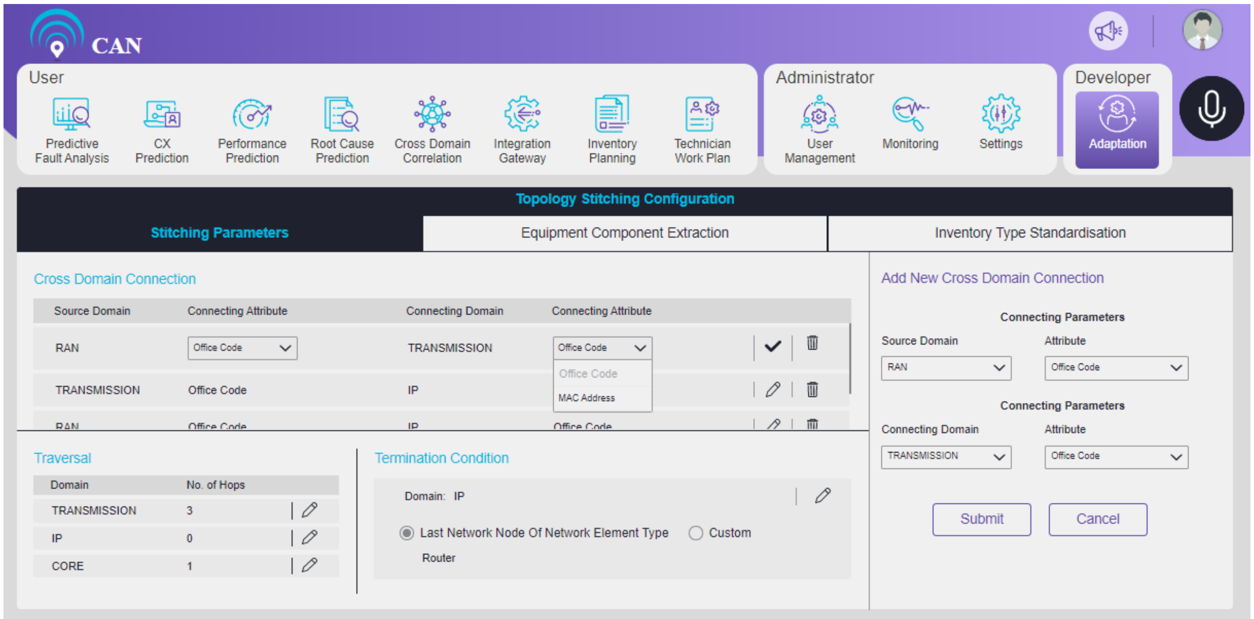
onnecting Parameters

TRANSMISSION
Attribute: Office Code

Figure 15.142 - Add New Cross Domain Connection

To Edit Cross Domain Connection

1. Click the edit icon✎.
2. User can only change the **Connecting Attribute**.
3. Click update icon ✓ to update the cross-domain connection.
4. Click the delete icon 🗑 to delete a cross-domain connection.



Cross Domain Connection

Source Domain	Connecting Attribute	Connecting Domain	Connecting Attribute
RAN	Office Code	TRANSMISSION	Office Code Office Code MAC Address
TRANSMISSION	Office Code	IP	Office Code
RAN	Office Code	IP	Office Code

Traversal

Domain	No. of Hops
TRANSMISSION	3
IP	0
CORE	1

Termination Condition

Domain: IP

● Last Network Node Of Network Element Type ○ Custom

Router

Add New Cross Domain Connection

Connecting Parameters

Source Domain: RAN
Attribute: Office Code

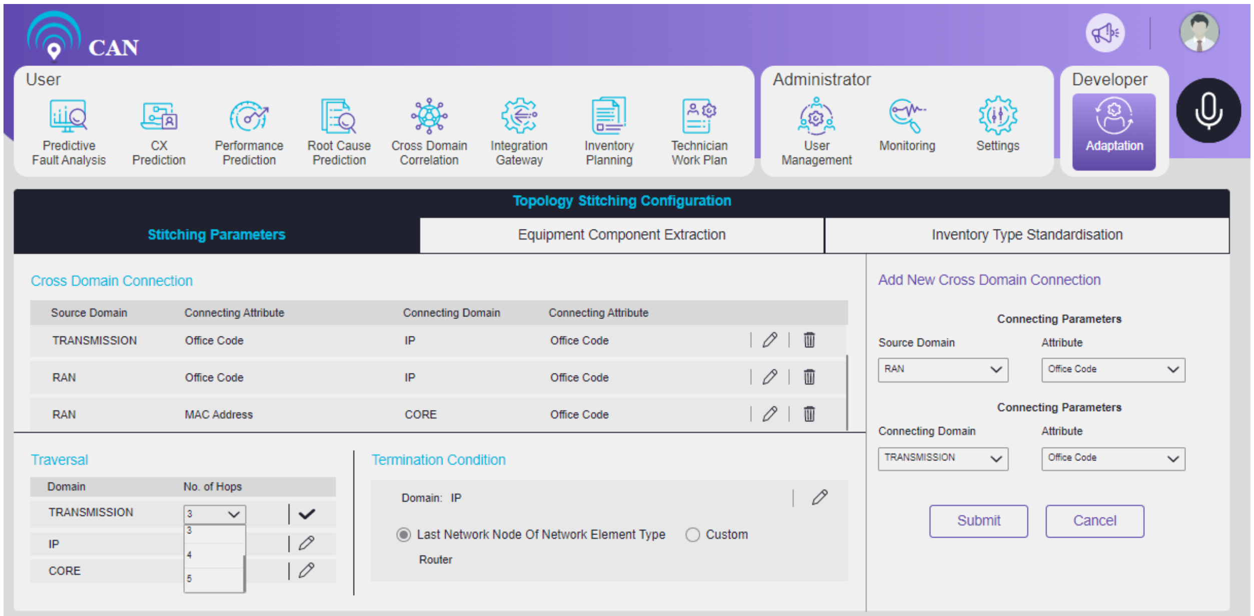
Connecting Parameters

Connecting Domain: TRANSMISSION
Attribute: Office Code

Figure 15.143 - Edit a Connection

To Edit Traversal

Traversal condition determines how connection traverse within a domain based on **No. of Hops**. By default, CAN provides 2 hops, 4 hops and 1 hop for Transmission, IP and Core respectively. User can select the desired hops from the dropdown by clicking the edit icon🖉.



Cross Domain Connection

Source Domain	Connecting Attribute	Connecting Domain	Connecting Attribute
TRANSMISSION	Office Code	IP	Office Code
RAN	Office Code	IP	Office Code
RAN	MAC Address	CORE	Office Code

Traversal

Domain	No. of Hops
TRANSMISSION	3 3 4 5
IP	
CORE	

Termination Condition

Domain: IP

● Last Network Node Of Network Element Type ○ Custom

Router

Add New Cross Domain Connection

Connecting Parameters

Source Domain: RAN

Attribute: Office Code

Connecting Parameters

Connecting Domain: TRANSMISSION

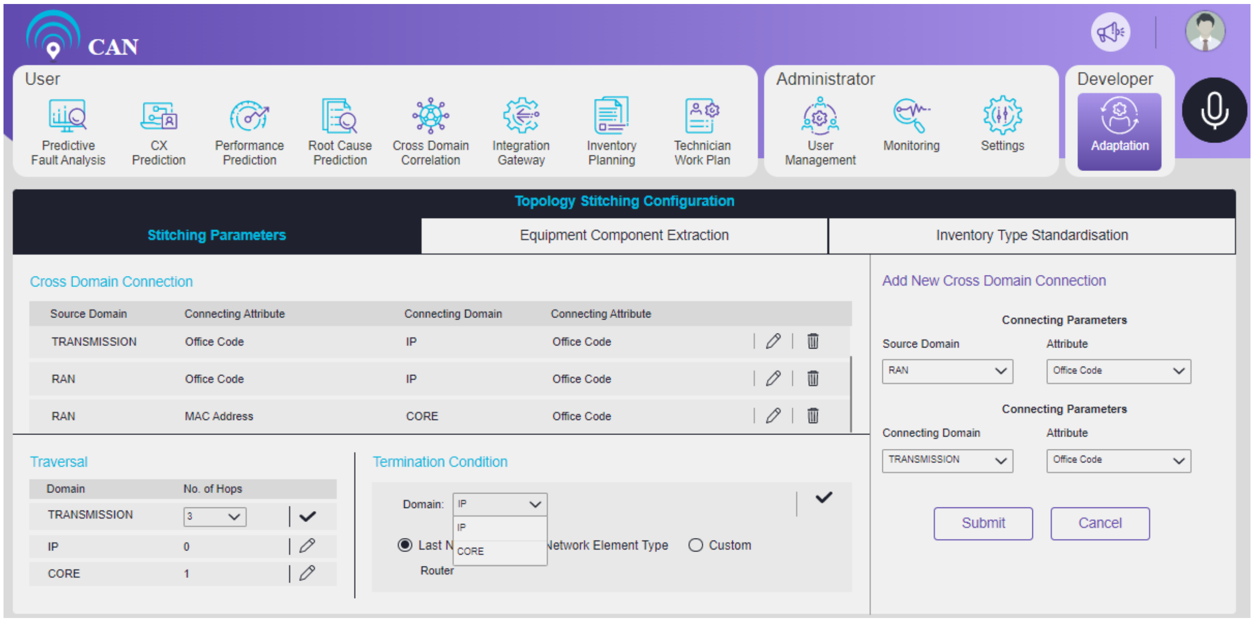
Attribute: Office Code

Submit Cancel

Figure 15.144 - Connection Traversal

To Edit Termination Condition

Termination Condition specifies the destination node. User can click on the edit icon🖉 to select the end domain IP or Core from the dropdown. By default, the termination condition is the **Last Network Node of Network Element Type** i.e. Router.



Cross Domain Connection

Source Domain	Connecting Attribute	Connecting Domain	Connecting Attribute
TRANSMISSION	Office Code	IP	Office Code
RAN	Office Code	IP	Office Code
RAN	MAC Address	CORE	Office Code

Traversal

Domain	No. of Hops
TRANSMISSION	3
IP	0
CORE	1

Termination Condition

Domain: IP (IP, CORE)

● Last N… Router ○ …Network Element Type ○ Custom

Add New Cross Domain Connection

Connecting Parameters

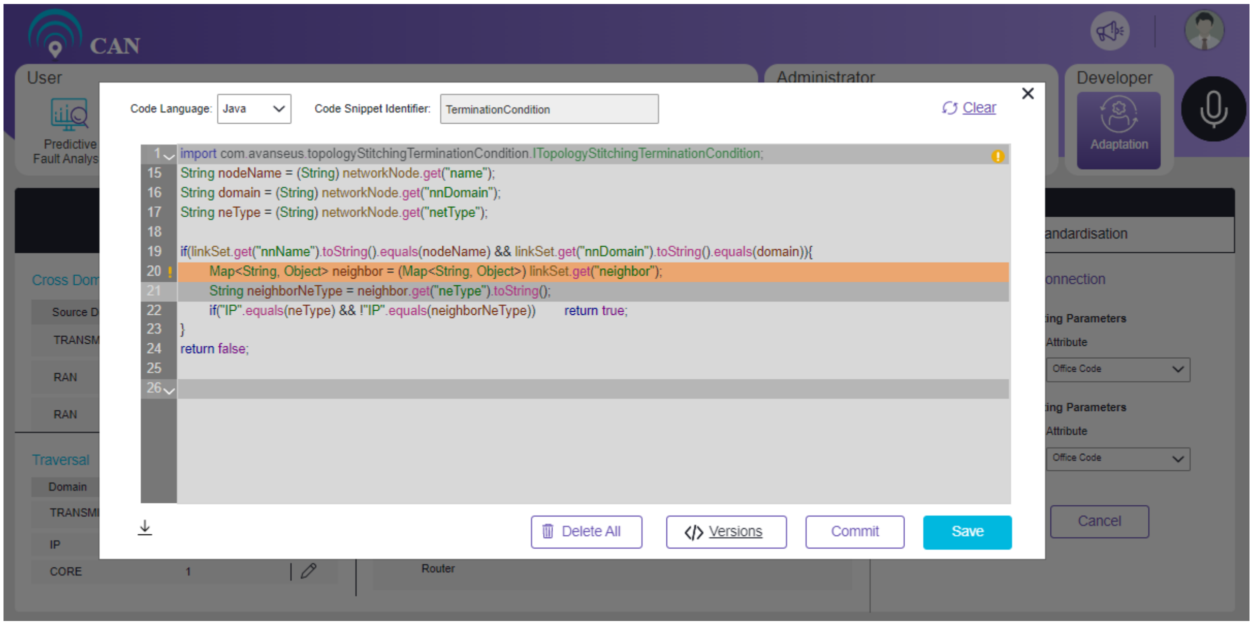
Source Domain: RAN Attribute: Office Code

Connecting Parameters

Connecting Domain: TRANSMISSION Attribute: Office Code

Figure 15.145 – Termination Condition Domain Selection

When user clicks the **Custom** radio button, we are providing IDE to write the custom logic that is used as termination condition based on user requirement.



Code Language: Java

Code Snippet Identifier: TerminationCondition

```java
import com.avanseus.topologyStitchingTerminationCondition.ITopologyStitchingTerminationCondition;
String nodeName = (String) networkNode.get("name");
String domain = (String) networkNode.get("nnDomain");
String neType = (String) networkNode.get("netType");

if(linkSet.get("nnName").toString().equals(nodeName) && linkSet.get("nnDomain").toString().equals(domain)){
    Map<String, Object> neighbor = (Map<String, Object>) linkSet.get("neighbor");
    String neighborNeType = neighbor.get("neType").toString();
    if("IP".equals(neType) && !"IP".equals(neighborNeType))       return true;
}
return false;

```

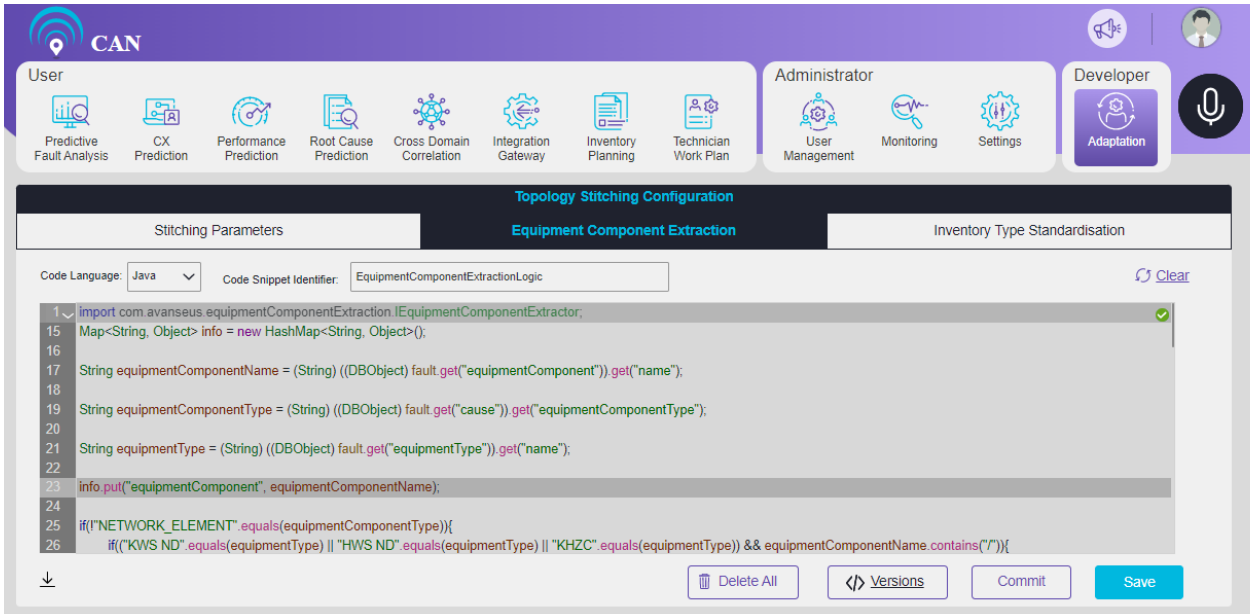
Figure 15.146 - Custom Termination Condition

When the traversal enter IP domain, termination condition is checked for every node. Once the condition is met, we exit the traversal. Otherwise, traversal continues based on hops until the condition is met.

Equipment Component Extraction

After the path discovery using stitching parameters, we need to extract the equipment components i.e. slot number, daughter slot number, port number, etc. to identify port fault and link fault. The faults are displayed in the Predictive Fault Analysis screen.

Avanseus provides default logic. User has the option to write, edit, save different versions and download the code.



Code Language: Java

Code Snippet Identifier: EquipmentComponentExtractionLogic

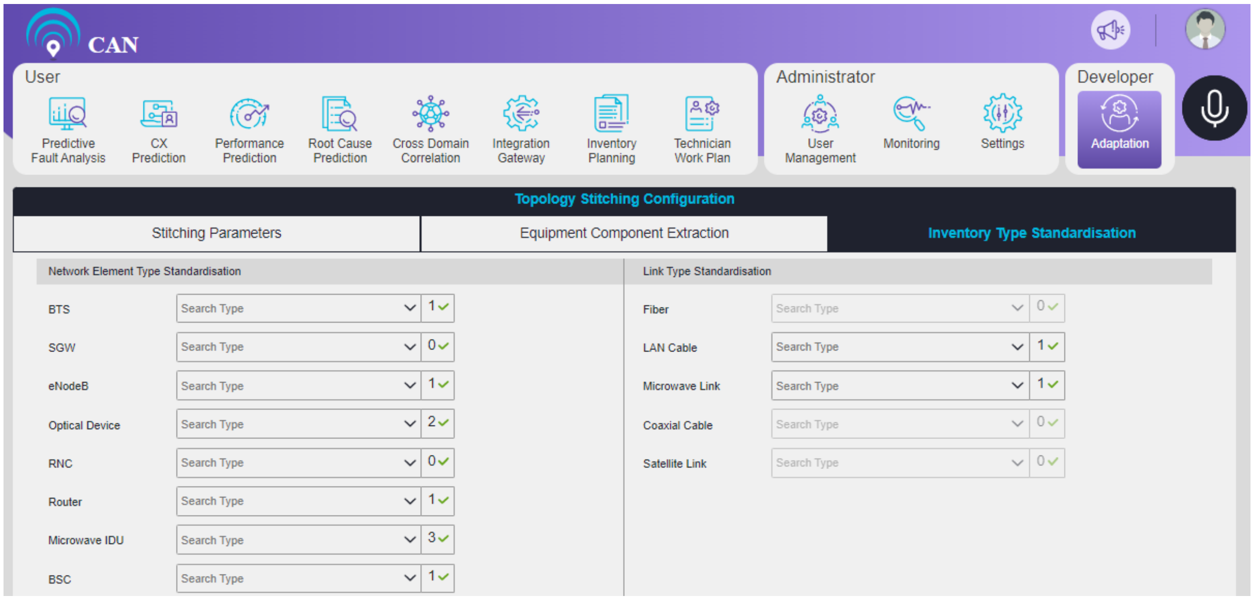
```
import com.avanseus.equipmentComponentExtraction.IEquipmentComponentExtractor;
Map<String, Object> info = new HashMap<String, Object>();

String equipmentComponentName = (String) ((DBObject) fault.get("equipmentComponent")).get("name");

String equipmentComponentType = (String) ((DBObject) fault.get("cause")).get("equipmentComponentType");

String equipmentType = (String) ((DBObject) fault.get("equipmentType")).get("name");

info.put("equipmentComponent", equipmentComponentName);

if(!"NETWORK_ELEMENT".equals(equipmentComponentType)){
      if(("KWS ND".equals(equipmentType) || "HWS ND".equals(equipmentType) || "KHZC".equals(equipmentType)) && equipmentComponentName.contains("/")){
```

Figure 15.147 - Equipment Component Extraction

Inventory Type Standardisation

When customer provides the inventory data, it is not standardized. The inventory data is mapped to the default network element type and link type in the system.

There are two Inventory Type Standardisation: **Network Element Standardisation** and **Link Type Standardisation**.



Network Element Type Standardisation

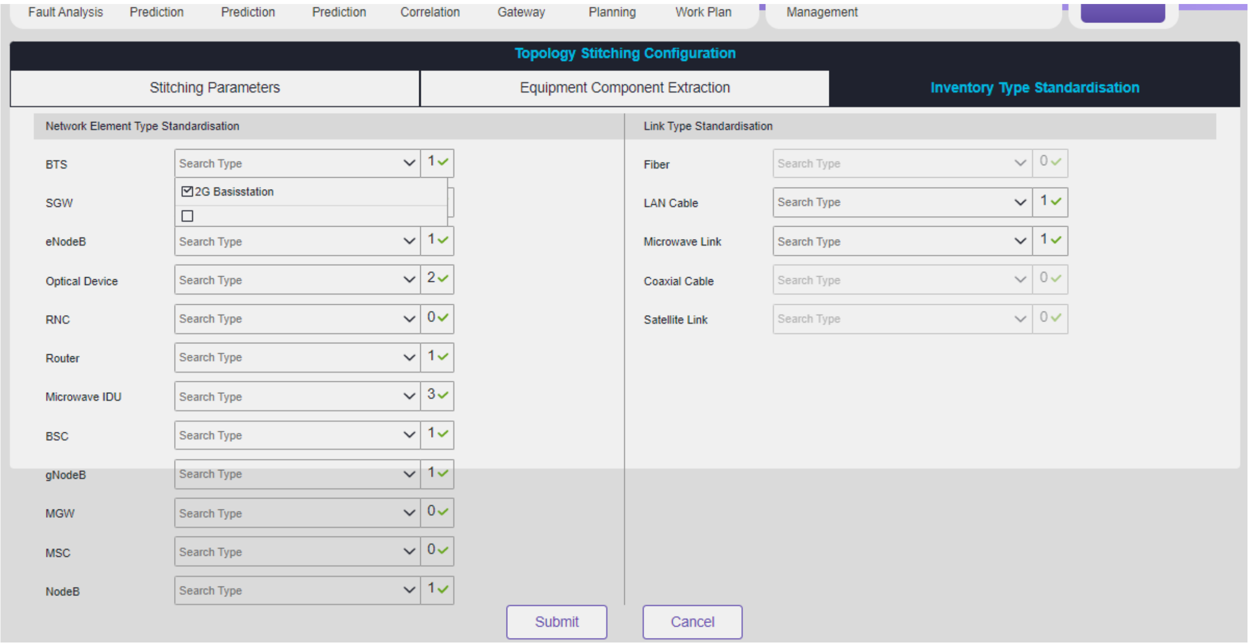
BTS	Search Type	1 ✓
SGW	Search Type	0 ✓
eNodeB	Search Type	1 ✓
Optical Device	Search Type	2 ✓
RNC	Search Type	0 ✓
Router	Search Type	1 ✓
Microwave IDU	Search Type	3 ✓
BSC	Search Type	1 ✓

Link Type Standardisation

Fiber	Search Type	0 ✓
LAN Cable	Search Type	1 ✓
Microwave Link	Search Type	1 ✓
Coaxial Cable	Search Type	0 ✓
Satellite Link	Search Type	0 ✓

Figure 15.148 - Inventory Type Standardisation

The standardized data is displayed on UI. Select the network elements and links from the dropdown based on the requirement and click the **Submit** button.



Network Element Type Standardisation

BTS	Search Type ☑ 2G Basisstation ☐	1 ✓
SGW		
eNodeB	Search Type	1 ✓
Optical Device	Search Type	2 ✓
RNC	Search Type	0 ✓
Router	Search Type	1 ✓
Microwave IDU	Search Type	3 ✓
BSC	Search Type	1 ✓
gNodeB	Search Type	1 ✓
MGW	Search Type	0 ✓
MSC	Search Type	0 ✓
NodeB	Search Type	1 ✓

Link Type Standardisation

Fiber	Search Type	0 ✓
LAN Cable	Search Type	1 ✓
Microwave Link	Search Type	1 ✓
Coaxial Cable	Search Type	0 ✓
Satellite Link	Search Type	0 ✓

Figure 15.149 - Inventory Type Dropdown

Topology Discovery Configuration

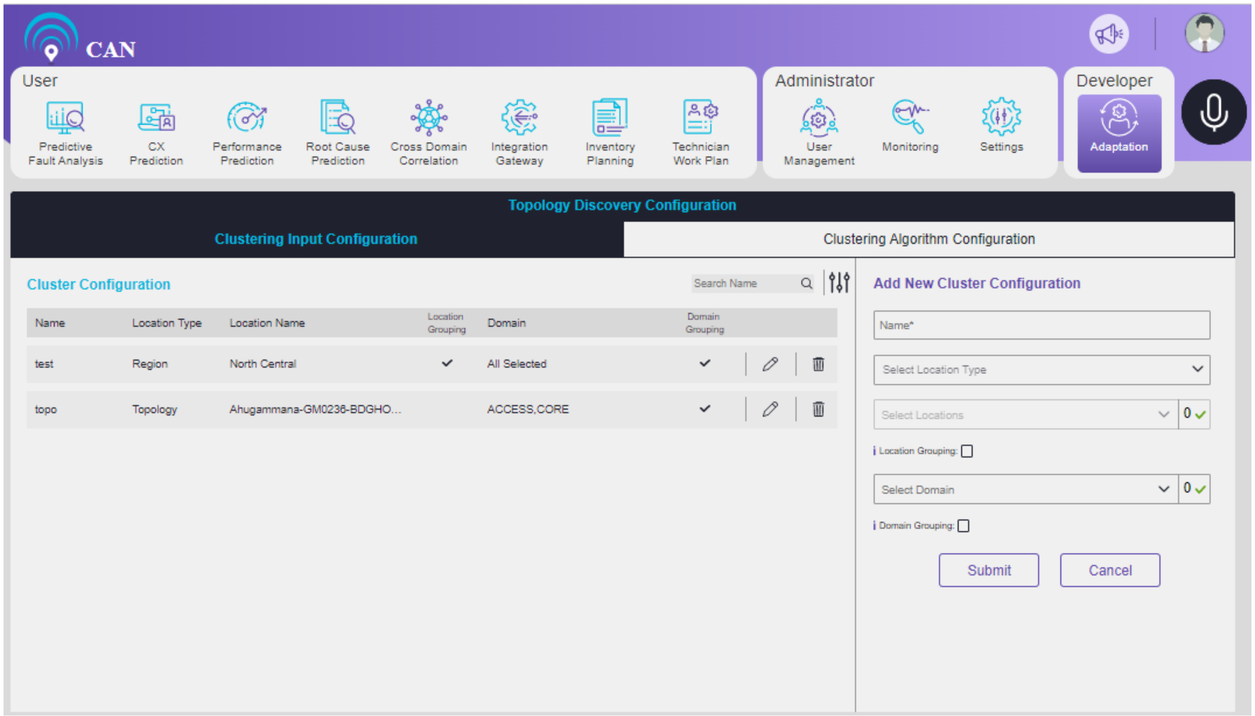
Topology Discovery Configuration is used in generating clusters. The generated clusters are displayed in the Cross Domain Correlation screen.

Topology Discovery Configuration has two tabs:

1. Clustering Input Configuration
2. Clustering Algorithm Configuration

Clustering Input Configuration

Clustering input configuration is used to configure the clustering data on various levels (Nation, Zone, Office Code, etc.). Input is provided to run the clustering for a preferred level. By default, Topology Discovery Configuration lands on this screen.

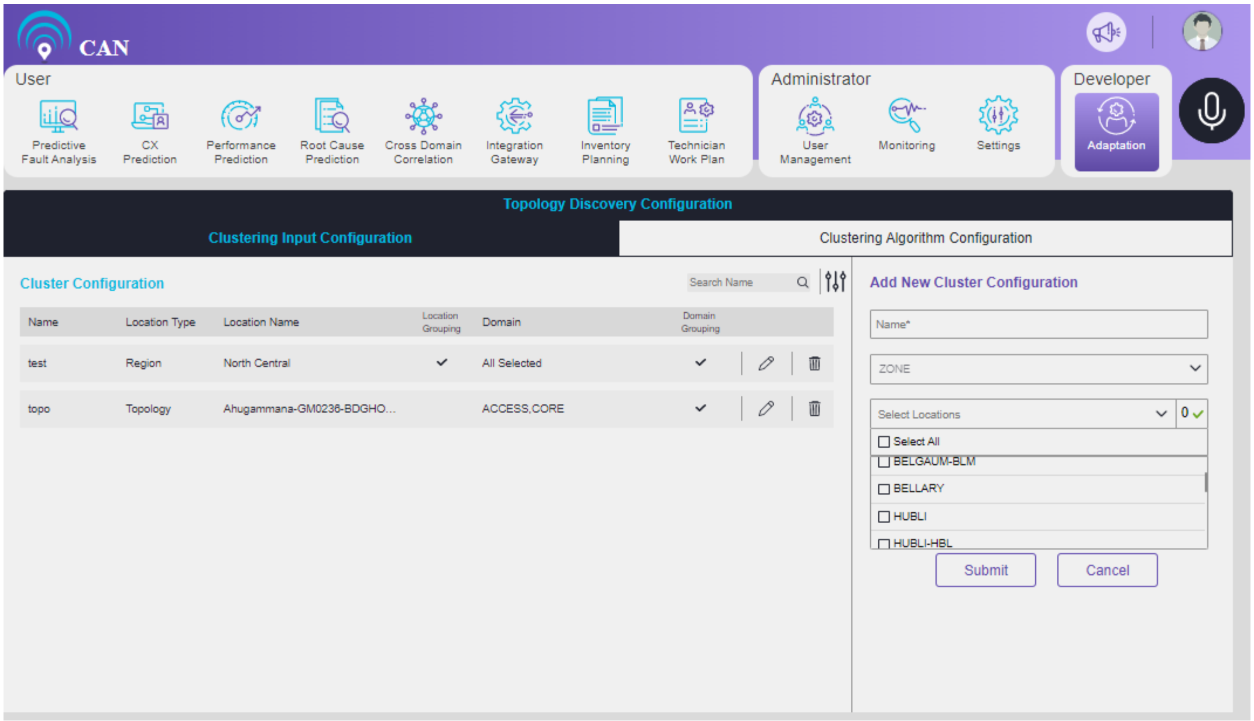


Name	Location Type	Location Name	Location Grouping	Domain	Domain Grouping
test	Region	North Central	✓	All Selected	✓
topo	Topology	Ahugammana-GM0236-BDGHO...		ACCESS,CORE	✓

Figure 15.150 - Clustering Input Configuration Screen

To Add New Cluster Configuration

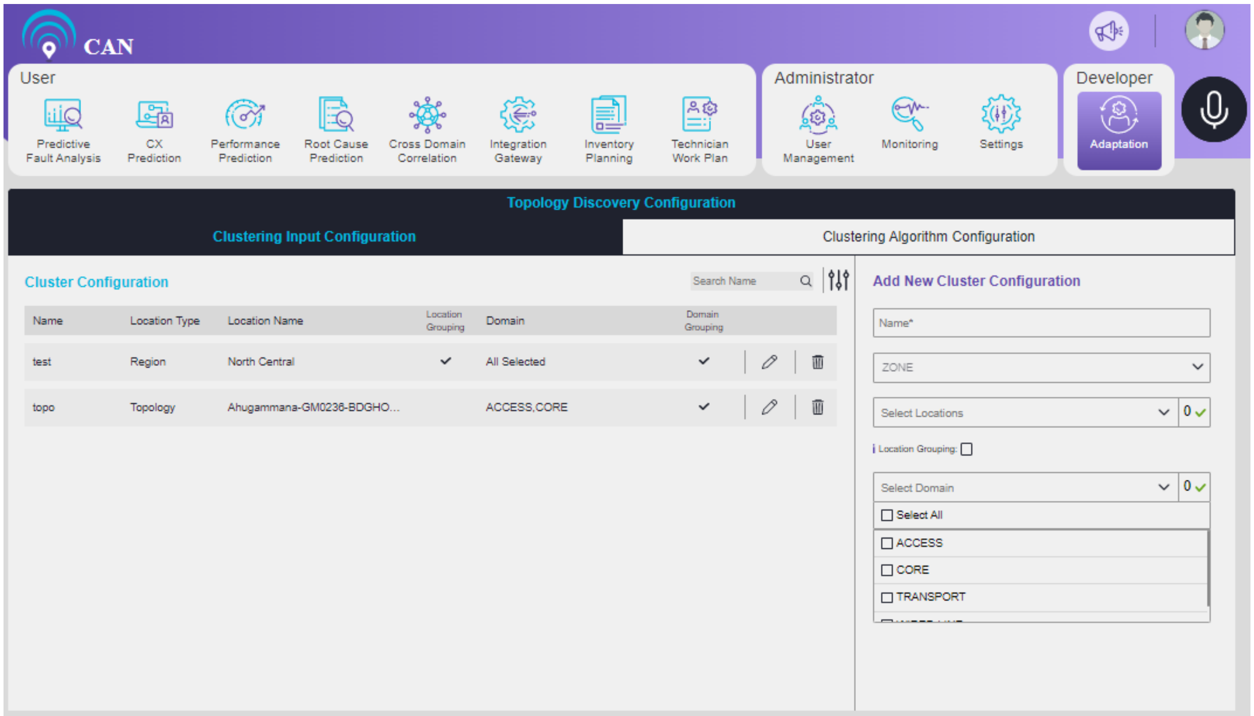
1. Enter a configuration name (**Name**).
2. Select **Location Type** (Nation, Division, Region, Zone, Office_Code and Topology) from the dropdown.
3. Select **Locations** from the dropdown for the selected Location Type. User can select one, many or all the locations by clicking the checkboxes.
4. **Location Grouping** indicates whether to run clustering combined or separately.



Name	Location Type	Location Name	Location Grouping	Domain	Domain Grouping
test	Region	North Central	✓	All Selected	✓
topo	Topology	Ahugammana-GM0236-BDGHO...		ACCESS,CORE	✓

Figure 15.151 - Location Dropdown

5. Select **Domain** (Access, Core, Transport and Wired Line) from the dropdown. User can select one, many or all the domains by clicking the checkboxes.
6. **Domain Grouping** indicates whether to run clustering combined or separately.



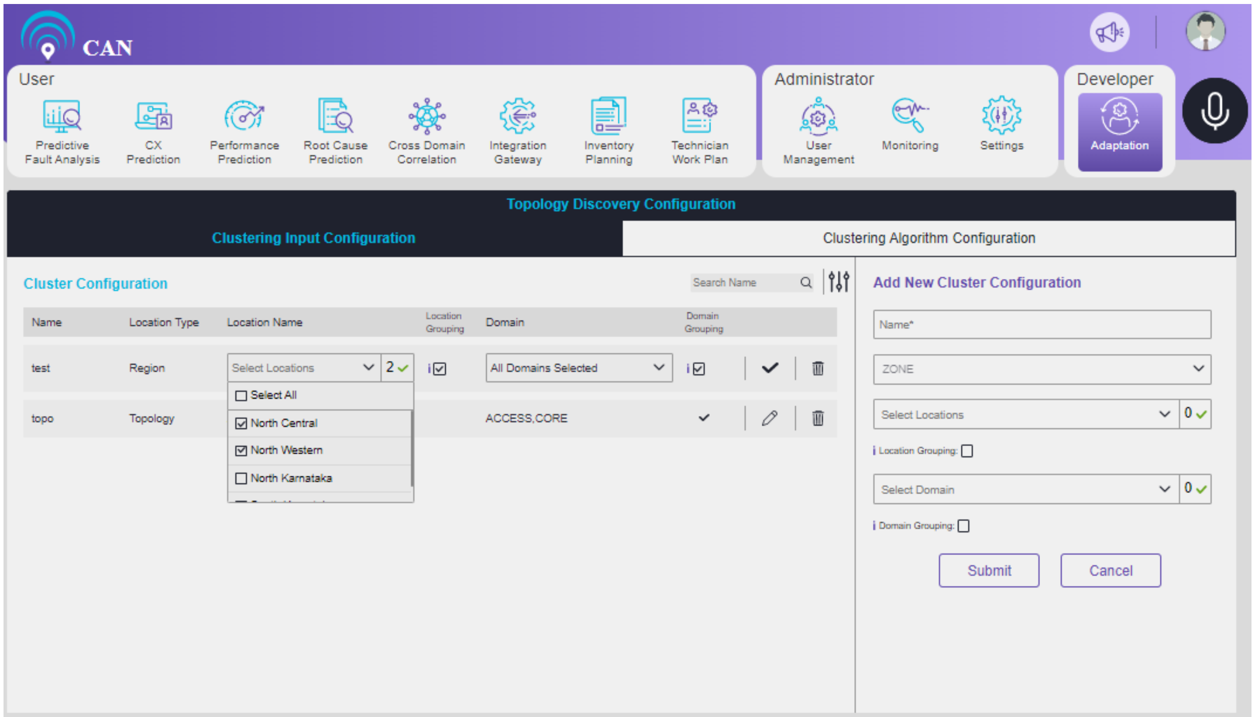
Name	Location Type	Location Name	Location Grouping	Domain	Domain Grouping
test	Region	North Central	✓	All Selected	✓
topo	Topology	Ahugammana-GM0236-BDGHO...		ACCESS,CORE	✓

Figure 15.152 - Domain Dropdown

7. Click **Submit** to add new configuration.

To Edit Existing Cluster Configuration

1. Click the Edit icon✎.
2. Select/Unselect the **Location** and **Domain**.
3. Select/Unselect the Location Grouping and Domain Grouping.
4. Click the Update icon ✓ to save the changes.
5. Click Delete icon 🗑 to delete the configuration.



Cluster Configuration

Name	Location Type	Location Name	Location Grouping	Domain	Domain Grouping
test	Region	Select Locations 2 ✓	☑	All Domains Selected	☑
topo	Topology			ACCESS,CORE	✓

□ Select All
☑ North Central
☑ North Western
□ North Karnataka

Add New Cluster Configuration

Name*

ZONE

Select Locations 0 ✓

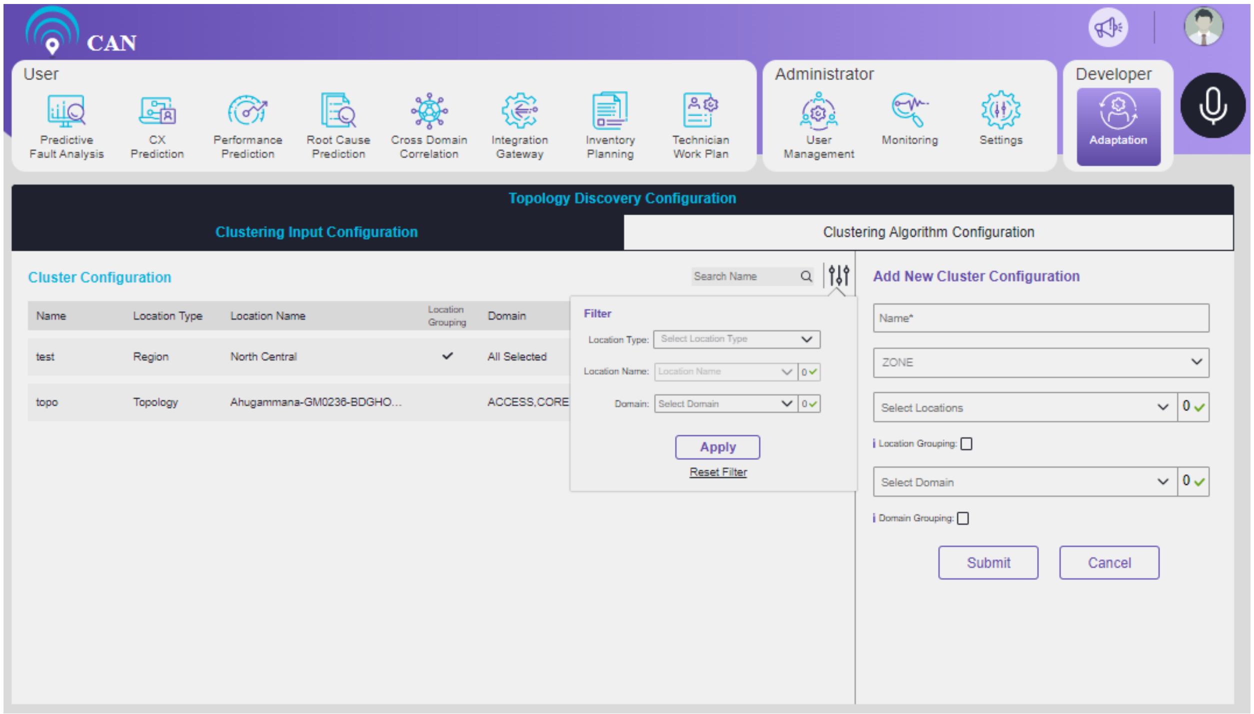
Location Grouping: □

Select Domain 0 ✓

Domain Grouping: □

Figure 15.153 - Edit Cluster Configuration

6. User can search a configuration based on the **Name**.
7. Click on the Filter icon and select the preferred **Location Type**, **Location Name** and **Domain** from the dropdown.
8. Click **Apply** to filter the configurations.
9. Click Reset Filter to display all the configurations.



Cluster Configuration

Name	Location Type	Location Name	Location Grouping	Domain
test	Region	North Central	✓	All Selected
topo	Topology	Ahugammana-GM0236-BDGHO...		ACCESS,CORE

Filter

Location Type: Select Location Type

Location Name: Location Name 0 ✓

Domain: Select Domain 0 ✓

Add New Cluster Configuration

Name*

ZONE

Select Locations 0 ✓

Location Grouping: □

Select Domain 0 ✓

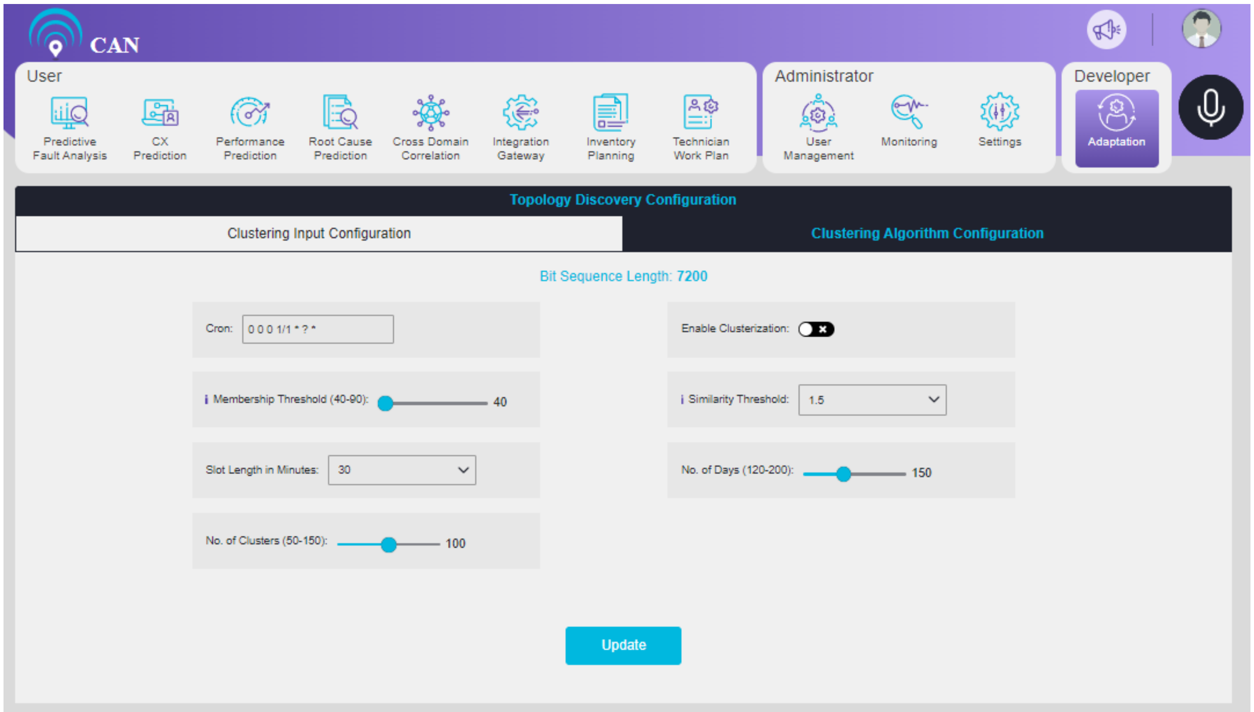
Domain Grouping: □

Figure 15.154 - Filter Cluster Configuration

Clustering Algorithm Configuration

Algorithm configuration is used in changing the constants that are directly corresponding to the outcome of Clustering Algorithm.

1. Set the algorithm parameters as per the requirement.
    a. **Enable clusterization** - Enable clusterization switch decides whether to display the configuration part or do the clustering.
    b. **Cron** - It runs the "Clustering Algorithm" automatically at specific time.
    c. **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).
    d. **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).
    e. **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.
    f. **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).
    g. **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).
2. Click **Update** button to save the changes.



Bit Sequence Length: 7200

Cron: 0 0 0 1/1 * ? *

Enable Clusterization: ✗

Membership Threshold (40-90): 40

Similarity Threshold: 1.5

Slot Length in Minutes: 30

No. of Days (120-200): 150

No. of Clusters (50-150): 100

Figure 15.155 - Clustering Algorithm Configuration Screen

Page Intentionally Left Blank

16. 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.

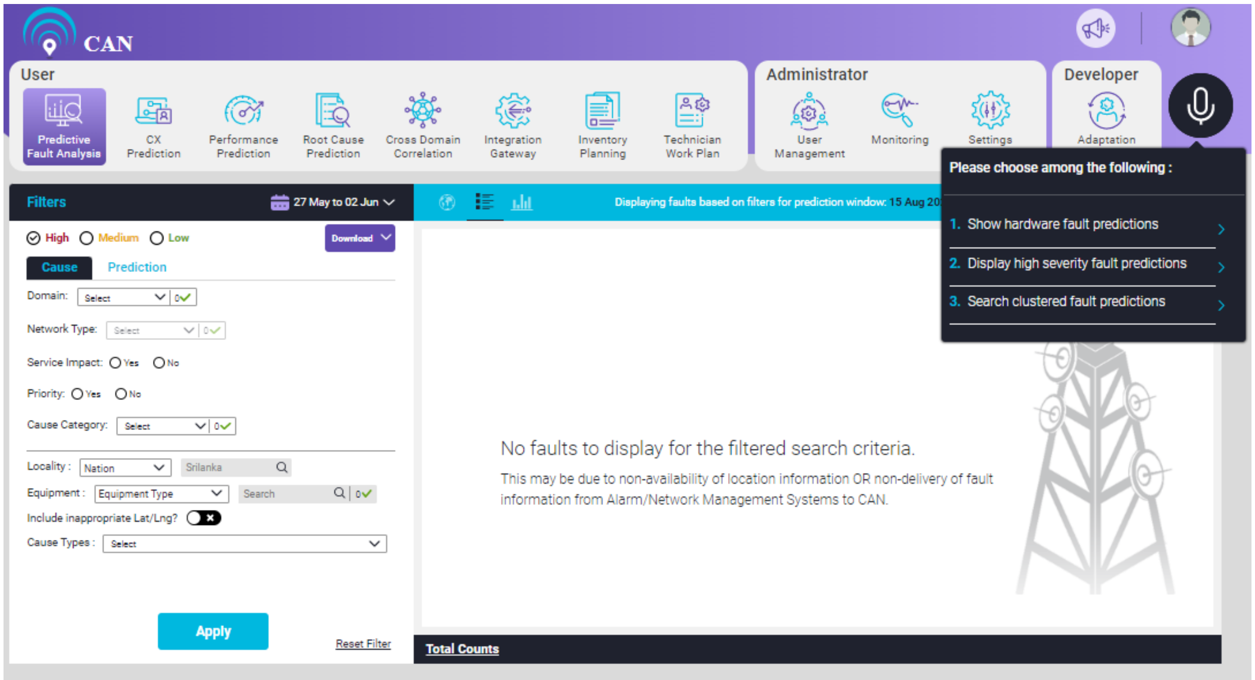
VBI provide answers to user's queries in the voice form as well as it also displays the query result on the screen. The queries must be in US English or IN English.

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 should not 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.



Please choose among the following :

1. Show hardware fault predictions
2. Display high severity fault predictions
3. Search clustered fault predictions

Displaying faults based on filters for prediction window: 15 Aug 20

Domain: Select

Network Type: Select

Service Impact: ○ Yes ○ No

Priority: ○ Yes ○ No

Cause Category: Select

Locality : Nation Srilanka

Equipment : Equipment Type Search

Include inappropriate Lat/Lng?

Cause Types : Select

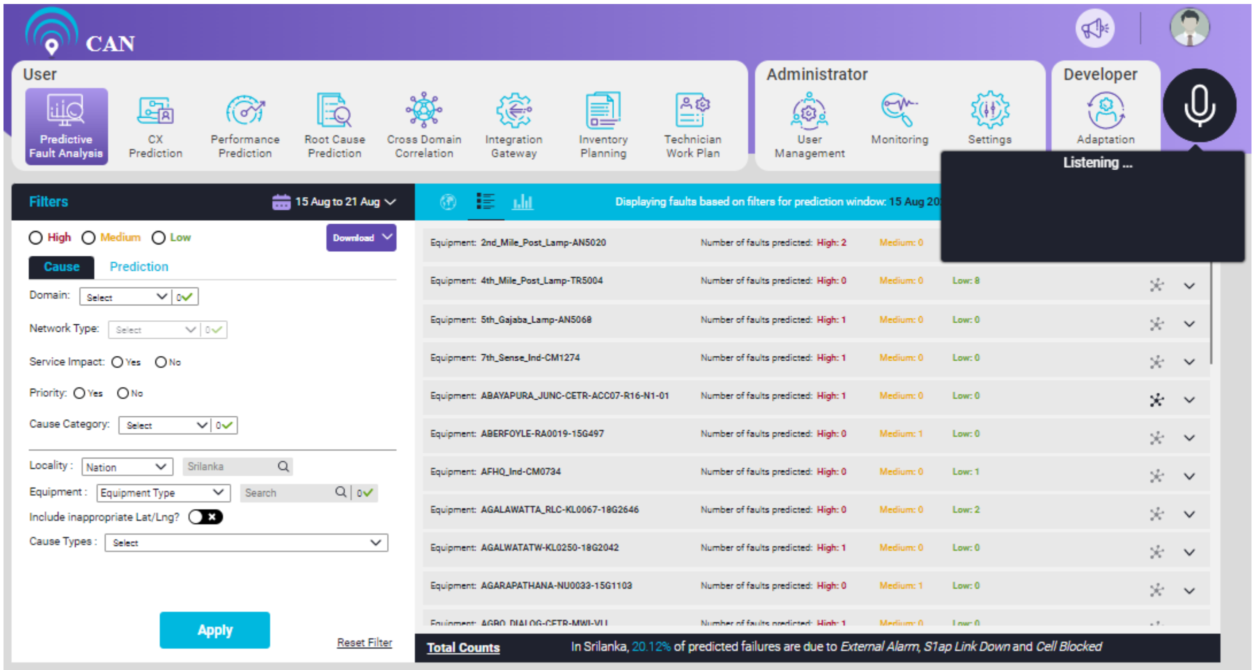
No faults to display for the filtered search criteria.

This may be due to non-availability of location information OR non-delivery of fault information from Alarm/Network Management Systems to CAN.

Figure 16.1 - 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 is converted to text.



○ High ○ Medium ○ Low

Domain: Select | 0✓

Network Type: Select | 0✓

Service Impact: ○ Yes ○ No

Priority: ○ Yes ○ No

Cause Category: Select | 0✓

Locality : Nation | Srilanka

Equipment : Equipment Type | Search | 0✓

Include inappropriate Lat/Lng?

Cause Types : Select

Displaying faults based on filters for prediction window: 15 Aug 20

Equipment: 2nd_Mile_Post_Lamp-AN5020 Number of faults predicted: High: 2 Medium: 0

Equipment: 4th_Mile_Post_Lamp-TR5004 Number of faults predicted: High: 0 Medium: 0 Low: 8

Equipment: 5th_Gajaba_Lamp-AN5068 Number of faults predicted: High: 1 Medium: 0 Low: 0

Equipment: 7th_Sense_Ind-CM1274 Number of faults predicted: High: 1 Medium: 0 Low: 0

Equipment: ABAYAPURA_JUNC-CETR-ACC07-R16-N1-01 Number of faults predicted: High: 1 Medium: 0 Low: 0

Equipment: ABERFOYLE-RA0019-15G497 Number of faults predicted: High: 0 Medium: 1 Low: 0

Equipment: AFHQ_Ind-CM0734 Number of faults predicted: High: 0 Medium: 0 Low: 1

Equipment: AGALAWATTA_RLC-KL0067-18G2646 Number of faults predicted: High: 0 Medium: 0 Low: 2

Equipment: AGALWATATW-KL0250-18G2042 Number of faults predicted: High: 1 Medium: 0 Low: 0

Equipment: AGARAPATHANA-NU0033-15G1103 Number of faults predicted: High: 0 Medium: 1 Low: 0

Equipment: AGBO_DIALOG-CETR-MWI-VLI Number of faults predicted: High: 1 Medium: 0 Low: 0

Total Counts In Srilanka, 20.12% of predicted failures are due to *External Alarm, S1ap Link Down* and *Cell Blocked*

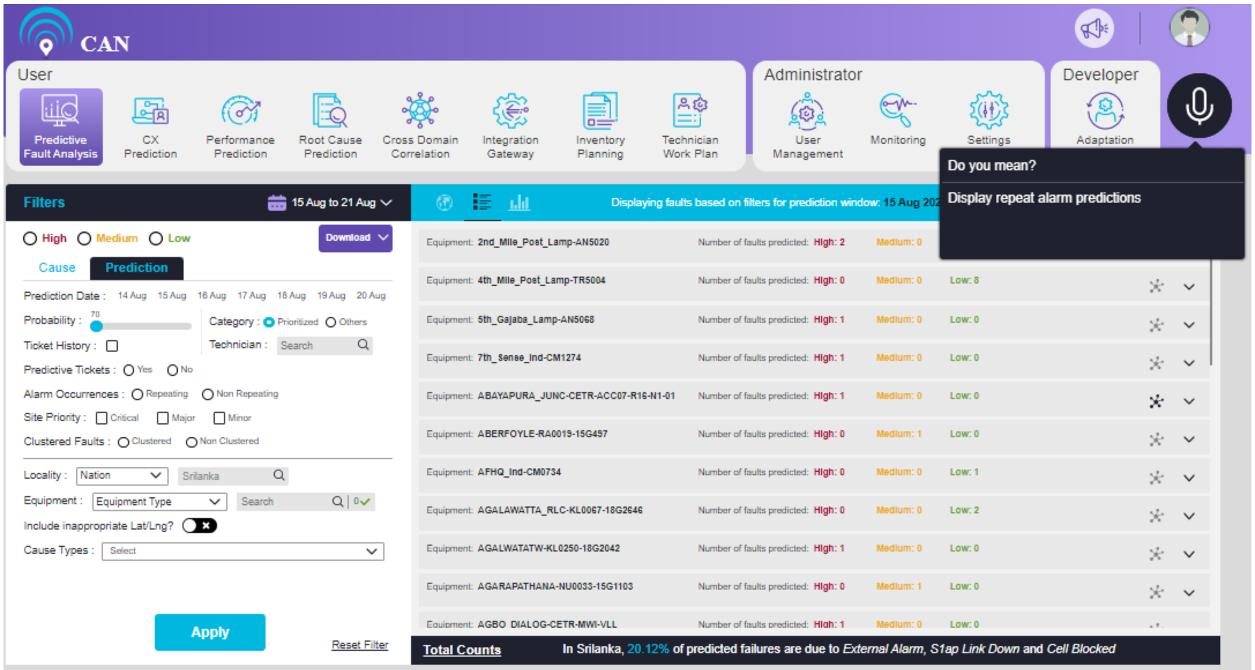
Figure 16.2 - Voice Commands conversion to text

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”? Along with that suggestion.



Do you mean?

Display repeat alarm predictions

15 Aug to 21 Aug

○ High ○ Medium ○ Low

Prediction Date : 14 Aug 15 Aug 16 Aug 17 Aug 18 Aug 19 Aug 20 Aug

Probability : 70

Category : ● Prioritized ○ Others

Ticket History : □

Technician : Search

Predictive Tickets : ○ Yes ○ No

Alarm Occurrences : ○ Repeating ○ Non Repeating

Site Priority : □ Critical □ Major □ Minor

Clustered Faults : ○ Clustered ○ Non Clustered

Locality : Nation Srilanka

Equipment : Equipment Type Search 0✓

Include inappropriate Lat/Lng? ✕

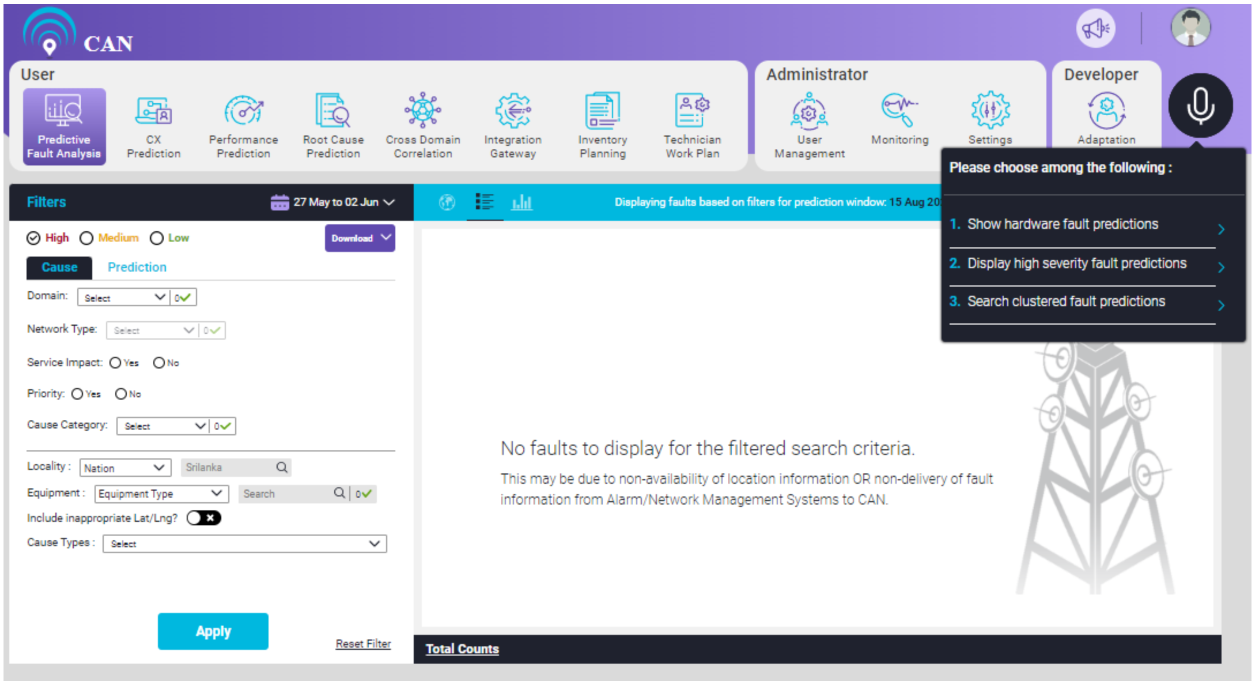
Cause Types : Select

Displaying faults based on filters for prediction window: 15 Aug 202

Equipment	Number of faults predicted: High	Medium	Low
2nd_Mile_Post_Lamp-AN5020	High: 2	Medium: 0	
4th_Mile_Post_Lamp-TR5004	High: 0	Medium: 0	Low: 8
5th_Gajaba_Lamp-AN5068	High: 1	Medium: 0	Low: 0
7th_Sense_Ind-CM1274	High: 1	Medium: 0	Low: 0
ABAYAPURA_JUNC-CETR-ACC07-R16-N1-01	High: 1	Medium: 0	Low: 0
ABERFOYLE-RA0019-15G457	High: 0	Medium: 1	Low: 0
AFHQ_Ind-CM0734	High: 0	Medium: 0	Low: 1
AGALAWATTA_RLC-KL0067-18G2646	High: 0	Medium: 0	Low: 2
AGALWATATW-KL0250-18G2042	High: 1	Medium: 0	Low: 0
AGARAPATHANA-NU0033-15G1103	High: 0	Medium: 1	Low: 0
AGBO_DIALOG-CETR-MWI-VLL	High: 1	Medium: 0	Low: 0

In Srilanka, 20.12% of predicted failures are due to *External Alarm*, *S1ap Link Down* and *Cell Blocked*

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



Displaying faults based on filters for prediction window: 15 Aug 20

Please choose among the following :

1. Show hardware fault predictions
2. Display high severity fault predictions
3. Search clustered fault predictions

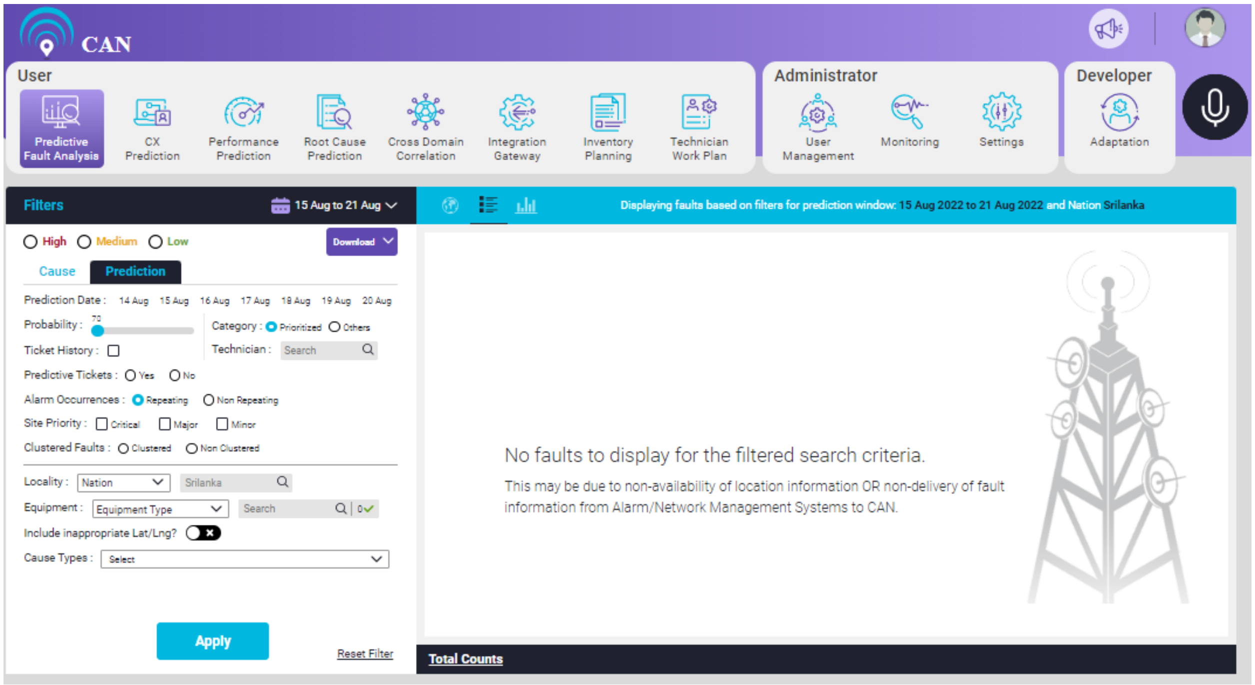
No faults to display for the filtered search criteria.

This may be due to non-availability of location information OR non-delivery of fault information from Alarm/Network Management Systems to CAN.

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 would audibly inform “Sorry, no valid records found”, please speak again. The screen will display that “No faults to display for the filtered search criteria”.



Displaying faults based on filters for prediction window: 15 Aug 2022 to 21 Aug 2022 and Nation Srilanka

No faults to display for the filtered search criteria.

This may be due to non-availability of location information OR non-delivery of fault information from Alarm/Network Management Systems to CAN.

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

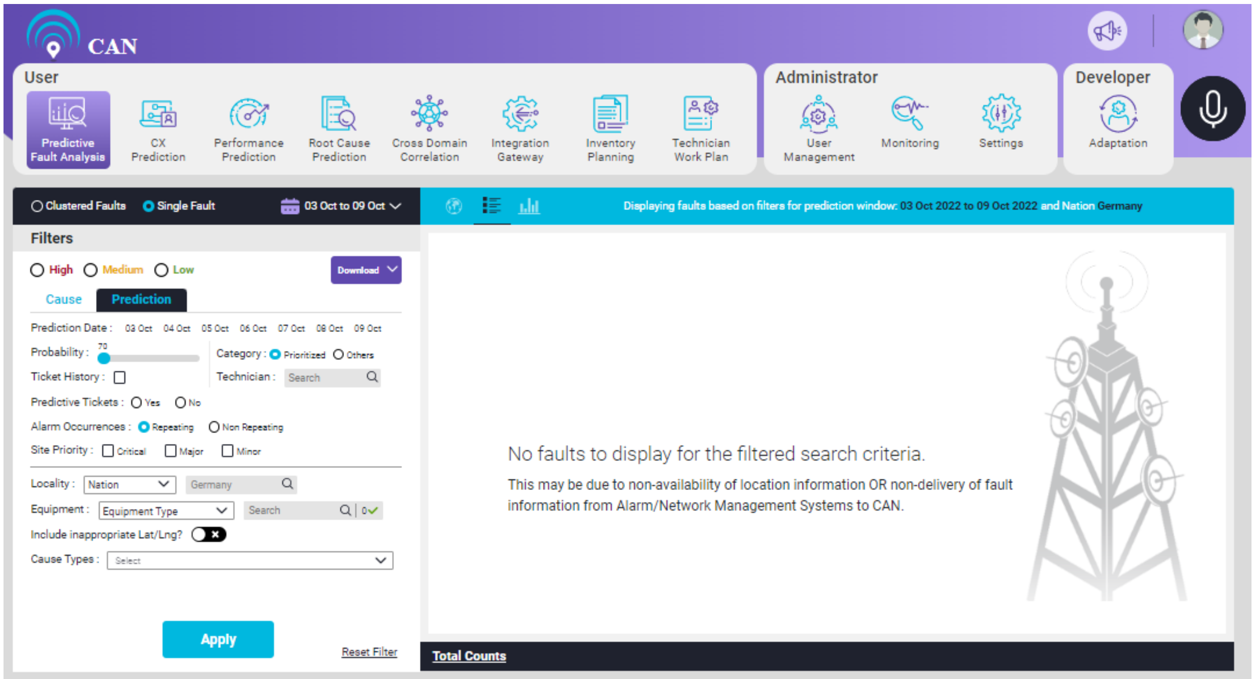
User can ask the 13 queries for which CAN will provide appropriate response with adequate semantics. The list of queries are as follows:

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.



○ Clustered Faults ● Single Fault

03 Oct to 09 Oct

Displaying faults based on filters for prediction window: 03 Oct 2022 to 09 Oct 2022 and Nation Germany

Filters

○ High ○ Medium ○ Low

Prediction Date : 03 Oct 04 Oct 05 Oct 06 Oct 07 Oct 08 Oct 09 Oct

Probability : 70

Category : ● Prioritized ○ Others

Ticket History : □

Technician : Search

Predictive Tickets : ○ Yes ○ No

Alarm Occurrences : ● Repeating ○ Non Repeating

Site Priority : □ Critical □ Major □ Minor

Locality : Nation Germany

Equipment : Equipment Type Search | 0✓

Include inappropriate Lat/Lng? ✕

Cause Types : Select

No faults to display for the filtered search criteria.

This may be due to non-availability of location information OR non-delivery of fault information from Alarm/Network Management Systems to CAN.

Figure 16.3 - Repeat Alarm Predictions

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

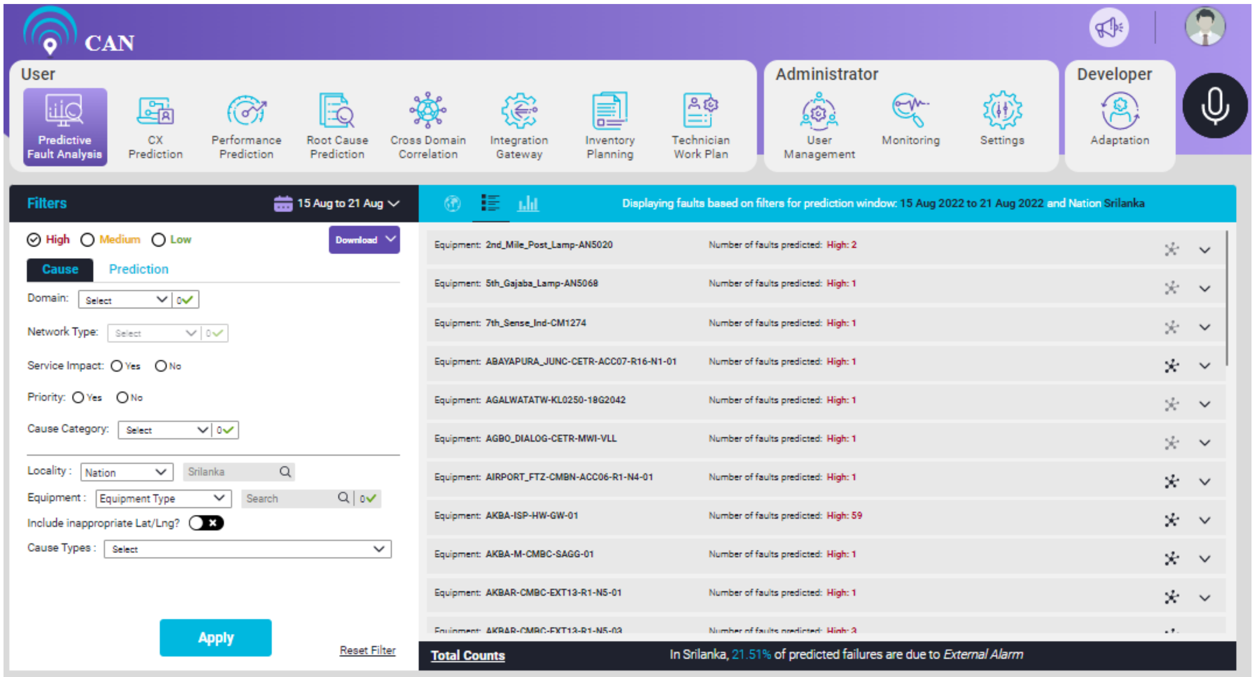
When user asks the query, the screen navigates the user to Predictive Fault Analysis screen. The screen shows the selected Site Priority filter as "Critical" checked in the check box under the prediction tab. The Site Priority have three check boxes: Critical, Major and Minor.

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”.



Filters 15 Aug to 21 Aug

☑ High ○ Medium ○ Low

Cause Prediction

Domain: Select 0✓

Network Type: Select 0✓

Service Impact: ○ Yes ○ No

Priority: ○ Yes ○ No

Cause Category: Select 0✓

Locality : Nation Srilanka

Equipment : Equipment Type Search 0✓

Include inappropriate Lat/Lng? ✕

Cause Types : Select

Displaying faults based on filters for prediction window: 15 Aug 2022 to 21 Aug 2022 and Nation Srilanka

Equipment: 2nd_Mile_Post_Lamp-AN5020	Number of faults predicted: High: 2
Equipment: 5th_Gajaba_Lamp-AN5068	Number of faults predicted: High: 1
Equipment: 7th_Sense_Ind-CM1274	Number of faults predicted: High: 1
Equipment: ABAYAPURA_JUNC-CETR-ACC07-R16-N1-01	Number of faults predicted: High: 1
Equipment: AGALWATATW-KL0250-18G2042	Number of faults predicted: High: 1
Equipment: AGBO_DIALOG-CETR-MWI-VLL	Number of faults predicted: High: 1
Equipment: AIRPORT_FTZ-CMBN-ACC06-R1-N4-01	Number of faults predicted: High: 1
Equipment: AKBA-ISP-HW-GW-01	Number of faults predicted: High: 59
Equipment: AKBA-M-CMBC-SAGG-01	Number of faults predicted: High: 1
Equipment: AKBAR-CMBC-EXT13-R1-N5-01	Number of faults predicted: High: 1
Equipment: AKBAR-CMBC-EXT13-R1-N5-03	Number of faults predicted: High: 3

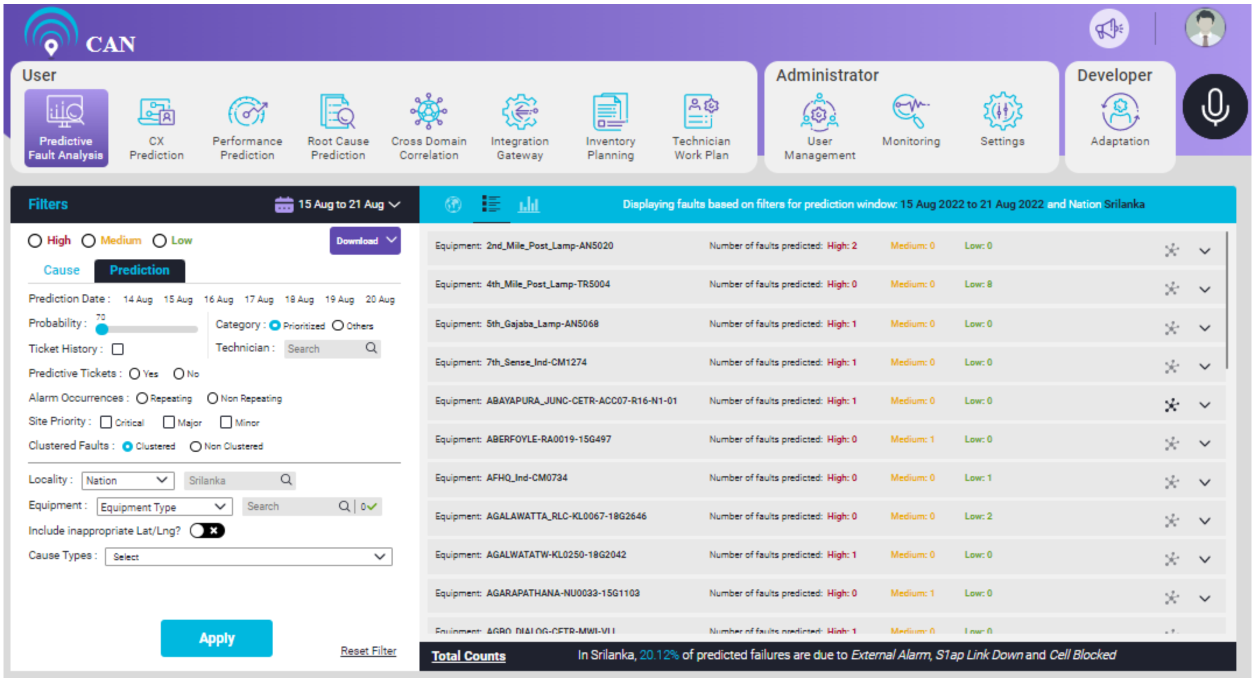
Total Counts In Srilanka, 21.51% of predicted failures are due to *External Alarm*

Figure 16.4 - 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”.



Filters 15 Aug to 21 Aug

○ High ○ Medium ○ Low

Cause | Prediction

Prediction Date : 14 Aug 15 Aug 16 Aug 17 Aug 18 Aug 19 Aug 20 Aug

Probability : 70 | Category : ● Prioritized ○ Others

Ticket History : □ | Technician : Search

Predictive Tickets : ○ Yes ○ No

Alarm Occurrences : ○ Repeating ○ Non Repeating

Site Priority : □ Critical □ Major □ Minor

Clustered Faults : ● Clustered ○ Non Clustered

Locality : Nation | Srilanka

Equipment : Equipment Type | Search | 0✓

Include inappropriate Lat/Lng? ☒

Cause Types : Select

Displaying faults based on filters for prediction window: 15 Aug 2022 to 21 Aug 2022 and Nation Srilanka

Equipment: 2nd_Mile_Post_Lamp-AN5020	Number of faults predicted: High: 2	Medium: 0	Low: 0
Equipment: 4th_Mile_Post_Lamp-TR5004	Number of faults predicted: High: 0	Medium: 0	Low: 8
Equipment: 5th_Gajaba_Lamp-AN5068	Number of faults predicted: High: 1	Medium: 0	Low: 0
Equipment: 7th_Sense_Ind-CM1274	Number of faults predicted: High: 1	Medium: 0	Low: 0
Equipment: ABAYAPURA_JUNC-CETR-ACC07-R16-N1-01	Number of faults predicted: High: 1	Medium: 0	Low: 0
Equipment: ABERFOYLE-RA0019-15G497	Number of faults predicted: High: 0	Medium: 1	Low: 0
Equipment: AFHQ_Ind-CM0734	Number of faults predicted: High: 0	Medium: 0	Low: 1
Equipment: AGALAWATTA_RLC-KL0067-18G2646	Number of faults predicted: High: 0	Medium: 0	Low: 2
Equipment: AGALWATATW-KL0250-18G2042	Number of faults predicted: High: 1	Medium: 0	Low: 0
Equipment: AGARAPATHANA-NU0033-15G1103	Number of faults predicted: High: 0	Medium: 1	Low: 0
Equipment: AGRO_DIALOG-CETR-MWI-VLI	Number of faults predicted: High: 1	Medium: 0	Low: 0

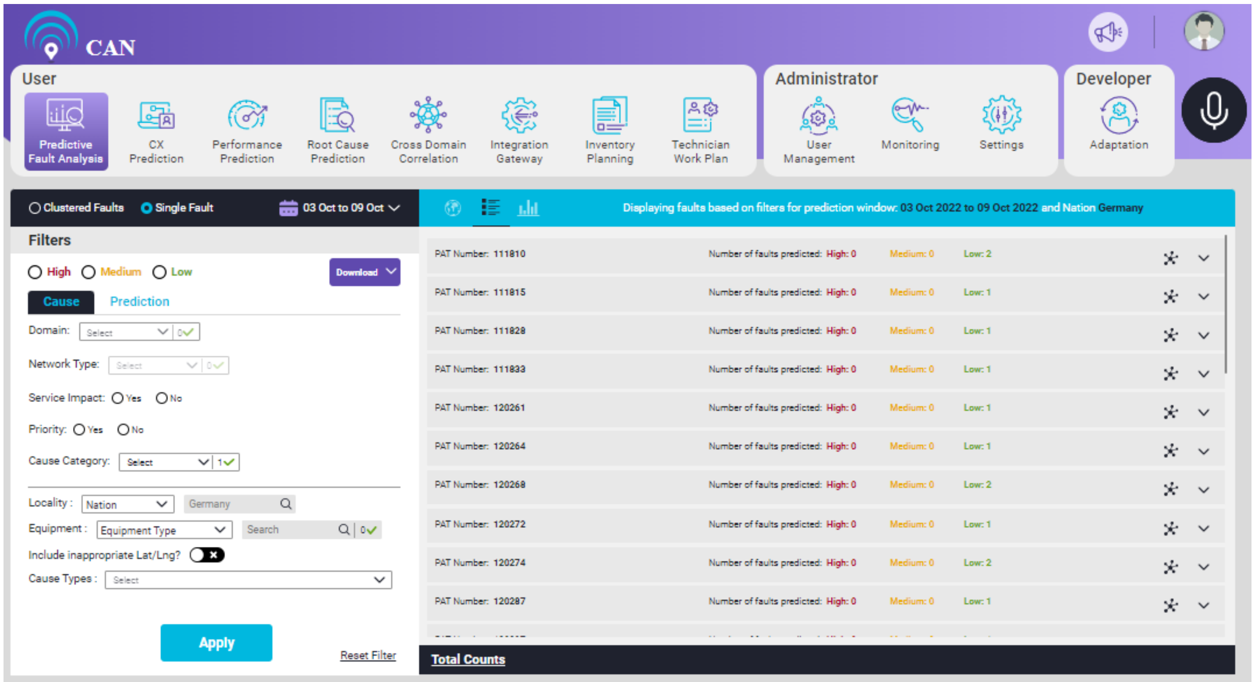
Total Counts In Srilanka, 20.12% of predicted failures are due to *External Alarm, S1ap Link Down* and *Cell Blocked*

Figure 16.5 - 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".



○ Clustered Faults ● Single Fault 03 Oct to 09 Oct

Filters

○ High ○ Medium ○ Low

Cause | Prediction

Domain: Select | 0✓

Network Type: Select | 0✓

Service Impact: ○ Yes ○ No

Priority: ○ Yes ○ No

Cause Category: Select | 1✓

Locality : Nation | Germany

Equipment : Equipment Type | Search | 0✓

Include inappropriate Lat/Lng? ☒

Cause Types : Select

Displaying faults based on filters for prediction window: 03 Oct 2022 to 09 Oct 2022 and Nation Germany

PAT Number: 111810	Number of faults predicted: High: 0	Medium: 0	Low: 2
PAT Number: 111815	Number of faults predicted: High: 0	Medium: 0	Low: 1
PAT Number: 111828	Number of faults predicted: High: 0	Medium: 0	Low: 1
PAT Number: 111833	Number of faults predicted: High: 0	Medium: 0	Low: 1
PAT Number: 120261	Number of faults predicted: High: 0	Medium: 0	Low: 1
PAT Number: 120264	Number of faults predicted: High: 0	Medium: 0	Low: 1
PAT Number: 120268	Number of faults predicted: High: 0	Medium: 0	Low: 2
PAT Number: 120272	Number of faults predicted: High: 0	Medium: 0	Low: 1
PAT Number: 120274	Number of faults predicted: High: 0	Medium: 0	Low: 2
PAT Number: 120287	Number of faults predicted: High: 0	Medium: 0	Low: 1

Total Counts

Figure 16.6 - 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:

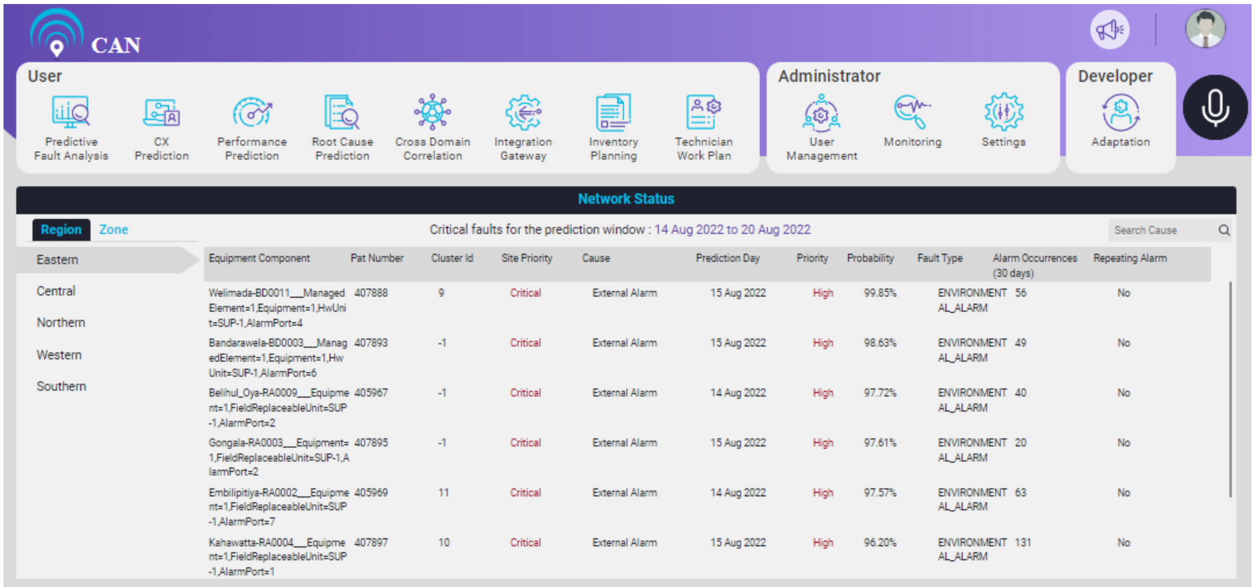
- Equipment Component
- Pat-Number
- Cluster Id
- Site Priority
- Cause
- Prediction Day
- Priority
- Probability
- Fault Type,
- Alarm Occurrences
- Repeating Alarms

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).



Network Status

Eastern
Central
Northern
Western
Southern

Critical faults for the prediction window : 14 Aug 2022 to 20 Aug 2022

Equipment Component	Pat Number	Cluster Id	Site Priority	Cause	Prediction Day	Priority	Probability	Fault Type	Alarm Occurrences (30 days)	Repeating Alarm
Welimada-BD0011__Managed Element=1,Equipment=1,HwUnit=SUP-1,AlarmPort=4	407888	9	Critical	External Alarm	15 Aug 2022	High	99.85%	ENVIRONMENTAL_ALARM	56	No
Bandarawela-BD0003__ManagedElement=1,Equipment=1,HwUnit=SUP-1,AlarmPort=6	407893	-1	Critical	External Alarm	15 Aug 2022	High	98.63%	ENVIRONMENTAL_ALARM	49	No
Belihul_Oya-RA0009__Equipment=1,FieldReplaceableUnit=SUP-1,AlarmPort=2	405967	-1	Critical	External Alarm	14 Aug 2022	High	97.72%	ENVIRONMENTAL_ALARM	40	No
Gongala-RA0003__Equipment=1,FieldReplaceableUnit=SUP-1,AlarmPort=2	407895	-1	Critical	External Alarm	15 Aug 2022	High	97.61%	ENVIRONMENTAL_ALARM	20	No
Embilipitiya-RA0002__Equipment=1,FieldReplaceableUnit=SUP-1,AlarmPort=7	405969	11	Critical	External Alarm	14 Aug 2022	High	97.57%	ENVIRONMENTAL_ALARM	63	No
Kahawatta-RA0004__Equipment=1,FieldReplaceableUnit=SUP-1,AlarmPort=1	407897	10	Critical	External Alarm	15 Aug 2022	High	96.20%	ENVIRONMENTAL_ALARM	131	No

Figure 16.7 - Network Status