HCLSoftware

HCL IntelliOps
Event Management

Configuration Guide

Version 1.0

Contents

1 Preface 25

1.1 Intended Audience 25

1.2 About this Guide 25

1.3 Related Documents 25

1.4 Conventions 25

2 Introduction 27

2.1 Overview of IEM 27

2.2 Key Features 27

3 Getting Started 28

4 IEM Collector 29

4.1 Overview for NiFi 29

4.1.1 NiFi Architecture 29

4.2 Prerequisites 30

4.2.1 System Requirements For NiFi 30

4.2.2 Supported OS for NIFI 30

4.2.3 Supported Web Browsers 31

4.2.4 Hardware Sizing Recommendation 31

4.2.5 Port Requirement for NiFi 32

4.3 Overview of IMM 32

4.4 Prerequisite for IMM 32

4.4.1 Supported OS for IMM 32

4.4.2 Supported Web Browsers 32

4.4.3 Hardware Sizing Recommendation 32

4.4.4 Port Requirement for IMM 32

5 IMM Interface 34

6 IEM Configuration 35

6.1 Customer Creation 35

6.1.1 Add New Customer 36

6.1.2 Onboarding Steps View 38

6.1.3 Enable/Disable State 39
6.1.4 View Customer 40
6.1.5 Edit Customer 41
6.1.6 Delete Customer 42
6.1.7 Download Published API 43
6.1.8 Download Installer 43
6.1.9 Download License 43
6.1.10 Renew License 44
6.1.11 Manage Onboarded Customer 45
7 IEM Interface 190
7.1 Login to HCL IEM 190
7.1.1 Metric View 191
7.1.2 Service View 191
7.1.3 Topology View 192
7.2 Data View 192
7.2.1 Events 193
7.2.2 Alerts 200
7.2.3 Actionable 211
7.2.4 All Events View 235
7.2.5 Noise Events View 239
8 Integration 243
8.1 Out Of Box NiFi Connectors Integrations 243
8.1.1 iEM Accumulator (iEA) 243
8.1.2 AppDynamics - Entity 244
8.1.3 AppDynamics – Event 245
8.1.4 AppDynamics - Metrics 246
8.1.5 Datadog – Event 247
8.1.6 Dynatrace – Event 248
8.1.7 Generic Rest – Event 249
8.1.8 LogicMonitor – Event 250

8.1.9 New Relic – Event 251
8.1.10 NiFi-iEM HeartBeat 252
8.1.11 ServiceNow – Service 252
8.1.12 SolarWinds Hybrid Cloud Observability – Event 253
8.1.13 SolarWinds Hybrid Cloud Observability – Metrics 254
8.1.14 Zabbix – Event 255
8.1.15 vRealize Operations (vROps) - Event 256
9 Glossary of Terms 257
9.1 Key Terminology Used in IEM 257

Table of Figures

Figure 1 – IEM Onboarding Flow 28

Figure 2 - Content and Provenance repository 29

Figure 3 - Repositories 30

Figure 4 - Customer Page 35

Figure 5 - Navigation for Create New Customer 36

Figure 6 - Customer Creation 36

Figure 7 - Customer details 37

Figure 8 - Customer Creation Process 37

Figure 9 - Customer Creation Onboarding Steps 37

Figure 10 - Customer Creation Onboarding Steps (Cont.) 38

Figure 11 - Customer Page 38

Figure 12 - Onboarding Steps View 38

Figure 13 - Customer Creation Onboarding Steps 39

Figure 14 - Customer Creation Onboarding Steps (Cont.) 39

Figure 15 - Customer Creation Onboarding Steps (Cont.) 39

Figure 16 – Enable/Disable Customer 40

Figure 17 – Customer Page 40

Figure 18 - Customer Details 41

Figure 19 - Edit Customer 41

Figure 20 - Customer Edit Screen 42

Figure 21 – Customer Details 42

Figure 22 - Delete Customer 42

Figure 23 - Confirmation pop-up 43

Figure 24 - Download Publish API 43

Figure 25 - Download Installer 43

Figure 26 - Download License 44

Figure 27 - Renew License 44

Figure 28 - Status of Customer 44

Figure 29 - Customer Creation Onboarding Steps 45

Figure 30 - Customer Creation Onboarding Steps (Cont.) 45
Figure 31 – Customer Details 46
Figure 32 - SSO Configuration Page 46
Figure 33 – New Role 48
Figure 34 - Role Creation 48
Figure 35 - Navigation Page for Assigning an Action to a Role 49
Figure 36- Assigning Actions for a Role 49
Figure 37 - Alert Message 50
Figure 38 - Role Page 50
Figure 39 – Edit Roles 51
Figure 40 - Edit a Role Description 51
Figure 41 - Selecting Actions for a Role 52
Figure 42- Selecting Actions for a Role 52
Figure 43 - Alert Message 53
Figure 44 - Delete Role 53
Figure 45 - Confirmation pop-up 53
Figure 46 - Alert Message 54
Figure 47 – Updated Grid 54
Figure 48 - View Role 54
Figure 49 - Viewed Role 55
Figure 50 - Assign User 55
Figure 51 - Assign user Email ID 56
Figure 52 - User Email ID 56
Figure 53 - Alert Message 56
Figure 54 - Apply Filter Operation 57
Figure 55 - Apply Filter Operation 57
Figure 56 - Apply Filter Result 57
Figure 57 - Navigation for Add New User 58
Figure 58 - Create a User 58
Figure 59 - User Email Id 59

Figure 60 - Username 59
Figure 61- Alert Message 60
Figure 62 - Generate Password for User 60
Figure 63 - Copy Password 60
Figure 64 - Alert Message 61
Figure 65- User Page 62
Figure 66 - Edit User 62
Figure 67 - Edit Details 63
Figure 68 – Update button 63
Figure 69 - Alert Message 64
Figure 70 - Delete User 64
Figure 71 - Delete User 65
Figure 72 - Confirmation pop-up 65
Figure 73 - Alert Message 65
Figure 74 - Assign Group to a user 65
Figure 75 - Group Dropdown 66
Figure 76 - Selecting the Group for the Dropdown 66
Figure 77 - Alert Message 66
Figure 78 - Assign role 67
Figure 79 - Role Dropdown 67
Figure 80 - Selecting User Role Dropdown to a User 67
Figure 81 - Alert Message 68
Figure 82 - Enable /Disable User 68
Figure 83 – Confirmation of User Disabled 68
Figure 84 - Confirmation of User Enabled 68
Figure 85 - Apply Filter Operation 69
Figure 86 - Applying Filter Operations 69
Figure 87 - Apply Filter Result 69
Figure 88 - Group Page 70
Figure 89 - Navigation Page for Group 70

Figure 90 - Create a Group 71
Figure 91 – Add Filter 71
Figure 92 - Filter for Group 72
Figure 93 - Dropdown for fields 72
Figure 94- Dropdown for Operator 73
Figure 95 - Add Base Filters 73
Figure 96 - Alert Message 73
Figure 97 - Alert Message 74
Figure 98 - Alert Message 74
Figure 99 - Add New Group 74
Figure 100 - Copy Event Filter 75
Figure 101 - Copy Expression 75
Figure 102 - Selecting Copy Expression 75
Figure 103 - Alert message 75
Figure 104 - Alerts Filter 76
Figure 105 - Alert Message 76
Figure 106 - Edit Group 76
Figure 107 - Edit Filter 77
Figure 108 - Update Group Name and Filter 77
Figure 109 - Alert Message 77
Figure 110 – Delete Group 78
Figure 111 - Confirmation pop-up 78
Figure 112 – Alert Message 78
Figure 113 - Assign Users in a Group 79
Figure 114 - Assign User Pop-up 79
Figure 115 - Assign User Email ID 79
Figure 116 - Confirmation Pop-up Message 80
Figure 117 - Apply Filter Operation 80
Figure 118 - Apply Filter Operation 81
Figure 119 - Apply Filter Result 81

Figure 120 - Entity Page 82
Figure 121 - Navigation for Create an Entity 82
Figure 122 - Bulk Upload Entities 83
Figure 123 - Add Entity Name 83
Figure 124 - Dropdown List for Column 84
Figure 125 - Selected Column 84
Figure 126 - Selecting Multiple Columns 85
Figure 127 - Add New Column 85
Figure 128 - Multiple Enter Value for Entity 86
Figure 129 - Alert Message 86
Figure 130 - Grid View for Entity 86
Figure 131 - Bulk Upload Entities 87
Figure 132 - Bulk Upload Entities 87
Figure 133 - Template Format of Bulk Entity 87
Figure 134 - Template Format of Bulk Entity 88
Figure 135 - Template with Entity data. 88
Figure 136 - Selecting file from local Directory 88
Figure 137 - Upload csv file 88
Figure 138 – Submit Button 89
Figure 139 - Edit Entity 89
Figure 140 - Edit Details 90
Figure 141 - Alert Message 90
Figure 142 - Grid View for Entity 90
Figure 143 - Figure – Entity Page 91
Figure 144 - Delete Entities 91
Figure 145 - Delete Entities 91
Figure 146 - Confirmation pop-up 92
Figure 147 - Alert Message 92
Figure 148 – Entity Removed from the Data Grid 92
Figure 149 - Select Entities for Operation 93

Figure 150 - Merge Entities 93
Figure 151 - Merge Rows 93
Figure 152 - Alert Message 94
Figure 153 – Cancel Button 94
Figure 154 - Selected Entity Perform Operations 95
Figure 155 - Selected Entity Mark as Noise 95
Figure 156 - Success Popup for Mark as Noise 95
Figure 157 - Alert Message 96
Figure 158 - Selected Entities as Maintenance Window 96
Figure 159 - Maintenance Window Configuration 97
Figure 160 - Date selection for Noise Rule 97
Figure 161 - Time Interval for Noise Rule 98
Figure 162 - Recurring for Noise Rule 98
Figure 163 - Maintenance Window Configuration for Noise 99
Figure 164 - Day Selection for Noise 99
Figure 165 - Maintenance Window 100
Figure 166 - On Day Selection for Recurring 100
Figure 167 - On day and Time Interval 101
Figure 168 - Alert Message 101
Figure 169 - Apply Filter Operation 102
Figure 170 - Apply Filter Operation 102
Figure 171 - Apply Filter Result 102
Figure 172 - Topology Page 103
Figure 173 - Add Topology 104
Figure 174 - Bulk Upload Topologies 104
Figure 175 - Topology Creation 104
Figure 176 - Parent Entity Selection 105
Figure 177 - Alert Message 105
Figure 178 - Grid View for Topology 105
Figure 179 - Bulk Upload CSV 106

Figure 180 - Template Format of Bulk Topology 106
Figure 181 - CSV File of Parent and child entities 106
Figure 182 - Uploading the Topologies 106
Figure 183 – Success popup 107
Figure 184 - Delete Topology 107
Figure 185 - Bulk Delete Topology 108
Figure 186 - Confirmation pop-up 108
Figure 187 - Alert Message 108
Figure 188 - Service Hierarchy Page 109
Figure 189 - Service Creation 109
Figure 190 - Service Add Configuration 110
Figure 191 - Selecting Dropdown 110
Figure 192 - Alert Message 111
Figure 193 - Grid View for Service Hierarchy 111
Figure 194 - Edit Service 111
Figure 195 - Editing Service 112
Figure 196 - Alert Message 112
Figure 197 - Selecting Services 112
Figure 198 - Deleting Services 113
Figure 199 - Confirmation pop-up 113
Figure 200 - Alert Message 113
Figure 201 - Mapping Service 114
Figure 202 - Define Topology 114
Figure 203 - Applying Parent Service 115
Figure 204 - Alert Message 115
Figure 205 - Parent Service Name 116
Figure 206 - Parent List Services 116
Figure 207 - Alert Message 117
Figure 208 - Map Entities 117
Figure 209 - Selected Entities for Service 118

Figure 210 - Alert Message 118
Figure 211 - Apply Filter Operation 119
Figure 212 - Apply Filter Operation 119
Figure 213 - Apply Filter Result 119
Figure 214 - Noise Maintenance Page 120
Figure 215 - New Noise Rule Creation 121
Figure 216 - Add Base Filters 121
Figure 217 - Base Filters Menu 122
Figure 218 - Selection of The Field 122
Figure 219 - Selection of The Operator 123
Figure 220 - Rule Name for Noise 123
Figure 221 - Define Maintenance for Noise Rule 124
Figure 222 - Define Maintenance for Noise Rule 124
Figure 223 - Alert Message 125
Figure 224 - Define Maintenance for Noise 125
Figure 225 - Edit Option for Noise Rule 126
Figure 226 - Editing Noise Rule 126
Figure 227 – Success popup. 127
Figure 228 - Selected Noise Rules 127
Figure 229 - Confirmation pop-up 127
Figure 230 - Alert Message 128
Figure 231 - Apply Filter Operation 128
Figure 232 - Apply Filter Operation 129
Figure 233 - Apply Filter Result 129
Figure 234 - Correlation View 131
Figure 235 - Creating New Correlation Rule 131
Figure 236 - Correlation Page 132
Figure 237 - Create New Name 132
Figure 238 - Definition Section 133
Figure 239 - Topology Filter 133

Figure 240 - Selecting Topology Level Types 133
Figure 241 - Selecting Sliding and Tumbling 134
Figure 242 - Include Alert If 134
Figure 243 - Selecting All Fields 135
Figure 244 - Exclude Alert If 135
Figure 245 - Group By 135
Figure 246 - Selecting Group By 136
Figure 247 - Process For 136
Figure 248 – Trigger 136
Figure 249 - Mark as Casual 137
Figure 250 - Click on +Criteria 137
Figure 251 - Delete of Extra Criteria 138
Figure 252 - Set Using Expression 138
Figure 253 - Specific Actionable Details 139
Figure 254 - Actionable Title 139
Figure 255 - Actionable Title Drop-down 139
Figure 256 - Actionable Description 140
Figure 257 - Actionable Entity 140
Figure 258 - Enter all Fields 141
Figure 259 - 141
Figure 260 - Actionable Severity 142
Figure 261 – Exit if 142
Figure 262 - Exit If 143
Figure 263 - Exit If Condition 143
Figure 264 - Process For 143
Figure 265 - Entity Fields 144
Figure 266 - Select Condition 144
Figure 267 - Delete Condition 145
Figure 268 - Action 145
Figure 269 - Click on +Action Rule 145

Figure 270 - Action Rules 146
Figure 271 - Delete Action Rule 146
Figure 272 - Click on +AND 147
Figure 273 - Selecting the Rule 147
Figure 274 – Count 148
Figure 275 - Change Severity 148
Figure 276 - Click on +AND 148
Figure 277 - Change State 149
Figure 278 - Select the Fields 149
Figure 279 - For Change State Select 149
Figure 280 - Change Title 150
Figure 281 - Creation of ticket 150
Figure 282 - Actions Rules 151
Figure 283 - Click on Submit 151
Figure 284 - Grid View for Correlation Rules 152
Figure 285 - Edit Correlation Rule 152
Figure 286 - Edit Correlation Rule (Cont.) 152
Figure 287 - Updated Correlation Rules 153
Figure 288 - Alert Message 153
Figure 289 - Delete Correlation 154
Figure 290 - Confirmation pop-up 154
Figure 291 - Alert Message 154
Figure 292 - Change the Priority 155
Figure 293 - Select the Change Priority Dropdown 155
Figure 294 - Select the Change Priority Dropdown 155
Figure 295 - Alert Message 156
Figure 296 - Clone Action 156
Figure 297 - Clone Connection Integration 156
Figure 298 - Alert Message 157
Figure 299 - Enable /Disable Correlation Rules 157

Figure 300 - Alert Message 158
Figure 301 - Success Pop-up for Enable 158
Figure 302 - Apply Filter Operation 159
Figure 303 - Apply Filter Operation 159
Figure 304 - Apply Filter Result 159
Figure 305 - Integration Page 160
Figure 306 - Creating New Integration 161
Figure 307 - Create an Integration 161
Figure 308 - Create an Integration 162
Figure 309 - Existing Connection 162
Figure 310 - Existing Connection 163
Figure 311 - Navigation Bar for Create a New Connection 163
Figure 312 - Creating New Name for Connection 163
Figure 313 - Advance Options 164
Figure 314 - Alert Message 164
Figure 315 - Alert Message 165
Figure 316 - Existing Connection 165
Figure 317 - Create New Connection 165
Figure 318 - Create New Connection 166
Figure 319 - Definition Section 166
Figure 320 - Definition Section 167
Figure 321 - Method Type 167
Figure 322 - Table Name 167
Figure 323 - Extract Keys 168
Figure 324 - Request Body 168
Figure 325 - Extract Keys 168
Figure 326 - Response 169
Figure 327 - Define Payload Json 169
Figure 328 - Extract Payload Json 169
Figure 329 - Map Columns 170

Figure 330 - Map Columns 170
Figure 331 - Mapping State Column 170
Figure 332 - Alert Message 171
Figure 333 - Alert Message 171
Figure 334 - Clone Action 172
Figure 335 - Clone Connection Integration 172
Figure 336 - Alert Message 172
Figure 337- Edit Action 173
Figure 338 - Edit General Section 173
Figure 339 - Alert Message 174
Figure 340 - View Integration 174
Figure 341 - View Integration 174
Figure 342 - Delete Integration 175
Figure 343 - Confirmation pop-up 175
Figure 344 - Alert Message 175
Figure 345 - Apply Filter Operation 176
Figure 346 - Apply Filter Operation 176
Figure 347 - Apply Filter Result 177
Figure 348 - Algorithms Available objectives 178
Figure 349 - Selecting Dataset type for Available Objectives 178
Figure 350 - Algorithms available objectives 179
Figure 351 - Bulk Upload Al Algorithm Objectives 179
Figure 352 - Template for Bulk Al Algorithm Objectives 180
Figure 353 - Upload csv from Local Directory 180
Figure 354 - Evaluate 181
Figure 355 - Evaluate All 181
Figure 356 - Evaluate Objectives Dropdown 182
Figure 357 - Alert Message 182
Figure 358 - Evaluate Objective job on Processing Screen 182
Figure 359 - Select Dataset Type for Evaluated Objectives 183

Figure 360 - Evaluated Objectives 184
Figure 361 - Enable / Disable Evaluated Objectives 184
Figure 362 - Alert Message 185
Figure 363 - Enable Feedback in Evaluated Objectives 185
Figure 364 - Enable Feedback Dropdown 186
Figure 365 - View More action for Evaluated Objectives 186
Figure 366 - View More 187
Figure 367 - Select Dataset Type for Training Instances 187
Figure 368 - Training Instances 188
Figure 369 - Refresh Objectives 188
Figure 370 - Alert Message 189
Figure 371 - Cost Configuration 189
Figure 372 - HCLIEM Login Page 190
Figure 373 – Login Authentication 190
Figure 374 - FIGURE – Home Page Dashboard 191
Figure 375 – Metric View 191
Figure 376 – Service View 192
Figure 377 - Topology View 192
Figure 378 - View Events 193
Figure 379 - Add Column 194
Figure 380 - Add Column 194
Figure 381 - Save View 195
Figure 382 - Save View Events 195
Figure 383 - Popup confirmation 195
Figure 384 - Save As Events 196
Figure 385 – Save as Events 196
Figure 386 - Alert Message 196
Figure 387 – Select Events View Dropdown 197
Figure 388 – Live Events Data 197
Figure 389 – Live Events Data Disabled 198

Figure 390 – Refresh View Data Events 199
Figure 391 – Alert Message 199
Figure 392 - More Filter Operation 200
Figure 393- More Filter Operation 200
Figure 394– Alerts View 201
Figure 395– Deleting Bulk Alerts 201
Figure 396- Confirmation pop-up 202
Figure 397– Alert Message 202
Figure 398- Save Alerts 203
Figure 399- Save Alerts 203
Figure 400- Alert Message 203
Figure 401– Save As Alerts 204
Figure 402– Save As Alerts 204
Figure 403– Alert Message 205
Figure 404– Select Alerts View Dropdown 205
Figure 405– Add Column 205
Figure 406– Add Column 206
Figure 407 - Alerts Related Events 206
Figure 408- Mark as Incorrect 207
Figure 409– Alert Message 207
Figure 410 – Live Alerts Data 208
Figure 411 – Live Alerts Data Disabled 208
Figure 412- Refresh Data View Alerts 209
Figure 413 - Refresh Data View Alerts 209
Figure 414 - More Filter Operation 210
Figure 415 - More Filter Operation 210
Figure 416 - More Filter Operation 210
Figure 417 - Actionable View 211
Figure 418 – Deleting Bulk Actionable 212
Figure 419 - Confirmation Pop- up 212

Figure 420 - Alert Message 212
Figure 421 – Add Column 213
Figure 422 – Add Column 213
Figure 423 - Related Changes or Related Problems 214
Figure 424 – Related Problems & Related Changes 214
Figure 425 - Invite user 215
Figure 426 - Select Users 215
Figure 427 - Confirmation popup 216
Figure 428 – Chat Bot 216
Figure 429 – Add Comments to Actionable 217
Figure 430 – Add Comments to Actionable 217
Figure 431 – Activities 218
Figure 432 – Similar Actionable 218
Figure 433 – Service Hierarchy 219
Figure 434 – Timelines 220
Figure 435 – To Change Severity of Actionable 220
Figure 436 – Confirmation Pop- up 221
Figure 437 – Alert Message 221
Figure 438 – To Change Status for Actionable 222
Figure 439 – Confirmation Pop- up 222
Figure 440 – Alert Message 223
Figure 441 – Assign Actionable to Another User 223
Figure 442 – Alert Message 224
Figure 443 – Save Actionable 224
Figure 444 – Save Actionable 225
Figure 445 – Alert Message 225
Figure 446 – Save As Actionable 226
Figure 447 – Save As Actionable 226
Figure 448 – Alert Message 226
Figure 449 – Live Actionable Data 227

Figure 450 – Live Actionable Data Disabled 227
Figure 451 – Refresh time for Actionable 228
Figure 452 – Refresh time for Actionable 228
Figure 453 – Actionable Related Alerts 229
Figure 454 – Topology 229
Figure 455 – Update Ticket for Actionable 230
Figure 456 – Update Ticket for Actionable 230
Figure 457 – Success Message for Update Ticket 231
Figure 458 – Update Work Notes for Actionable 231
Figure 459 – Update Work Notes for Actionable 232
Figure 460 – Alert Message 232
Figure 461 - More Filter Operation 233
Figure 462 - More Filter Operation 233
Figure 463 - More Filter Operation 233
Figure 464– Select State Operation 234
Figure 465 – Update Work Notes for Actionable 234
Figure 466 – Update Work Notes for Actionable 235
Figure 467 – Alert Message 235
Figure 468 – All Events View 236
Figure 469 – Add Column 236
Figure 470 – Save as Events 237
Figure 471 – Refresh All Events 237
Figure 472 - Filter Operation 238
Figure 473 - Filter Operation 238
Figure 474 - Filter Operation 239
Figure 475 - Noise Events View 239
Figure 476 - Add Column 240
Figure 477 - Save as Events 240
Figure 478 - Refresh Noise Events 241
Figure 479 - Live Events Data 241

Figure 480 - Filter Operation 242
Figure 481 – iEM Accumulator (iEA) 243
Figure 482 – AppDynamics - Entity 244
Figure 483 – AppDynamics - Event 245
Figure 484 – AppDynamics - Metrics 246
Figure 485 – Datadog - Event 247
Figure 486 – Dynatrace - Event 248
Figure 487 – Generic Rest - Event 249
Figure 488 –LogicMonitor – Event 250
Figure 489 – New Relic - Event 251
Figure 490 – NiFi-iEM HeartBeat 252
Figure 491 – ServiceNow - Service 252
Figure 492 – SolarWinds Hybrid Cloud Observability - Event 253
Figure 493 –SolarWinds Hybrid Cloud Observability - Metrics 254
Figure 494 – Zabbix - Event 255
Figure 495 – vRealize Operations (vROps) - Event 256

List of Tables

Table 1 - Conventions 25

Table 2 – Predefined System Roles 47

Table 3 – Include Alert If Filter Fields 134

Table 4 - iEM Accumulator (iEA) - Integrations Fields 243

Table 5 - AppDynamics - Entity - Integrations Fields 244

Table 6 - AppDynamics - Event - Integrations Fields 245

Table 7 - AppDynamics – Metrics - Integrations Fields 246

Table 8 – Datadog – Event - Integrations Fields 247

Table 9 – Dynatrace – Event - Integrations Fields 248

Table 10 – Generic Rest - Event - Integrations Fields 249

Table 11 –LogicMonitor – Event - Integrations Fields 250

Table 12 – New Relic – Event - Integrations Fields 251

Table 13 NiFi-iEM HeartBeat - Integrations Fields 252

Table 14 – ServiceNow – Service - Integrations Fields 252

Table 15 – SolarWinds Hybrid Cloud Observability – Event - Integrations Fields 253

Table 16 –SolarWinds Hybrid Cloud Observability – Metrics - Integrations Fields 254

Table 17 – Zabbix – Event - Integrations Fields 255

Table 18 – vRealize Operations (vROps) – Event - Integrations Fields 256

Table 19 – Key Terminology Used in IEM 257

Document Revision History

This guide is updated with each release of the product or when necessary.

This table provides the revision history of this Configuration Guide.

Version Date	Description
January, 2024	HCL IEM Configuration Guide V_1.0

1 Preface

This section provides information about the HCL IntelliOps Event Management (IEM) Configuration Guide and includes the following topics:

- Intended Audience
- About This Guide
- Related Documents
- Conventions

1.1 Intended Audiences

This guide is intended for users for IEM configuration working towards resolution tickets generated by correlating similar alerts to create correct actionable.

It's good to have basic knowledge of Java, Data ingestion, transformation, and ETL to work with Apache NiFi.

1.2 About this Guide

This guide introduces us to the key concepts of HCL IEM and describes how to use the product. It provides an overview of configurations and instructions to perform different tasks.

This document includes the following topics:

- Introduction
- Getting Started
- IEM Collector
- IMM Interface
- IEM Configuration
- IEM Interface
- Integration
- Glossary of Terms

1.3 Related Documents

The following documents can be referred in addition to this guide for further information on the IEM platform:

- Introduction to HCL IEM Guide

1.4 Conventions

The following typographic conventions are used in this document:

Table 1 - Conventions

Convention	Element
Boldface	Indicates graphical user interface elements associated with an action, or terms defined in text or the glossary
Underlined blue face	Indicates cross-reference and links
Numbered lists	Indicates steps in a procedure to be followed in a sequence

Bulleted lists	Indicates a list of items that is not necessarily meant to be followed in a sequence

2 Introduction

2.1 Overview of IEM

HCL IntelliOps Event Management is an AI-powered IT event management platform on the cloud that transforms IT operations by incorporating AIOps capabilities into the system. Its machine learning-based advanced features, such as topology correlation, anomaly detection, and noise reduction, not only help reduce Mean Time to Detect (MTTD) and Mean Time to Recover (MTTR) of incidents but also proactively detect potential issues, prevent outages, and ensure service continuity for businesses.

This intelligent platform provides integrations with various monitoring tools and custom code within an ecosystem to ingest a vast volume of heterogeneous data in the form of events, metrics, performance, and configuration information. Its client-side component – IEM-(IMM) Integration Management Module collects raw events from various monitoring systems and send it to IEM, it also offers a unique feature of continuous service delivery in the case of connectivity loss with IEM Cloud, minimizing the impact of outages on IT operations.

IEM also fosters efficient collaboration across teams, ultimately improving system performance and agility. Its integration with ITSM tools packages industry best practices, significantly reducing duplicate incidents and enhancing the Root Cause Analysis process by automatically correlating incidents with Change Management.

2.2 Key Features

- **Early Anomaly Detection**: Utilizes metrics for early identification of true anomalies in the lifecycle. Metric anomaly system is available to identify anomalous metric point for outlier detection based on metric data being ingested.
- **Topology Based Alert Correlation**: OOB correlation rules available for Correlation of alerts based on relationships between entities defined in the system.
- **Temporal-Based Alert Correlation**: Leverages a robust correlation engine and condition-based correlation for automatic grouping and mapping of alerts with and efficient Feedback System to avoid irrelevant alert to actionable grouping.
- **OOB NiFi Connector Management via IMM (Integration Management Module) Portal**: Topology, Entity and Service data ingestion via NiFi in real-time.
- **Automated Noise Reduction**: Filters out irrelevant data to reduce noise and focus on meaningful events. There is Noise Rule Configuration with maintenance windows support.
- **Related Problems and Changes view of Actionable for Effective Diagnosis**: Helps in addressing impact assessment for continuous improvement and prioritize actionable based on their potential impact.
- **Real-Time Interactive Visualization**: Provides user-friendly dashboards for real-time interaction with Metric View, Service View, and Topology View. Timeline view is also available for events, alerts, and actionable.
- **Quick User's Collaboration**: Enables quick chat and collaboration with the team for efficient communication thereby reducing MTTR along with automated notifications to operators for assigned actionable.
- **Cost Saving View**: Significantly benefits by optimizing resources, improving operational efficiency, and reducing unnecessary expenditures on actionable resolution and reviving the degraded services.

3 Getting Started

The Following flow diagram displays the onboarding process of IEM:

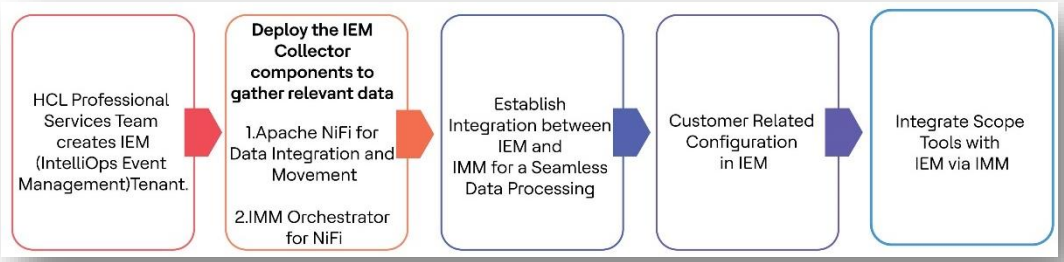

Figure 1 – IEM Onboarding Flow

4 IEM Collector

IEM Collector refers to effectively gathering data from diverse sources, providing a wide range of single click, custom integrations compliant with the industry standards for connectors and APIs. The events, data and performance connectors are developed in **Apache NiFi**. These **OOB NiFi** connectors can be leveraged for data ingestion very quickly via **IMM (Integration Management Module)** Portal.

4.1 Overview for NiFi

Apache NiFi is an **open-source** dataflow system based on the concepts of flow-based programming. It supports powerful and scalable directed graphs of data routing, transformation, and system mediation logic.

4.1.1 NiFi Architecture

Apache NiFi has a processor, flow controller, and web server that executes on the JVM machine. Additionally, it also includes three repositories, as shown in the figure, which are FlowFile repository, Content and Provenance repository.

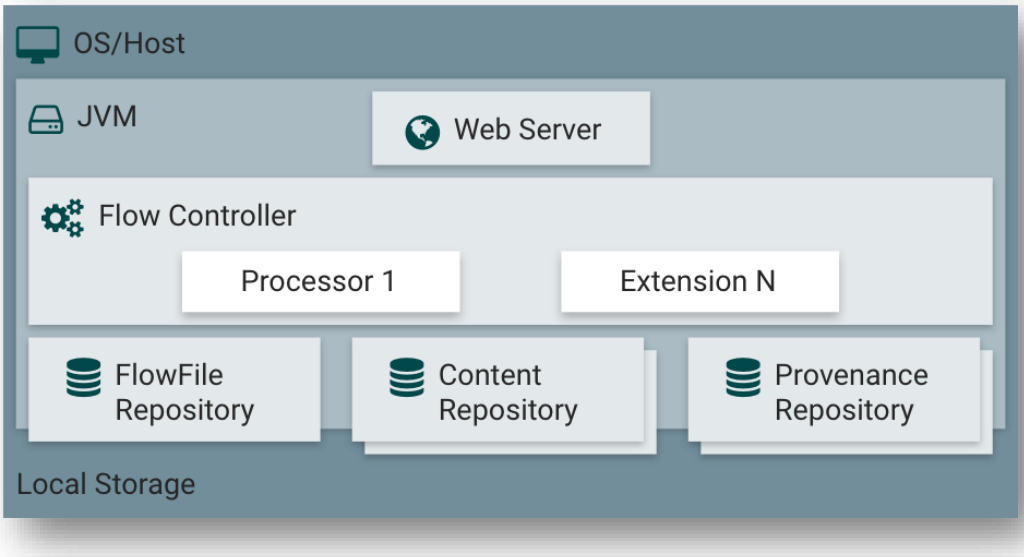

Figure 2 - Content and Provenance repository

NiFi executes within a JVM on a host operating system. The primary components of NiFi on the JVM are as follows:

Web Server: The purpose of the web server is to host NiFi's HTTP-based command and control API.

Flow Controller: The flow controller is the brains of the operation. It provides threads for extensions to run on and manages the schedule of when extensions receive resources to execute.

Extensions: There are various types of NiFi extensions which are described in other documents. The key point here is that extensions operate and execute within the JVM.

FlowFile Repository: The FlowFile Repository is where NiFi keeps track of the state of what it knows about a given FlowFile that is presently active in the flow. The implementation of the repository is pluggable. The default approach is a persistent Write-Ahead Log located on a specified disk partition.

Content Repository: The Content Repository is where the actual content bytes of a given FlowFile live. The implementation of the repository is pluggable. The default approach is a simple mechanism, which stores blocks of data in the file system. More than one file system storage location can be specified to get different physical partitions engaged to reduce contention on any single volume.

Provenance Repository: The Provenance Repository is where all provenance event data is stored. The repository construct is pluggable with the default implementation being to use one or more physical disk volumes. Within each location event data is indexed and searchable.

NiFi is also able to operate within a cluster.

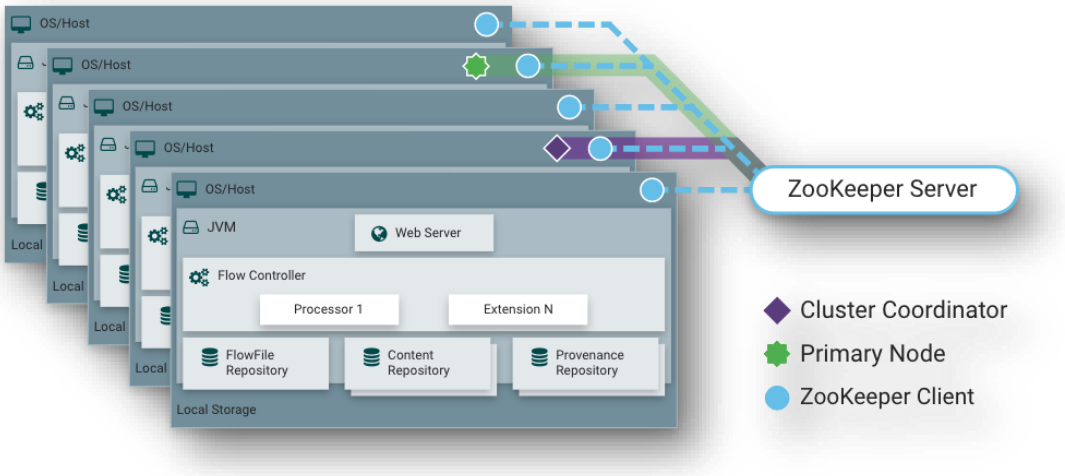

Figure 3 - Repositories

Starting with the NiFi 1.0 release, a Zero-Leader Clustering paradigm is employed. Each node in a NiFi cluster performs the same tasks on the data, but each operates on a different set of data.

Apache ZooKeeper elects a single node as the Cluster Coordinator, and failover is handled automatically by ZooKeeper. All cluster nodes report heartbeat and status information to the Cluster Coordinator. The Cluster Coordinator is responsible for disconnecting and connecting nodes.

Additionally, every cluster has one Primary Node, also elected by ZooKeeper. As a DataFlow manager, you can interact with the NiFi cluster through the user interface (UI) of any node. Any change you make is replicated to all nodes in the cluster, allowing for multiple entry points.

4.2 Prerequisites

Prerequisites are specific condition that needs to be met before initiating the configuration. Hence, mentioned below are pre-requisites for NiFi:

4.2.1 System Requirements For NiFi

Apache NiFi can run on something as simple as a laptop, but it can also be clustered across many enterprise-class servers. Therefore, the amount of hardware and memory needed will depend on the size and nature of the dataflow involved.

The data is stored on disk while NiFi is processing it. So NiFi needs to have sufficient disk space allocated for its various repositories, particularly the content repository, flowfile repository, and provenance repository. NiFi needs to be configured according to the following system requirements:

4.2.2 Supported OS for NIFI

- Linux (Recommended)
- Unix
- Windows
- macOS

Requires Java 8 or Java 11

4.2.3 Supported Web Browsers

- Microsoft Edge: Current & (Current - 1)
- Mozilla FireFox: Current & (Current - 1)
- Google Chrome: Current & (Current - 1)
- Safari: Current & (Current - 1)

4.2.4 Hardware Sizing Recommendation

NiFi is designed to take advantage of:

- all the cores on a machine
- all the network capacity
- all the disk speed
- many gigabytes of RAM (although usually not all) on a system

Hence, it is important that NiFi should be running on dedicated nodes. Following are the recommended server and sizing specifications for NiFi:

- Minimum of 3 nodes
- 8+ cores per node (more is better)
- At least 8 GB
- 6+ disks per node (SSD or spinning)

Required Sustained Throughput	Minimum Hardware Requirement
50 MB and thousands of events per second	• 1 or 2 nodes • 8 or more cores per node • 6 or more disks per node (SSD or spinning) • 2 GB memory per node • 1 GB bonded NICs
100 MB and tens of thousands of events per second	• 3 or 4 nodes • 16 or more cores per node • 6 or more disks per node (SSD or spinning) • 2 GB of memory per node • 1 GB bonded NICs
200 MB and hundreds of thousands of events per second	• 5 to 7 nodes • 24 or more cores per node (effective CPUs) • 12 or more disks per node (SSD or spinning) • 4 GB of memory per node • 10 GB bonded NICs

Required Sustained Throughput	Minimum Hardware Requirement
400 to 500 MB/sec and hundreds of thousands of events per second	• 7 - 10 nodes • 24 or more cores per node (effective CPUs) • 12 or more disks per node (SSD or spinning) • 6 GB of memory per node • B bonded NICs

4.2.5 Port Requirement for NiFi

The following ports are required for internal communication:

- Nifi remote socket port = 10443
- Nifi web https port = 9443
- Nifi cluster port = 11443
- Nifi cluster load balance port = 6342
- Nifi zookeeper connect port=2181, 2888, 3888

4.3 Overview of IMM

Integration Management Module (IMM) is a component of IntelliOps Event Management which is used for 3rd party tools integration and ingesting events, metric, performance, and configuration data into IntelliOps Event Management for performing event management functions.

Using IMM, we can reduce the implementation timeline significantly, allowing you to quickly get the NiFi connectors onboarded and take control of the event management ecosystem.

4.4 Prerequisite for IMM

Prerequisites are specific condition that needs to be met before initiating the configuration. Hence, mentioned below are pre-requisites for IMM:

4.4.1 Supported OS for IMM

- Linux RHEL 8.x

4.4.2 Supported Web Browsers

- Microsoft Edge: Current or previous version
- Mozilla FireFox: Current or previous version
- Google Chrome: Current or previous version
- Safari: Current or previous version

4.4.3 Hardware Sizing Recommendation

- 2 Web servers & 2 DB servers are required with below configuration:
  - WebServer: 2CPU, 4GB
  - DB Server: 4CPU, 8GB

4.4.4 Port Requirement for IMM

- IMM KRS Service -4000

- IMM API Service - 4100
- IMM Web Portal - 4200
- IMM Orchestrator Service - 4300

5 IMM Interface

Integration Management Module (IMM) is a component of IntelliOps Event Management which is used for 3rd party tools integration and ingesting events, metric, performance, and configuration data into IntelliOps Event Management for performing event management functions.

For detailed information on how to work with IMM Interface, please refer to the ***HCL IMM User Guide***.

6 IEM Configuration

The section provides detailed process of Customer Onboarding and configuration.

6.1 Customer Creation

Customer Creation" refers to the process of establishing a new customer profile or record within the event management system.

By Default, with the setup one environment customer is created named “Default”. Default customer cannot be deleted; it cannot be renamed though. This section enables us to create multiple customers to cater to a multi-tenant environment.

Following are the actions a logged in user can perform based on the role.

Please refer to ***Manage Roles*** section to understand more about role-based access control.

- Onboarded Customer
- In-progress Customer

Onboarded Customer:

Onboarded View displays the customers that have gone through onboarding process and certain actions can be performed that are displayed under Actions. The goal of customer onboarding in Event Management AIOps is to facilitate efficient introduction to the platform, ensuring that customers can quickly and effectively utilize the features of the system for managing events with the support of AI-driven capabilities.

1. In the top navigation bar, click Customer. Customer Grid will be displayed. This displays a list of all customers configured in the environment. When users are coming here for the first time, only the default customer will be listed with Edit option next to it.

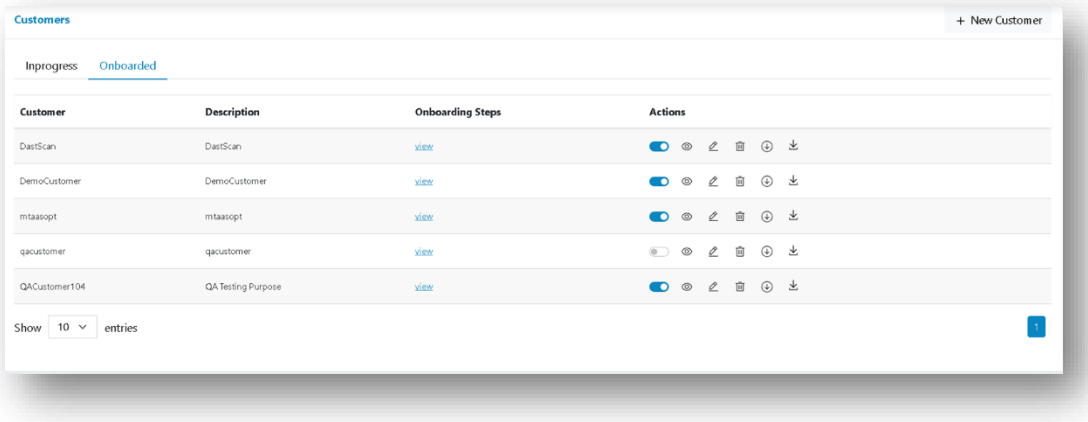

Figure 4 - Customer Page

- Add New Customer
- Onboarding Steps View
- Enable/Disable State
- View Customer
- Edit Customer
- Delete Customer
- Download Published API
- Download Installer

- Download License
- Renew License

6.1.1 Add New Customer

Customer Addition" refers to the process of integrating and introducing a new customer into our event management system. This encompasses the activities and procedures aimed at getting a customer started, providing necessary information, and ensuring a smooth transition into using the Event Management platform. The addition process in this context may involve both manual and automated tasks.

1. User can create a new customer by clicking on the **New Customer** button**.**

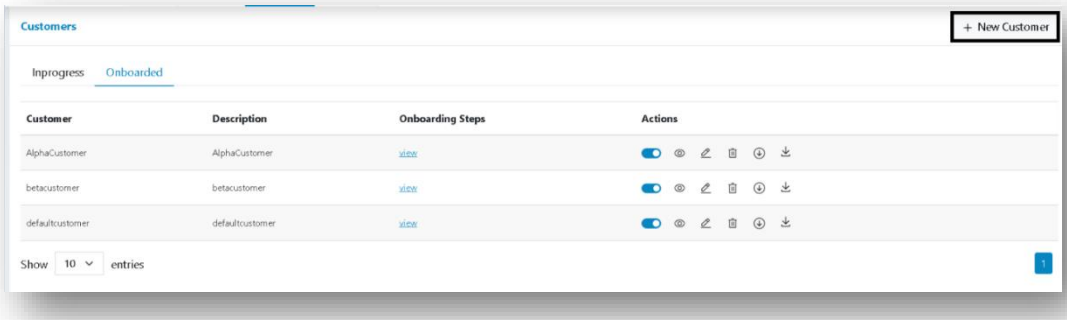

Figure 5 - Navigation for Create New Customer

2. Clicking on add customer a popup is displayed with an input option.

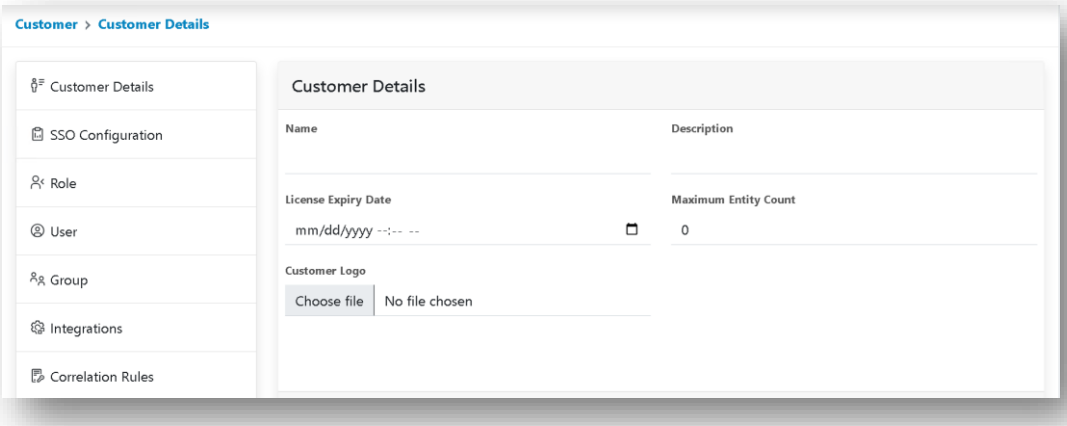

Figure 6 - Customer Creation

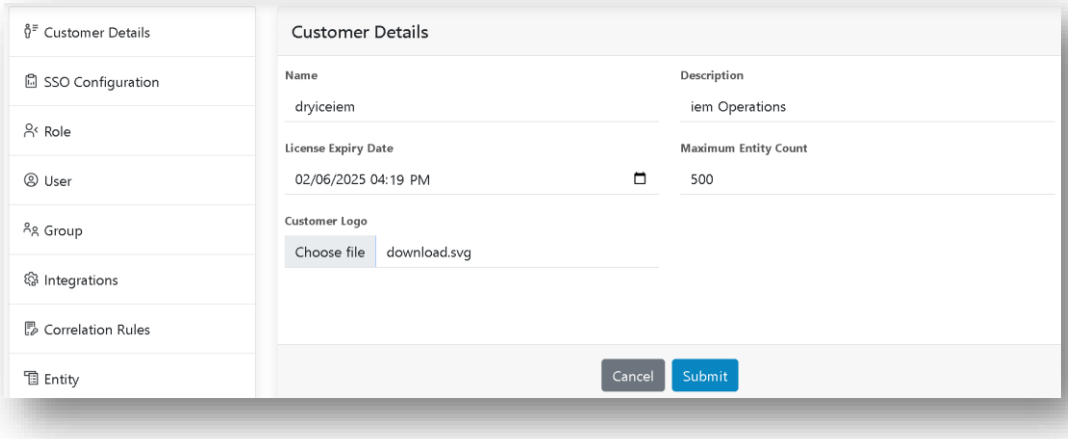

Figure 7 - Customer details

3. Specify the name, description, license expiry date and maximum entity count and the customer logo with .svg file format with max of 200kb image and click Submit.

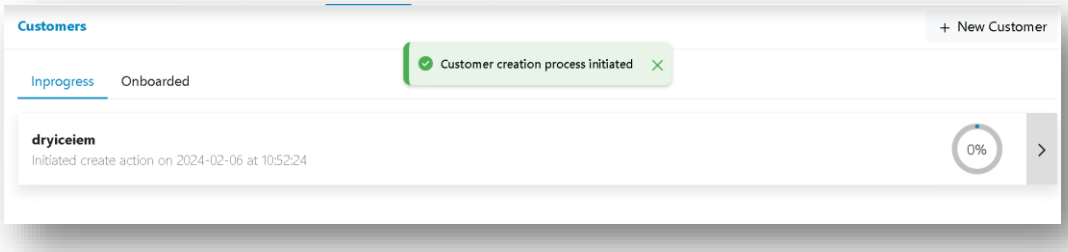

Figure 8 - Customer Creation Process

4. On successful creation, the customer will be listed in the main grid.
5. Click on **View Progress** button that will show about process flow with completion status of customer based on the configurations done.
6. The process flow with completion status will be shown like the image below for a particular customer in progress**.**

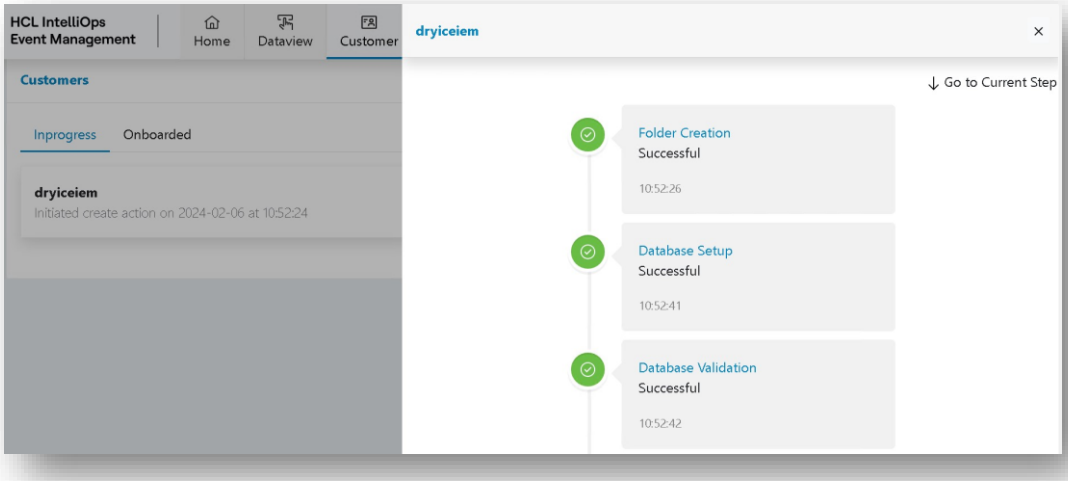

Figure 9 - Customer Creation Onboarding Steps

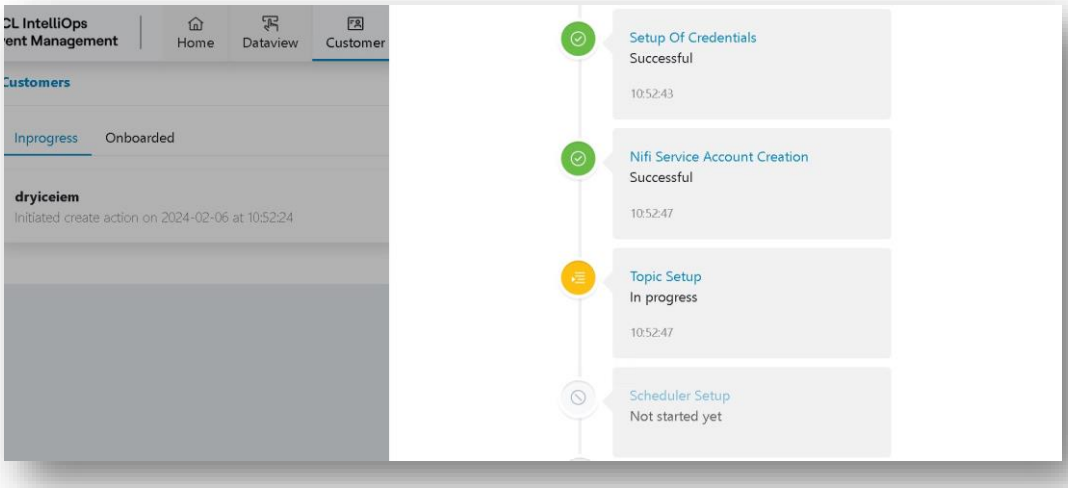

Figure 10 - Customer Creation Onboarding Steps (Cont.)

7. All the processes that are completed will be marked as complete status in green.
8. Hence the division of in-progress and onboarded shows the process flow completion for a particular customer. If the customer onboard processes are complete, then the customer will be put in the on-boarded grid like shown below.

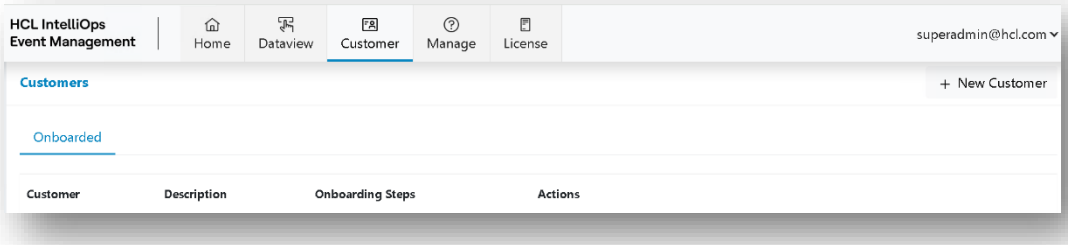

Figure 11 - Customer Page

6.1.2 Onboarding Steps View

If the customer onboard processes are completed, then the customer will be put in the Onboarded grid like shown below.

1. Click on the Onboarding Steps view button.

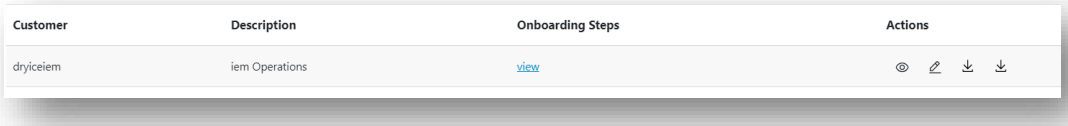

Figure 12 - Onboarding Steps View

2. Onboarded shows the process flow completion for a particular customer.

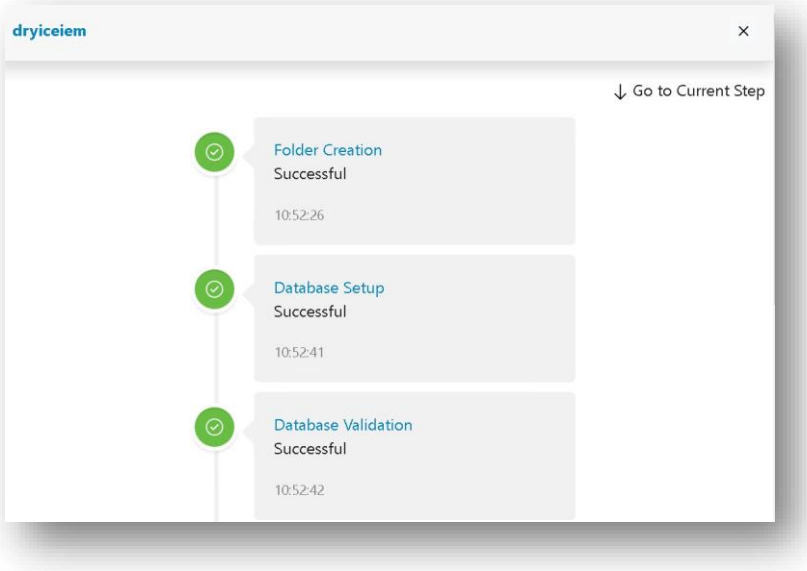

Figure 13 - Customer Creation Onboarding Steps

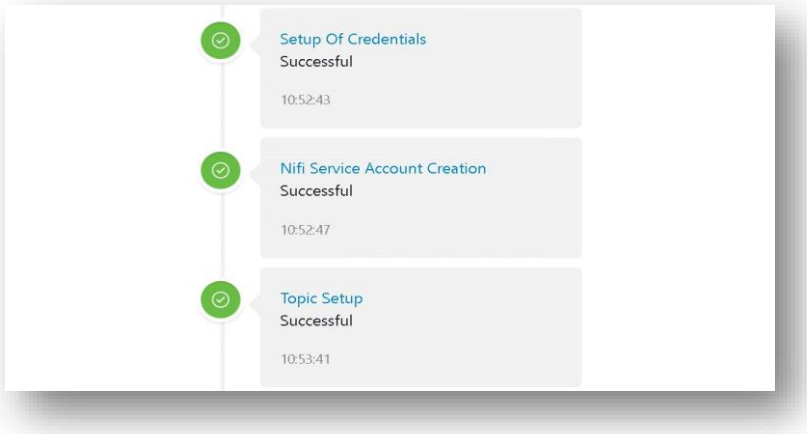

Figure 14 - Customer Creation Onboarding Steps (Cont.)

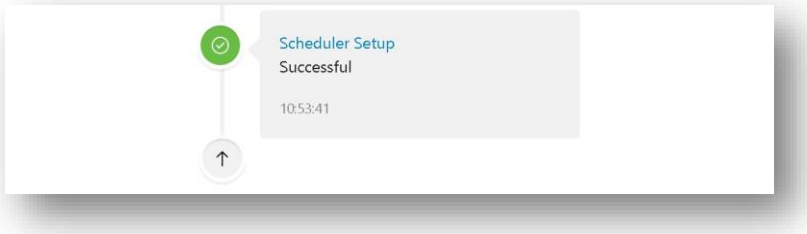

Figure 15 - Customer Creation Onboarding Steps (Cont.)

6.1.3 Enable/Disable State

To enable or disable a customer in an environment, there is provision of toggle switches to easily perform the required actions.

1. Click on the Enable/Disable toggle button next to the customer which needs to be Enabled/Disabled
2. Click on Enable/Disable icon, on success a confirmation pop-up message will be displayed.

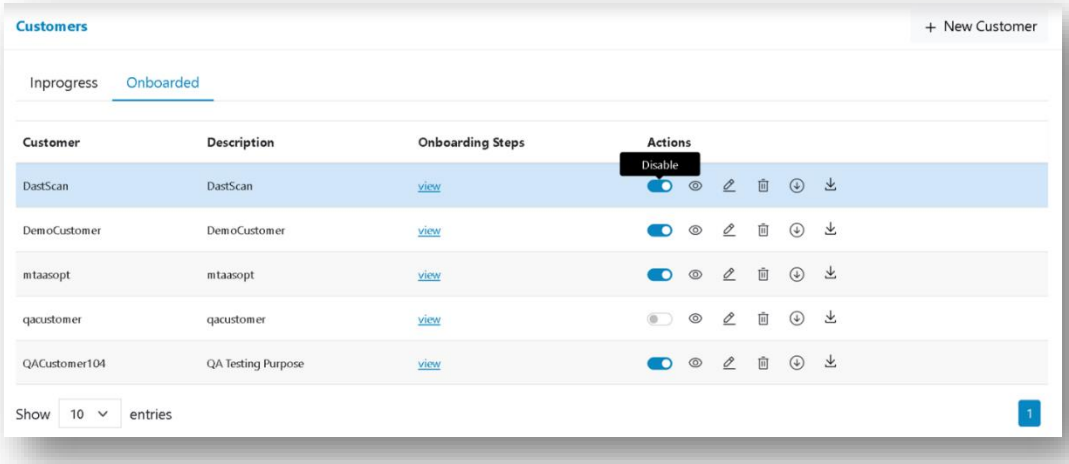

Figure 16 – Enable/Disable Customer

6.1.4 View Customer

This action enables to view the customers created in the environment.

1. The Action tab contains a view option, click on the view option to view the customers that are created.

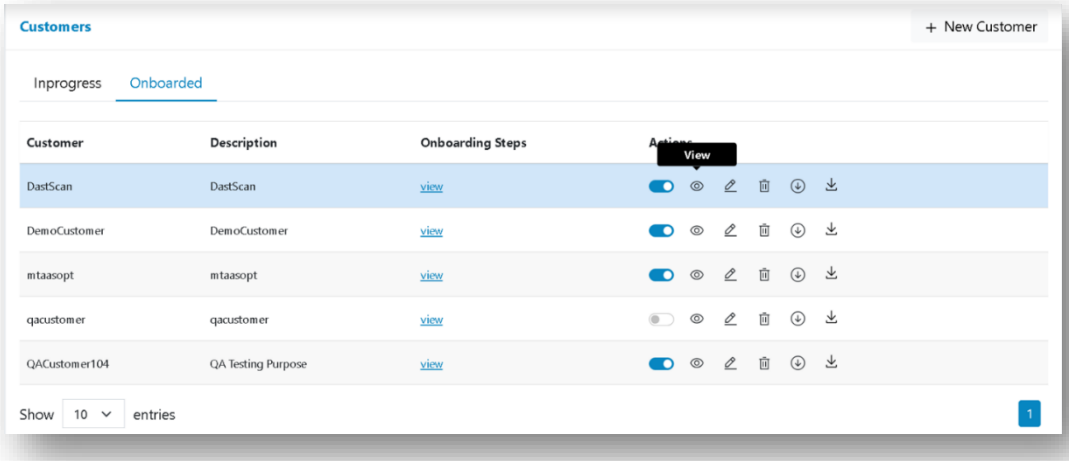

Figure 17 – Customer Page

2. Click on View for the respective Customer and pop up for the customer will be opened.
3. User cannot edit the details via View option. All the details related to customers created in the environment will be displayed.

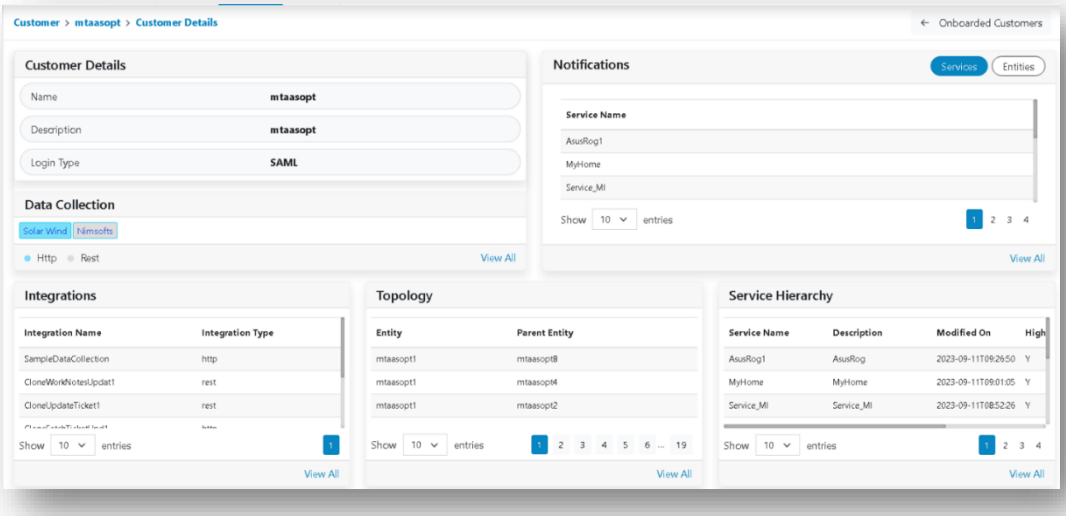

Figure 18 - Customer Details

6.1.5 Edit Customer

1. Click on the edit icon next to the customer whose details are to be modified.

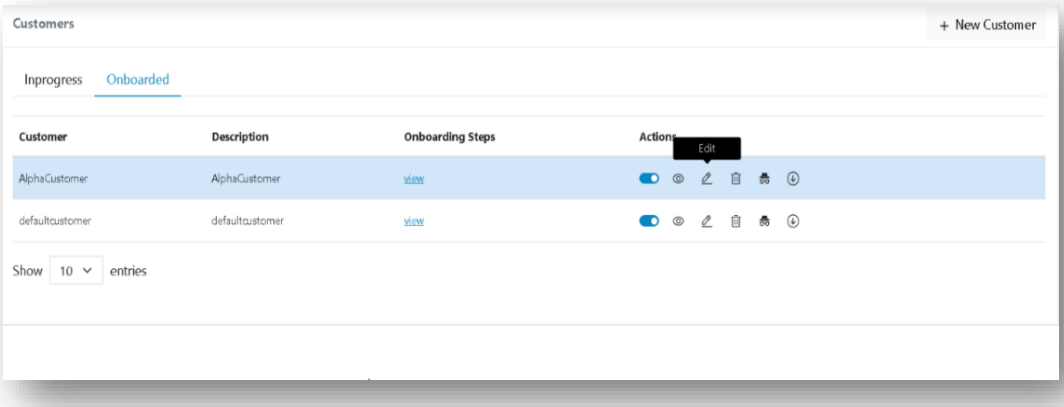

Figure 19 - Edit Customer

2. The form will appear with the saved details as shown.

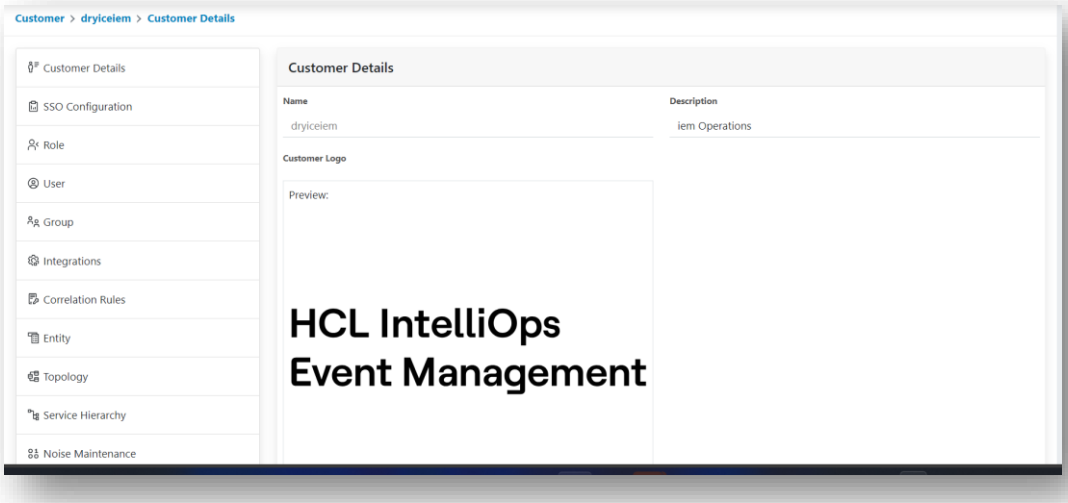

Figure 20 - Customer Edit Screen

3. Click **Update** to update the description and customer logo and after successful update it will navigate to Onboarded customer page.

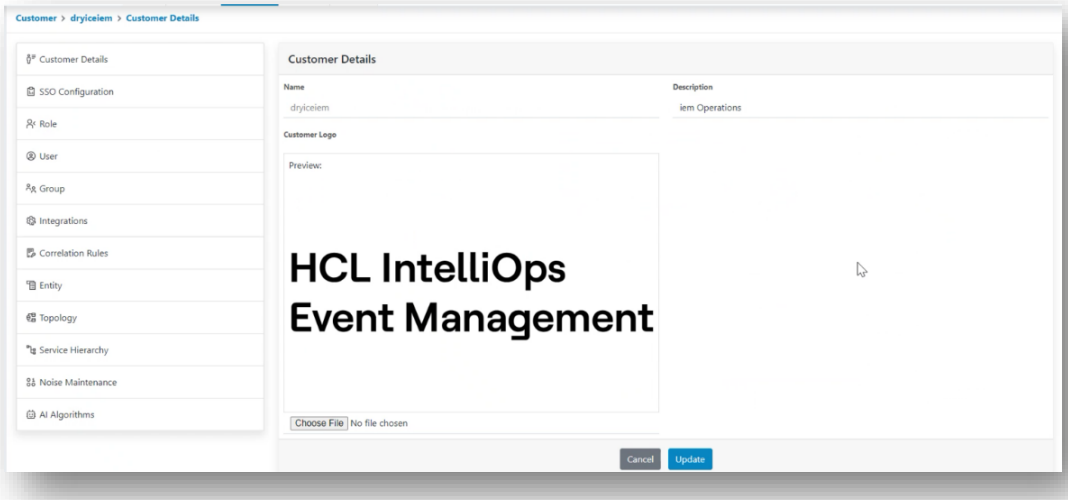

Figure 21 – Customer Details

6.1.6 Delete Customer

1. Click on the delete icon next to the customer which is to be deleted.

Figure 22 - Delete Customer

A confirmation box will be prompted.

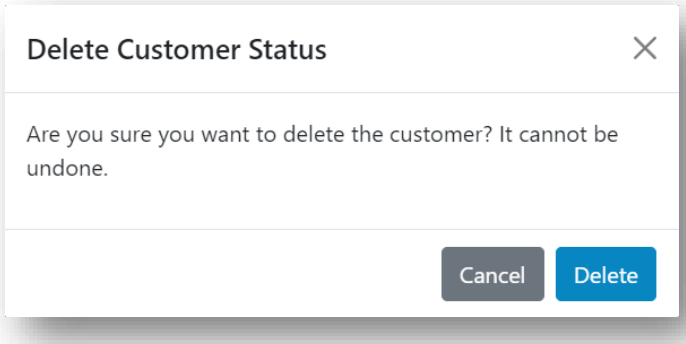

Figure 23 - Confirmation pop-up

2. Clicking **Delete**, deletes the customer permanently.

6.1.7 Download Published API

This action enables customer administrator/Superadmin to download Publish API for NiFi.

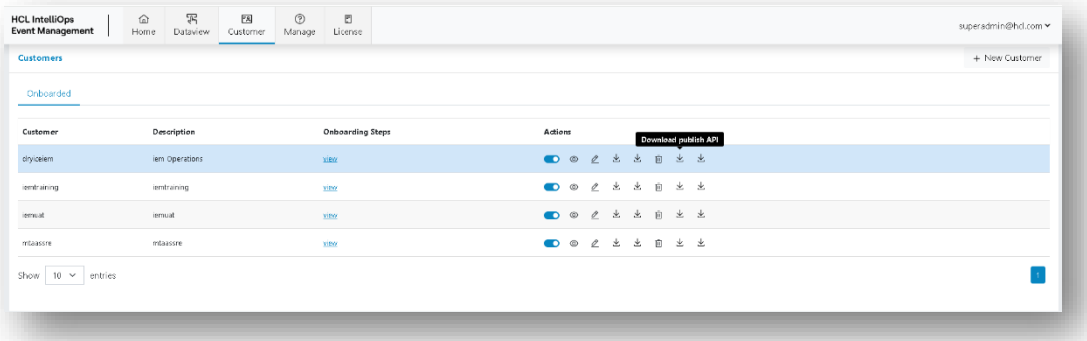

Figure 24 - Download Publish API

6.1.8 Download Installer

This action enables customer administrator/Super admin to download Installer for Integration Management Module (IMM)

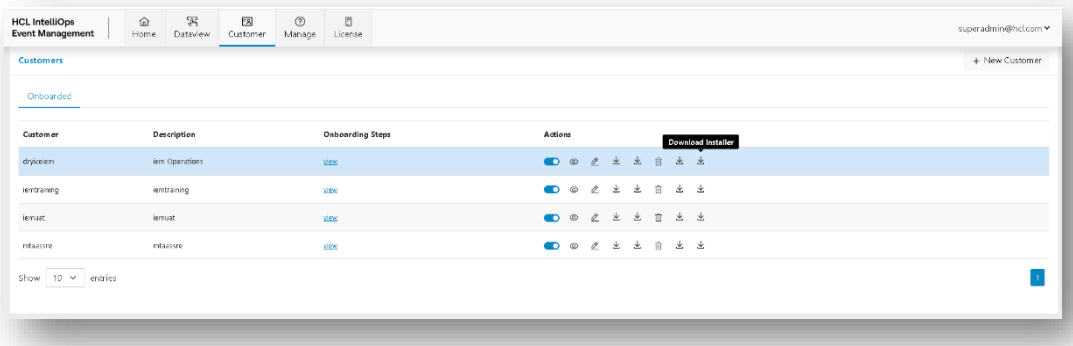

Figure 25 - Download Installer

6.1.9 Download License

This action enables customer administrator/Super admin to download IEM License

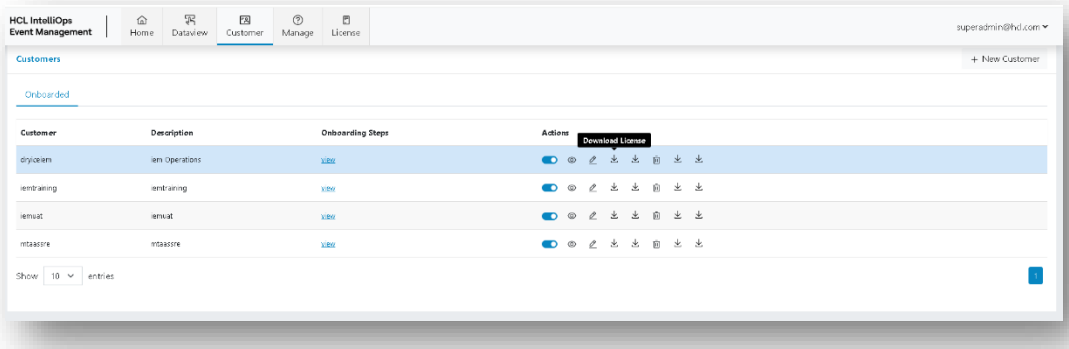

Figure 26 - Download License

6.1.10 Renew License

This action enables customer administrator/Super admin to Renew IEM License

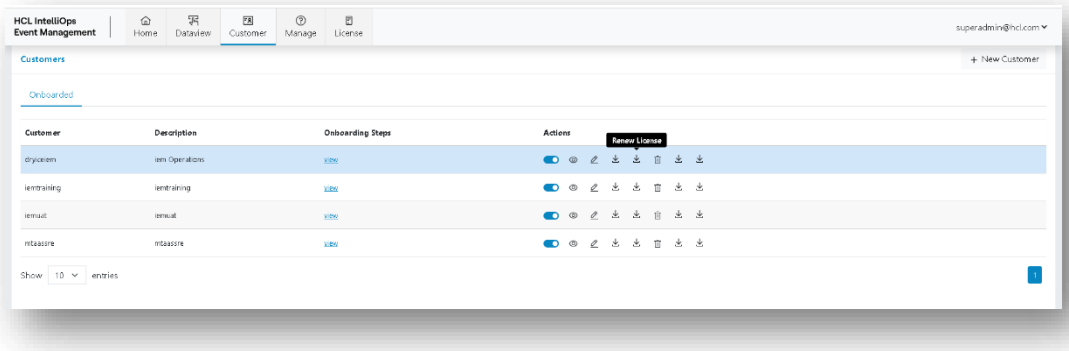

Figure 27 - Renew License

In-Progress:

The In-progress customer list contains the customers whose configuration processes are in line of completion.

Figure 28 - Status of Customer

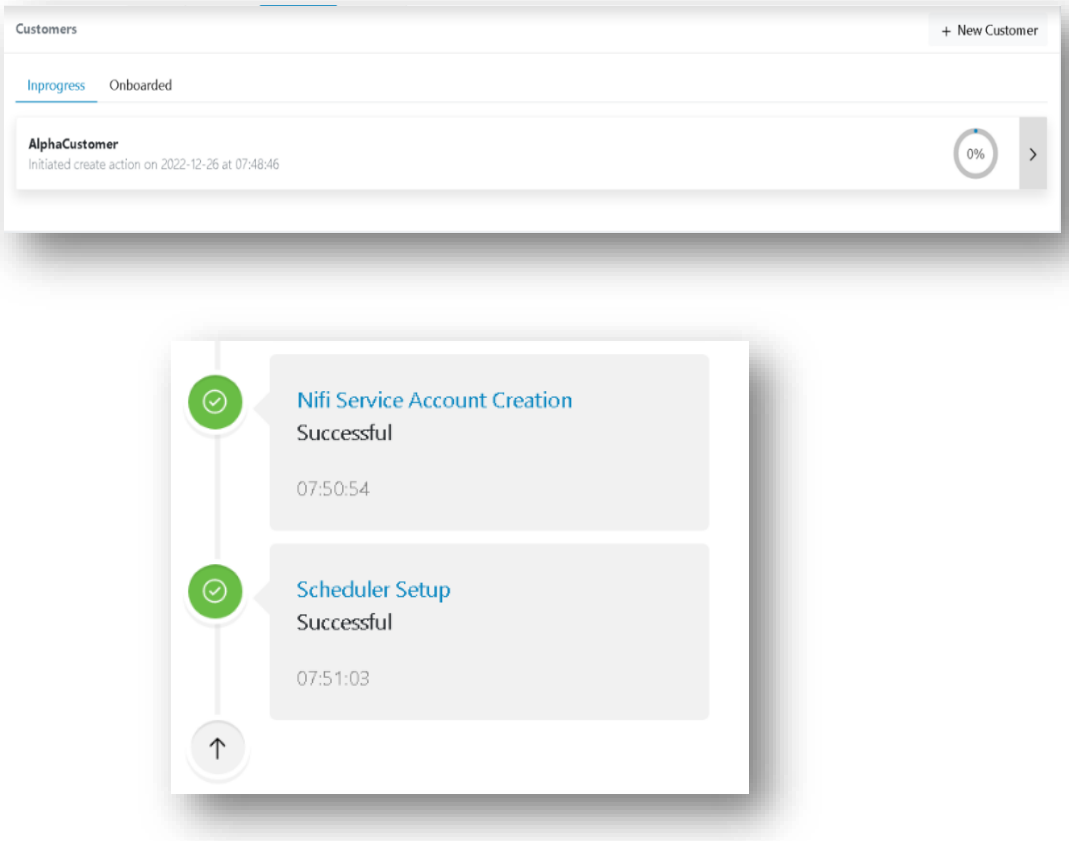

Figure 29 - Customer Creation Onboarding Steps

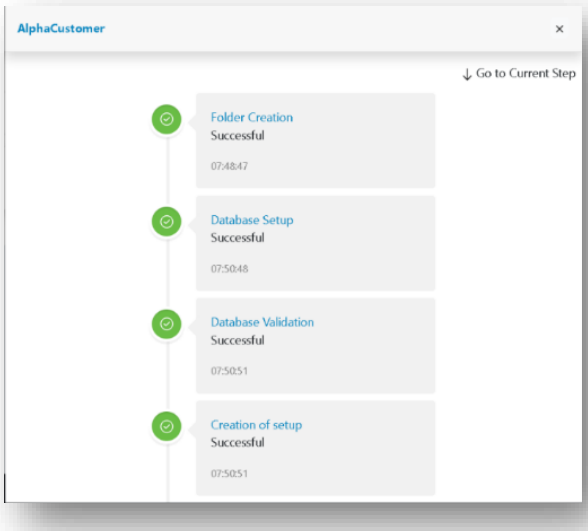

Figure 30 - Customer Creation Onboarding Steps (Cont.)

6.1.11 Manage Onboarded Customer

The section provides detailed steps on how to Manage the Onboarded customer in IEM.

6.1.11.1 Customer Details

The section provides the details of the customer configured in the environment. The following details are displayed:

- Name
- Description

- Customer logo

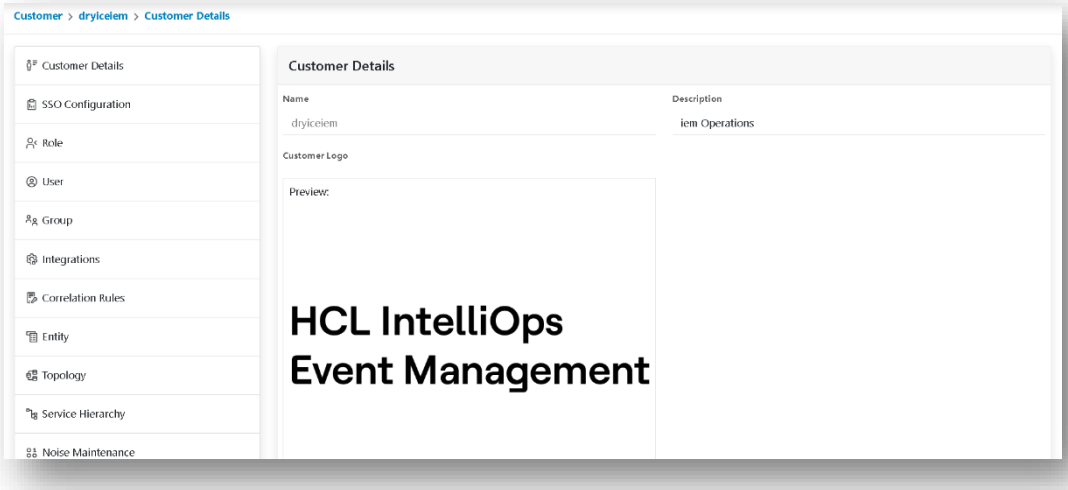

Figure 31 – Customer Details

6.1.11.2 SSO Configuration

Single Sign-On (SSO) configuration in IEM refers to the setup and integration of a Single Sign-On solution within the platform. SSO is a mechanism that enables users to access multiple applications or services with a single set of credentials, eliminating the need to remember separate usernames and passwords for each system. With SSO user can establish a secure method for authenticating users when they access IEM. Here, it is mainly used for SAML Authentication for a customer.

1. When you click SSO Configuration, the new form will appear.
2. In that form user need to add the relevant data required in the fields.
3. Click on update. A confirmation message “Data updated successfully” is prompted to user. Click on close button. Clicking on **Skip** takes the user to the Role screen.

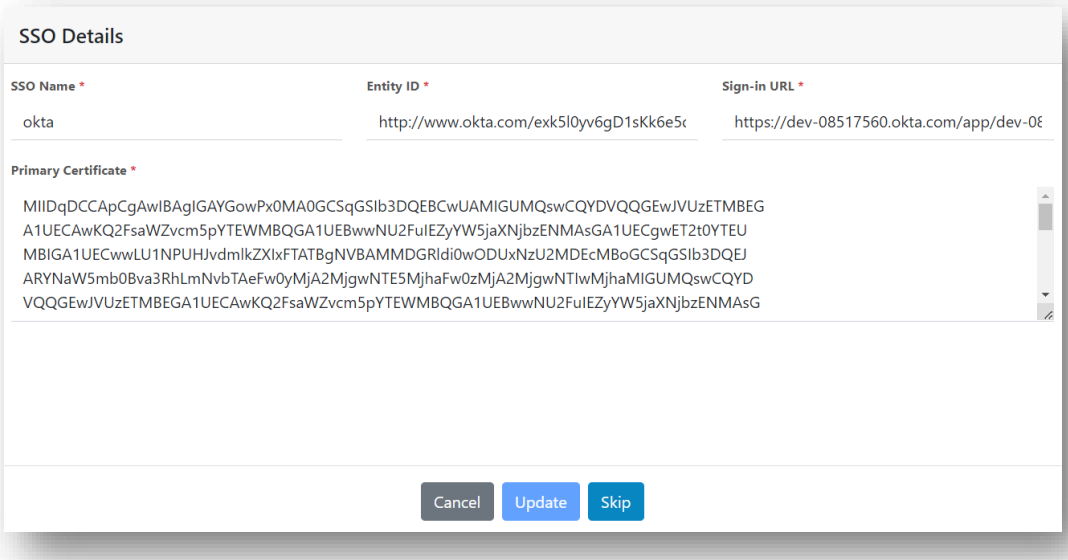

Figure 32 - SSO Configuration Page

6.1.11.3 Roles

Role screen has four roles by default and also allows user to create custom roles according to the requirements and if any new user is created "viewer" role has been assigned by default.

Add New Role

A user can perform an action on the page based on its role. A role is a named collection of privileges determining the tasks user can perform. Pairing a user or group with a role grants the user or groups certain rights to the system. The following table outlines the predefined system roles.

Table 2 – Predefined System Roles

Role	Description
Customer Admin	- All privileges for the administrative features in IEM environment for a particular customer - Access to all the configurations over console - Full operational and management control
Super Admin	- All Administrative privileges for all the customers configured in IEM environment. - Access to all the configurations over console - Full operational and management control
Operations User-Viewer	- Access to view Data View Page and Home over console but cannot make any changes
Operations User-Resolver	- Access to view all the data over Data View screen and mark the actionable as resolved over IEM. - Access Home Metric View
Operations User-Actionable user	- Access to view all the data over Data View screen and perform various actions over actionable. - Any view can be saved post adding additional columns - Access Home Metric View

This action enables us to create custom roles in the environment. Adding new roles involves the creation of additional user roles or profiles that grant specific permissions and access levels to the platform user. There are four default roles configured with pre-defined set of permissions.

1. Click on "**Customer**"→" **Customer Name**"→"**Role**."
2. Click on **"+ New Role**".

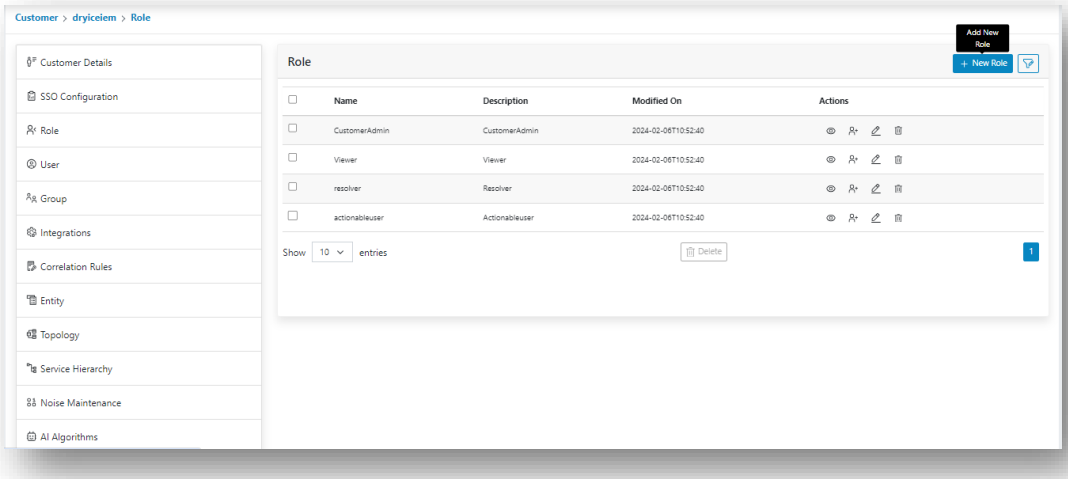

Figure 33 – New Role

3. After clicking the **"+New Role"** the following form is displayed.

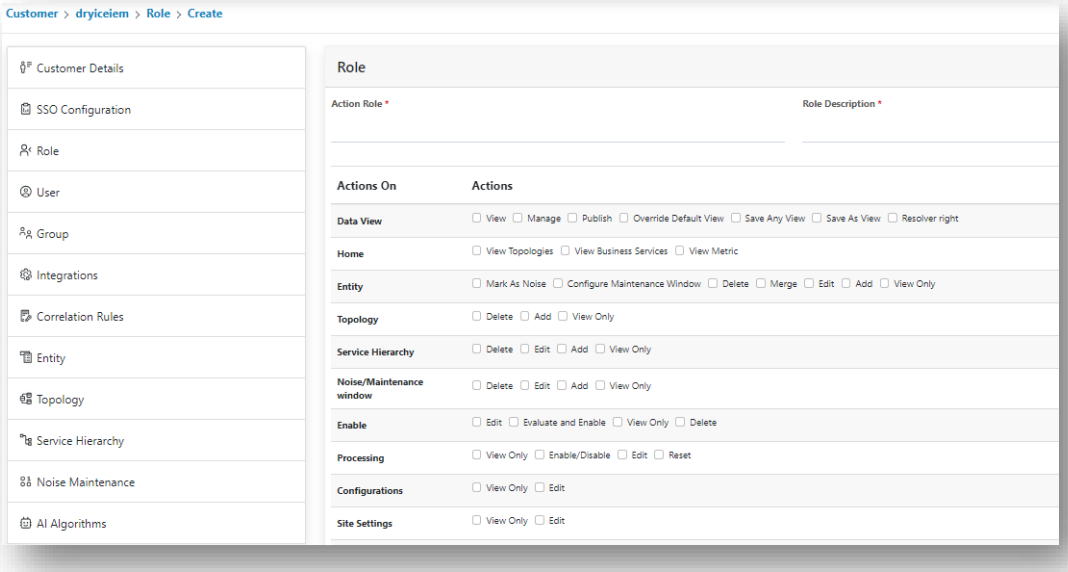

Figure 34 - Role Creation

4. Enter the **Role Name**. For example, let's name the role as 'customadminrole'.

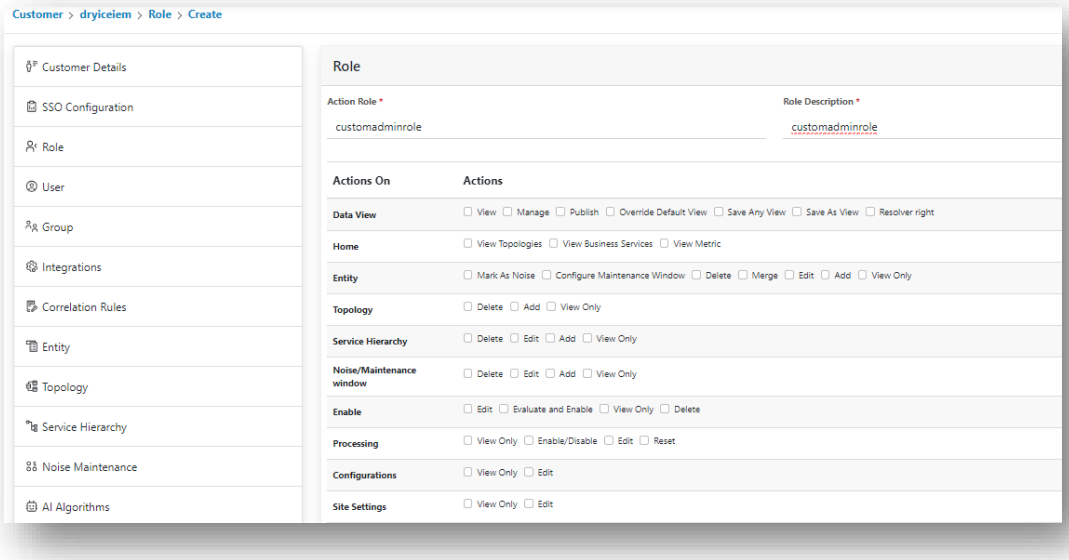

Figure 35 - Navigation Page for Assigning an Action to a Role

5. List of all the actions that can be taken would be available on the same page.

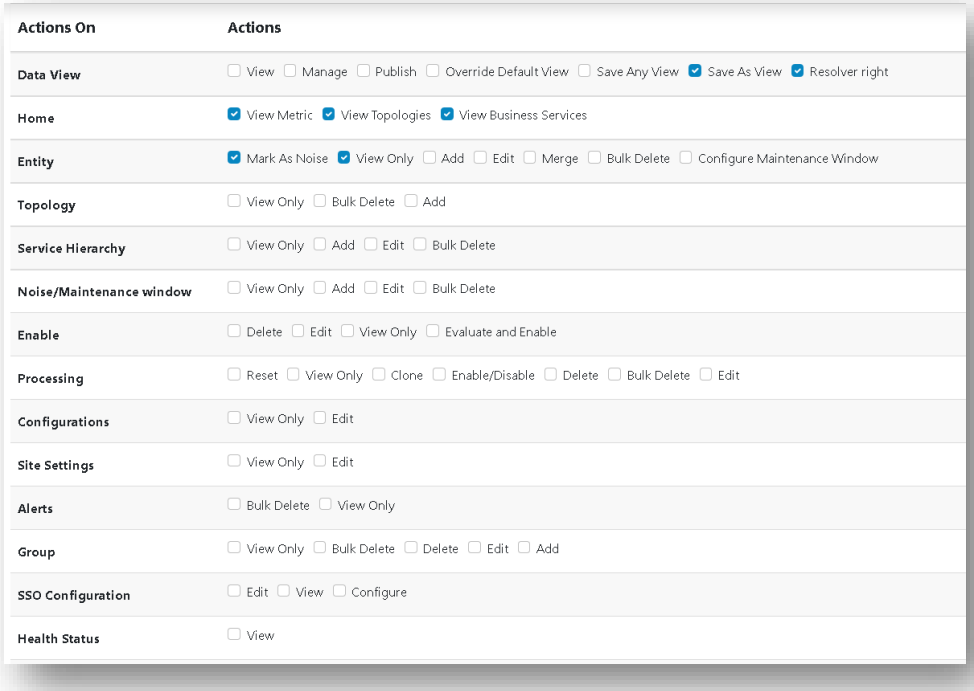

Figure 36- Assigning Actions for a Role

6. All the actions that's intended to be enabled for the role on this page can be selected in one go. **User can** select Add, Edit, Delete for the ~~actions~~.
7. Add as many **actions** as required. For this example, user will just keep the single page role.
8. Once all the actions are selected for the **newly created role** and the mapping is done, click on the Submit button.
9. On successful creation **of the role with action** the following pop-up message is prompted.

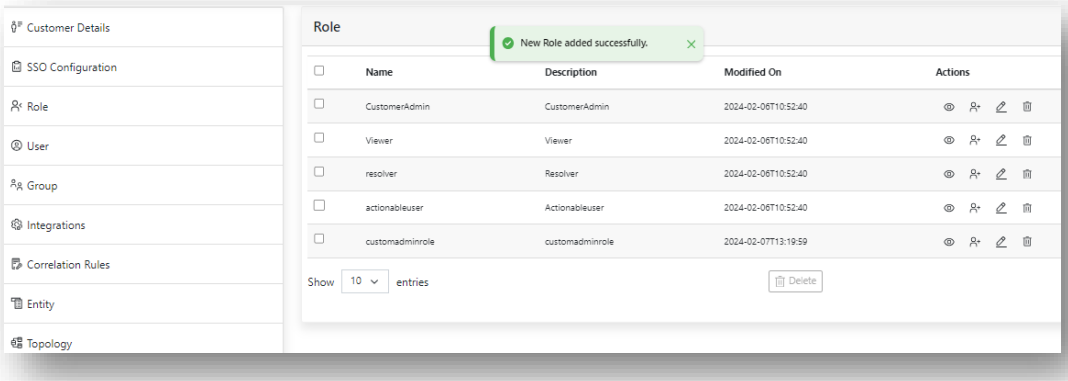

Figure 37 - Alert Message

10. The control will be redirected to the Grid view page and the new role will appear in the grid as shown above.

Managing Roles

This customization ensures that customer administrators have the necessary permissions to effectively access various configurations within their specific customer context.

This section enables user to Manage roles within the environment.

1. Click the “Customer”→ “Customer Name”→ “Role”.
2. Click on the **Role** Tab, the following page would be available.

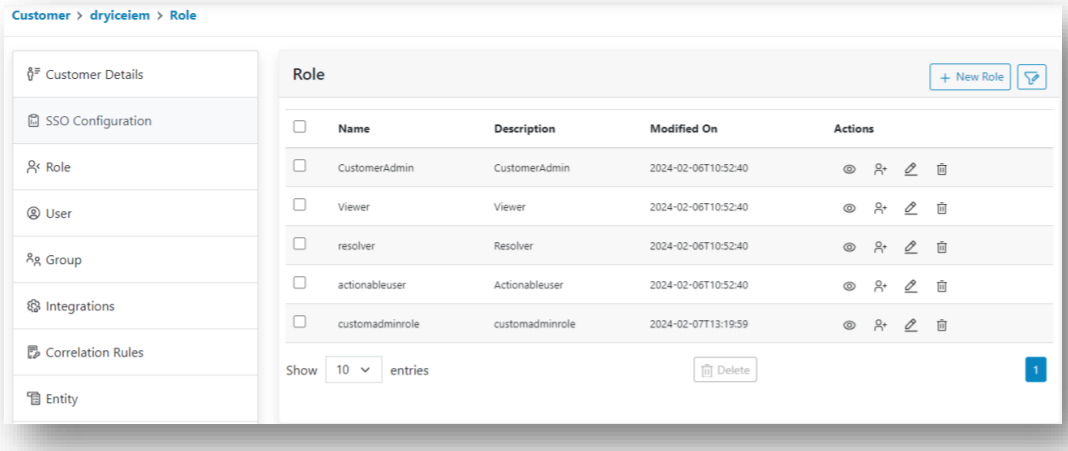

Figure 38 - Role Page

3. When user accesses the IEM console for the first time, only the default roles would be visible to the user.

The Default Roles cannot be edited.

4. By default, **IEM** has the following default roles enabled:

– **Customer Admin** – A role with full access to the environment. (User can Add\Delete\Edit)

– View user, Actionable User and Resolver **are** Operational user roles. These roles are accessed only on the Data View and Home page.

- **View user** –Has view only access.
- **Actionable user** – They can take actions on the actionable created in the environment but will not be able to mark them as resolved.

- **Resolver** – They have full access on the actionable, they can work upon actionable and even mark them as resolved.

Roles control the action that users perform on the page. The data visible to user is controlled by the customer and the group assigned to user.

Please Refer Users and Group sections to understand how the data is controlled.

Edit Role

This action enables users to edit the custom roles created in the environment.

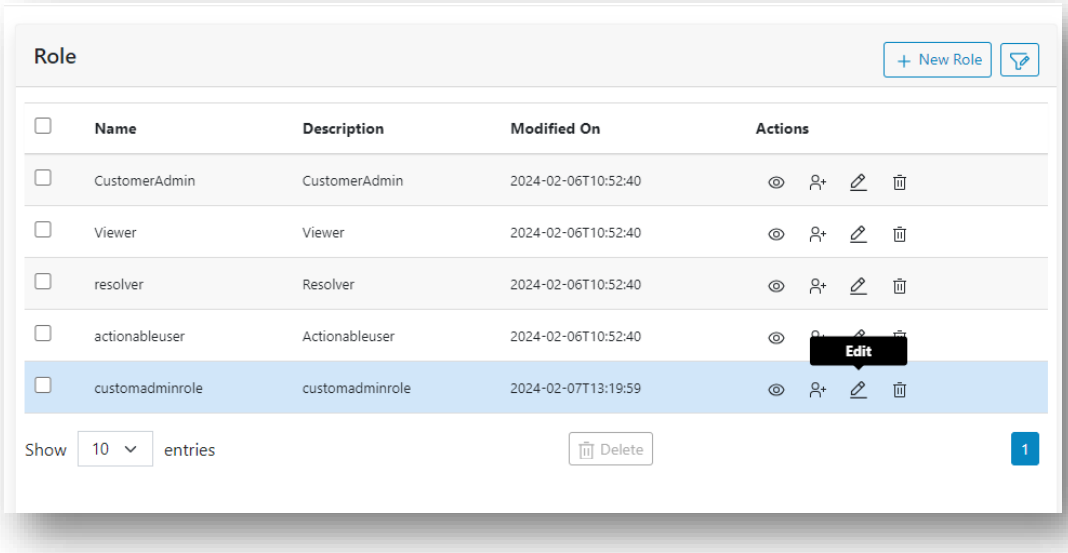

Figure 39 – Edit Roles

1. Click on the Edit icon next to the role.
2. The form will appear filled up with the saved data.

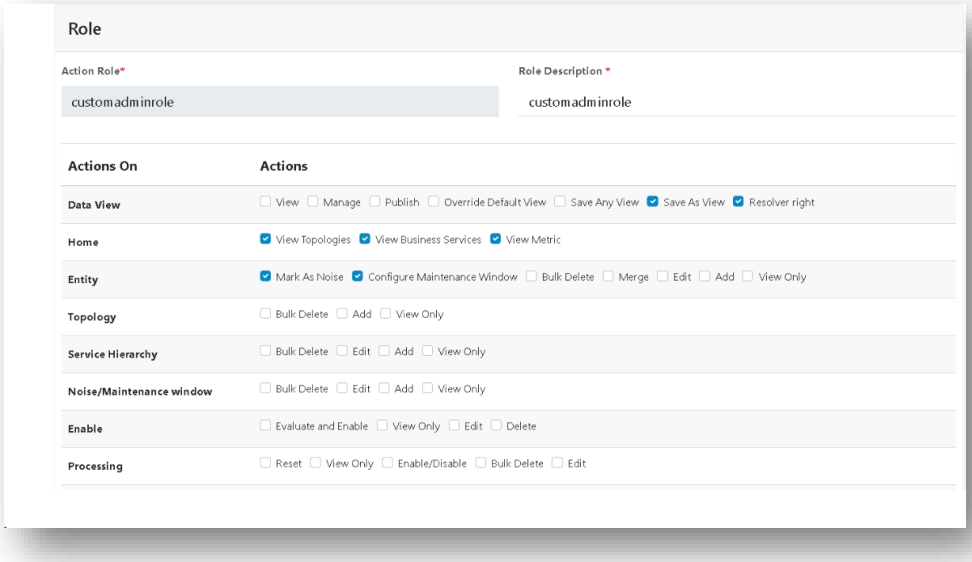

Figure 40 - Edit a Role Description

3. User can rename the role, add/remove more pages or add/remove actions that are mapped.

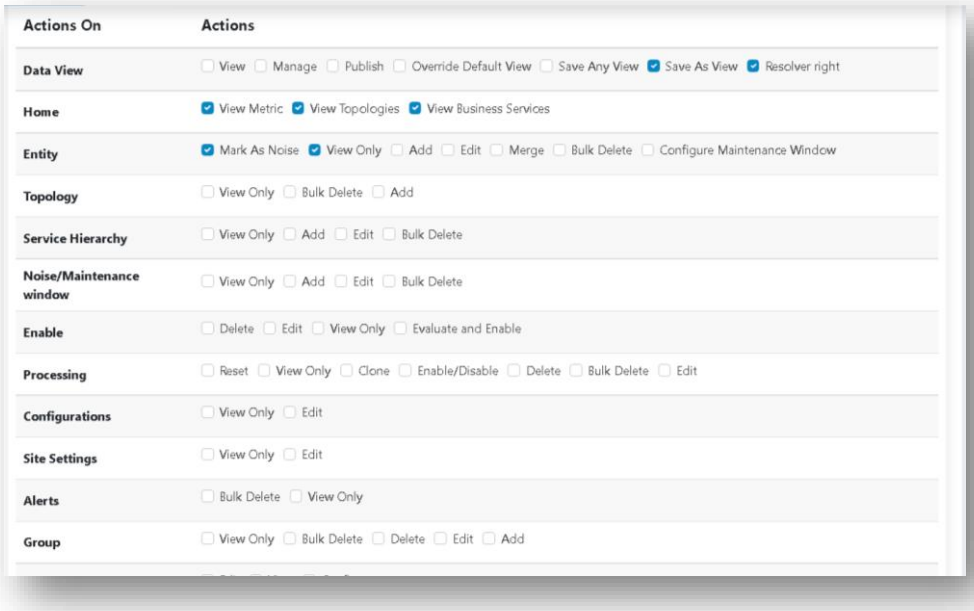

Figure 41 - Selecting Actions for a Role

4. And add a new *User* with *full actions* enabled. With all modifications the page looks like the below image.

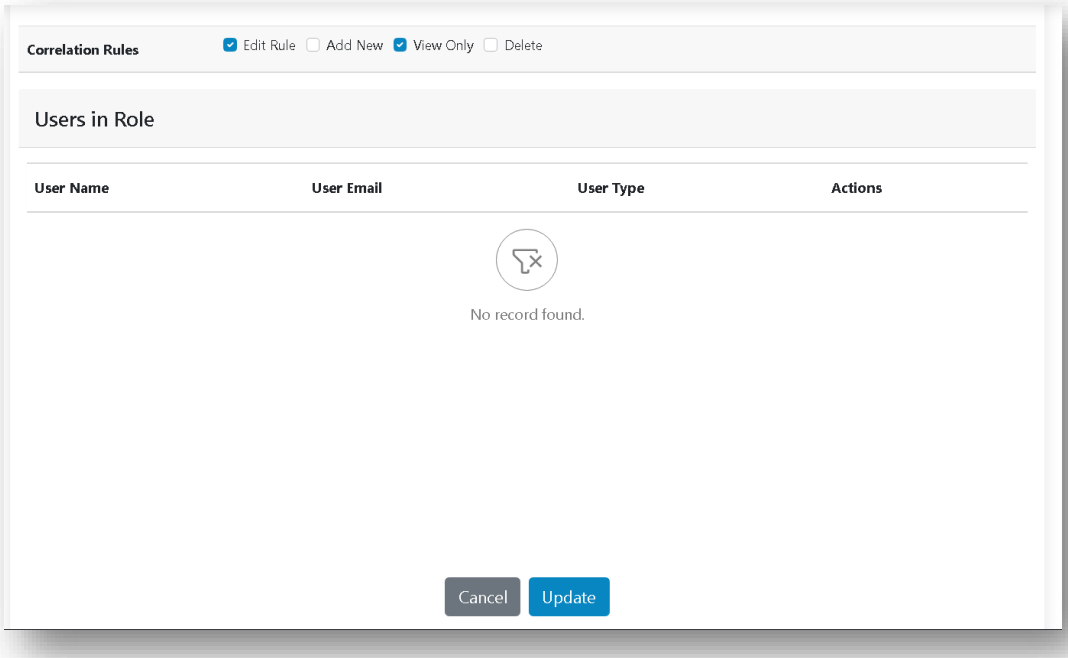

Figure 42- Selecting Actions for a Role

5. Post the changes are made, Click on the Update button.
6. On successful update the following message is displayed, post that the user will be redirected back to the grid view page.

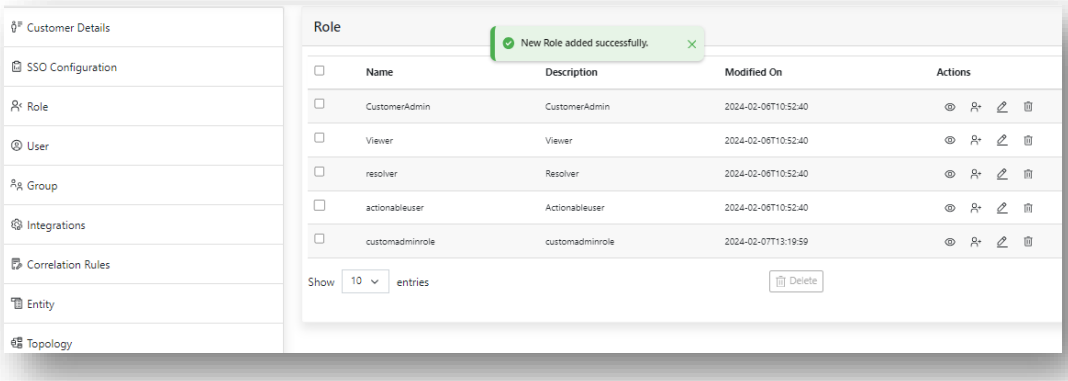

Figure 43 - Alert Message

Delete Role

This action enables us to delete the custom roles created in the environment.

1. For admin pages, select the roles that are to be deleted.
2. Click on the delete icon corresponding to the role that s to be deleted.
3. For Bulk delete, select the multiple roles, and click on the “Delete” icon at the bottom.

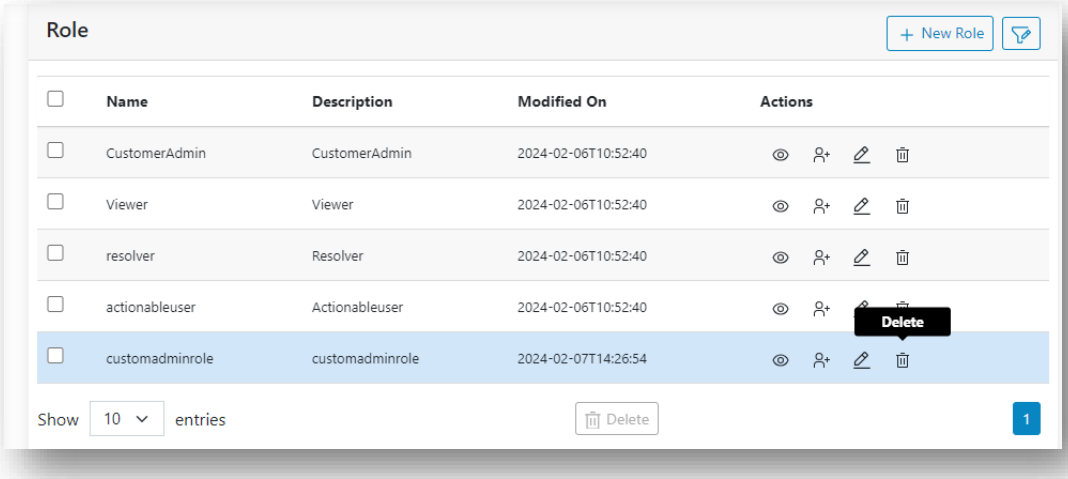

Figure 44 - Delete Role

4. User will be prompted for confirmation pop-up as shown.

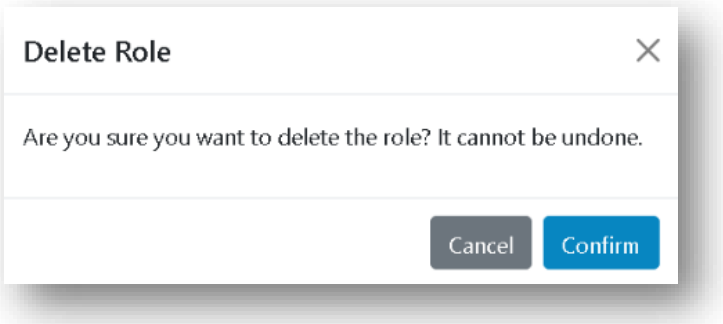

Figure 45 - Confirmation pop-up

5. Click **Confirm**. On successful deletion a confirmation message will be prompted

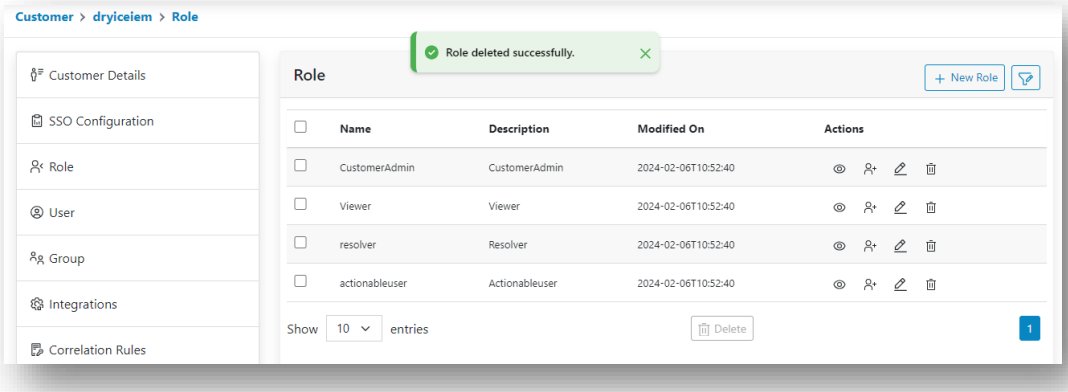

Figure 46 - Alert Message

6. The role will be no longer visible in the grid.

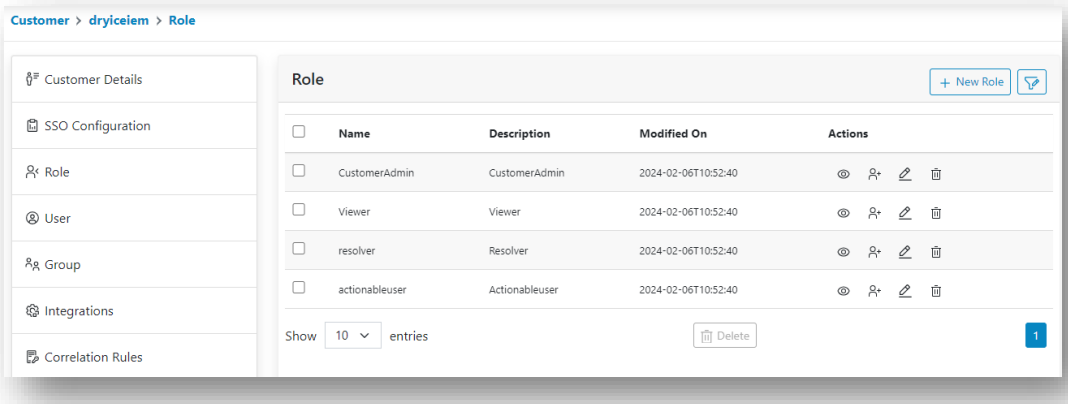

Figure 47 – Updated Grid

View Role

This action enables the users to view the custom roles created in the environment.

1. The **Action** tab contains a view option, click on the view icon to view the roles that are created.

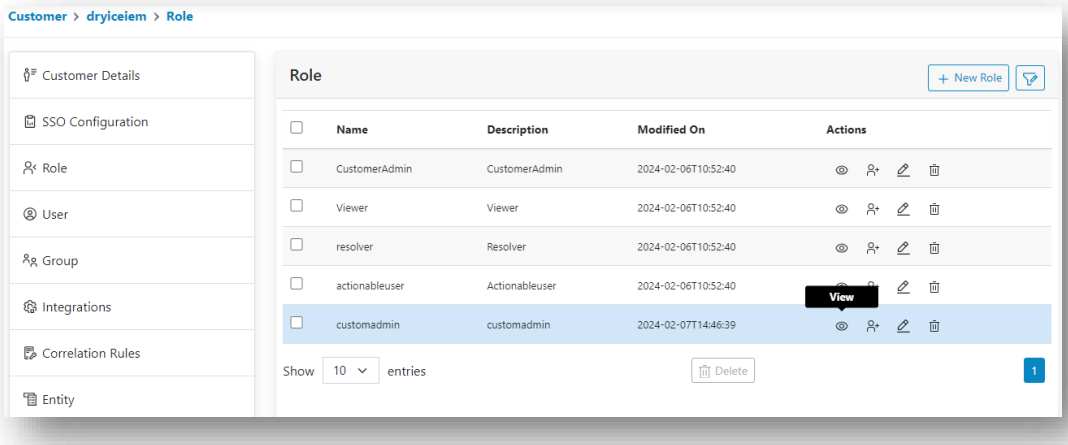

Figure 48 - View Role

2. Click on **View** for the “customadmin” role and the actions for the role will be displayed.
3. User cannot edit the role details via View option. Only the actions that are selected for the role will be displayed.

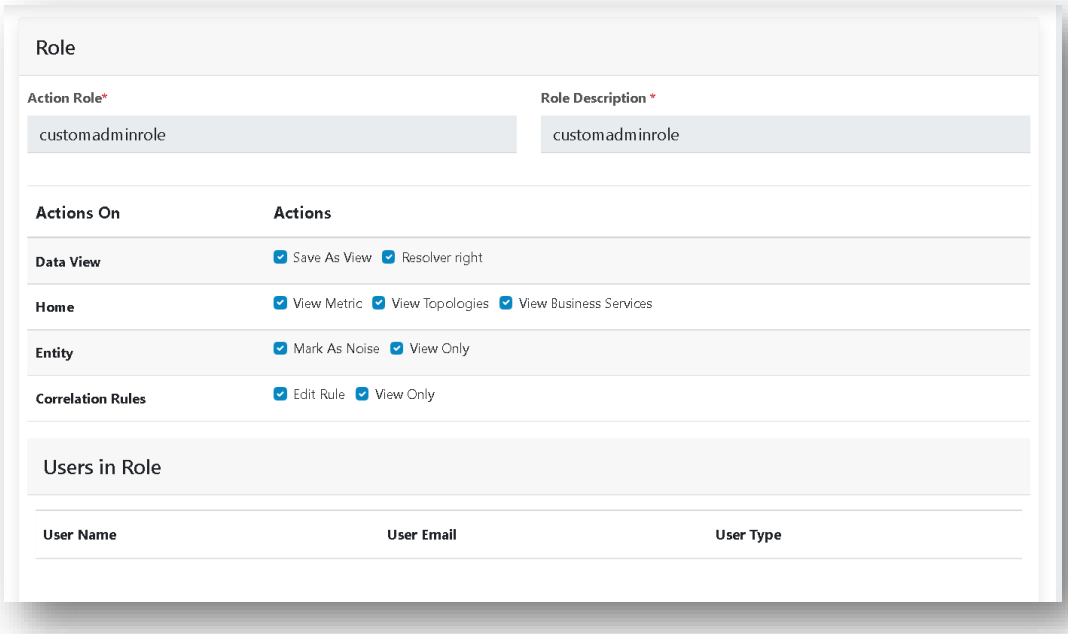

Figure 49 - Viewed Role

Assign User

This action enables user to assign users to the roles created in the environment.

1. The **Action** tab contains **Assign User** option, click on the Assign User icon to assign the roles to a particular user in the environment.

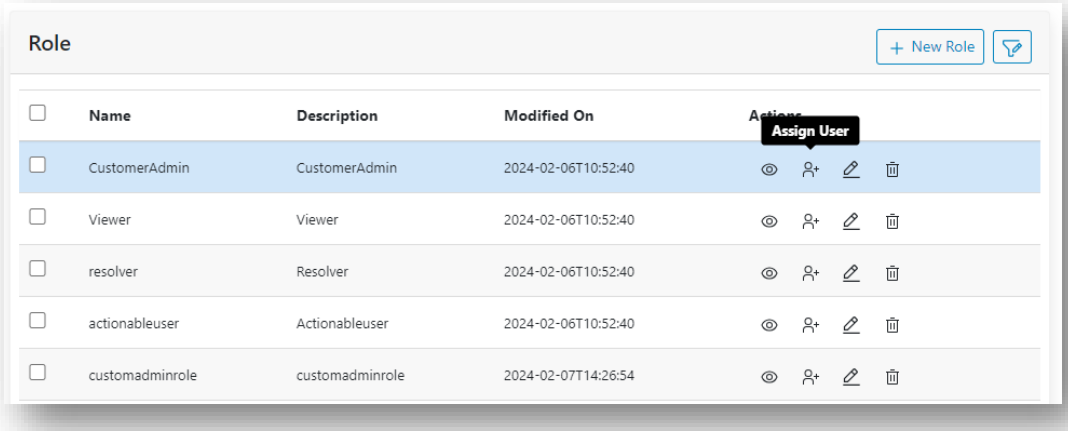

Figure 50 - Assign User

2. After clicking on the Assign User option, a pop up will be opened which will ask for User Email ID input.

Users can only be assigned by adding the User Email ID.

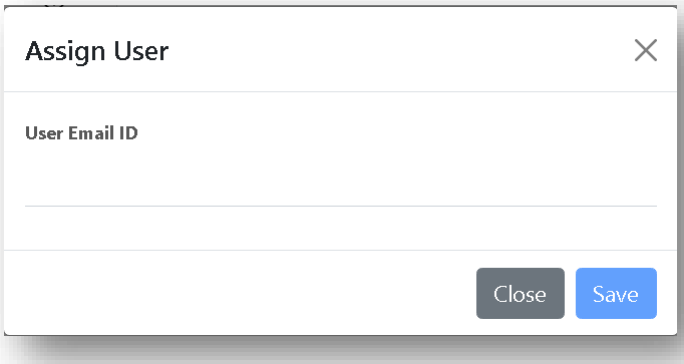

Figure 51 - Assign user Email ID

3. After adding the required User Email ID, click on the **Save** Button.

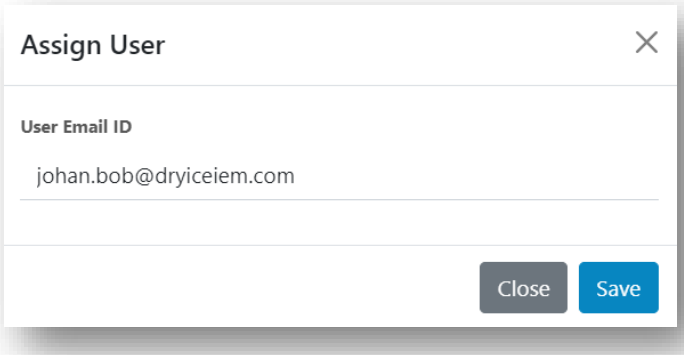

Figure 52 - User Email ID

4. On successful assignation, confirmation pop-up is displayed as shown below. User will be assigned successfully to that role.

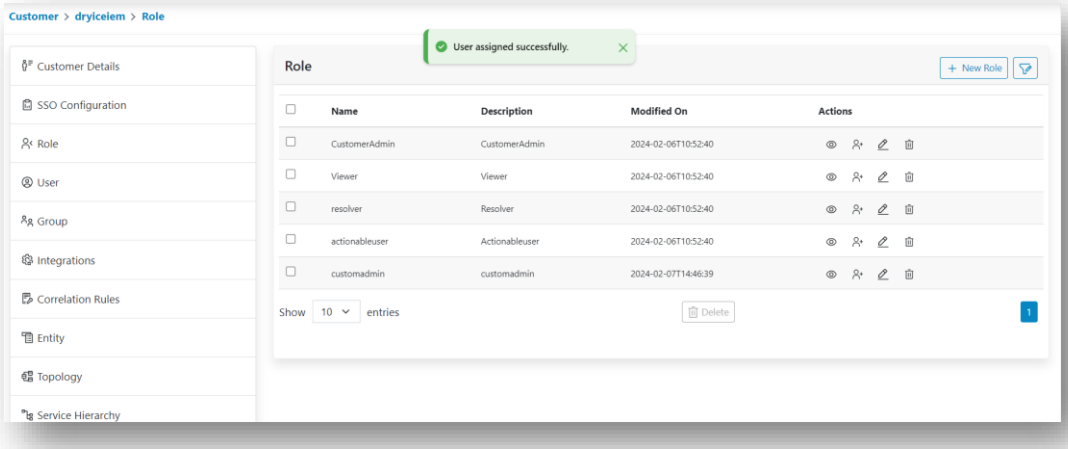

Figure 53 - Alert Message

Apply Filters

This action enables the users to apply filters on the roles created in the environment. The steps explain how to Apply filters for the Role Data:

1. Click on the Apply filter available action button present at the header of the console.

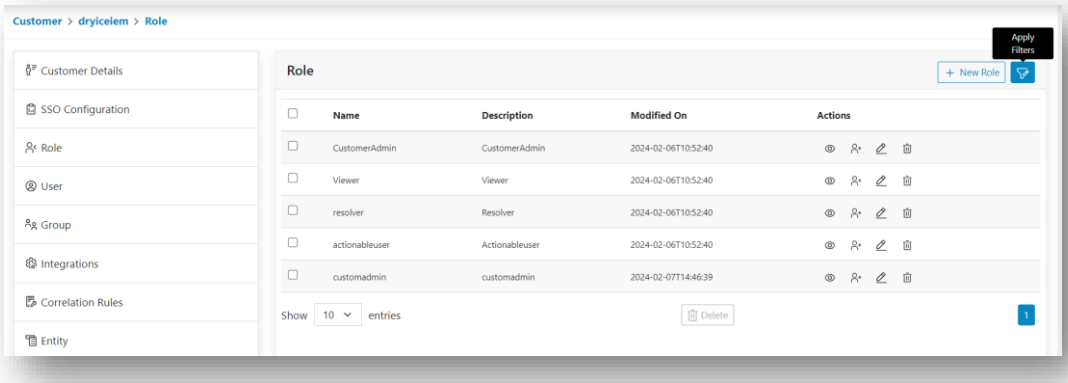

Figure 54 - Apply Filter Operation

2. The form will be appearing. From there user can select **Field** and **Operator** from drop down list and provide **Value** (The name of the Role). Then click on the **Apply** button.

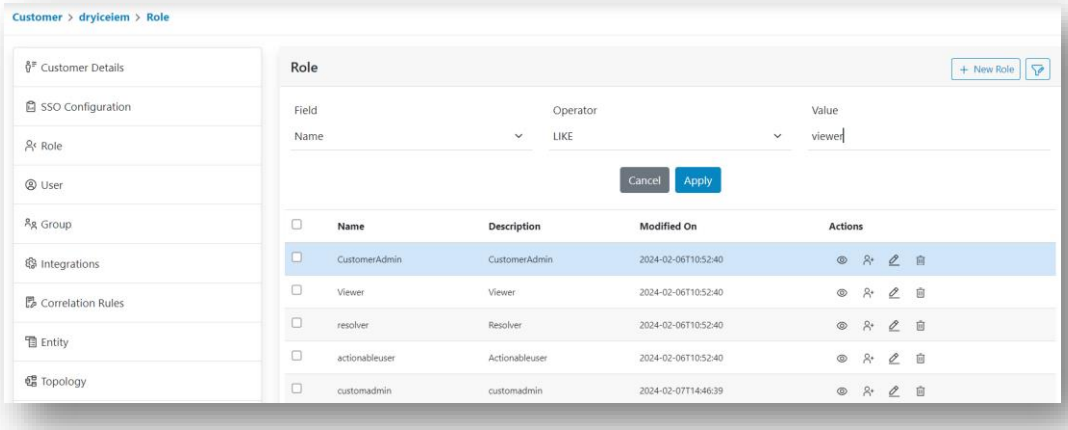

Figure 55 - Apply Filter Operation

3. User can see the result of applied filter.

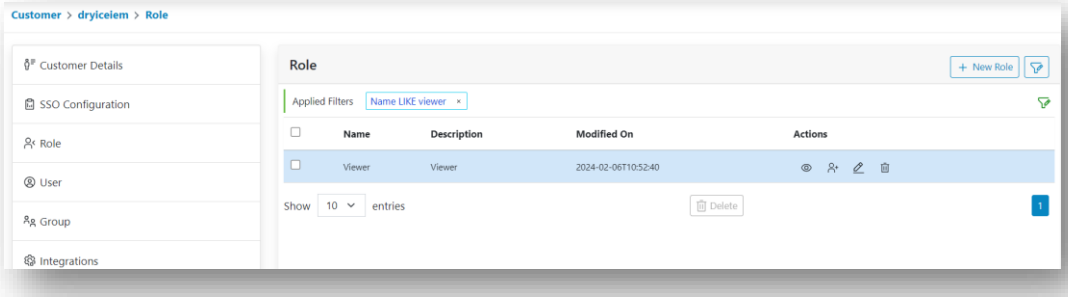

Figure 56 - Apply Filter Result

6.1.11.4 Users

"User" refers to an individual or entity within an organization who interacts with the platform to monitor, manage, and respond to events in the IT environment. Users in IEM have various roles and responsibilities, and their interactions with the system could include tasks such as configuring rules, analyzing alerts, and taking actions based on the insights provided by IEM.

This action enables us to add new users to the environment.

1. Go to the “User” option.
2. Click on “+New User” icon.

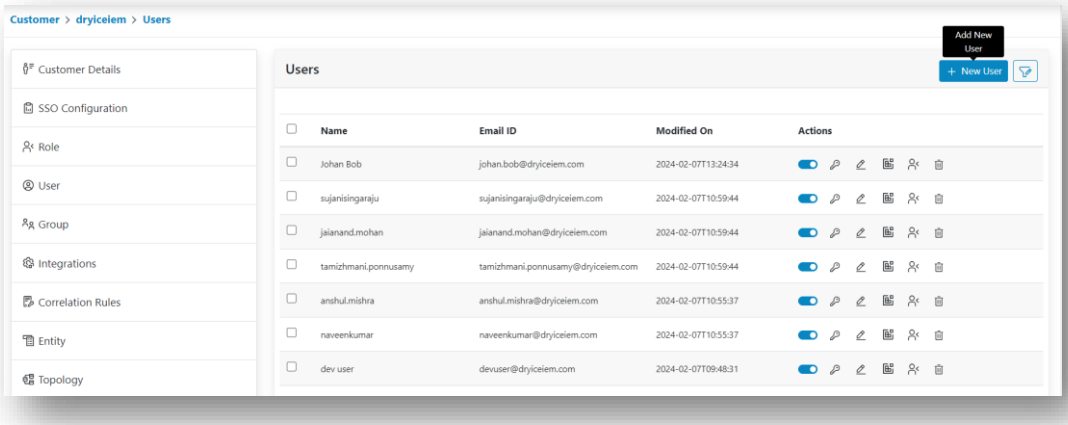

Figure 57 - Navigation for Add New User

3. The following form is displayed.

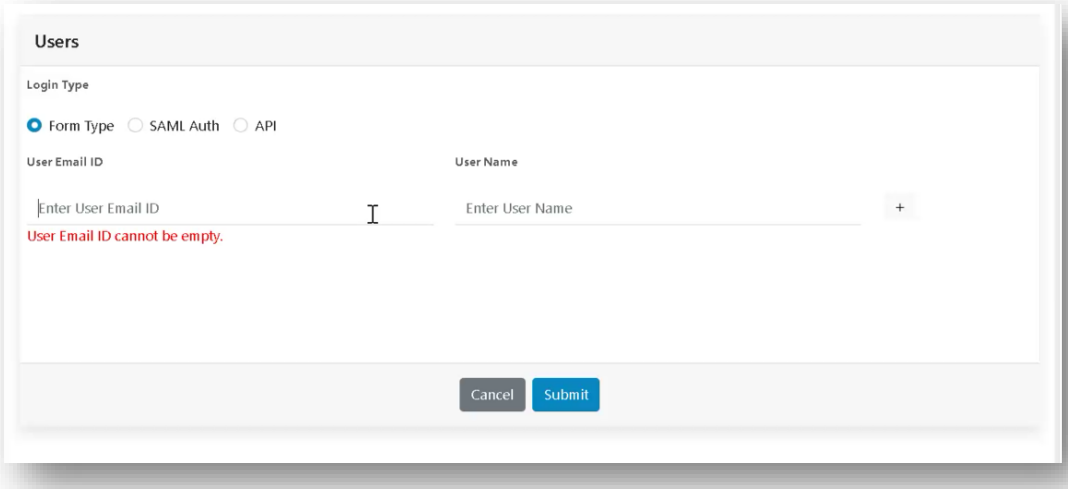

Figure 58 - Create a User

4. User needs to select the particular login type and enter a valid **User Email ID** and the **User Name**.

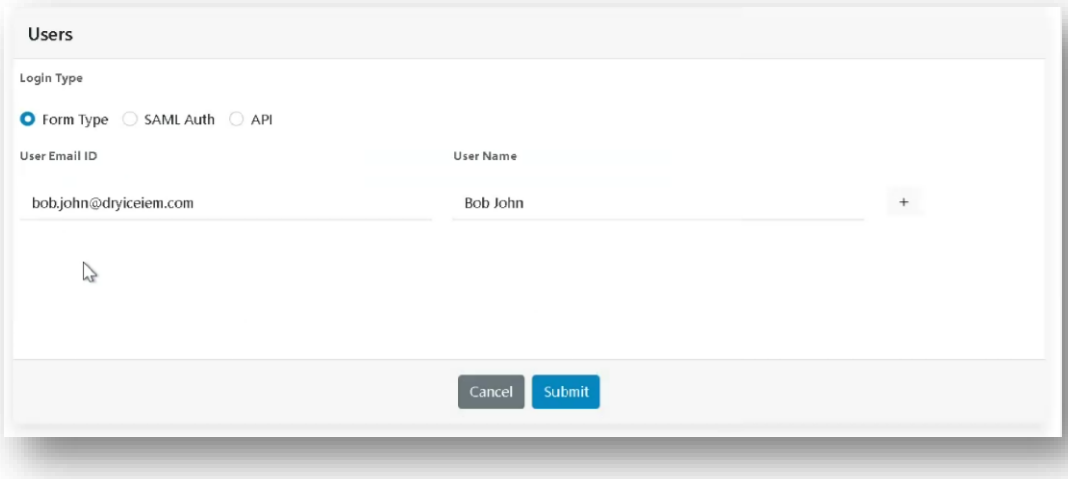

Figure 59 - User Email Id

Follow the validation check prompts to ensure that the email id provided is valid.

5. Provide the full name for the user.

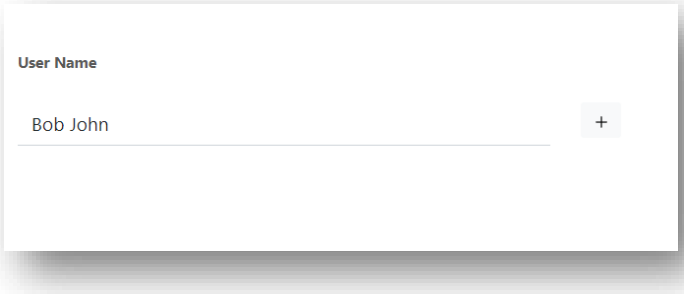

Figure 60 - Username

6. Click on **Submit**.

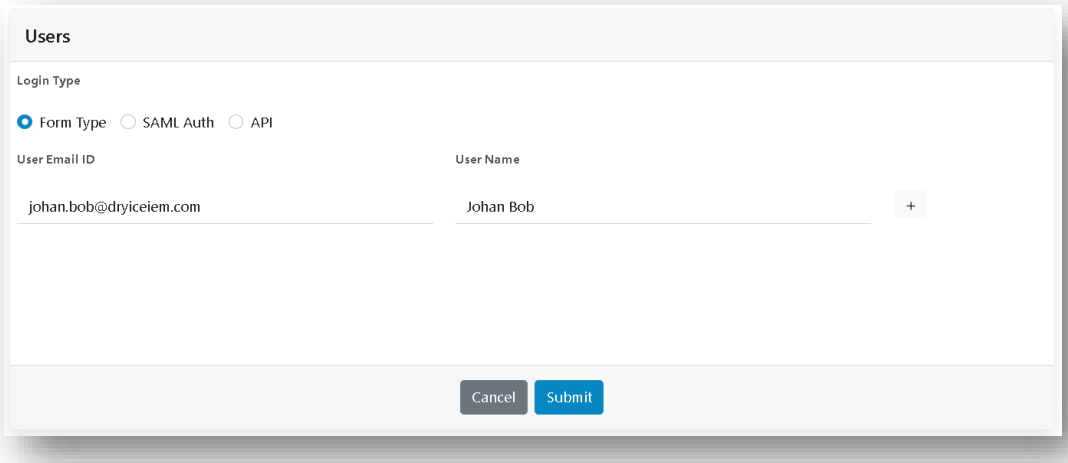

Figure 64 – Submit Button

7. On successful creation, a confirmation pop-up is displayed as shown in the following figure:

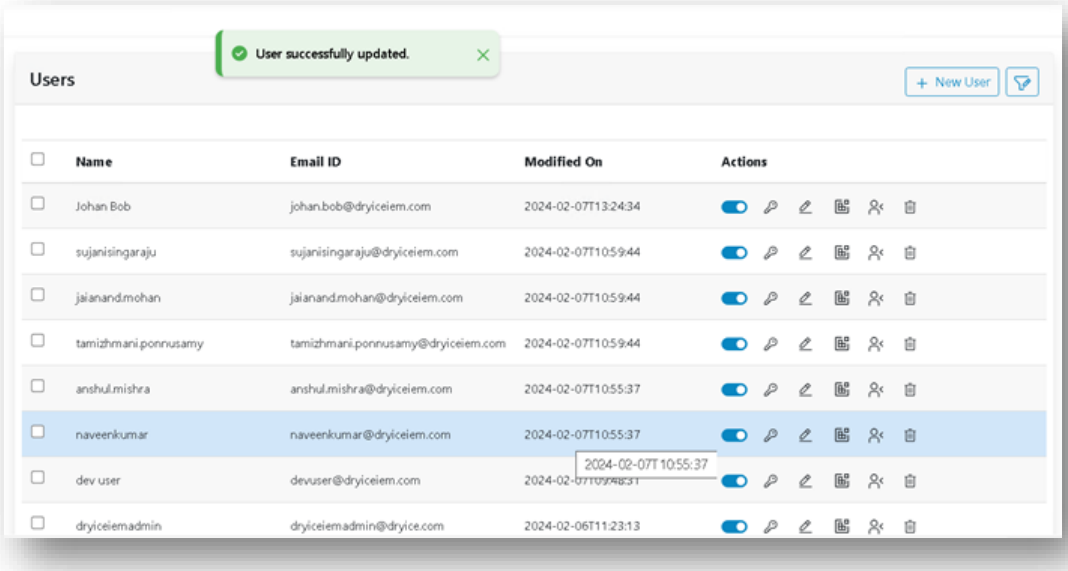

Figure 61- Alert Message

Generate Password

This step enables users to create the password for the user.

1. Click on **Generate Password** icon next to the user for whom the password is to be generated.

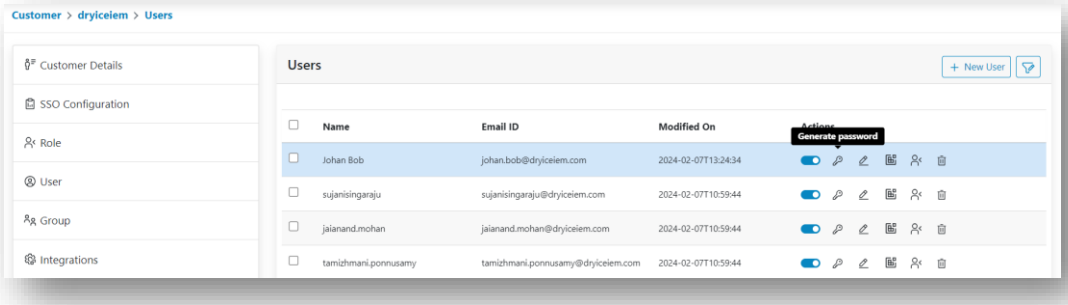

Figure 62 - Generate Password for User

2. The following pop up is displayed.

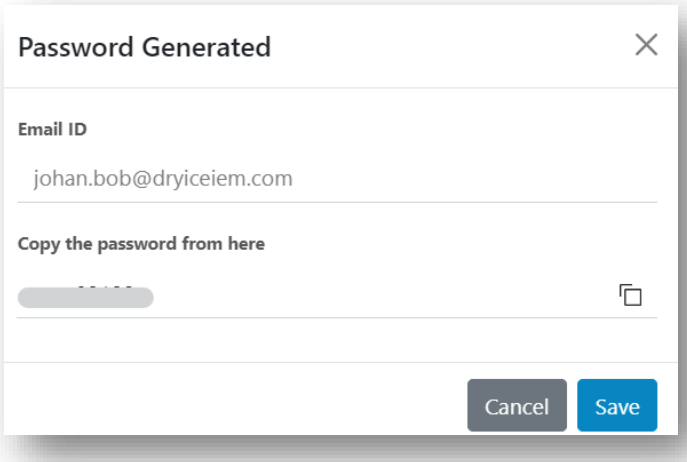

Figure 63 - Copy Password

3. A system generated random password is displayed. Change it if required else copy it by clicking on the Copy icon next to the password.
4. Click on **Save** to update the new password for the user.
5. On successful update the following confirmation is displayed.

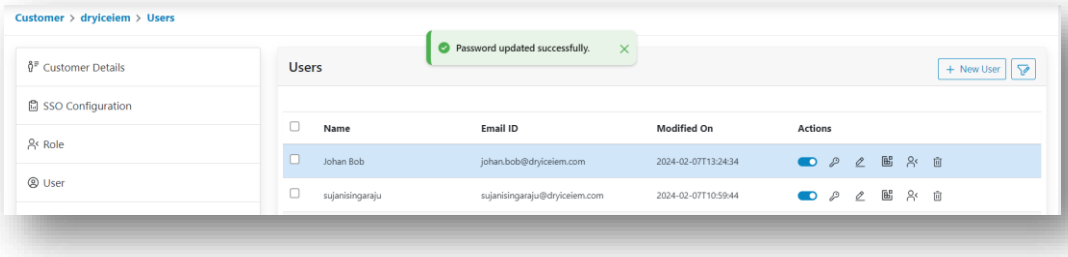

Figure 64 - Alert Message

6. Now the password can be shared with the user one to one.

Manage Users

This section contains the steps to Manage users.

1. Click on “Customer” → “Customer Name”→ “Users”
2. A navigation menu bar on the left side will be visible. Click on the “**User**” Tab.
3. On clicking on the User from the menu the following form is opened:

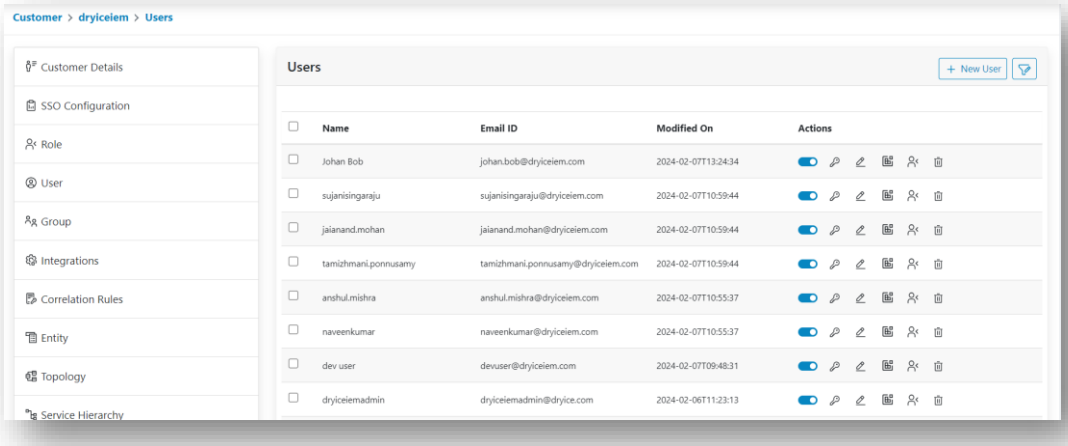

Figure 65- User Page

4. All the available users created in the environment are listed in the grid view.

When the user screen is accessed for the very first time only the superadmin user will be displayed. Like with the other pages user can perform action on the page based on the role assigned.

Edit User

This action enables users to edit an existing user in the environment.

1. Click on the edit icon next to the user whose details are to be modified.

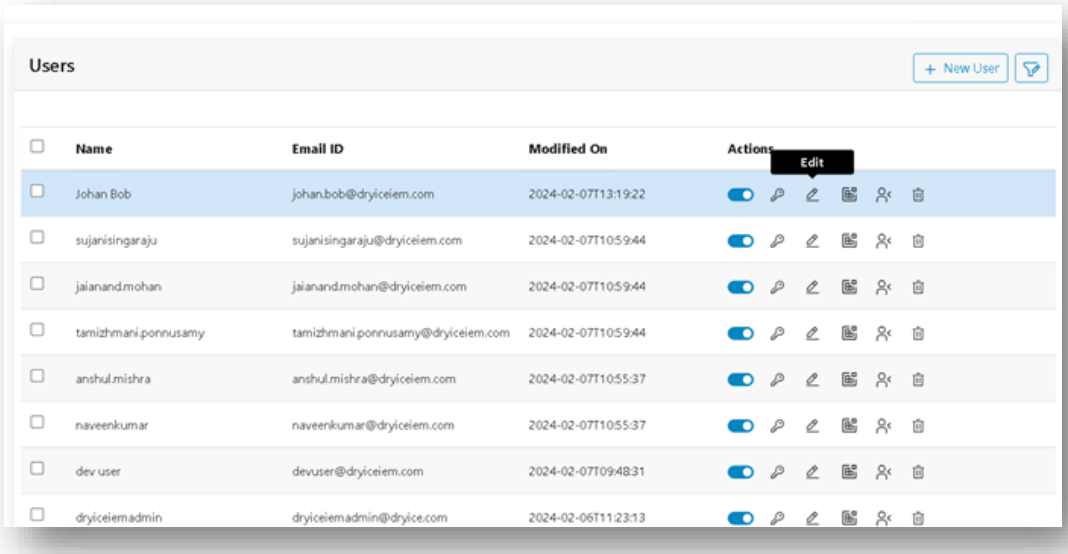

Figure 66 - Edit User

2. The form will appear with the saved details as shown.

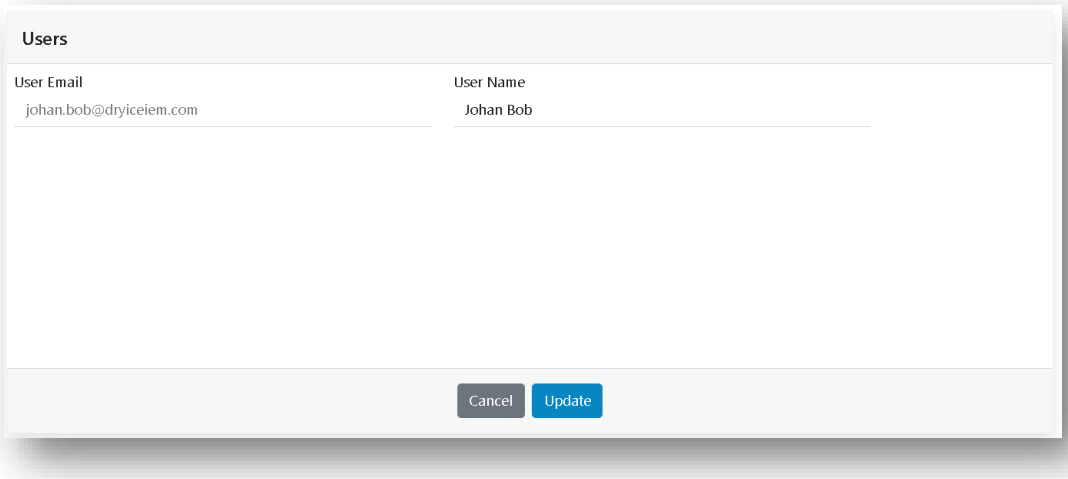

Figure 67 - Edit Details

3. Except the email id, remaining details can be modified the way it was done while adding a new user.
4. After editing click on the **update** button.

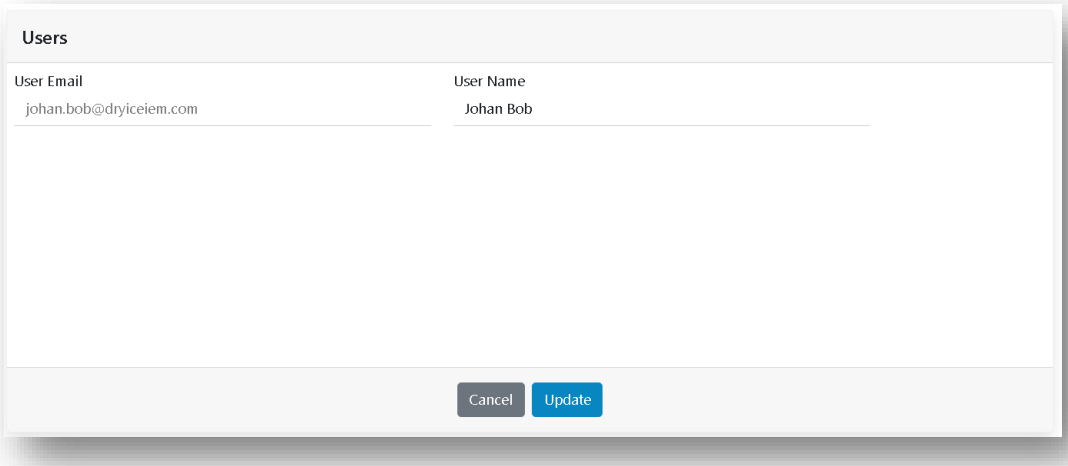

Figure 68 – Update button

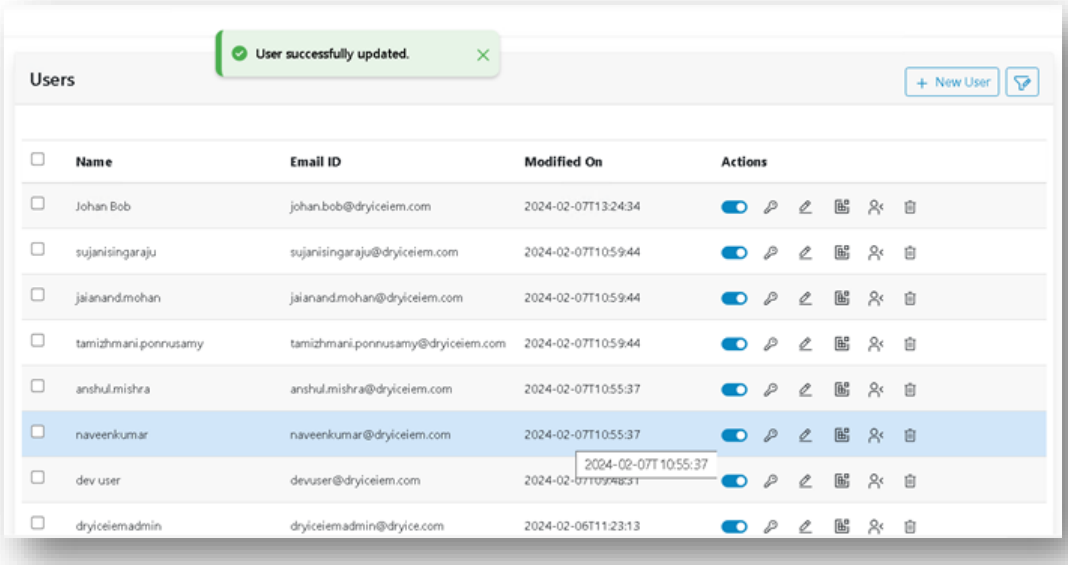

Figure 69 - Alert Message

5. On successful update a pop-up message is prompted as shown in the above image.

Delete User

1. Go to the **User** Tab.
2. User can select the one or more users and delete the users. Select all the users to be deleted from the system. After selecting the users click on **Delete** button shown below the data table.

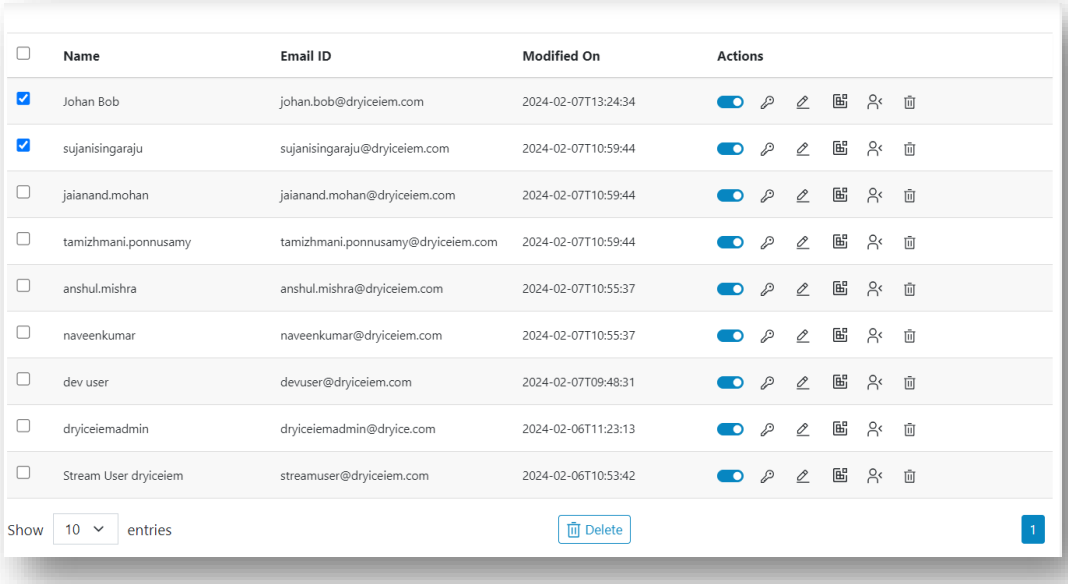

Figure 70 - Delete User

3. User can also delete the user by clicking on the delete icon shown next to the user.

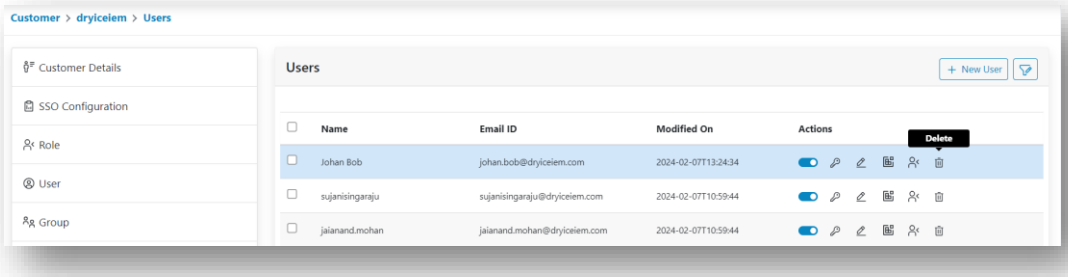

Figure 71 - Delete User

4. User will be prompted to confirm the deletion. Click on the confirm button.

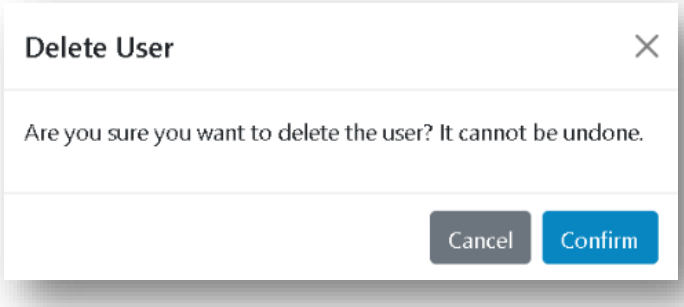

Figure 72 - Confirmation pop-up

5. On success a confirmation pop-up message will be displayed.

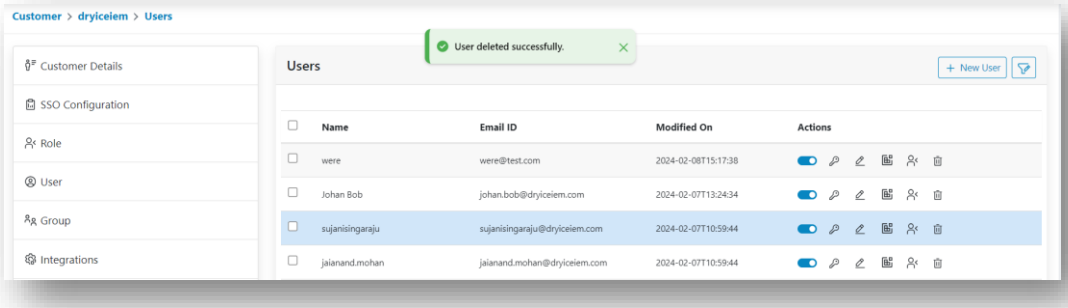

Figure 73 - Alert Message

Assign Group

1. Click on the **Group** icon next to the user to assign the Group.

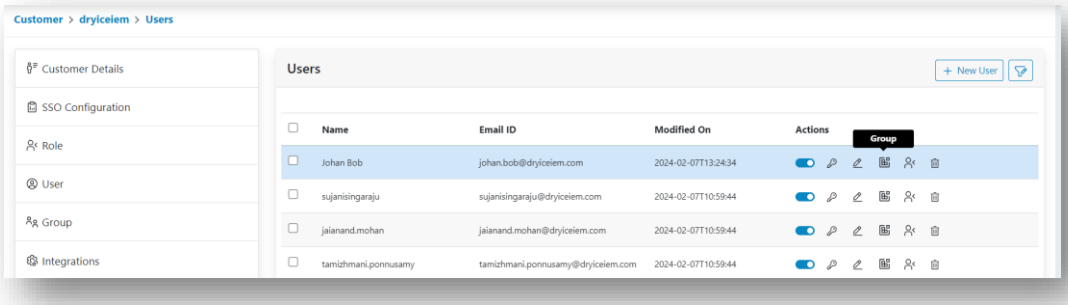

Figure 74 - Assign Group to a user

2. The form will appear with the saved details as shown.

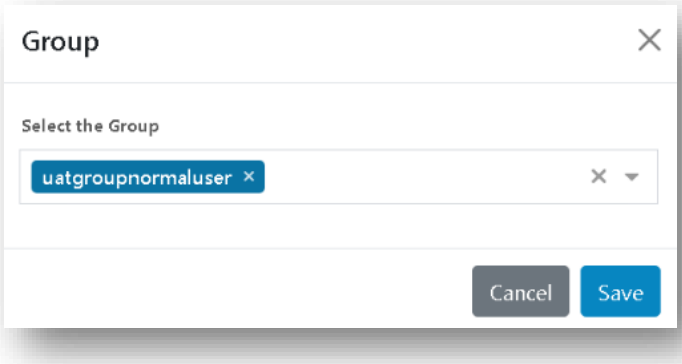

Figure 75 - Group Dropdown

3. User can select one or more groups from the dropdown. Click on the **Save** button.

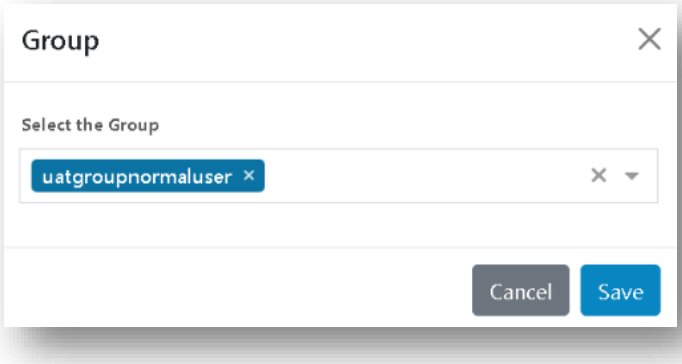

Figure 76 - Selecting the Group for the Dropdown

4. On successful assignation for group the following pop-up message is prompted.

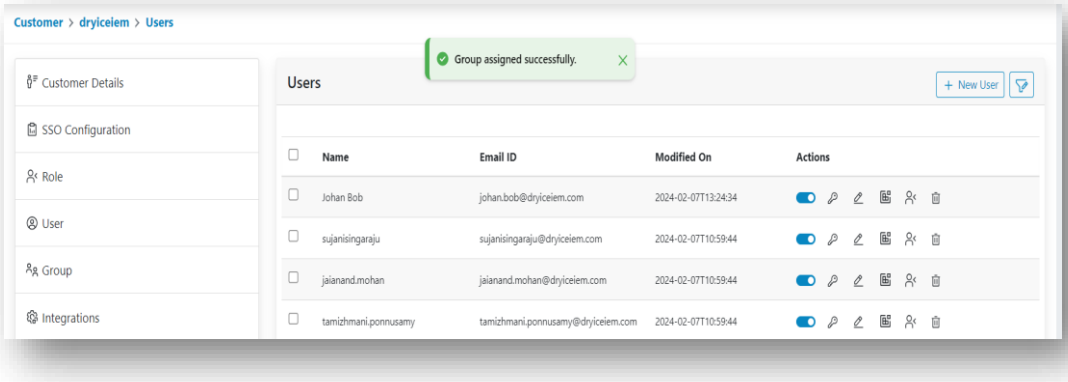

Figure 77 - Alert Message

Assign Role

1. Click on the **User Role** icon next to the user to Assign Role.

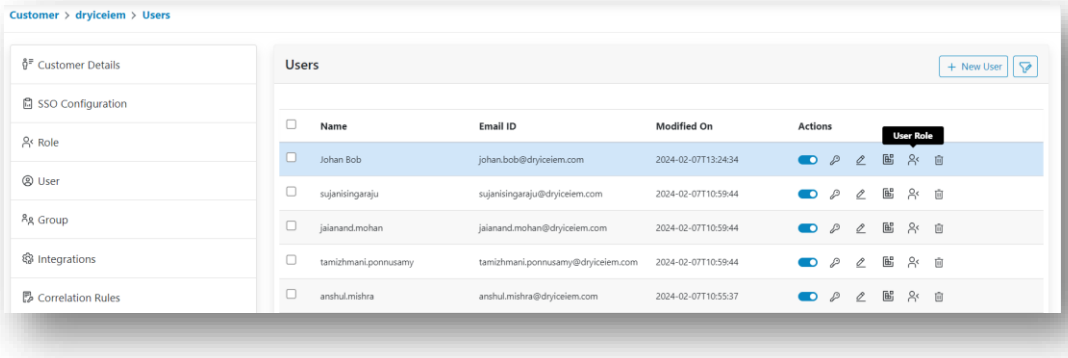

Figure 78 - Assign role

2. The form will appear with the saved details as shown.

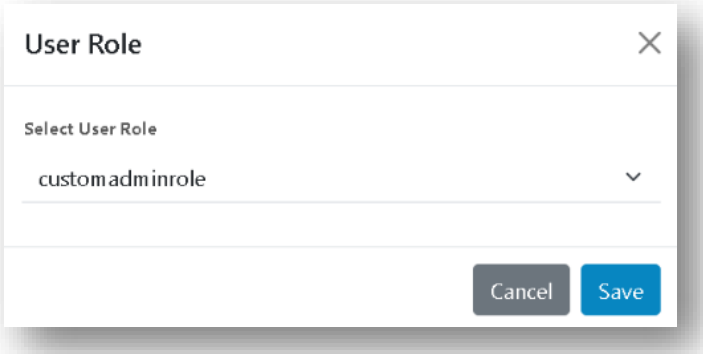

Figure 79 - Role Dropdown

3. Users need to select **User Role** from the dropdown. Click on the **Save** button.

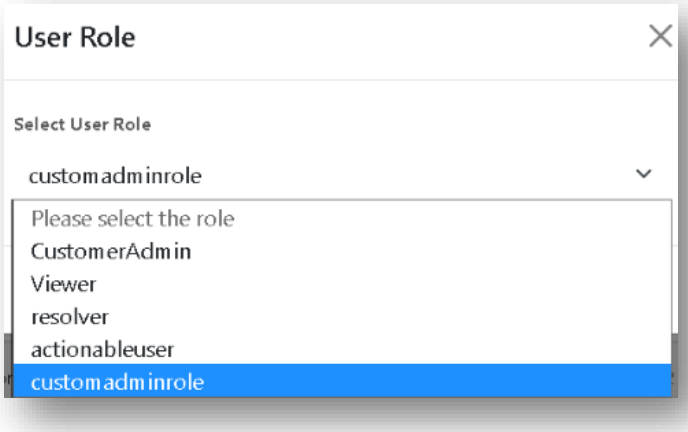

Figure 80 - Selecting User Role Dropdown to a User

4. On successfully assigning the role, the following pop-up message would be prompted.

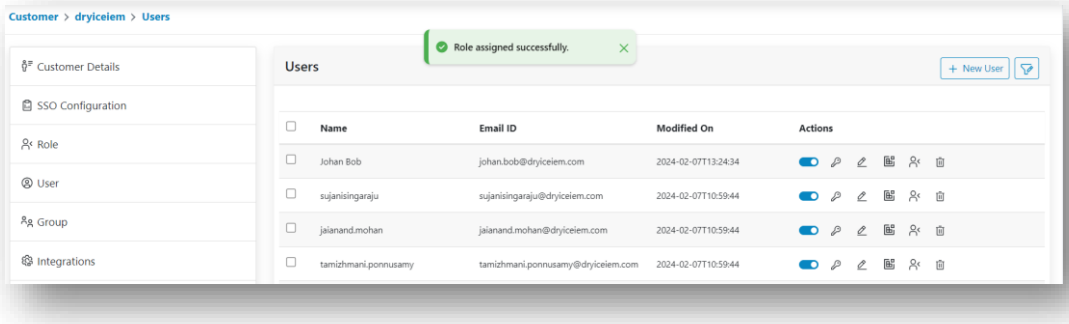

Figure 81 - Alert Message

Enable/Disable User

1. Click on the **User** Tab.

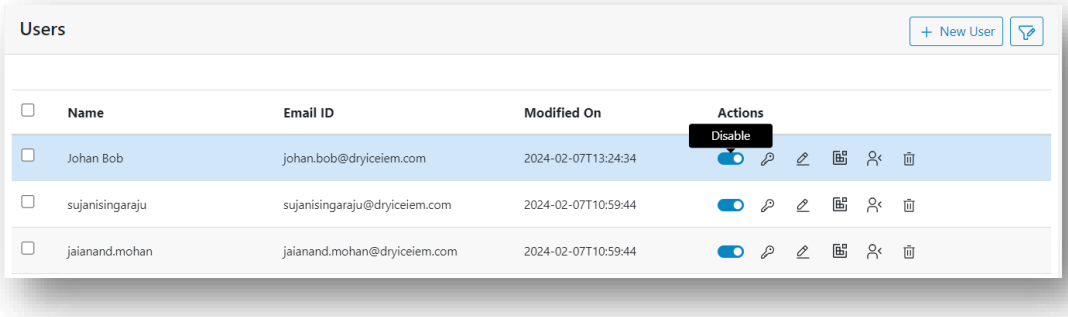

Figure 82 - Enable /Disable User

2. Click on the **Enable/Disable** toggle button next to the user that needs to be Enabled/Disabled.
3. On success, a confirmation pop-up message will be displayed.

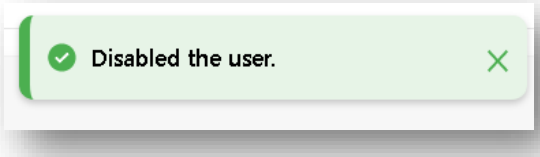

Figure 83 – Confirmation of User Disabled

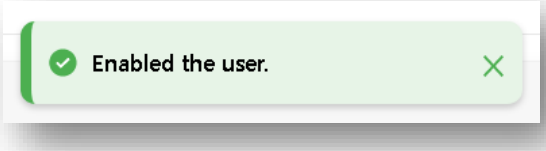

Figure 84 - Confirmation of User Enabled

Apply Filters

This action enables users to apply filters to search users created in the environment. The steps explain how to Apply filters for the User Data:

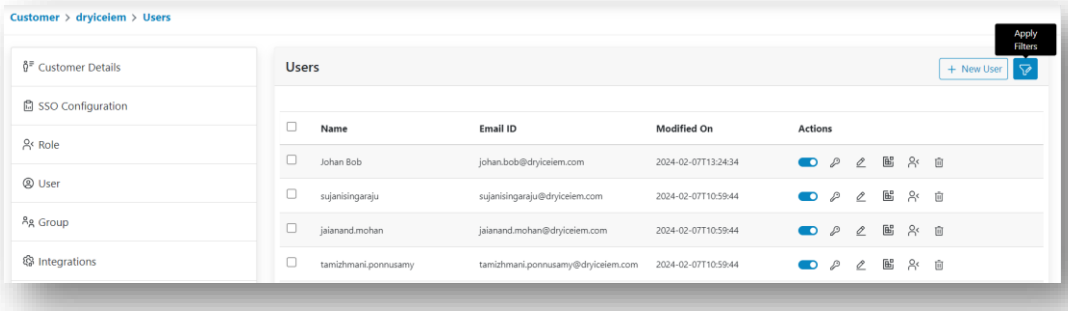

Figure 85 - Apply Filter Operation

1. Click on the **Apply Filter** action button present at the header of the console.

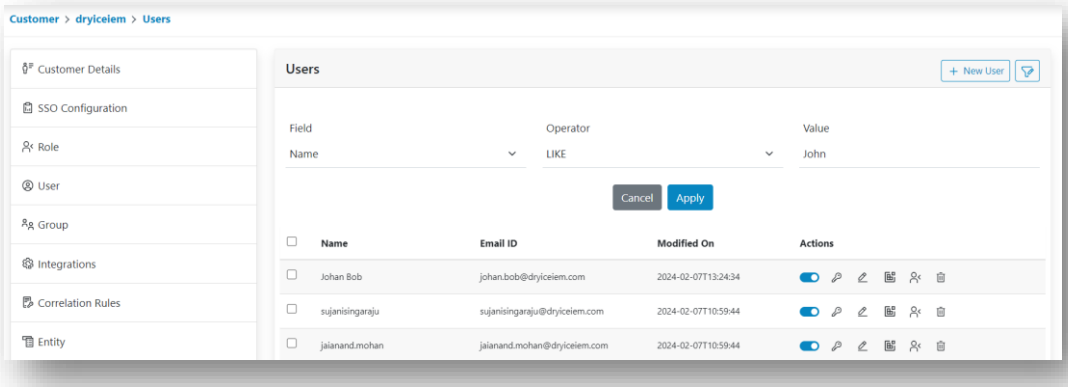

Figure 86 - Applying Filter Operations

2. The **Users** form that appears. Select **Field** and **Operator** from drop down list and provide **Value**. Then click on the **Apply** button.
3. User can view the result of the applied filter once user clicks **Apply** button.

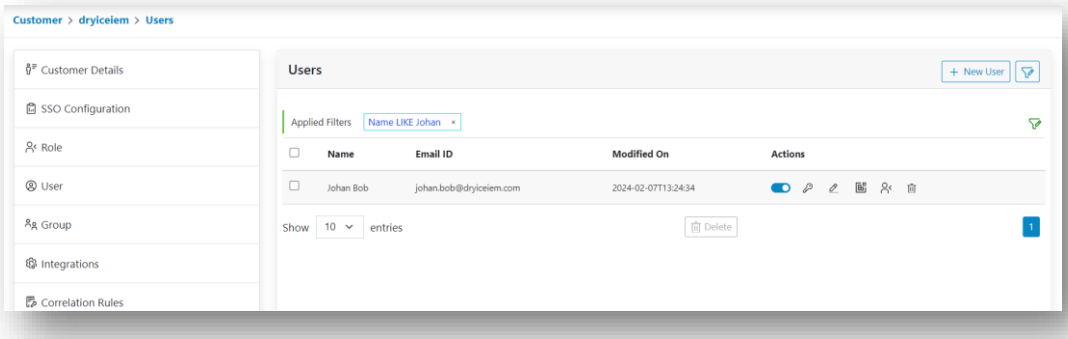

Figure 87 - Apply Filter Result

6.1.11.5 Group

This section enables to Manage groups. Groups are primarily used for controlling data access on the main user view i.e., Data View. In addition to the customer check if user need to restrict further the data visible to user based on other fields, then group menu is used for achieving the same.

1. Click the customer onboard section (Please refer the hyperlink given below), for customer, click on customer action edit section. Click on the Group page, Group menu item to access this page. As user click on the menu item the following form is opened.

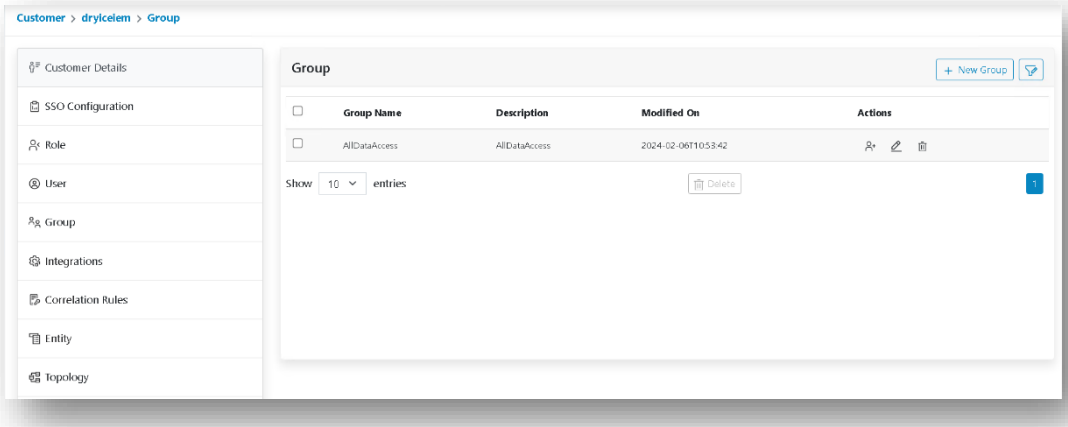

Figure 88 - Group Page

2. Groups created in the environment will be listed in the grid view.

When users access it for the first time, no group is displayed.

Add New Group

1. Click on the **Customer** Tab and then the **Customer Name** (In this case “AlphaCustomer”)
2. Click on the **Group** Tab.
3. At the right side on the top Click on **+ New Group** icon.

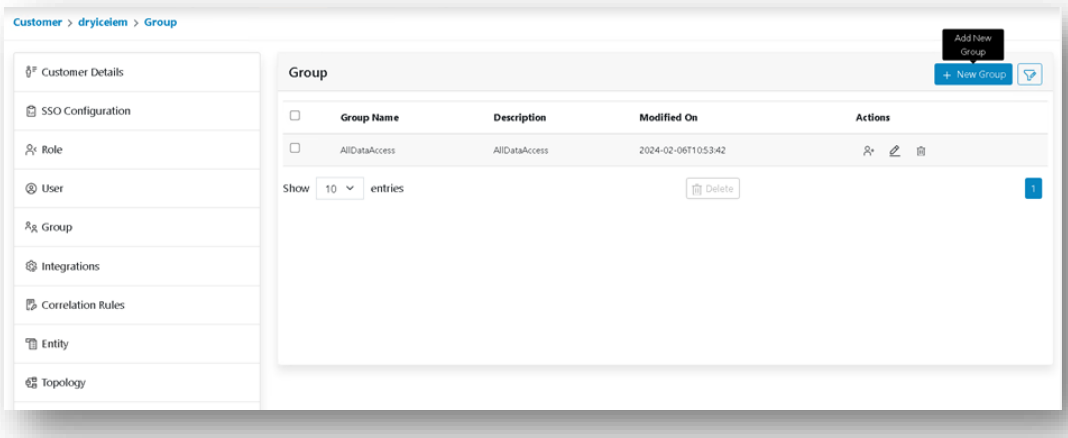

Figure 89 - Navigation Page for Group

4. A new form will appear.

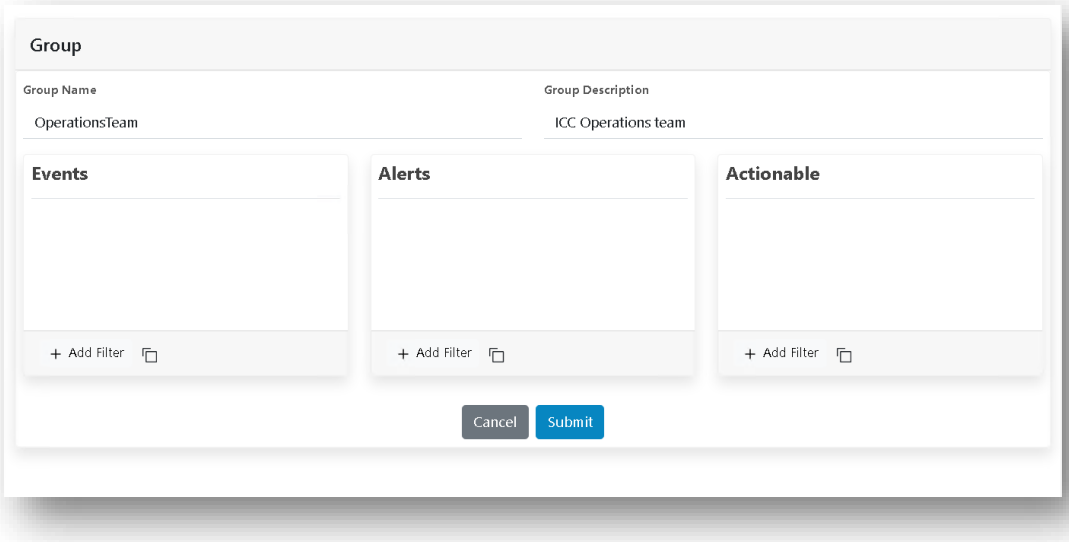

Figure 90 - Create a Group

5. On the above page specify the **Group Name**.

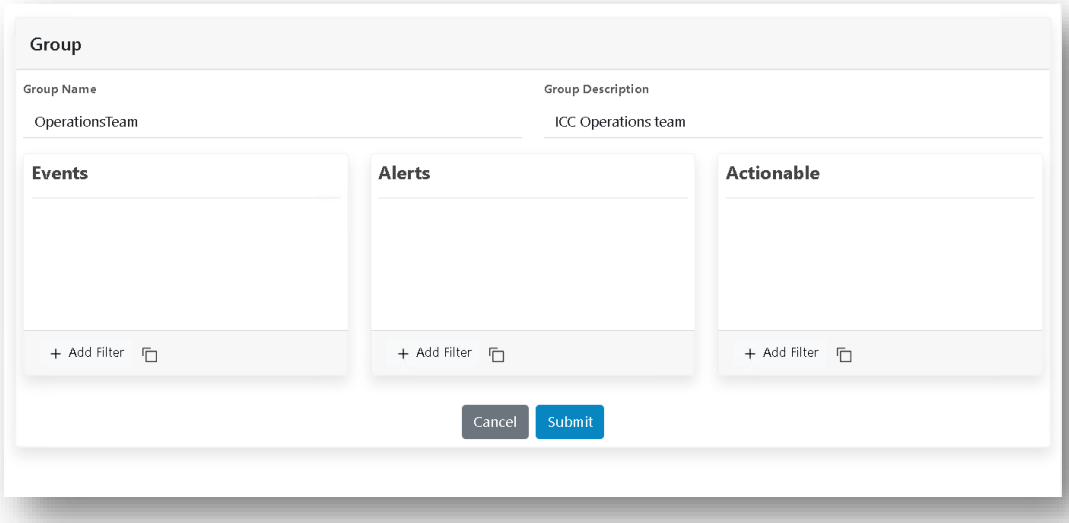

Figure 91 – Add Filter

6. Next, user can specify the data filter. Click on the Edit icon next to the Dataset for which the data restriction is to be enabled.
7. A Data filter is used as a condition to limit the data view into a group for which it was specifically created, the filter conditions will be shown in the below steps.
8. Click on the **Add** icon. The following pop-up will be enabled.

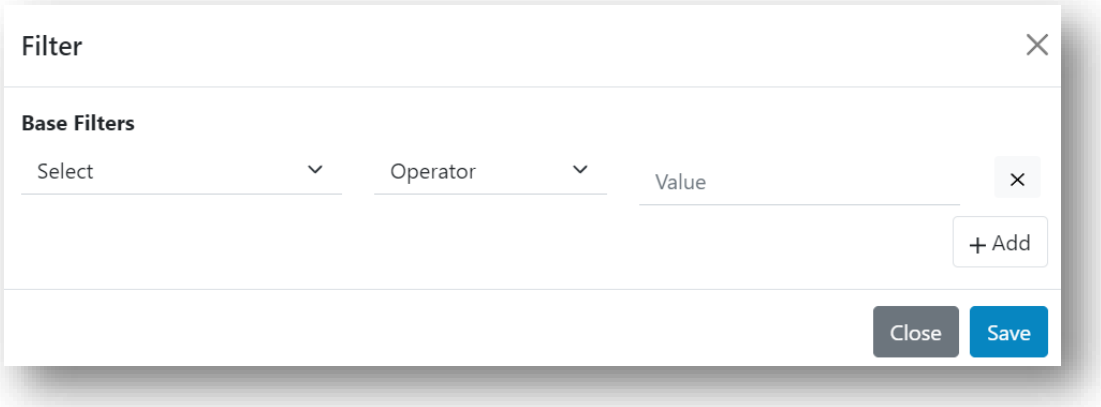

Figure 92 - Filter for Group

9. The field dropdown lists all the available fields of the selected dataset.

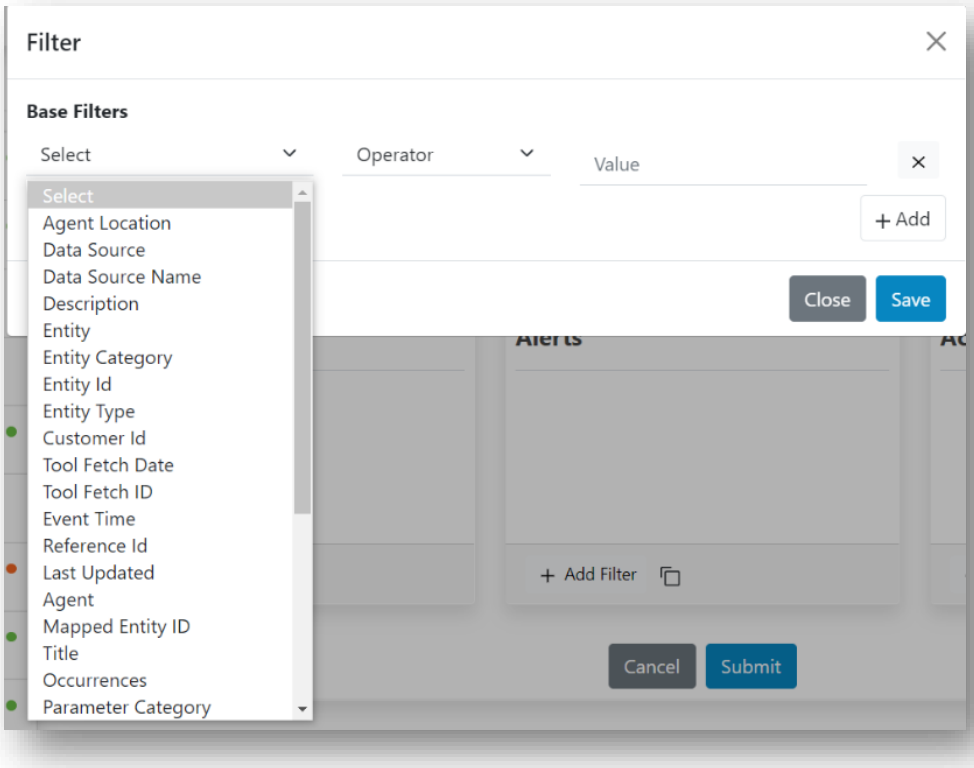

Figure 93 - Dropdown for fields

10. As the field is selected, the operator dropdown is populated based on the field data type.

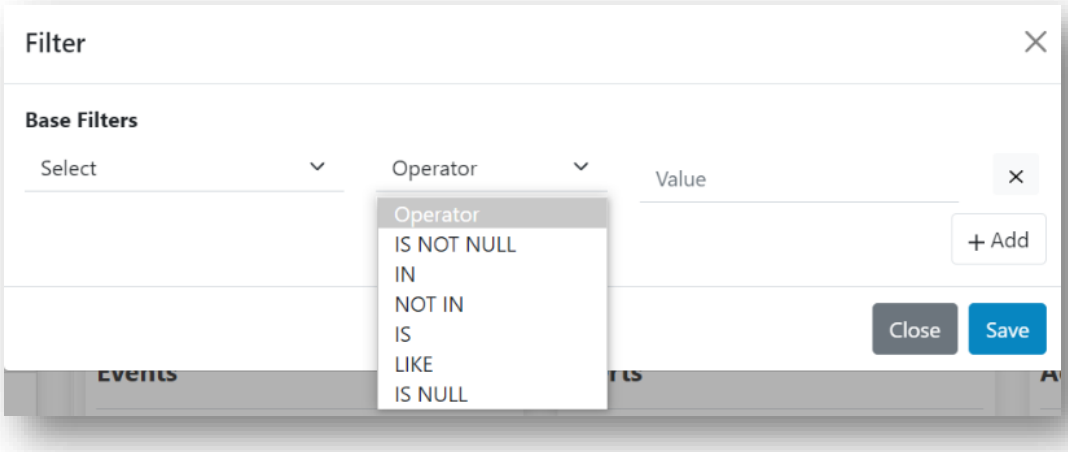

Figure 94- Dropdown for Operator

11. Based on selected **Field** and **Operator**, provide the **Value** in the Value field.

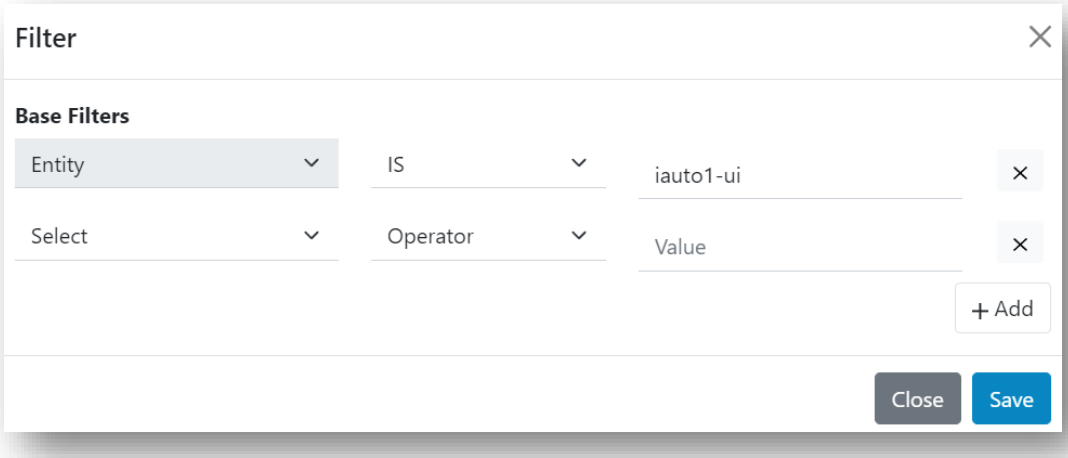

Figure 95 - Add Base Filters

12. In the above example, the user has added “Entity” like “iauto”, which means the events of the “iauto” console only will be forwarded to this group, rest events would be dropped off.
13. User can also add more conditions for adding more conditions by clicking on **+Add** button. Once the “+Add” button is clicked a new row appe ars as shown in the above image.

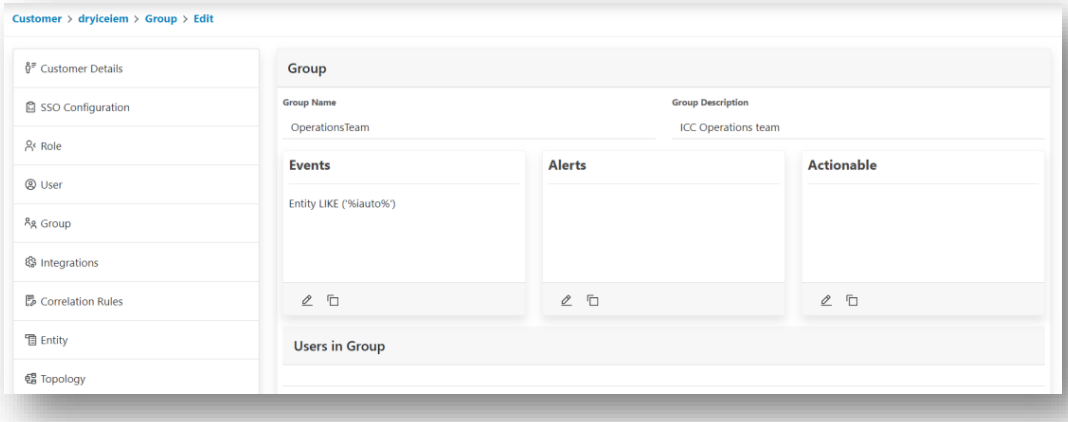

Figure 96 - Alert Message

14. Once all the conditions are specified, click on **Save**. On success the following pop-up message will be prompted.

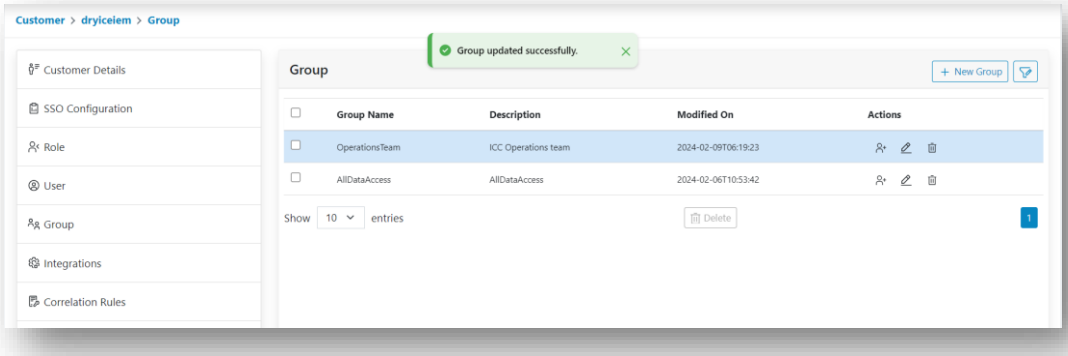

Figure 97 - Alert Message

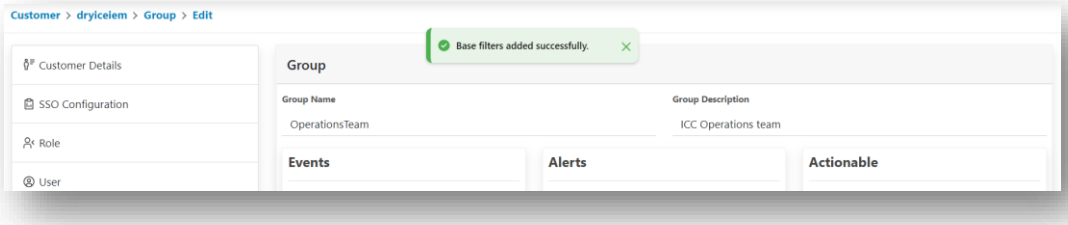

Figure 98 - Alert Message

15. Close the success message. The condition will start appearing next to the dataset as shown:

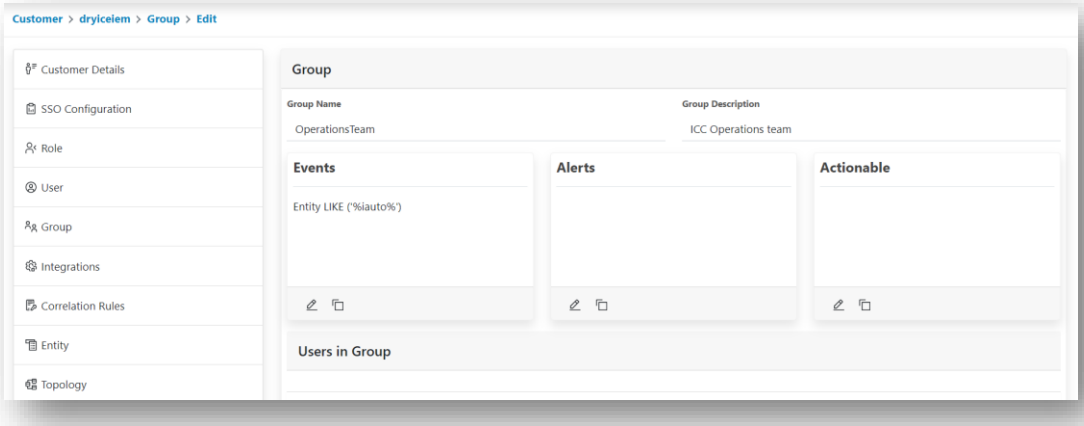

Figure 99 - Add New Group

16. For the other datasets as well, user can use the same method to create the conditions. However, user do have copy action available, if the same criteria are to be applied across datasets, click on copy icon next to the dataset for which condition is to be copied as shown in the below image.

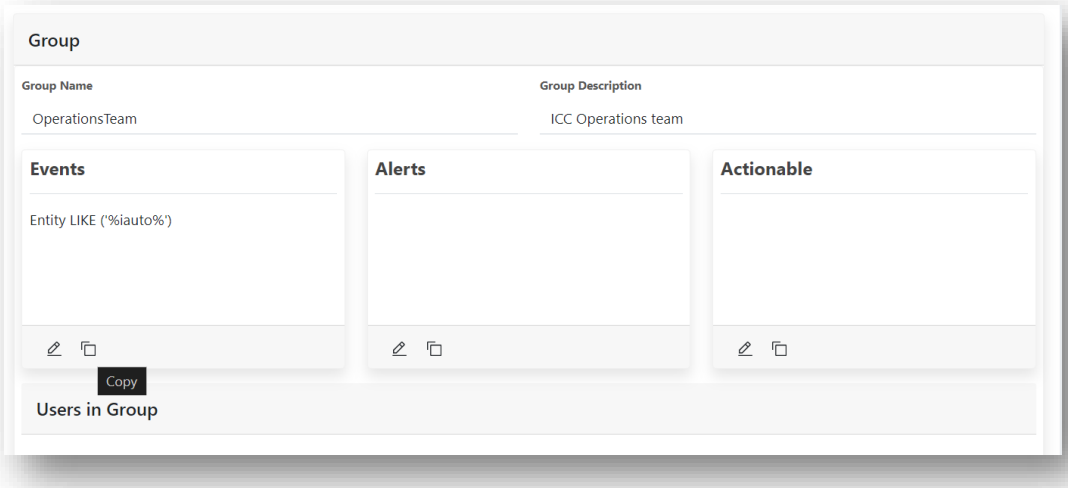

Figure 100 - Copy Event Filter

17. On clicking copy, the following popup is displayed, select the filter where the data is to be copied.

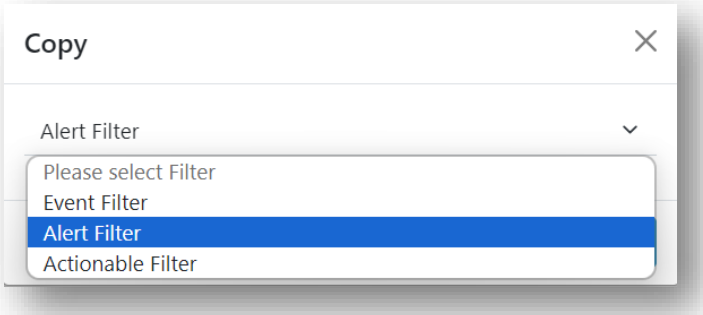

Figure 101 - Copy Expression

18. After specifying the filter, click on the **Save** button.

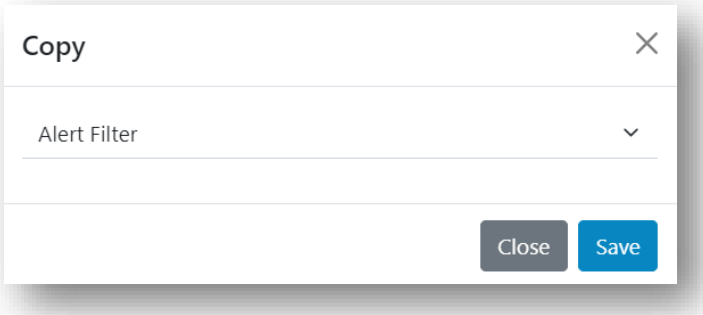

Figure 102 - Selecting Copy Expression

19. On success the following pop-up message is prompted.

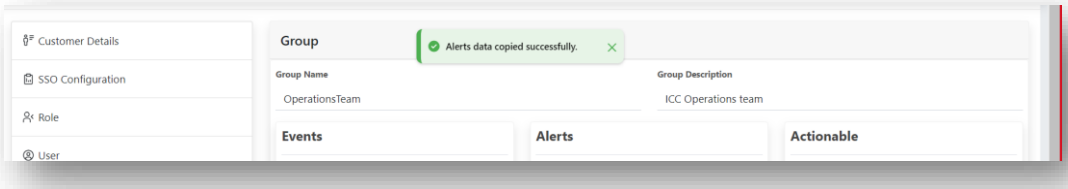

Figure 103 - Alert message

20. The filter criteria can be copied to the next dataset filter as well.

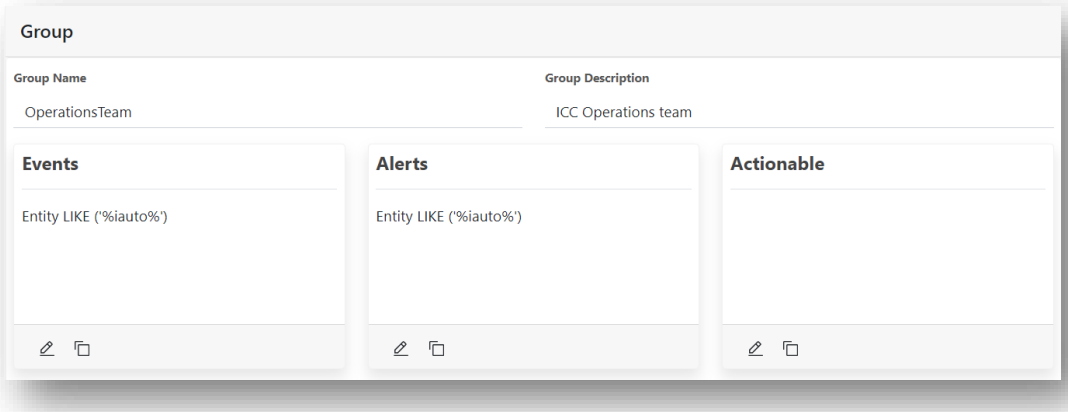

Figure 104 - Alerts Filter

21. Once all the data filters are applied, click on Submit.
22. On successful creation the following message is prompted to user.

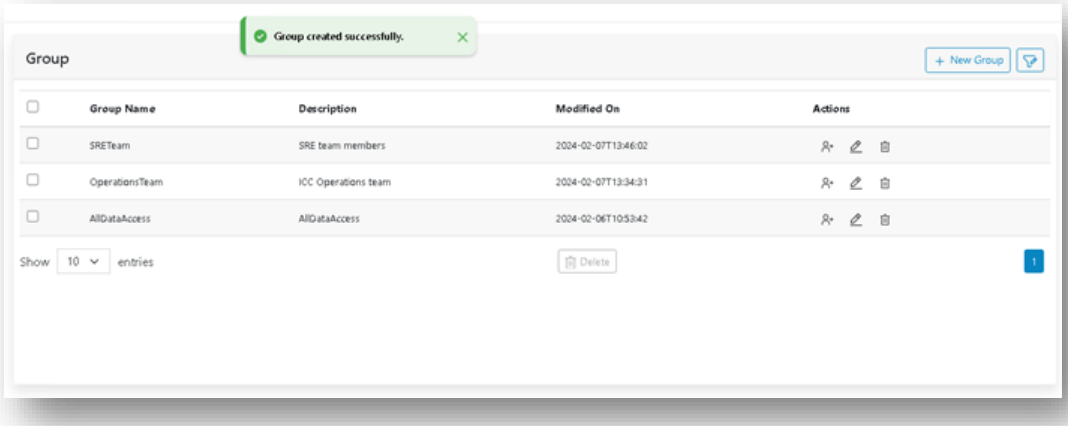

Figure 105 - Alert Message

23. The control will be redirected to the grid view with the new group listed.

Edit Group

1. Click on the edit icon next to the group to be edited as shown below:

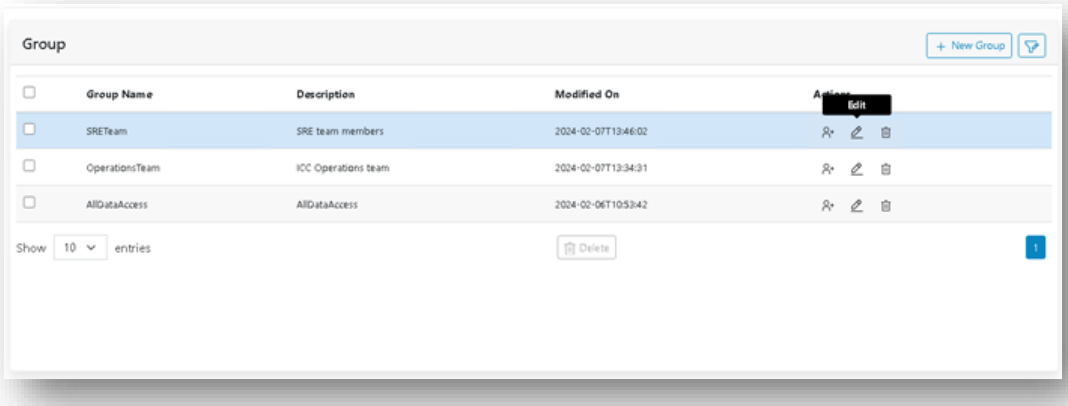

Figure 106 - Edit Group

2. The form will appear prefilled with the saved data.

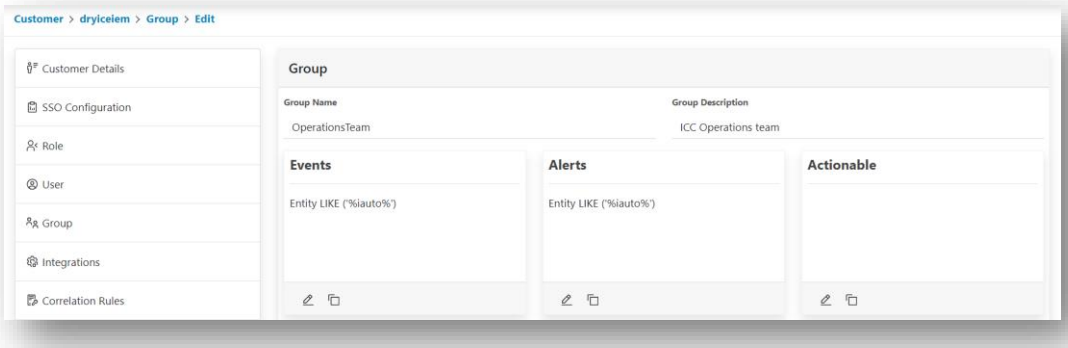

Figure 107 - Edit Filter

3. User can edit the name or update the filter criteria's the way user did while adding new group.

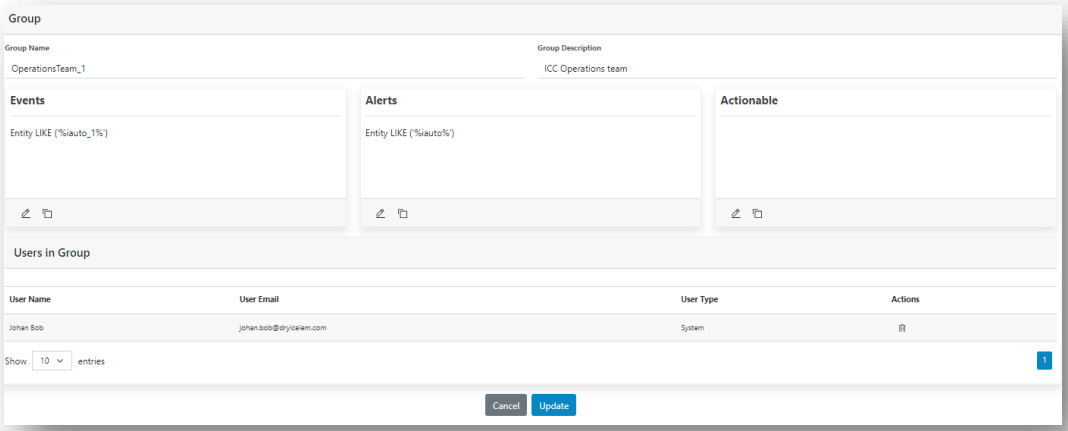

Figure 108 - Update Group Name and Filter

4. In the above figure, the Group Name is updated to OperationsTeam_1. There is additional filter updated under Events filter from iauto to iauto_1.
5. Once all the fields are updated, click on Update.
6. On successful update, the following confirmation pop-up message is displayed.

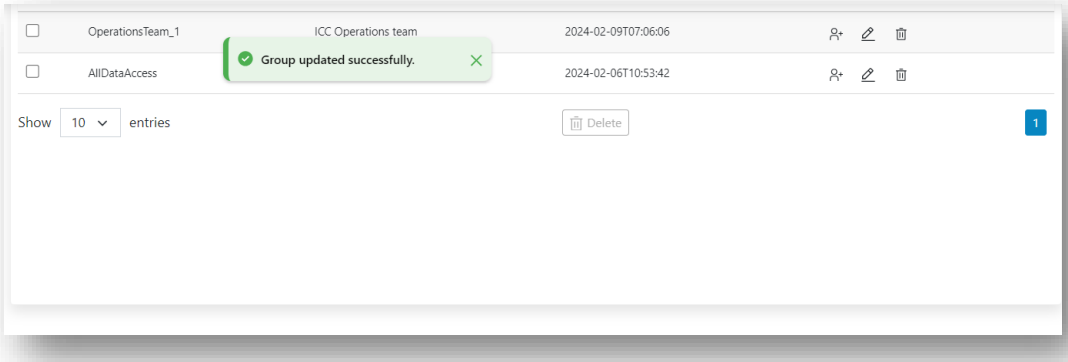

Figure 109 - Alert Message

7. Close the success message. The control will be redirected back to the grid view.

Delete Group

User can delete the group individually or using the bulk delete option. Let's look at the individual delete option first.

1. Click on the delete icon next to the group that is to be deleted.

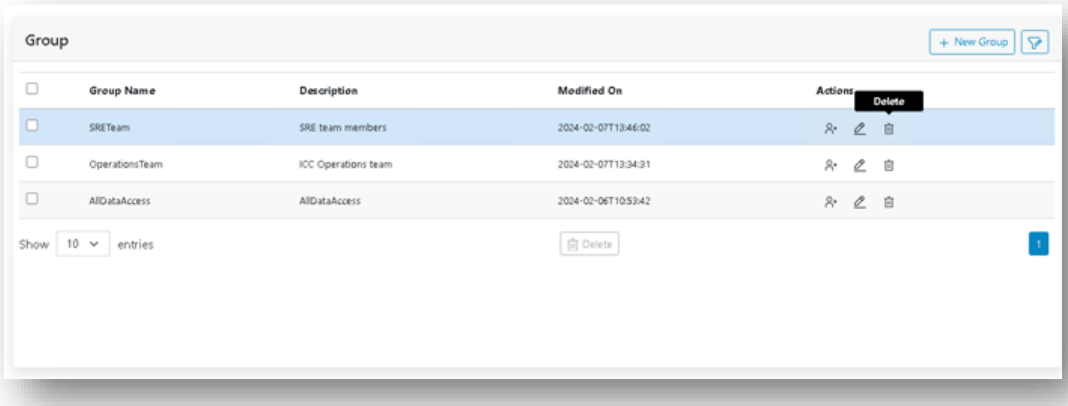

Figure 110 – Delete Group

2. Confirmation pop-up appears.

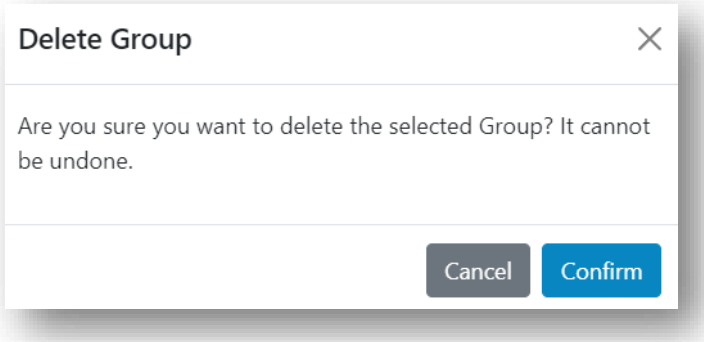

Figure 111 - Confirmation pop-up

3. Click **Confirm**. A confirmation pop-up is displayed. Refreshes the grid with the group removed.

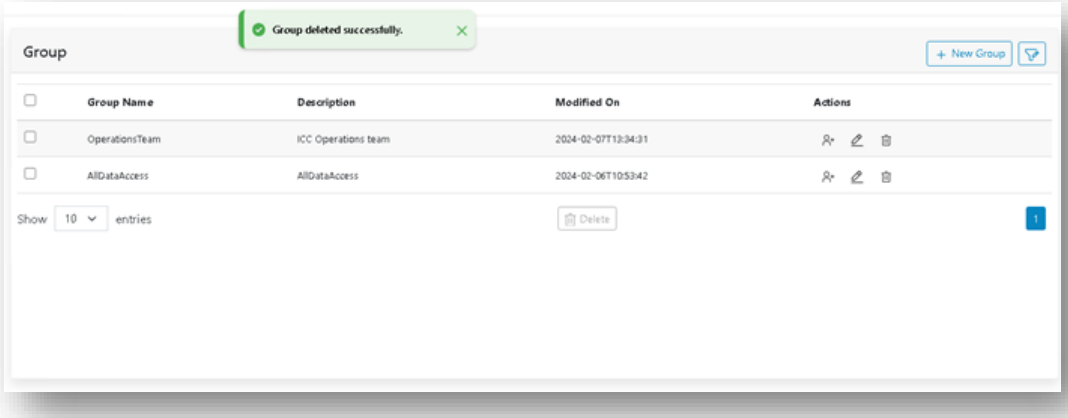

Figure 112 – Alert Message

Below is the **bulk deletion** option.

1. Select the groups that are to be deleted. As the groups are selected, the icons in the footer will be enabled.
2. Click on the Delete icon. The steps will be same as in individual delete post that.
3. Confirmation will be requested, Click Confirm. On successful deletion confirmation will be displayed and the grid will be refreshed with the groups no longer displayed.

This action enables us to assign users to roles created in the environment.

1. Click on **Customer → Customer Name→ Group**.

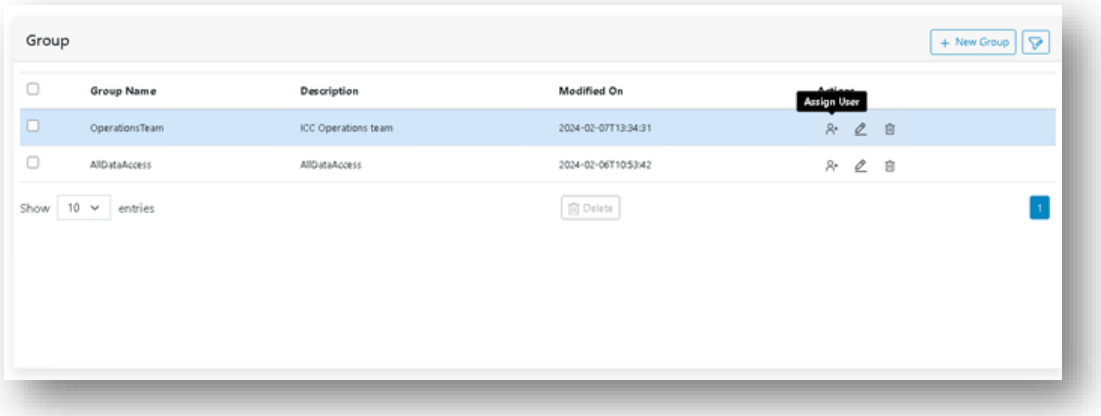

Figure 113 - Assign Users in a Group

2. The Action tab contains Assign User option, click on the Assign User option to assign the Group to a particular user in the environment.
3. After clicking on the Assign User option, a pop up will be opened which will ask for User Email ID input.

Users can only be assigned by adding the User Email ID.

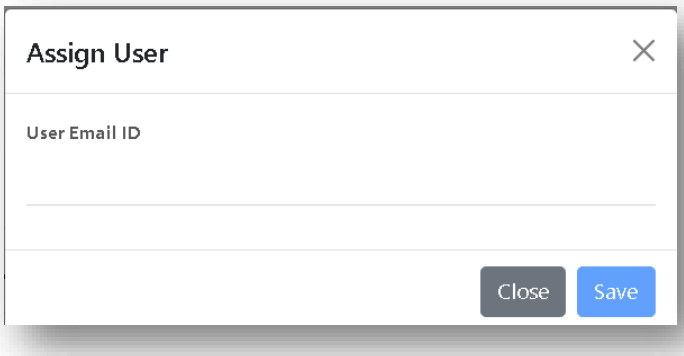

Figure 114 - Assign User Pop-up

4. After adding the required User Email ID, click on the **Save** Button.

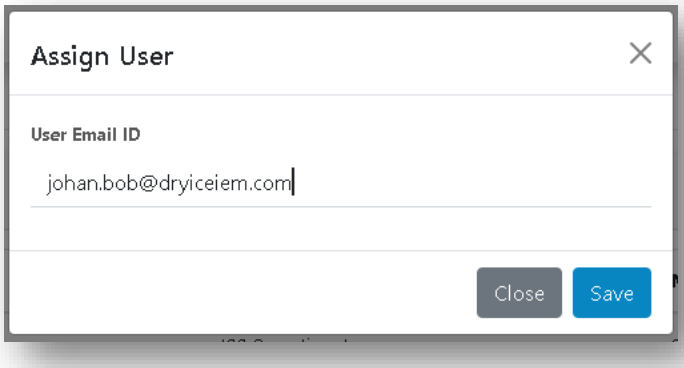

Figure 115 - Assign User Email ID

5. On successful assignation, a confirmation pop-up is displayed as shown in the following figure. The user will be assigned successfully to that group.

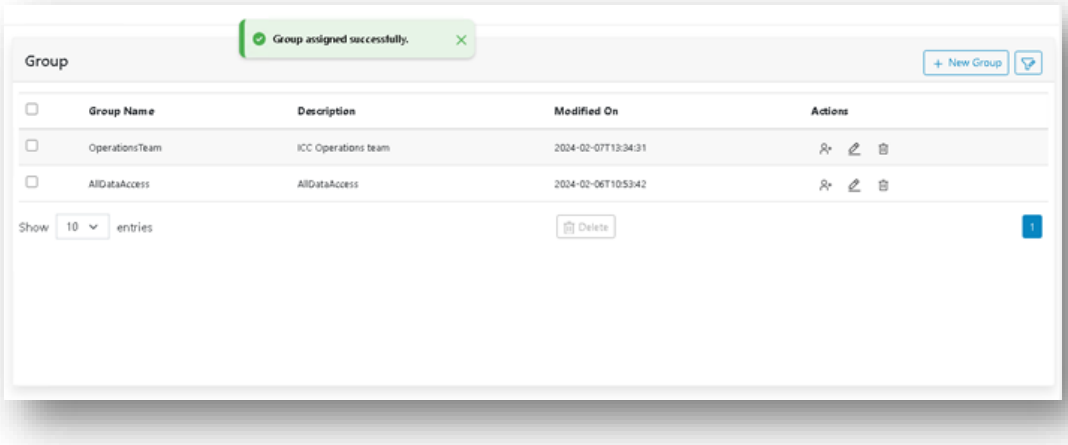

Figure 116 - Confirmation Pop-up Message

Apply Filters

The steps provide information on how to Apply filter to the Group Data.

1. Click on **Customer→ Customer Name→ Group**.

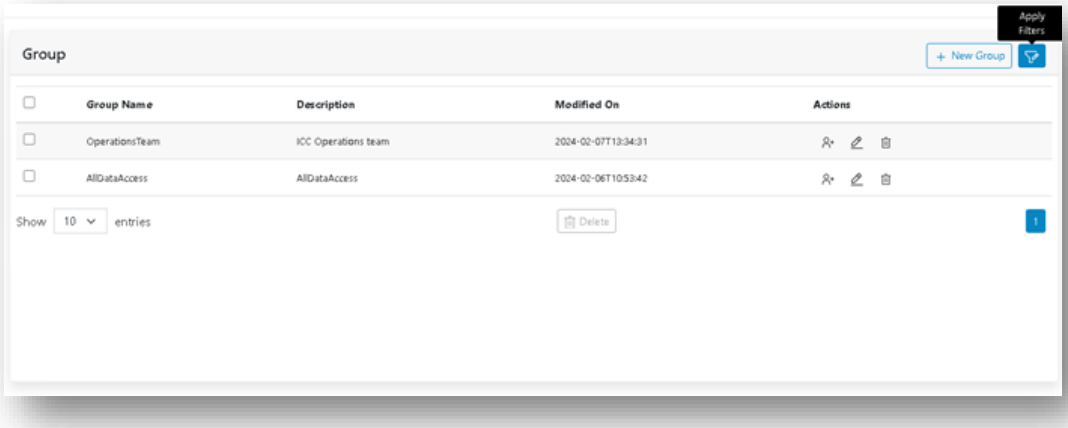

Figure 117 - Apply Filter Operation

2. Click on the Apply filter action button present at the header of the console.
3. The form will appear where user can select **Field** and **Operator** from drop down list and user must provide the **Value**.
4. Then click on the **Apply** button.

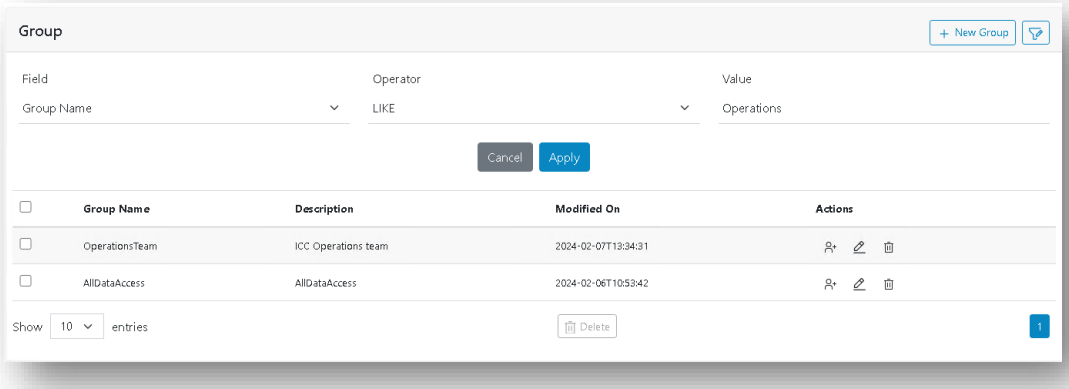

Figure 118 - Apply Filter Operation

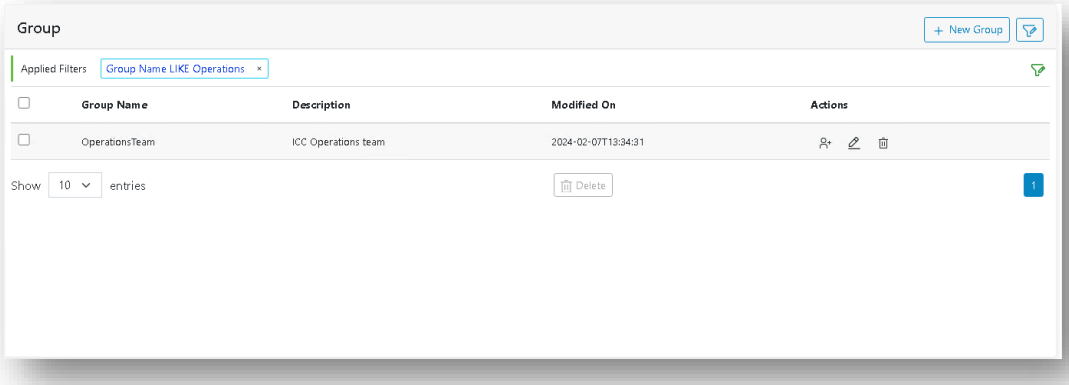

Figure 119 - Apply Filter Result

5. User can see the result of applied filter.

6.1.11.6 Entity

An Entity in IEM can be referred to any configuration item (CI) against which the event has been triggered or received in IEM.

The section enables us to provide details associated with the entity, enabling enriching the events, alerts, and actionable data within the system based on its mapped entity. This enriched data can be further used while defining correlation rules or while working on the data view screen. Example, providing details such as location, data center, applications (primary, secondary etc.) while defining the entities. As these details are added, it becomes available in the correlation rule configuration page as **we**ll as in additional columns in the data view page, which can be then used accordingly by the respective users.

Likewise, with other screens the users can perform actions based on their assigned roles.

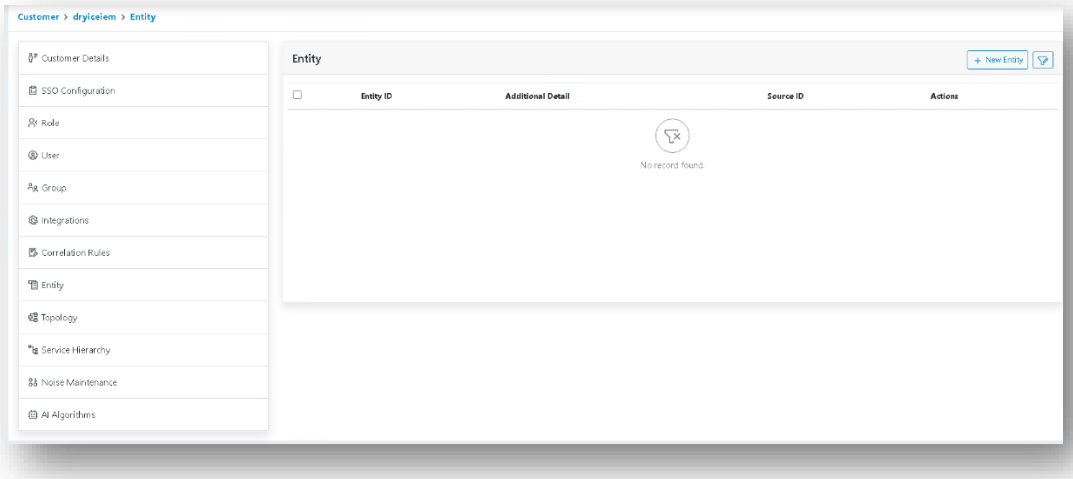

Figure 120 - Entity Page

1. Click the customer onboard section. For a specific customer, click on Customer - edit section. Click on the Entity page, where Entity records for the selected customer will be displayed in the grid view once new entities have been created by the user.
2. Following actions can be performed on the page.
    - Add New
    - Edit Existing
    - Delete
    - Mark Noise
    - Define Maintenance Schedule
    - Merge
    - Apply Filters

Add New Entity

Entity Records can be added using two methods: -

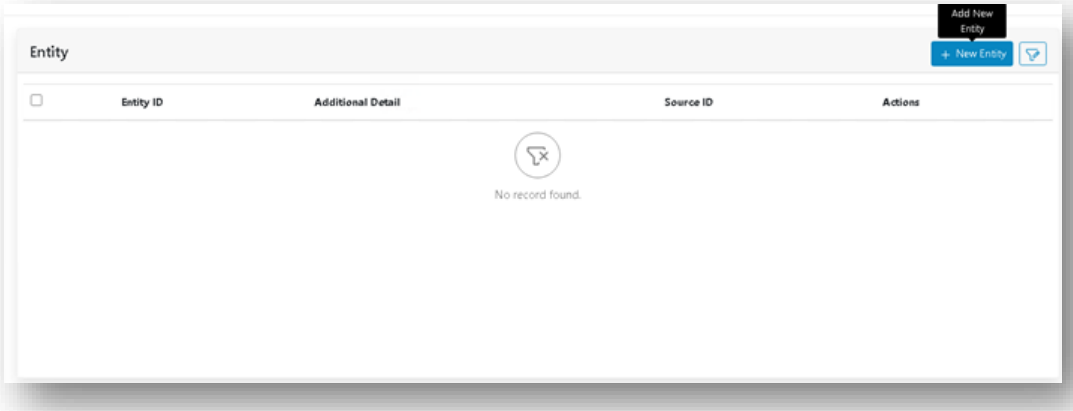

Figure 121 - Navigation for Create an Entity

1. Create New Entity by clicking on **+ New Entity** Button
2. Bulk Insertion can be done using the upload CSV option.
3. Choose a file based on the template available and upload it. Click on **Submit**.

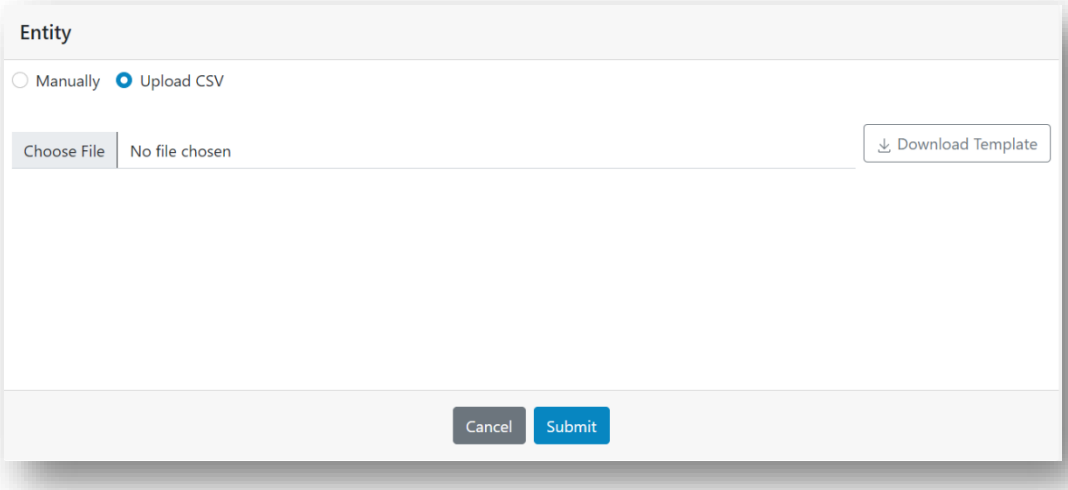

Figure 122 - Bulk Upload Entities

Prior to adding the records, ensure that CSV contains the proper data, as upload will enrich the records of the selected customer.

Let's look at each action.

Individual Record Addition

1. Click on **+Entity** button. This opens the following pop-up.

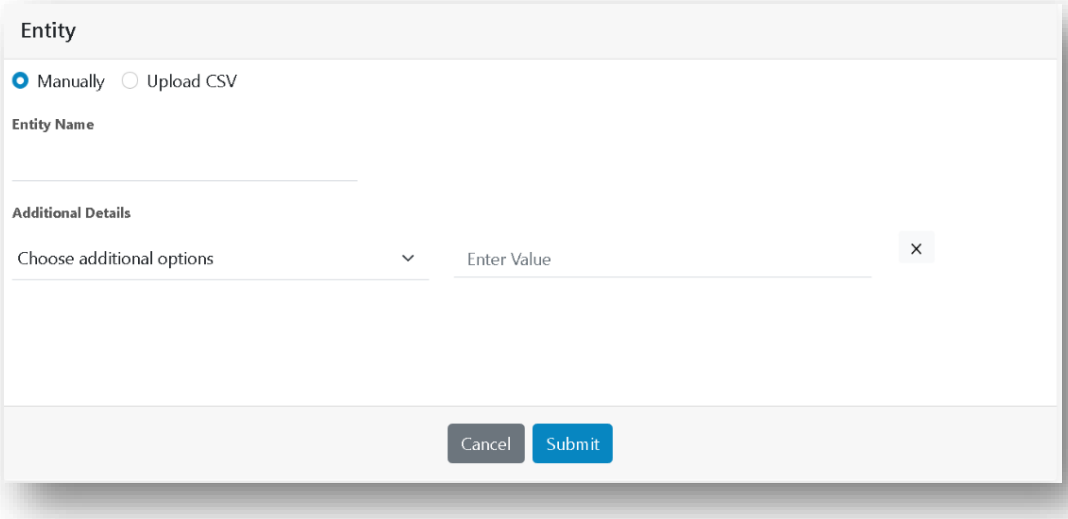

Figure 123 - Add Entity Name

2. Specify the **Entity Name** which is a mandatory column.
3. If required, other details can be added using, **Choose additional options**. As the dropdown is selected the existing keys created within the environment will be displayed with an option to add a new "custom key" as shown below.

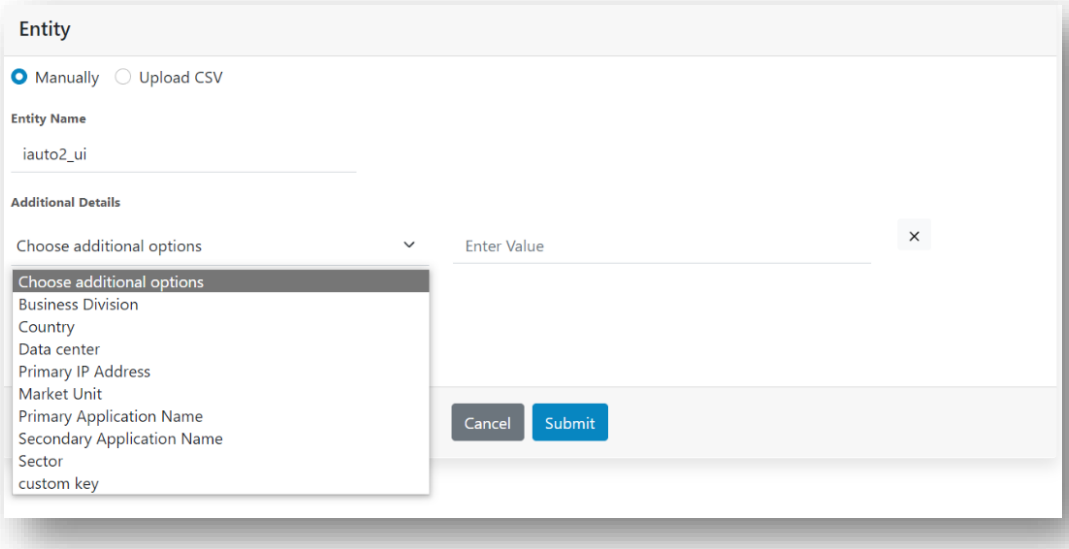

Figure 124 - Dropdown List for Column

Providing additional options is not mandatory and depends on the user's requirement of data enrichment.

4. Let's first select an existing key. Let's select 'Country'. As user selects country, the key will come populated in the first row enabling user to enter its value and a new record appears below it with the dropdown enabling user to add more details if required.

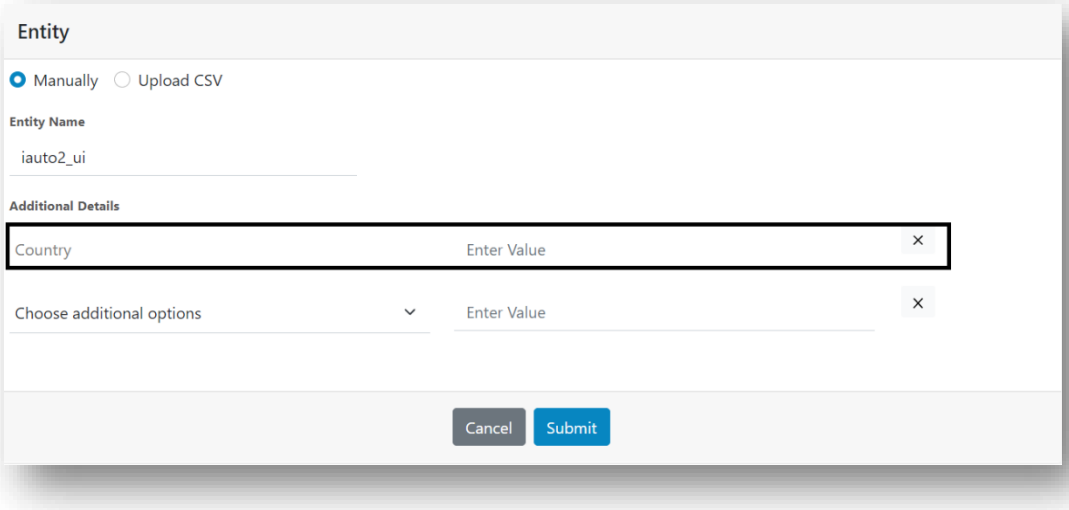

Figure 125 - Selected Column

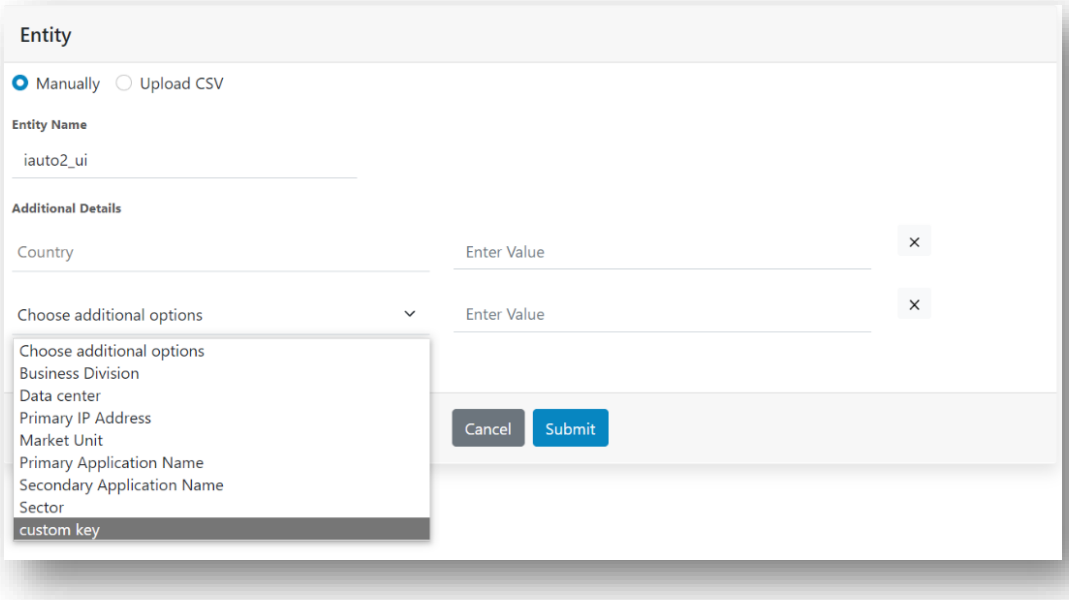

Figure 126 - Selecting Multiple Columns

5. Let's next create a new detail. Select "Custom key" from the dropdown.

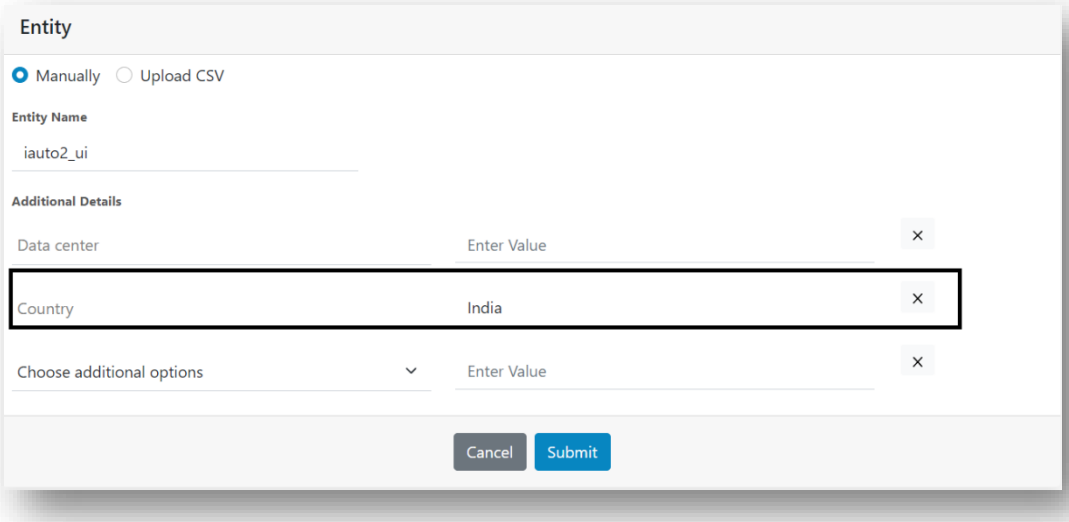

Figure 127 - Add New Column

6. As the option is selected, the dropdown is replaced with a text box enabling user to define the new key, and value appears next to it. A new row is added below it with the dropdown.

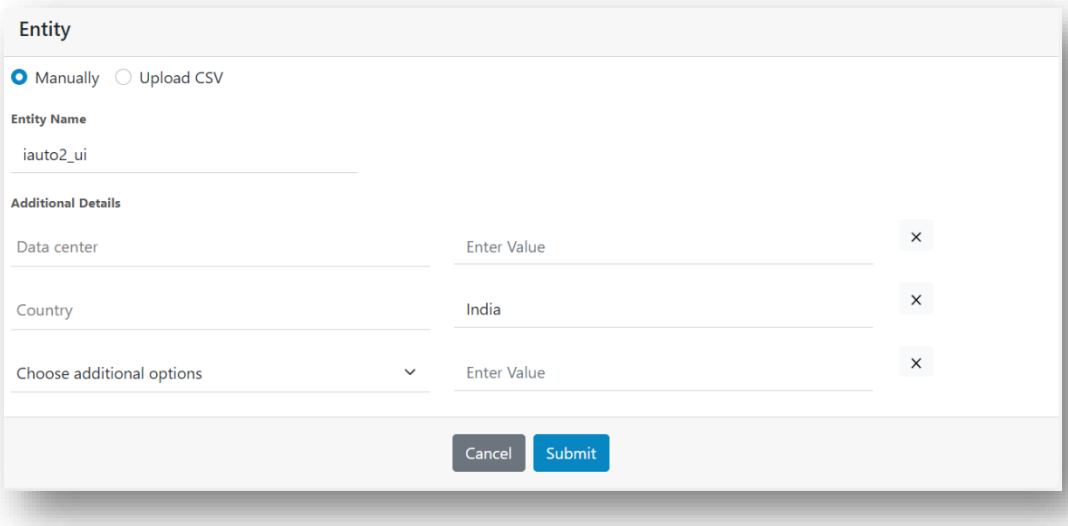

Figure 128 - Multiple Enter Value for Entity

7. In case more details need to be added, repeat step 1 to make use of an existing key or, follow steps 2, 3 and 4 as mentioned above to add Custom details using Custom Keys.
8. Click on **Submit** once done. On successful addition a prompt is displayed as shown.

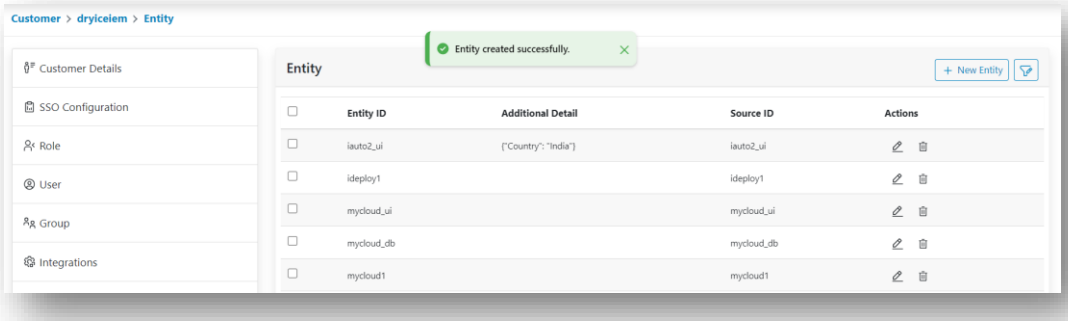

Figure 129 - Alert Message

9. The New Entity added will appear in the grid as shown above.

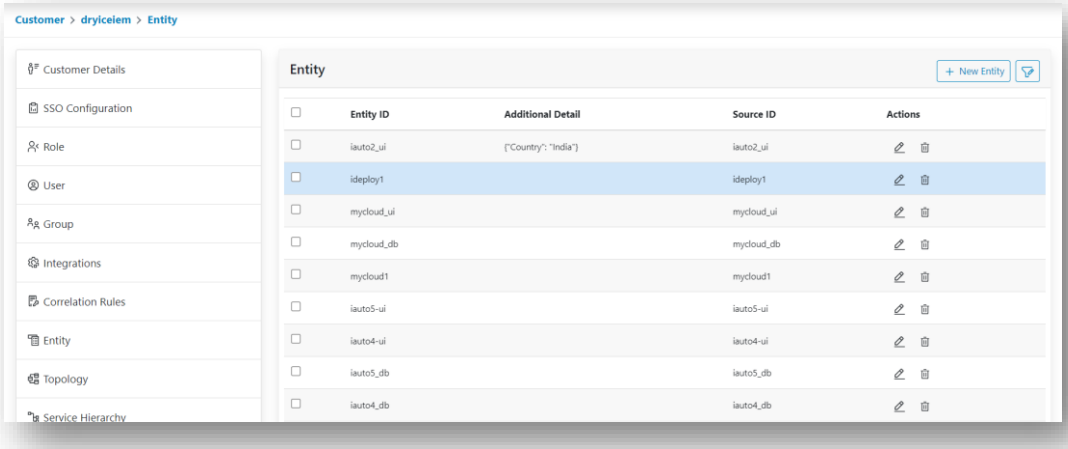

Figure 130 - Grid View for Entity

1. Click on New Entity and select Upload CSV radio button option as shown:

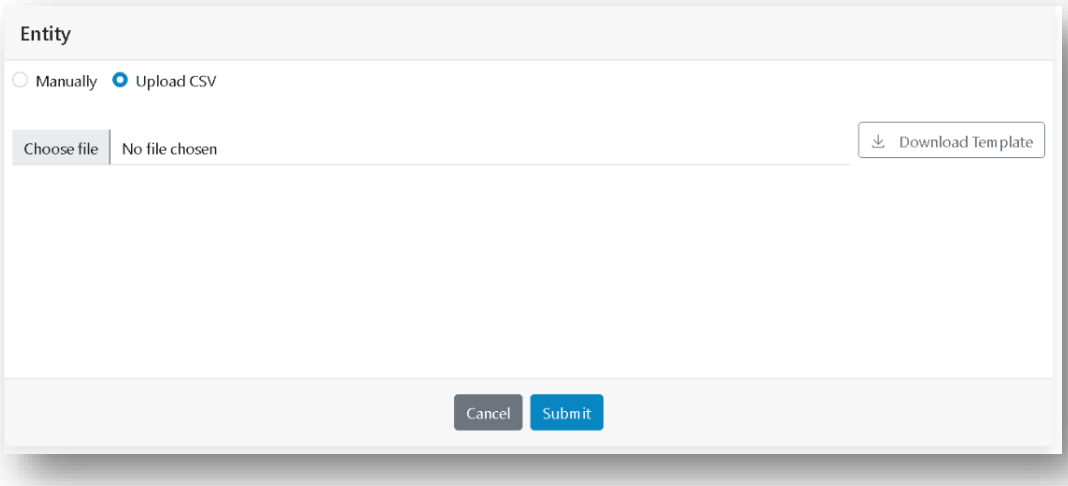

Figure 131 - Bulk Upload Entities

2. As user selects Upload CSV the following screen appears:

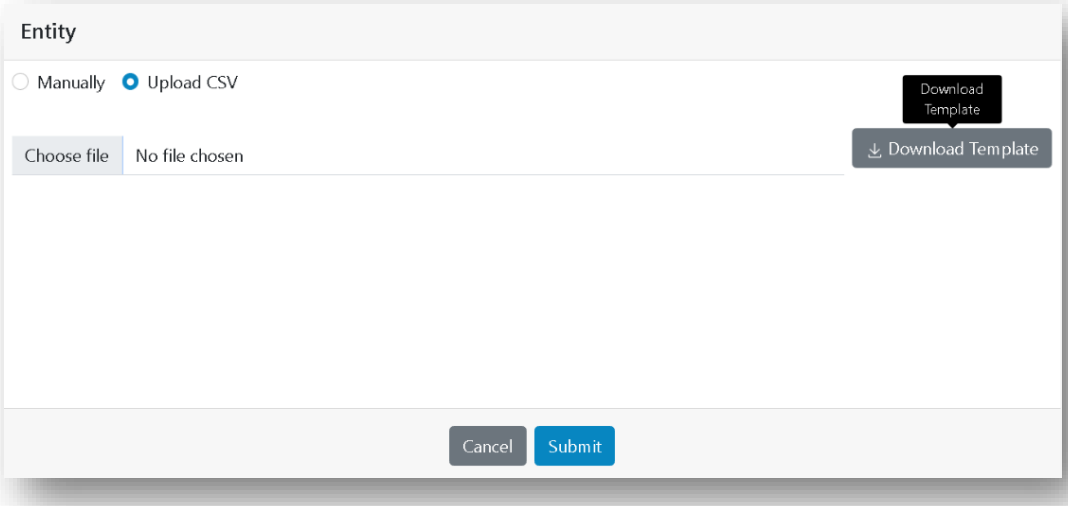

Figure 132 - Bulk Upload Entities

3. Click on the **Download Template** button. The following template is downloaded:

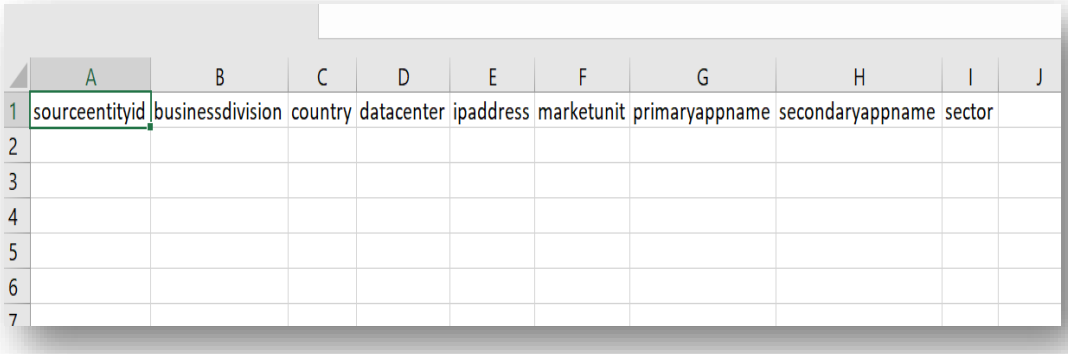

Figure 133 - Template Format of Bulk Entity

4. “Source entity id” is the mandatory column, rest are the additional details available in the environment.
5. User can choose to provide values of the additional details or can add more details as per Customer’s requirements, by adding columns in the downloaded template as shown below.

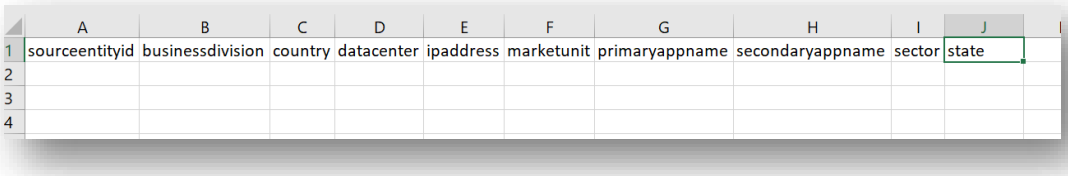

Figure 134 - Template Format of Bulk Entity

6. The new additional details will be added in the repository while the data is uploaded.

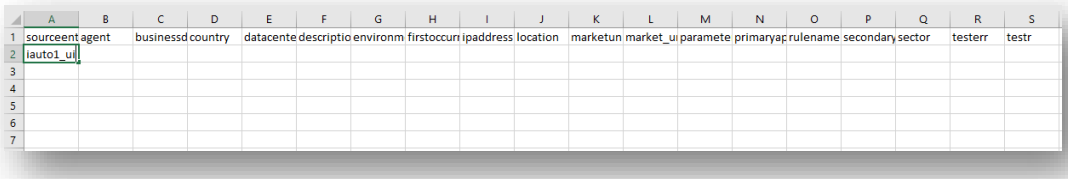

Figure 135 - Template with Entity data.

7. Add details in the excel and save the file as .CSV file. As user clicks on the upload CSV, the local directory browser appears as shown:

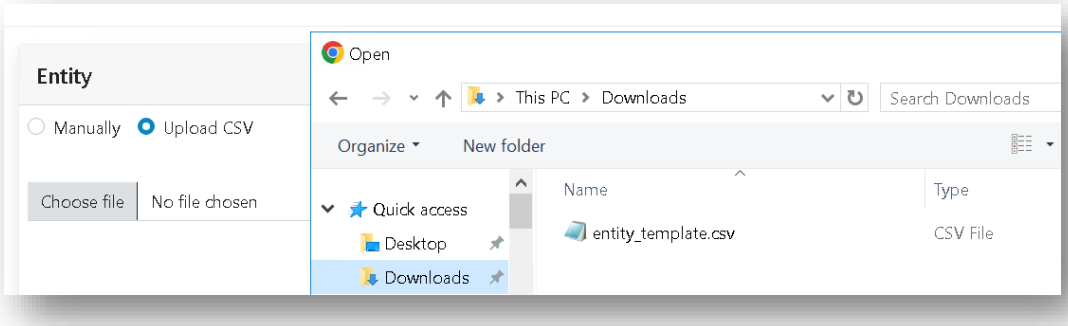

Figure 136 - Selecting file from local Directory

8. Browse to the local directory where the data file is saved and select the file. As the file is selected, it appears as shown:

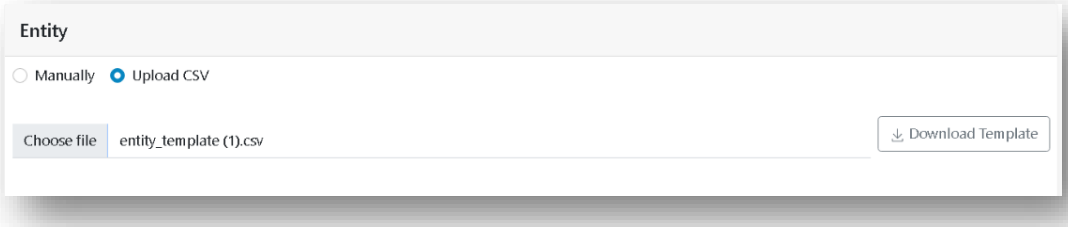

Figure 137 - Upload csv file

9. Click **Submit**. If the data in the excel file is as per the downloaded template, it will get submitted and a success message is shown. Close the success message.

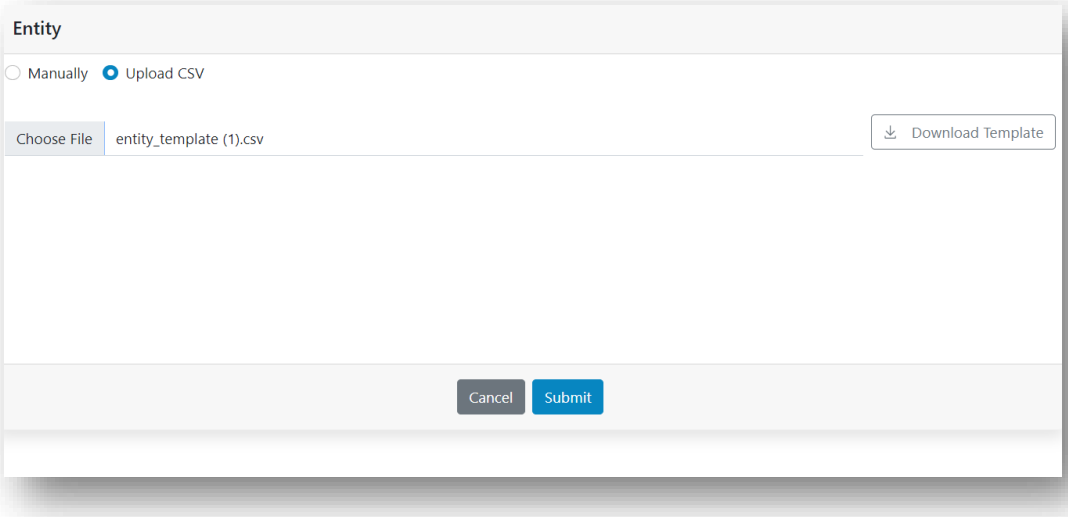

Figure 138 – Submit Button

In case Entity modification is required on MSP Tenant then BAU/Operations team should reach out to IEM PS team.

Edit Entity

Once the entities are added, the edit icon next to the entity record can be used to update its details.

1. Click on the Edit icon next to entity record which is to be updated.

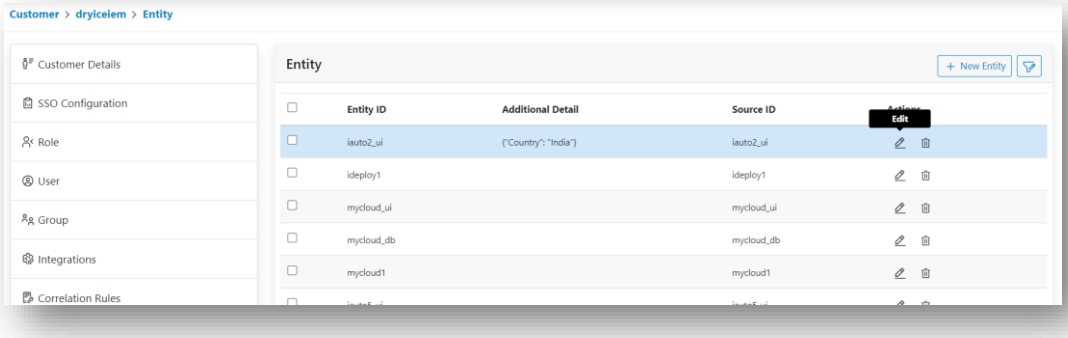

Figure 139 - Edit Entity

2. The form appears filled with details. User can add/edit/remove the additional details options. For example, parse let's add details of primary application, remove the state and update country to UK. Post changes, the form appears as below.

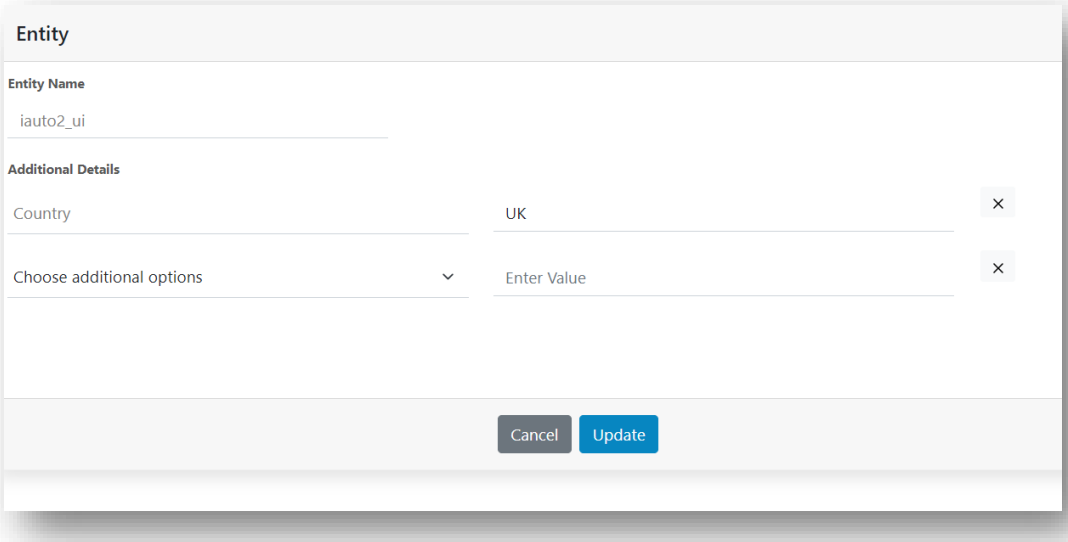

Figure 140 - Edit Details

3. Once complete click on Update. On successful update the following prompt is displayed.

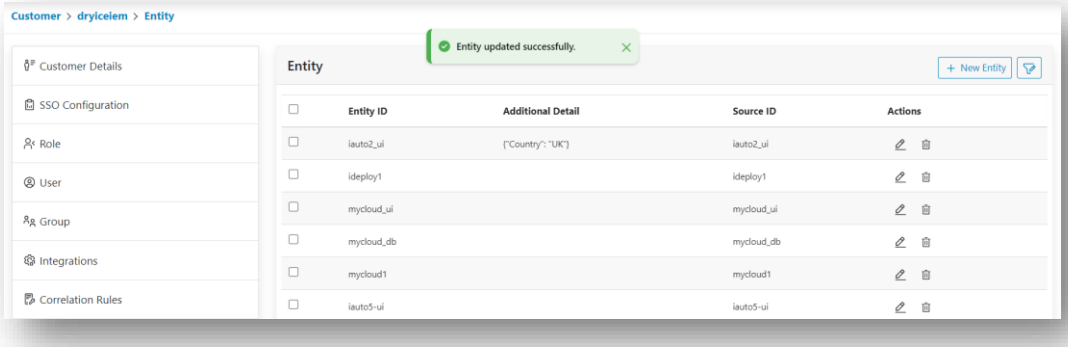

Figure 141 - Alert Message

4. Click on close, the updates will be visible in the grid view as shown below.

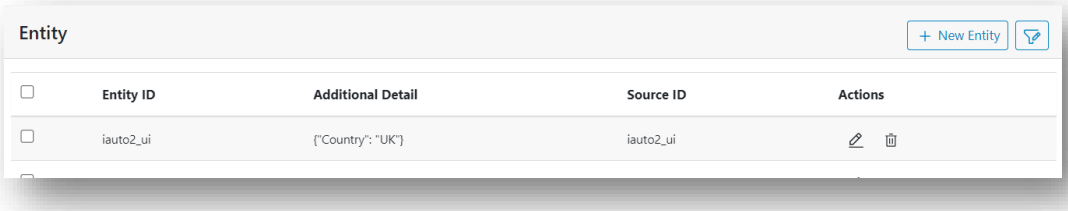

Figure 142 - Grid View for Entity

Delete Entity

If the entities are wrongly mapped or created, or need to be removed, provision of bulk delete is available on the page.

1. Click on the check boxes next to the entities to select the entity that is to be deleted.

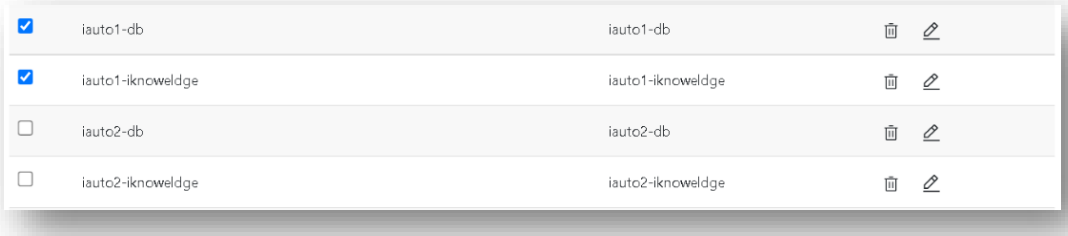

Figure 143 - Figure – Entity Page

Clicking the checkbox in the header will select all the entities displayed on the page.

2. When the entities are selected, the available icons at the bottom of the grid get enabled.

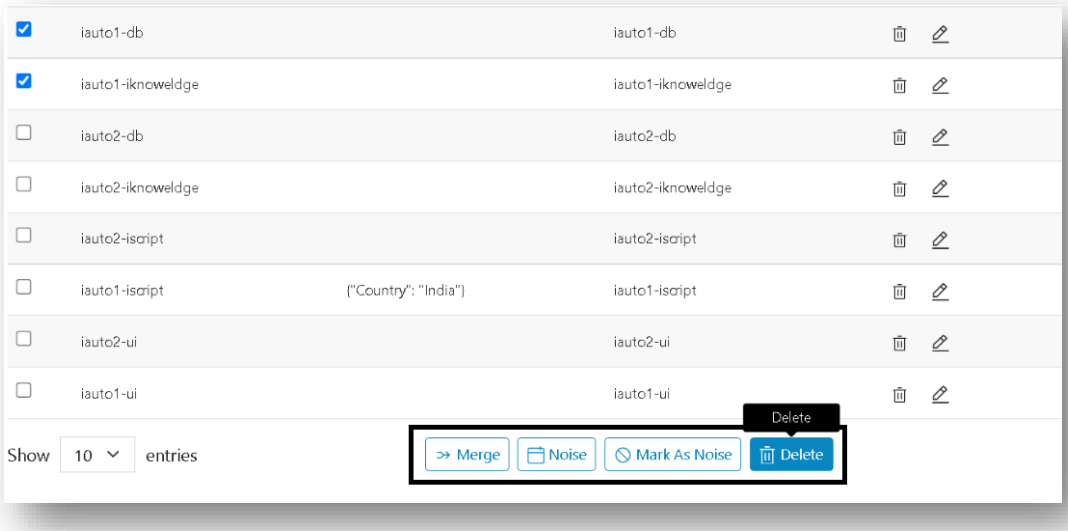

Figure 144 - Delete Entities

3. Click on the **Delete** button.

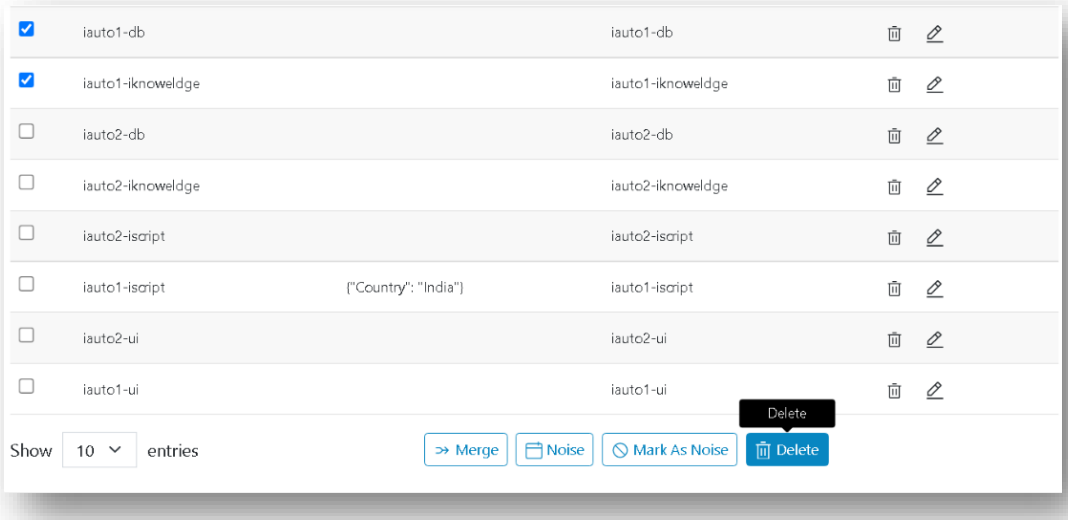

Figure 145 - Delete Entities

4. A confirmation box appears:

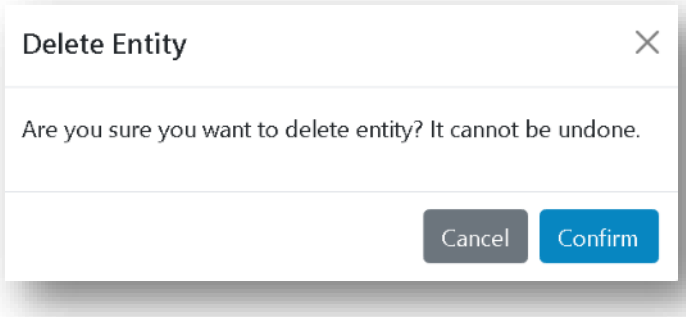

Figure 146 - Confirmation pop-up

5. If sure of the selected entities deletion, click **Confirm** else, click **Cancel** to revisit the selections made.
6. As **Confirm** is clicked, deletion process gets started. On successful deletion of the records, the rows are removed from the grid and a confirmation message box is prompted.

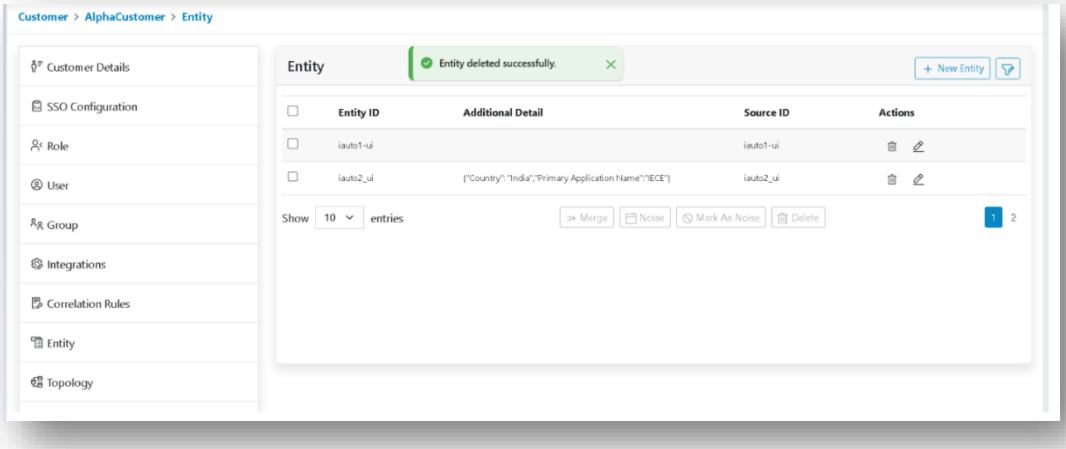

Figure 147 - Alert Message

7. Click **Close**. The rows are no longer available in the grid.

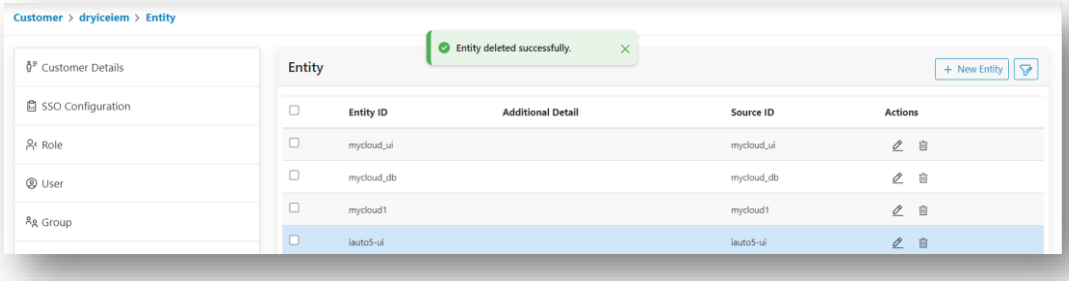

Figure 148 – Entity Removed from the Data Grid

Merge Entities

Merge is a feature which is available to merge related entities. As data can be uploaded from different repositories, many a times same entity is referred by different names across repository, so in here those entities can be selected and merged and tagged by a common name, so that the details can be used while defining correlation rule to correlate data coming from different repository. In that case if user use Entity (Master) from the fields list in the Group By field of the correlation rule screen, all data associated to the entity across different data sources will be grouped together. To know more about defining correlation rules refer to the Correlation Rules section.

1. Click on the check boxes next to the entities to be merged. Like while deleting, as entities are selected, all icons in the footer will be enabled.

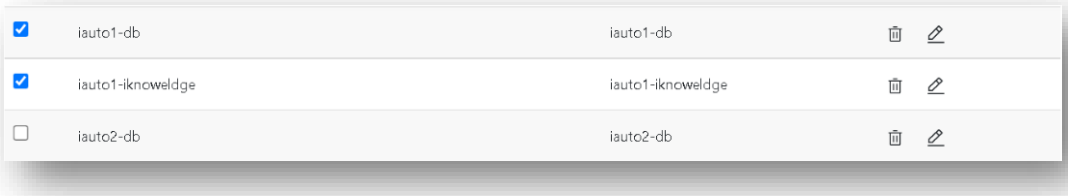

Figure 149 - Select Entities for Operation

2. Click on **Merge** button.

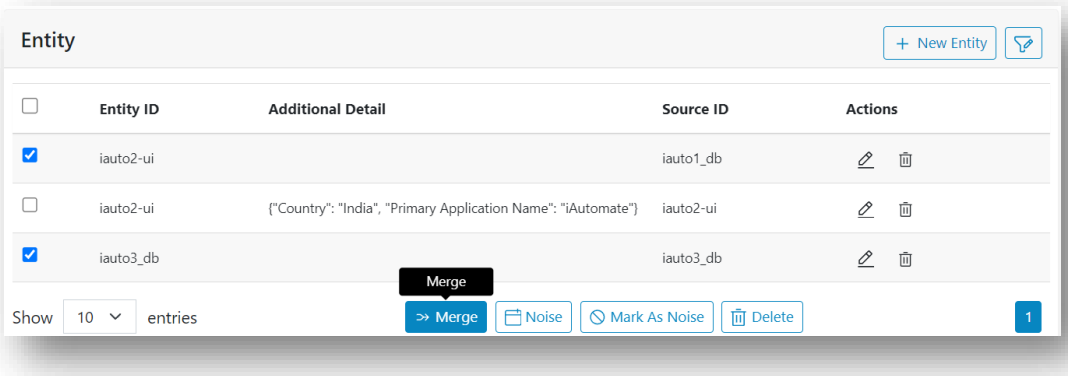

Figure 150 - Merge Entities

3. A pop up appears with the names of all selected entities appearing in the dropdown.

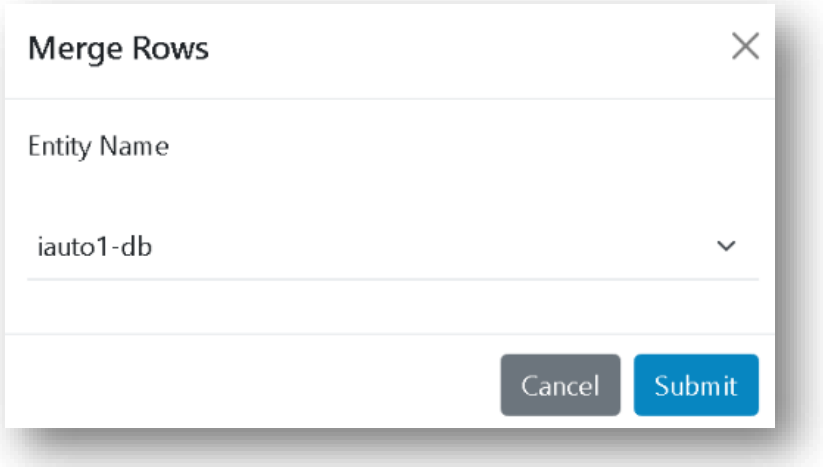

Figure 151 - Merge Rows

4. Select the name which will be primarily used for identifying these selected entities. For example, parse any one of the entity names from the dropdown, so that selected entity names will be changed to the entity name which is selected in the dropdown.
5. Click **Submit**, a confirmation box will be displayed.

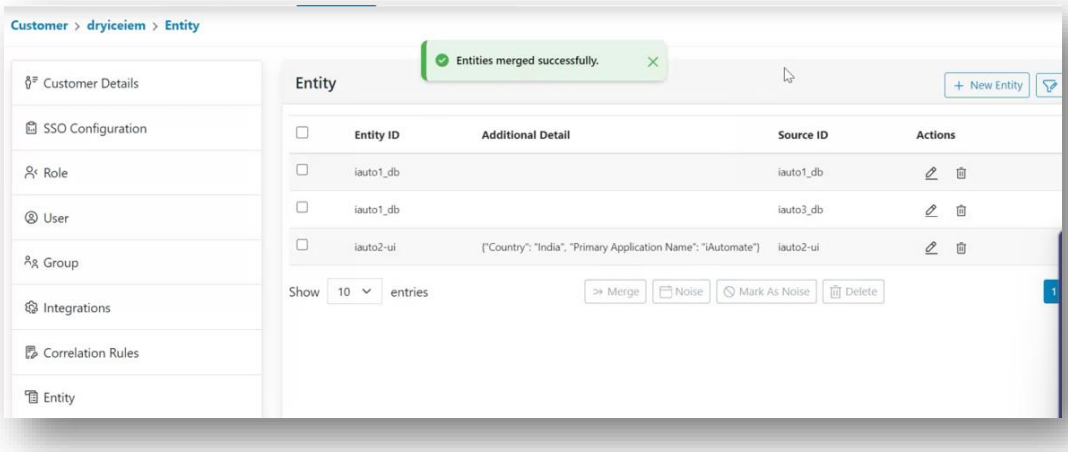

Figure 152 - Alert Message

6. Click **Cancel** and refresh the grid. All the entities, entity ID field will start appearing the same.

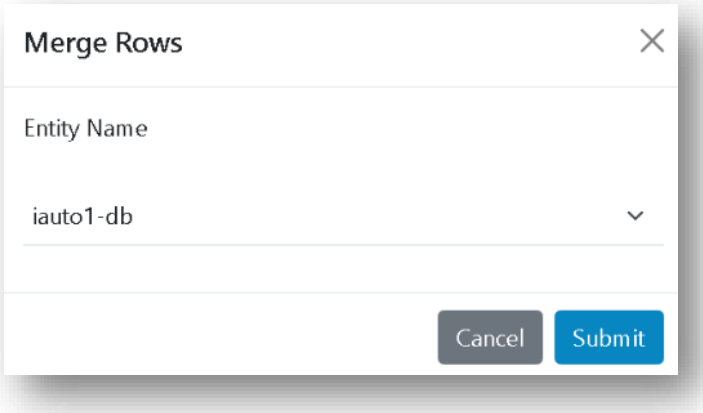

Figure 153 – Cancel Button

Source entity field is not changed, just the entity name changes to the referenced entity name.

Mark as Noise

As the entities are uploaded, this screen also enables user to filter out a few entities data completely. Example, entities such as those which may belong for development or for POC (Proof of Concept) purposes and the events generated can be completely ignored. These entities can be selected and marked as Noise from here. As user mark them as noise, any events received of the marked entities will be filtered out at the first event processing layer itself and will not move further in the processing pipeline.

1. Select the entities to be marked as noise by clicking on the corresponding check boxes. All the icons in the footer get enabled.

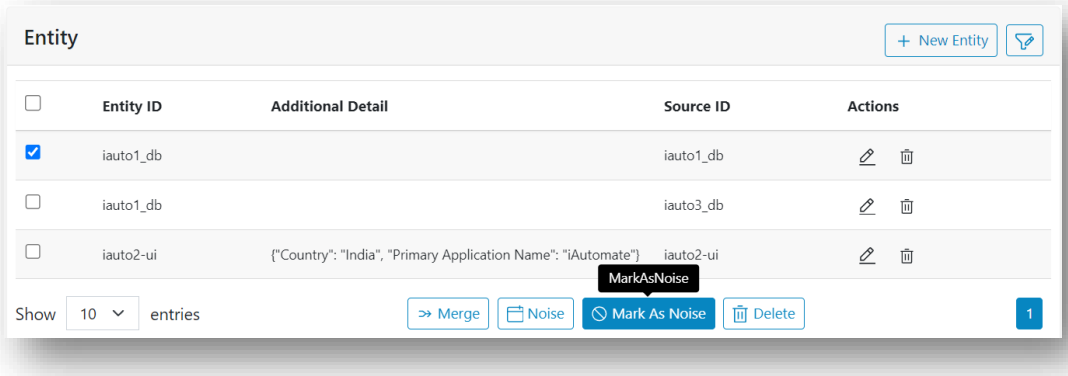

Figure 154 - Selected Entity Perform Operations

2. Click on **Mark as Noise** icon.

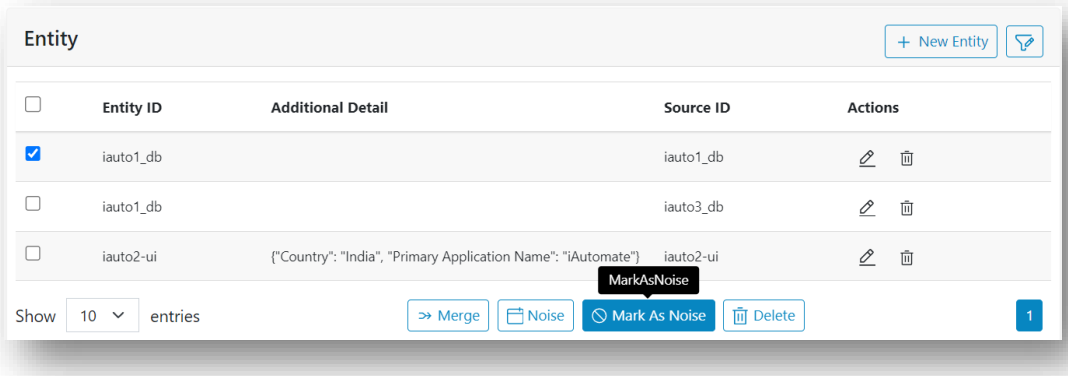

Figure 155 - Selected Entity Mark as Noise

3. As the icon is clicked, a confirmation box is displayed as shown below:

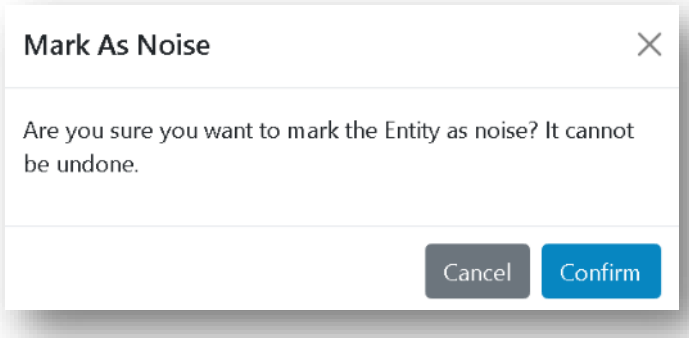

Figure 156 - Success Popup for Mark as Noise

4. Click **Confirm**.
5. On successful update the entities are marked as noise, and a success message is displayed as shown below:

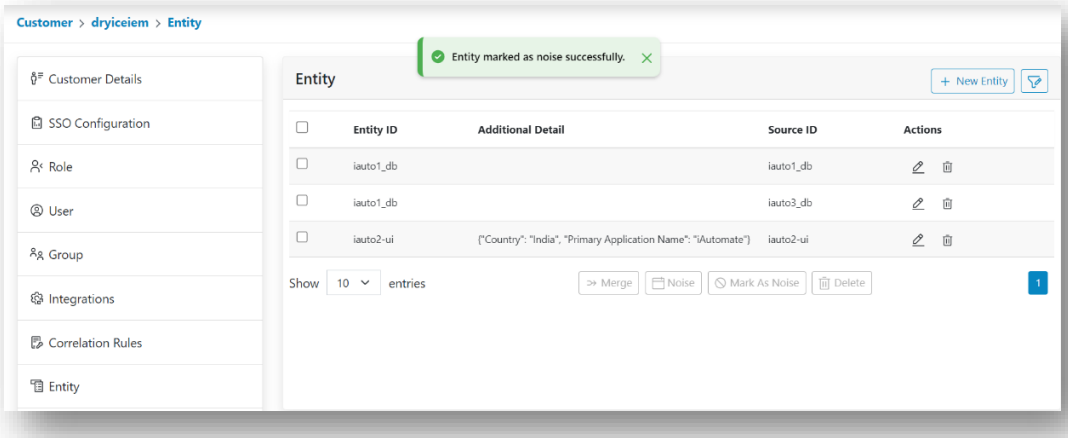

Figure 157 - Alert Message

Once marked as noise, the details start appearing on the noise/maintenance screen prefixed with "Noise". Refer to the noise/maintenance window section to know more about viewing the data.

Define Maintenance Window

This section enables the user to define a window (time range) for the selected entities during which any event data received from the entities can be filtered out. This time range can belong to any planned activities such as backup, maintenance schedule, upgrade etc. where though the event generation is expected but no processing is required and can be dropped.

1. Select the entities for which the window needs to be defined by clicking on the corresponding check boxes. once the entities are selected, the footer icons get enabled. Click on **Define Maintenance** window.

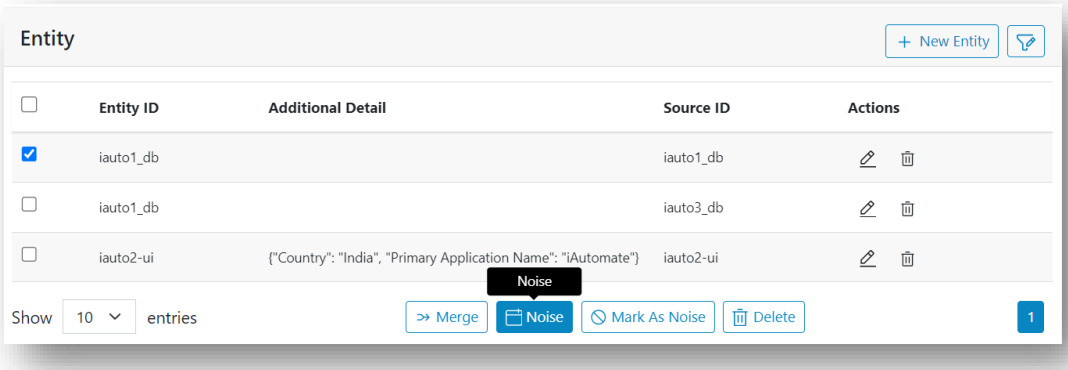

Figure 158 - Selected Entities as Maintenance Window

2. The following popup appears for configuration.

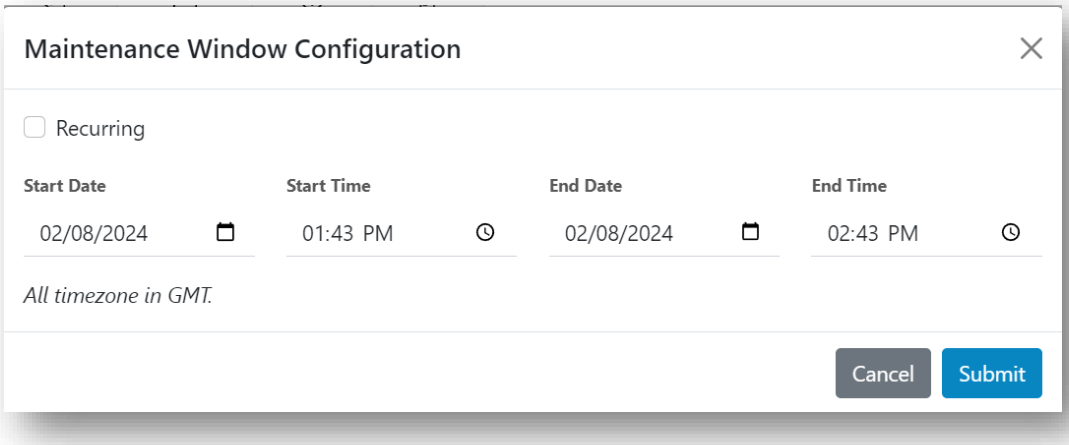

Figure 159 - Maintenance Window Configuration

3. By default, the current date is selected. The following option for configuration exists:

   a. Specify one-time duration. Here user needs to select the **Start Date** and **End Date** and specify the **Start Time** and **End Time** duration. On clicking the **Start Date**, a calendar appears as shown below enabling users to select the date.

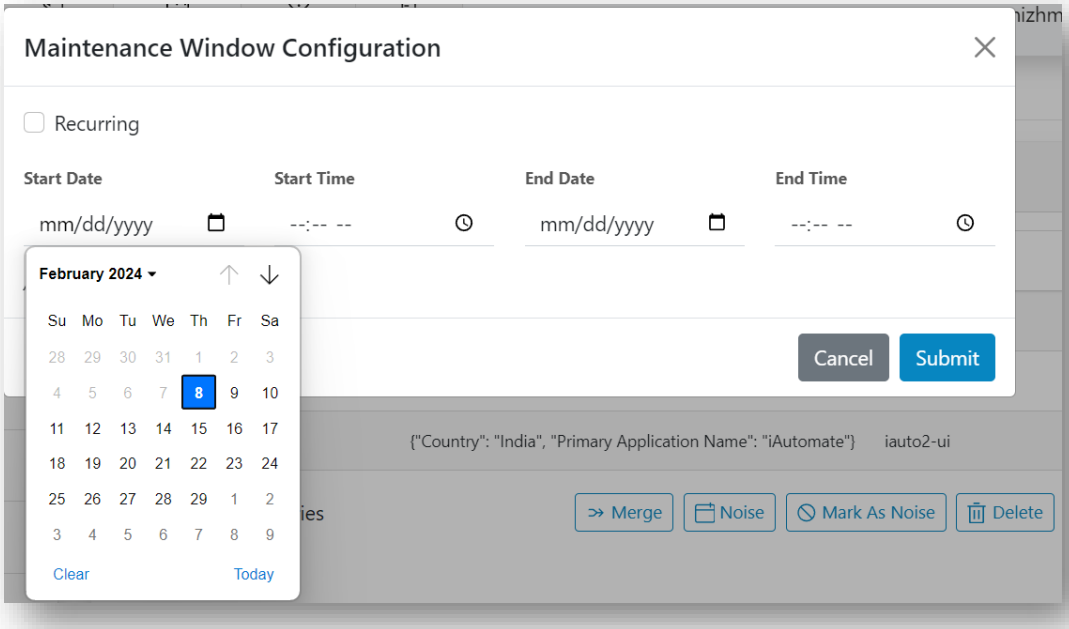

Figure 160 - Date selection for Noise Rule

   b. User can type in the time or use the clock icon next to the start time and the end time to specify the time range for the selected date. With the date and time selected the popup looks as below.

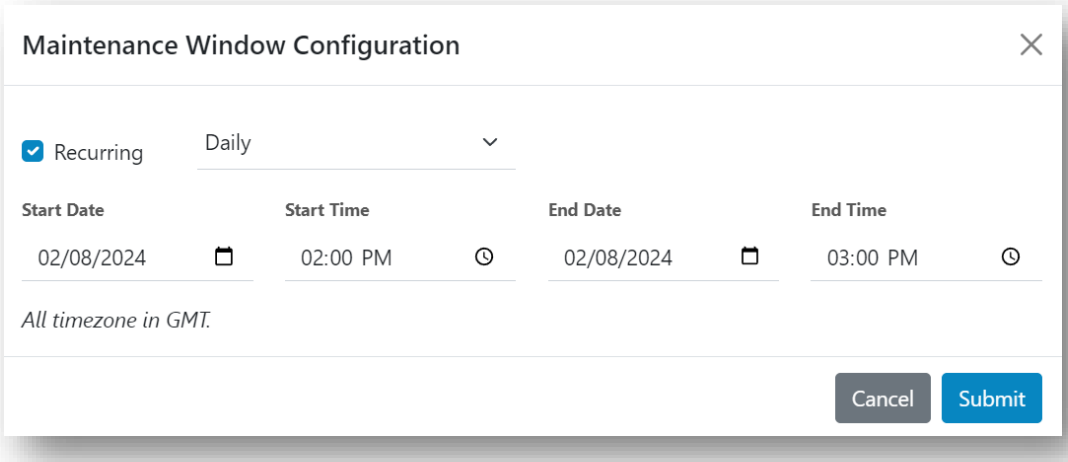

Figure 161 - Time Interval for Noise Rule

c. In the above image, the event data will be considered as noise from 2:00 PM to 3:00 PM on 8th February 2024.

The date and time are of UTC time zone.

d. Specify Recurring period. As recurring is selected, user have an option to define a daily, weekly, or monthly recurrence as shown below.

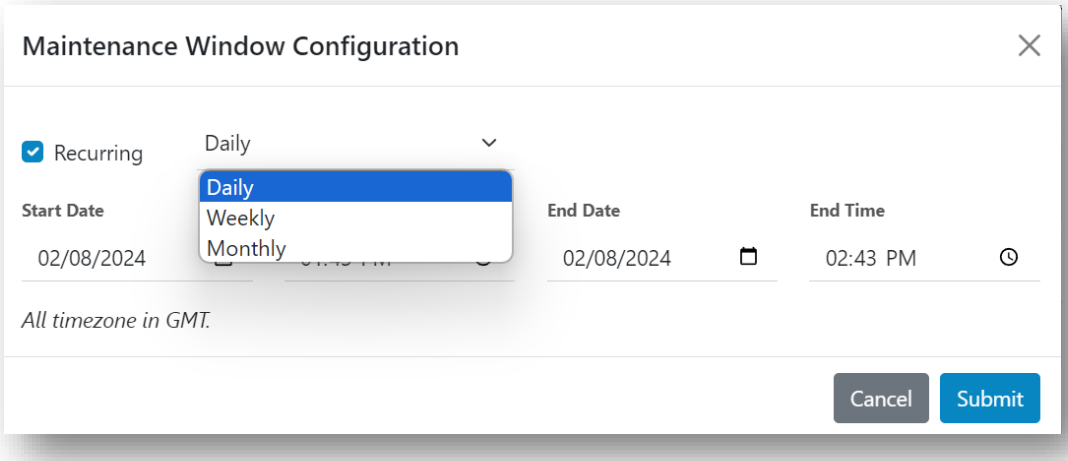

Figure 162 - Recurring for Noise Rule

e. Let's select Daily. As daily is selected user need to specify the date range by specifying the start date and end date. As user selected start date, in both these cases as well as the date field is selected, a calendar is displayed. Choose the date range. Once the date range is selected specify the Start Time and End Time the way user did for One time. For this example, parse, let's select the date range as 2:00 AM to 2:43 PM on 08th February 2024.

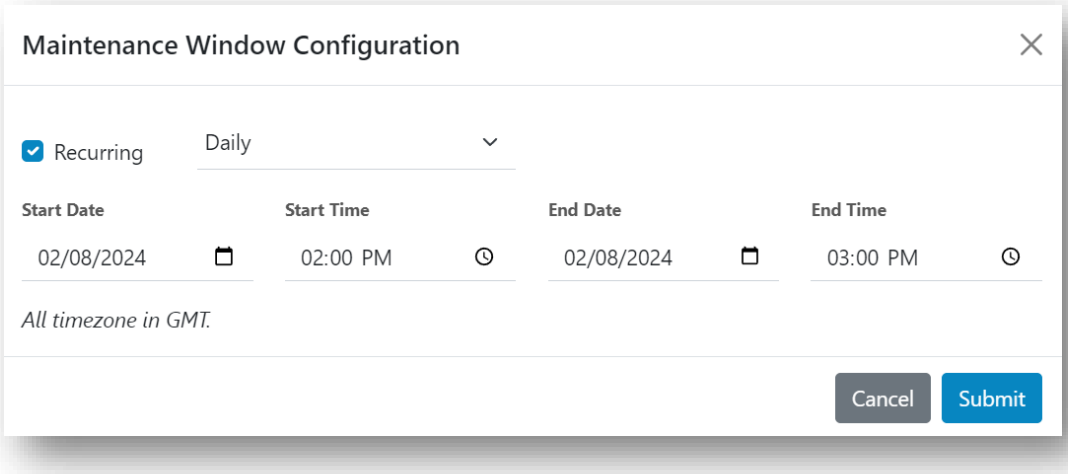

Figure 163 - Maintenance Window Configuration for Noise

f. The selection implies that any event data generated for the selected entities daily during the date range between 2-3 AM will be filtered out.

g. As day header is selected, a dropdown appears seeking input of the day along with the remaining selections.

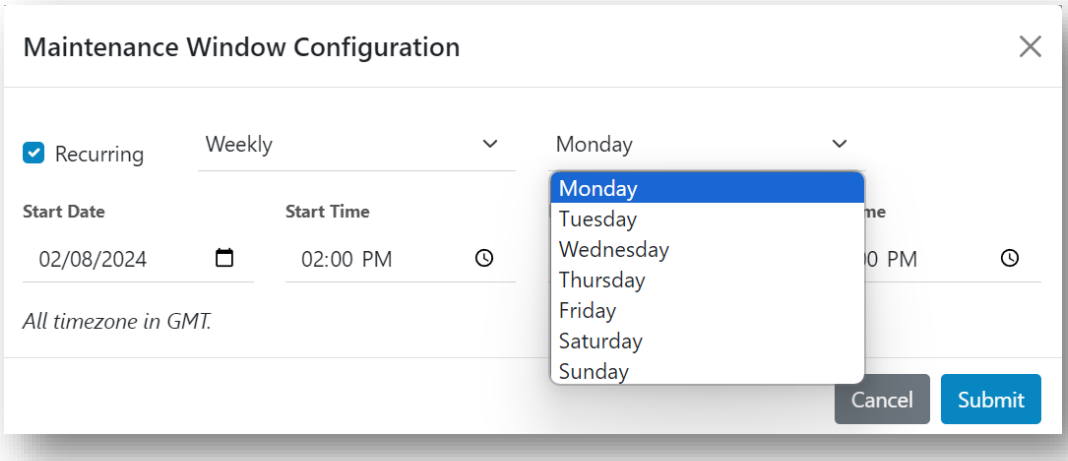

Figure 164 - Day Selection for Noise

For the example let's choose Wednesday. With the day selection the screen looks as below.

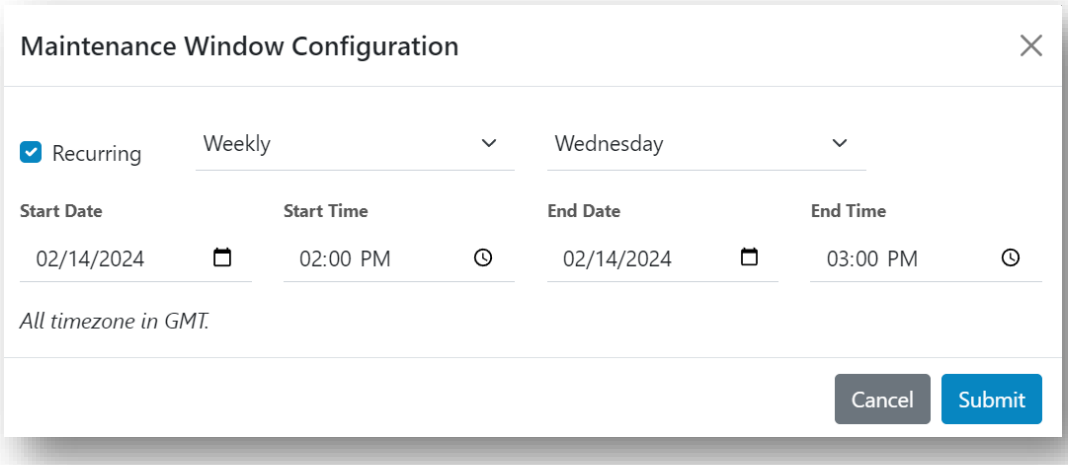

Figure 165 - Maintenance Window

h. The selection implies that any event data generated between 2-3 AM every Wednesday for the selected entities will be filtered out starting from 14th Feb 2024 till 14th Feb 2024.

i. Let's next look at the monthly recurring option. As Monthly is selected, a textbox appears enabling user to specify the day of the month as shown below.

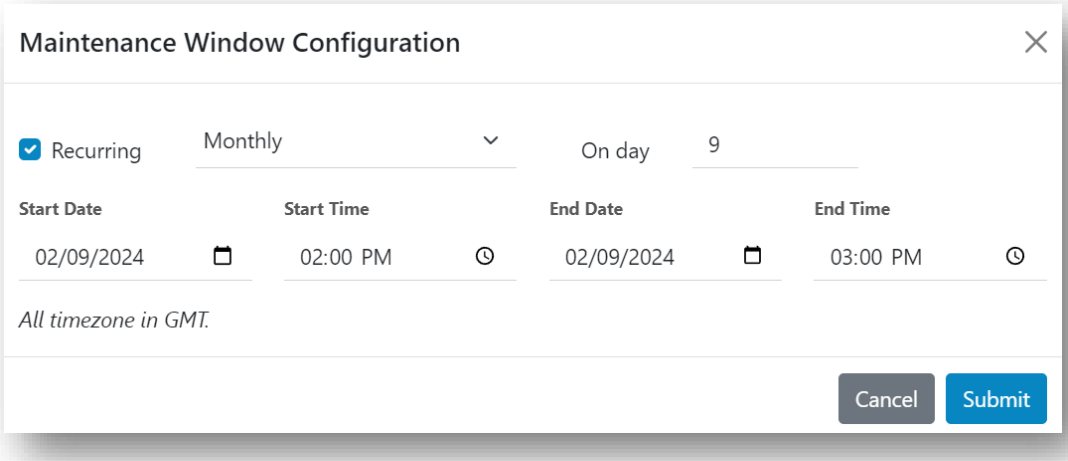

Figure 166 - On Day Selection for Recurring

For the example parse let's specify 20 as the day of the month. With the day input the screen looks as below.

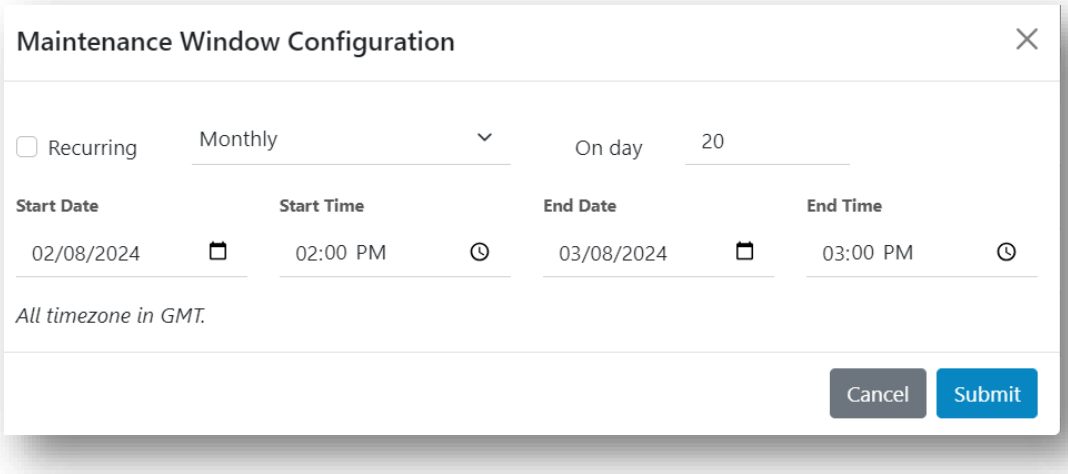

Figure 167 - On day and Time Interval

j. The selection implies that the event data generated between 2-3 AM on 20th day of every month for the selected entities will be filtered out starting on 8th Feb 2024. Once the period is specified as per the requirement, click on Submit.

4. On successful update, the details are saved, and a prompt of success is displayed as shown.

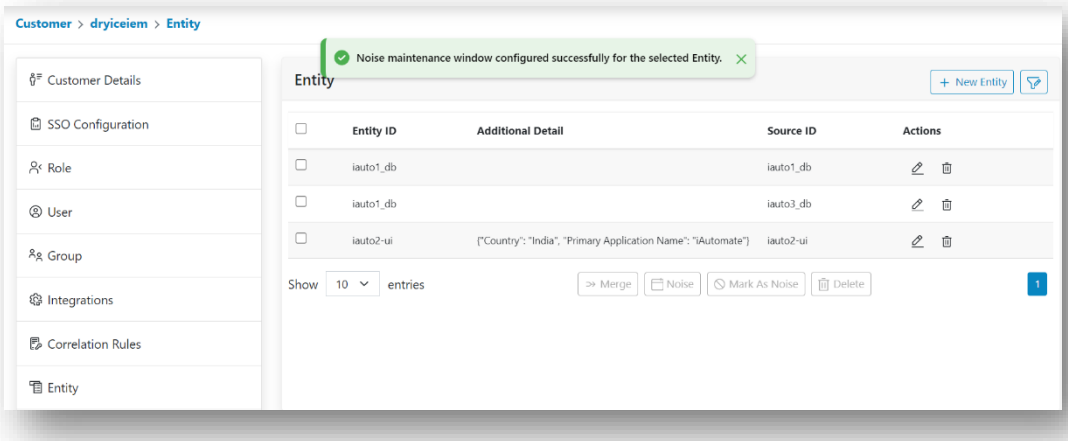

Figure 168 - Alert Message

The Number implies the number of entities whose data is updated. Since in this case user selected 2, both are updated so the count is displayed as 2.

5. Click Close.
6. Like noise the saved data will be visible on the noise/maintenance window, where rule name is prefixed with “Maintenance window defined for”.

Once an entity is marked, redefining or remarking will not work.

Apply Filters

The steps explain how to Apply filters to the Entity Data.

1. Click on the Apply filter available action button present at the below header of the console.

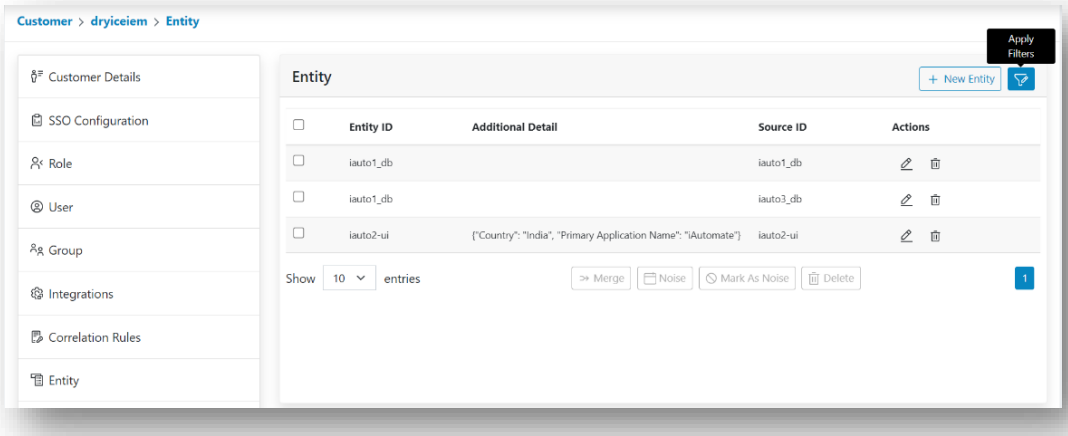

Figure 169 - Apply Filter Operation

2. The form will appear. From there user can select Field and operator from drop down list and should assign a value. Then click on the apply button.

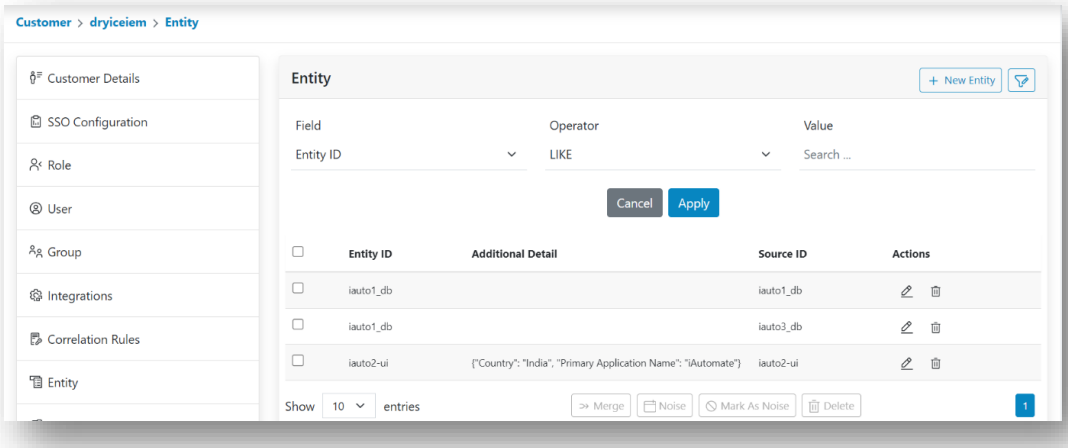

Figure 170 - Apply Filter Operation

3. User can see the result of applied filter.

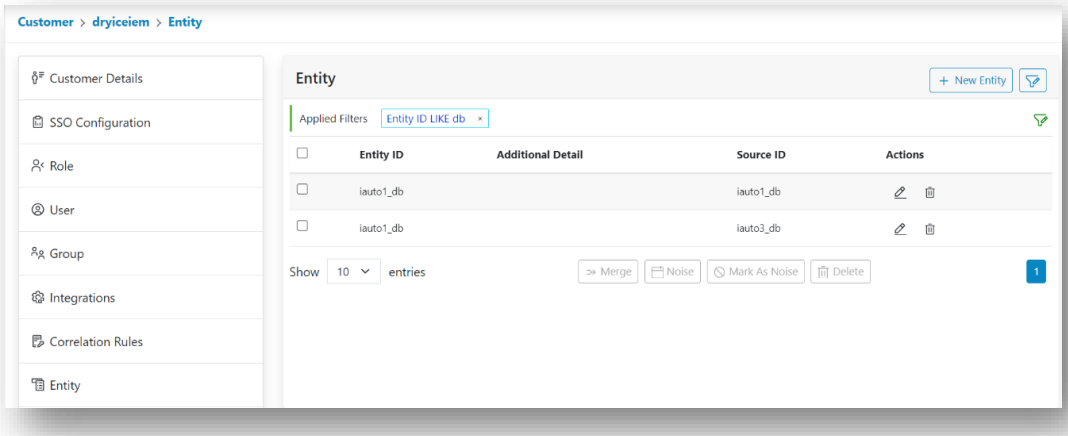

Figure 171 - Apply Filter Result

6.1.11.7 Topology

Topology helps to provide a comprehensive understanding of how different entities in the system are connected, allowing for effective monitoring, troubleshooting, and incident response.

Topology view that illustrates the relationships and connections between different components, such as servers, applications, databases, network devices, and other IT infrastructure elements will be displayed once the Topology is established in the system.

This section enables us to define the entity relationship data. If a rule is defined with topology filter selection, then the data is referred while correlating based on the rule definition. Refer to correlation rules to learn more about defining topology filter rules.

Like other screens user can perform actions based on their role.

1. Click the customer onboard section, for particular customers click on customer action edit section. Click on the Topology page, Records for the selected customer will be displayed in the grid view as shown.

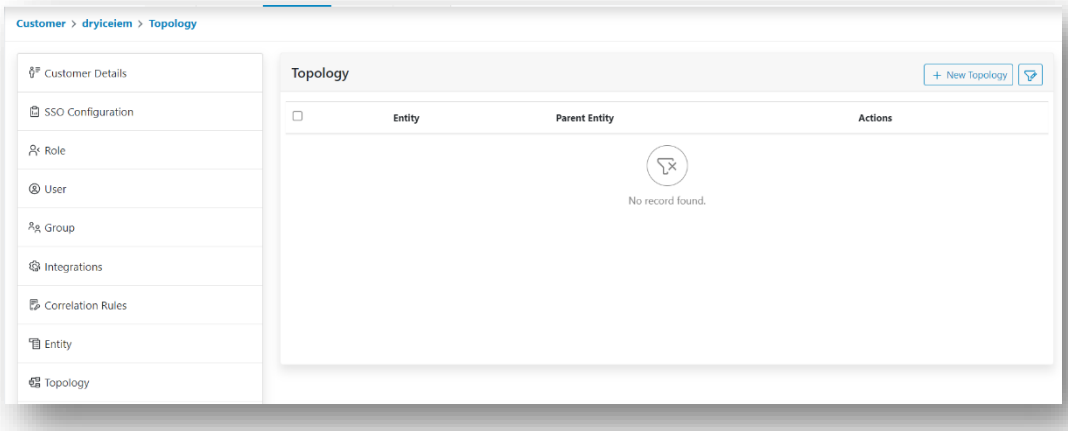

Figure 172 - Topology Page

2. Use the customer dropdown to change the customers and view data defined for it.
3. Following actions can be performed on the page:
   - Add New
   - Delete
   - Apply Filters

Add New Topology

Topology (Entity relationship) data can be added using the following two methods:

1. Create New by clicking on **+New Topology** Data Button.

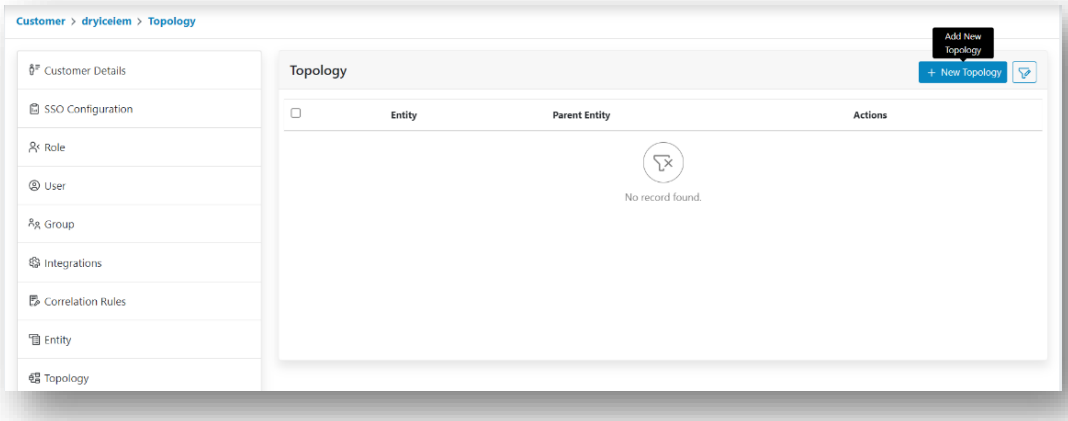

Figure 173 - Add Topology

2. Bulk Insertion can be done using the upload CSV option.
3. Choose a file based on the template available and upload it. Click on submit.

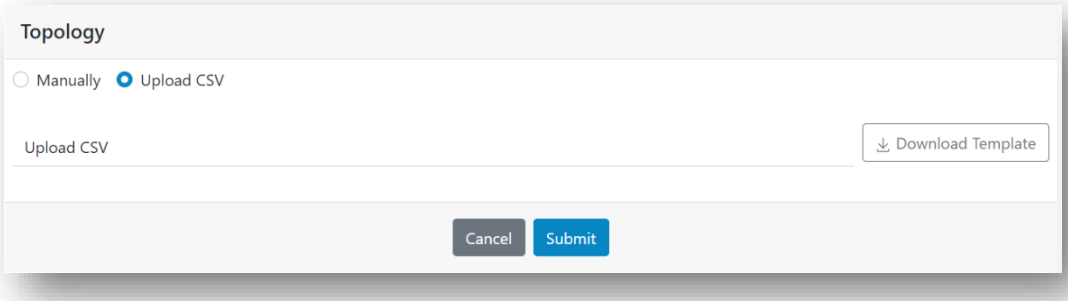

Figure 174 - Bulk Upload Topologies

Prior to adding the records ensure the Customer selection is proper. A new addition will enrich the records of the selected customer.

Let's next look at each action.

Individual Record Addition

1. Click on **+New Topology** Data button. This opens the following popup.

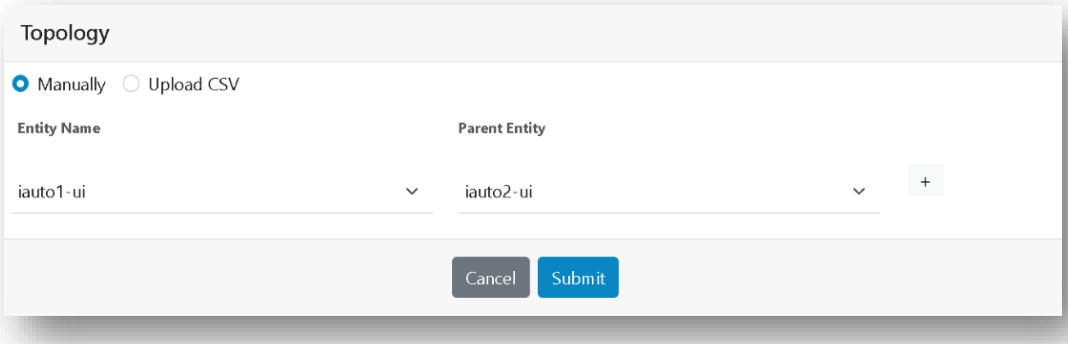

Figure 175 - Topology Creation

2. Entities which are configured for the selected customer using Configure -> Entity Screen appears in the Dropdown.
3. Select the entity and its parent entity from the dropdowns.

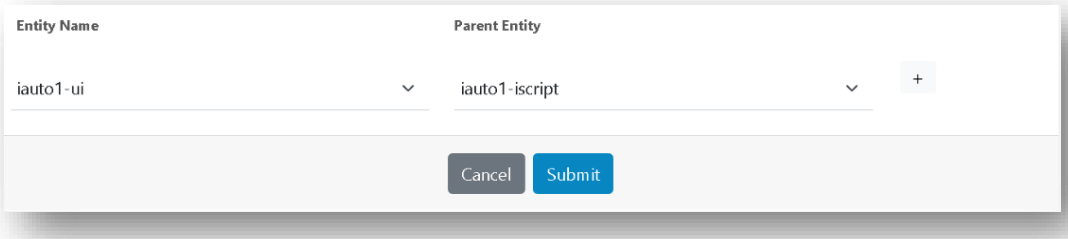

Figure 176 - Parent Entity Selection

4. Click on **Submit**.
5. On successful addition a prompt is displayed as shown.

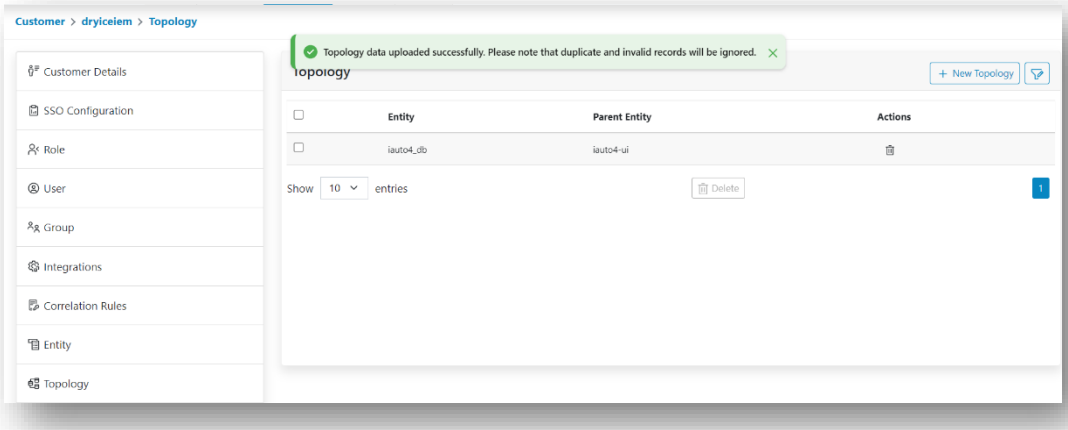

Figure 177 - Alert Message

6. The relationship data appears in the grid as shown.

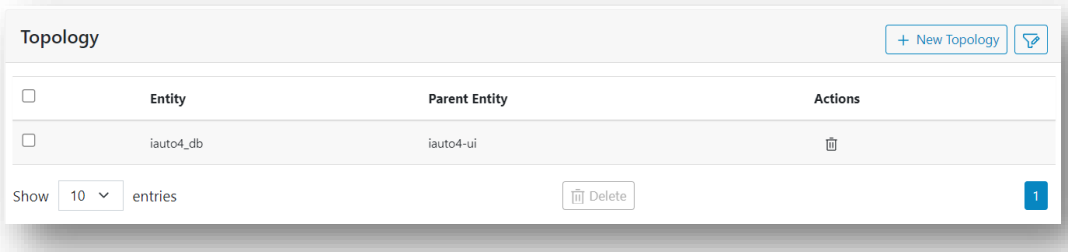

Figure 178 - Grid View for Topology

7. Using the similar approach, hierarchies can be defined between the entities.

Bulk Insert

In case large amount of data to be inserted in one go, the bulk insert option can be used.

1. Select Upload CSV option as shown. As user select Upload CSV the following record appears.

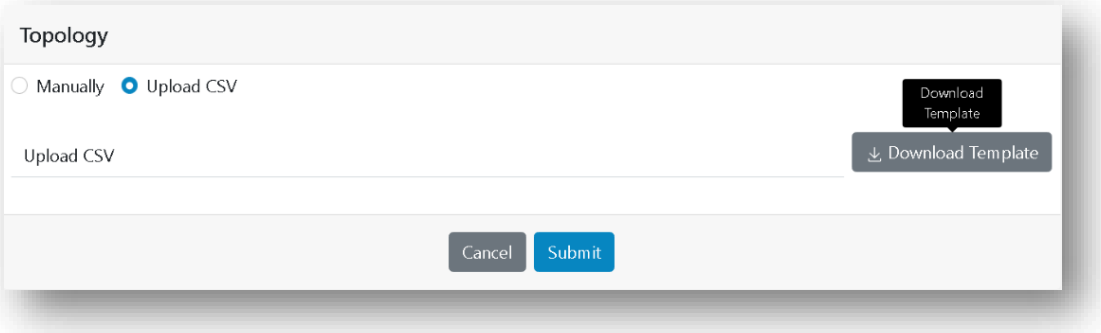

Figure 179 - Bulk Upload CSV

2. Click on the **Download Template** button. The following template is downloaded.

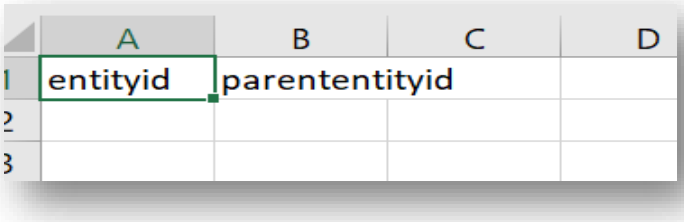

Figure 180 - Template Format of Bulk Topology

3. Define the parent child relationship data as shown. Save the CSV data.

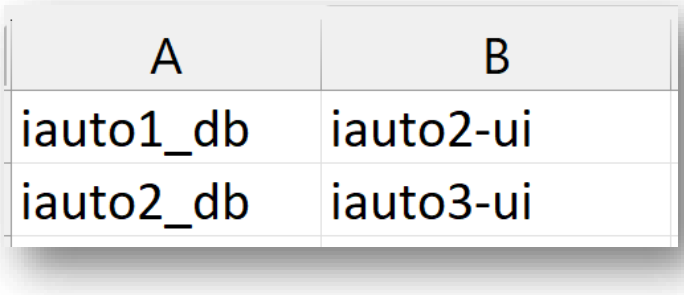

Figure 181 - CSV File of Parent and child entities

4. As the data is prepared, Upload the filled in excel by clicking on Upload CSV. Like with entities section browse to the local directory where the data file is saved and select the file. As the file is selected it appears as shown:

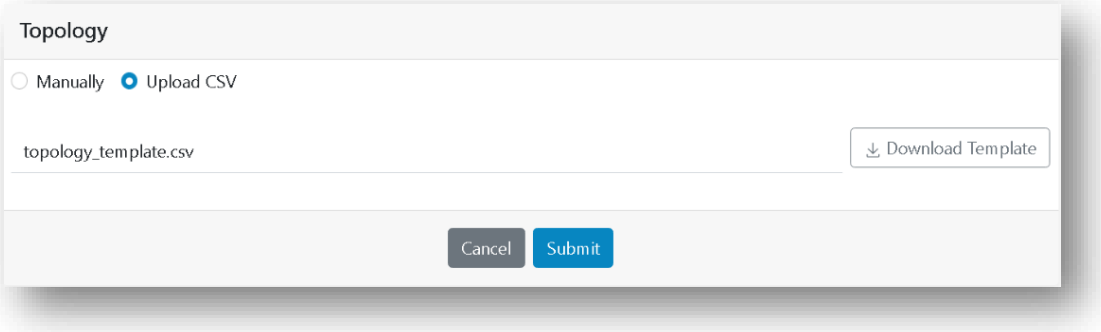

Figure 182 - Uploading the Topologies

5. Click **Submit**. On successful data creation, a confirmation box is displayed and the new data is displayed in the grid for the selected customer.

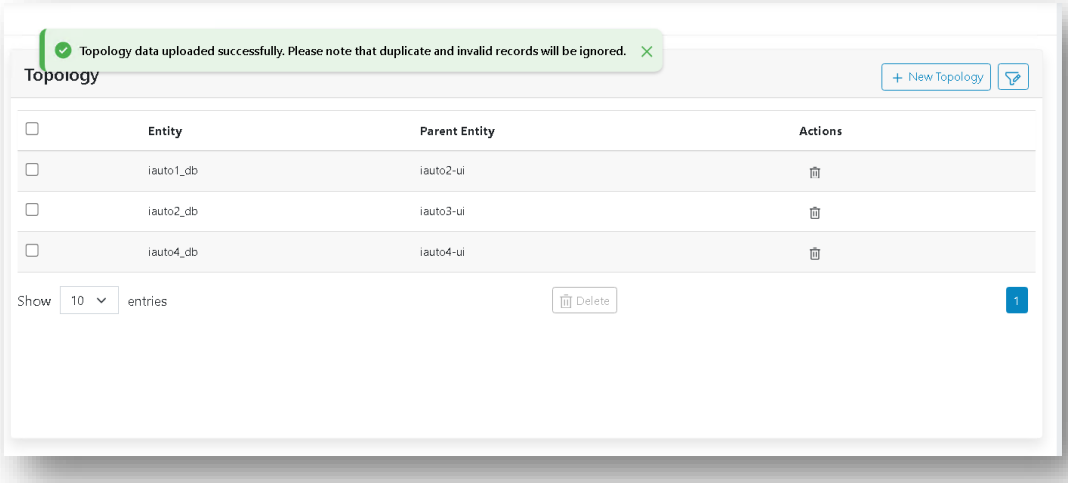

Figure 183 – Success popup

If entities are not pre-configured, uploading the sheet creates the entity records as well.

Delete Topology

If the relationship data are wrongly mapped or created or need to be removed, provision of bulk delete is available on the page.

1. Click on the check boxes next to the topology data to select the rows or relationship that needs to be deleted.

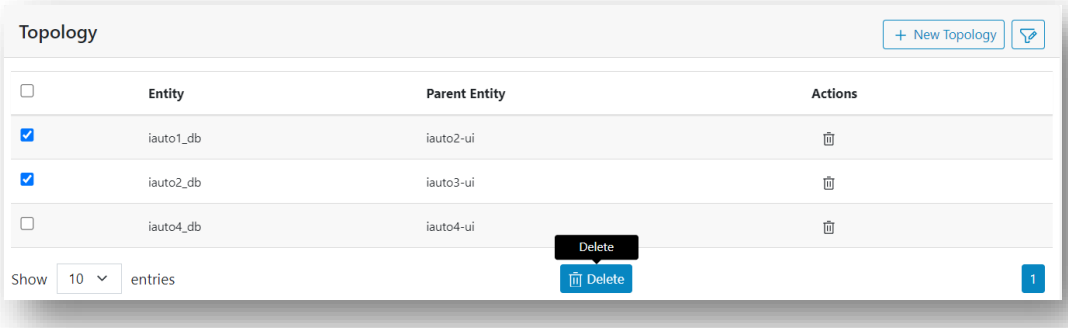

Figure 184 - Delete Topology

2. Like with the entities page as the rows are selected the icons on the footer of the grid are enabled and selection count is displayed as well.

Like entities, if all data is to be selected on the page, click on the checkbox in the header, it will select all the rows displayed on the page.

3. Click on the **Delete** icon.

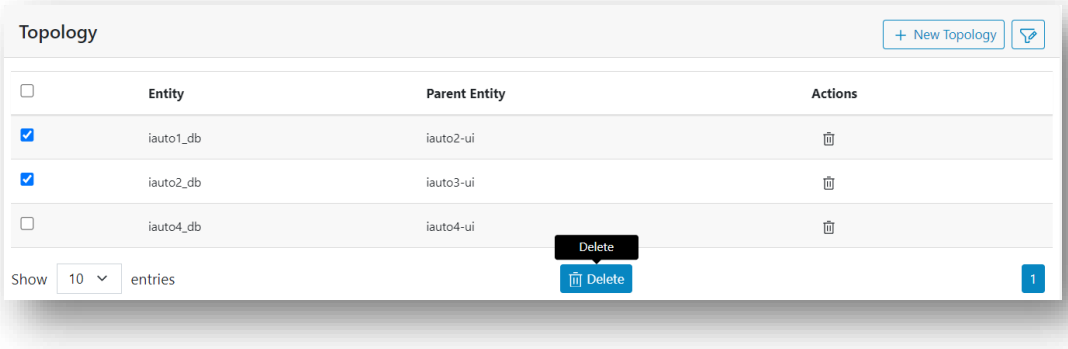

Figure 185 - Bulk Delete Topology

4. A confirmation box will be prompted.

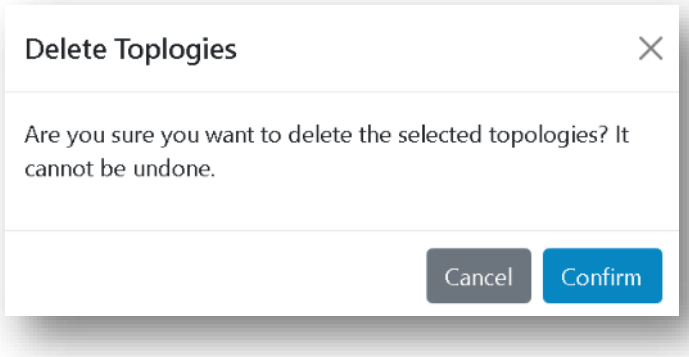

Figure 186 - Confirmation pop-up

5. Clicking Ok, deletes the selected relationship data.
6. On successful deletion rows are removed from the grid and a confirmation box is displayed.

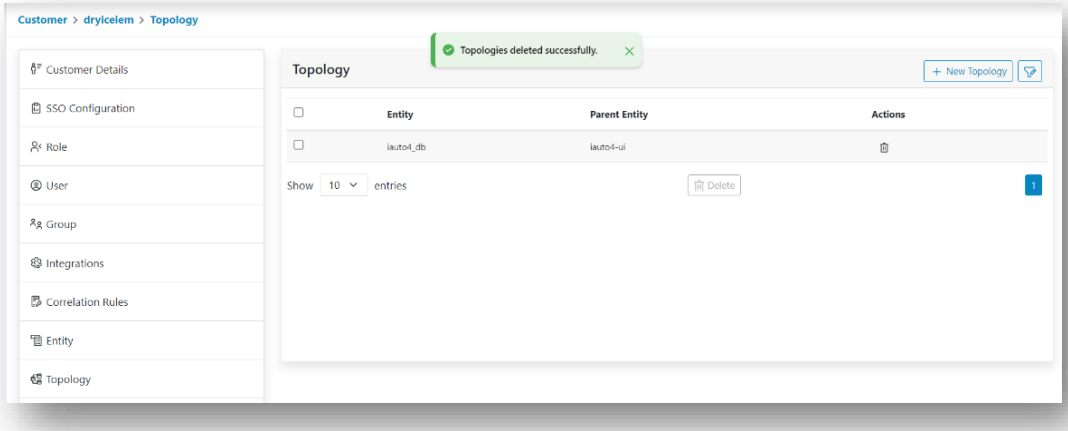

Figure 187 - Alert Message

6.1.11.8 Service Hierarchy

A service represents a business capability or functionality that is provided by the IT infrastructure.

A service is composed of various components, and there are dependencies between these components.

Understanding the relationships between components helps in mapping the service landscape and identifying potential points of failure.

In this section user define the service hierarchy. In here user create a service view and map it to the actual entities on which the alerts are created. This helps in populating the customer specific service view enabling the user to view the impact of events getting generated in the environment on the services in his/her environment.

Like other screens the user can perform actions based on their role.

1. Click the customer onboard section, for customer click on customer action edit section. Click on the Service Hierarchy page, Records for the selected customer will be displayed in the grid view as shown.

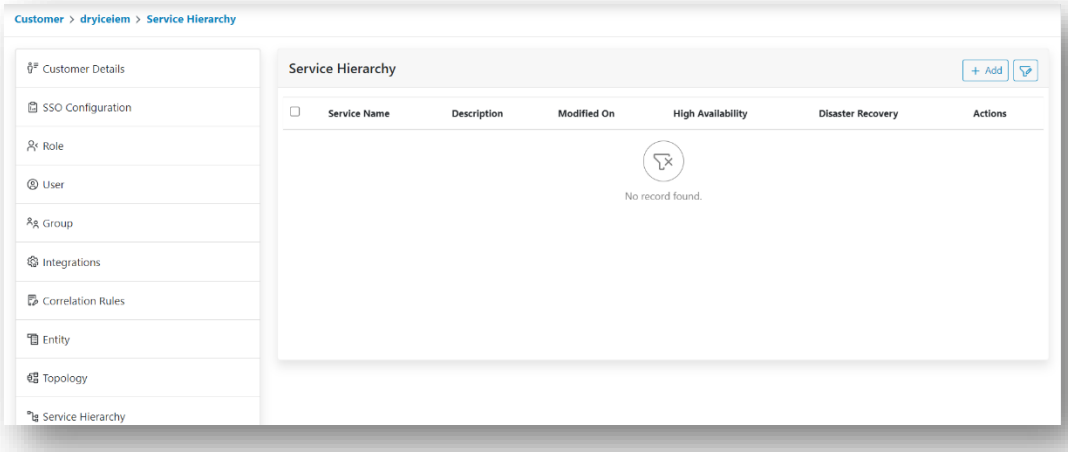

Figure 188 - Service Hierarchy Page

2. Use the customer dropdown to change the customers and view data defined for it.

   Following actions can be performed on the page:

   - Add New
   - Edit
   - Delete
   - Manage Relationship and Entities
   - Apply Filters

Add New Service Hierarchy

3. Click on **+ Add** button at the top of the grid to create a new Service.

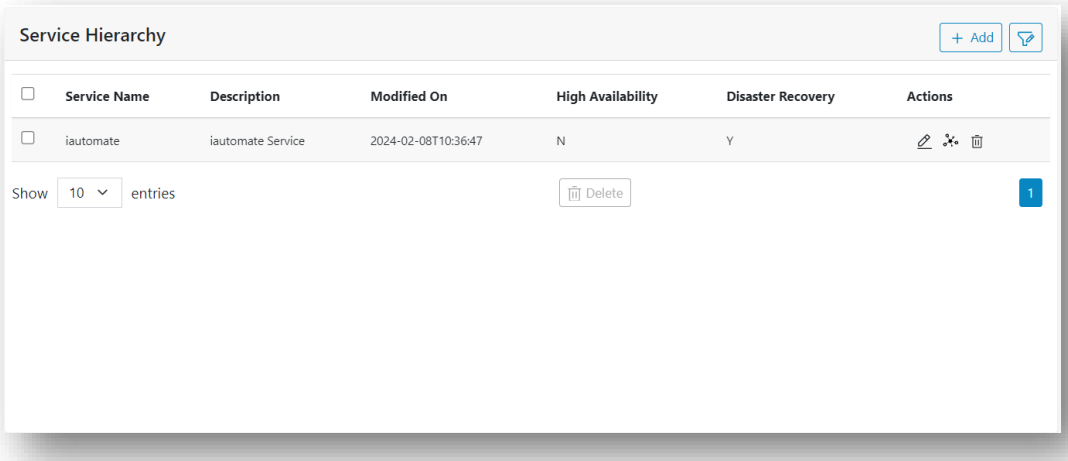

Figure 189 - Service Creation

Please ensure that the actual customer for which the data is being added is selected in the dropdown at the top of the page. As any addition will be mapped to the customer selected in the dropdown.

4. The following popup is displayed.

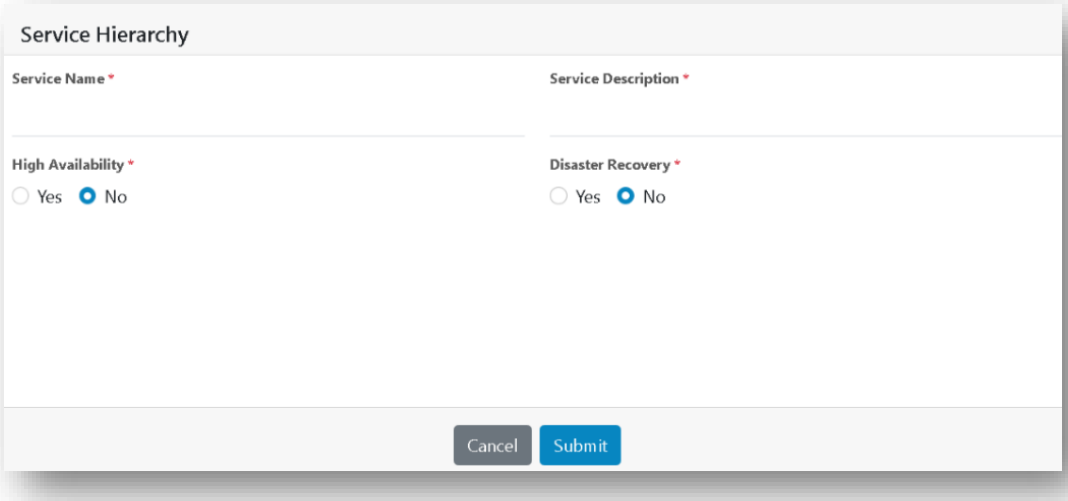

Figure 190 - Service Add Configuration

5. Enter the **Service Name** and **Description**.
6. Select radio button Yes or No for HA (High Availability) and for DR (Disaster Recovery)

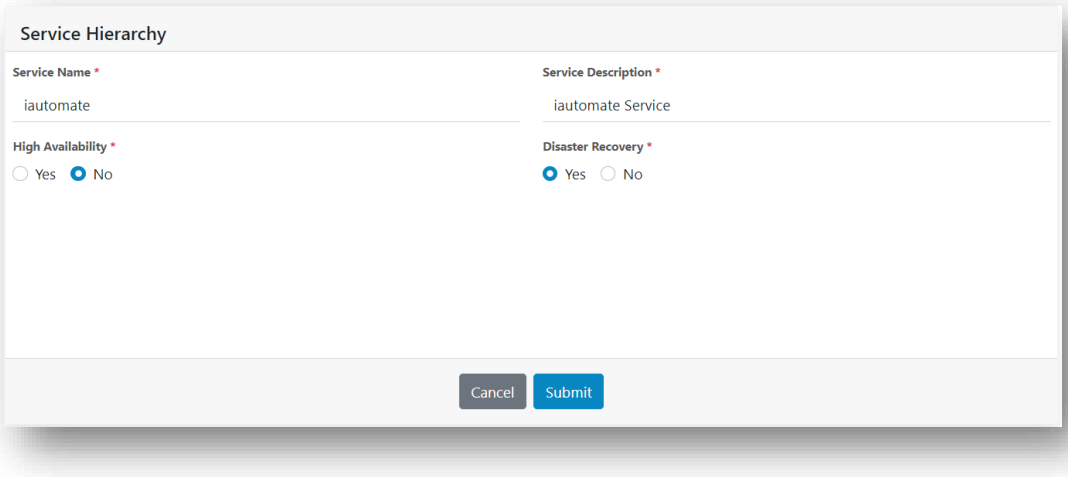

Figure 191 - Selecting Dropdown

7. Click **Submit**.
8. On successful addition the following message is displayed.

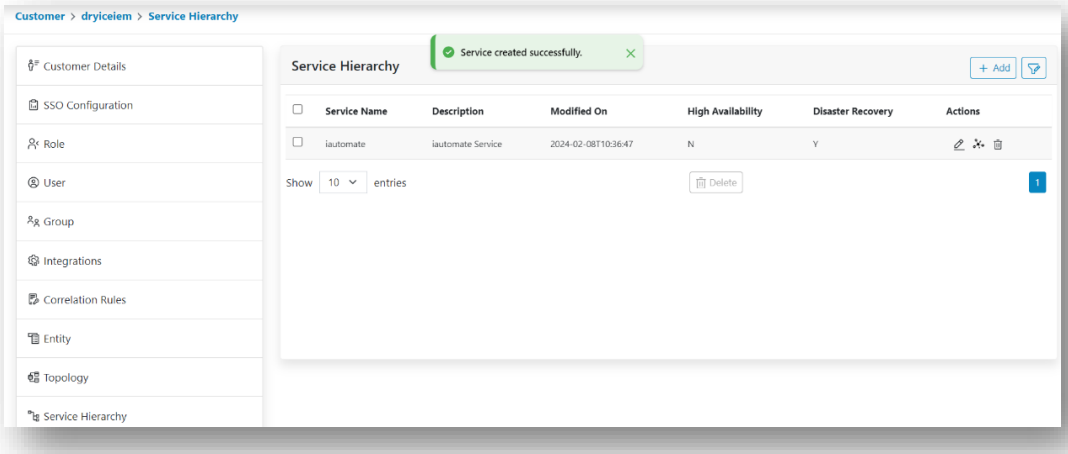

Figure 192 - Alert Message

9. The service will start appearing in the grid as shown below.

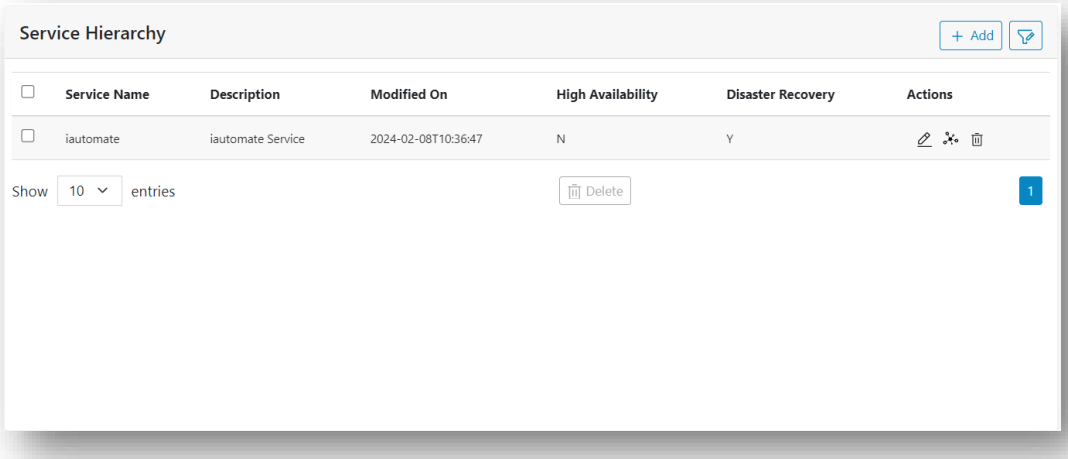

Figure 193 - Grid View for Service Hierarchy

Edit Service Hierarchy

1. Like in the other views, click on the edit icon next to the Service which needs to be edited.

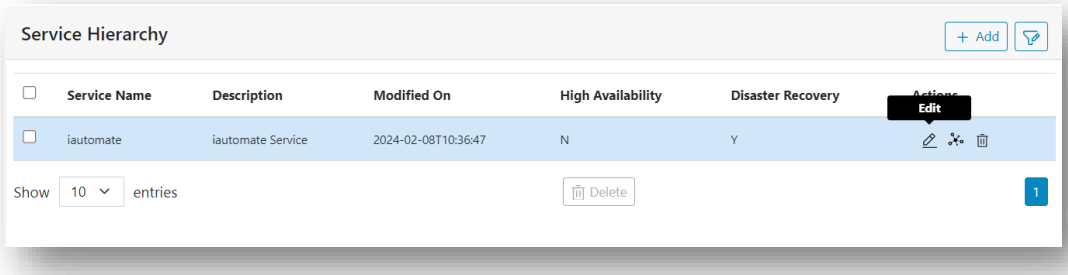

Figure 194 - Edit Service

2. Saved data according to popup.
3. Make the necessary changes. For this example, parse let's edit the Name.

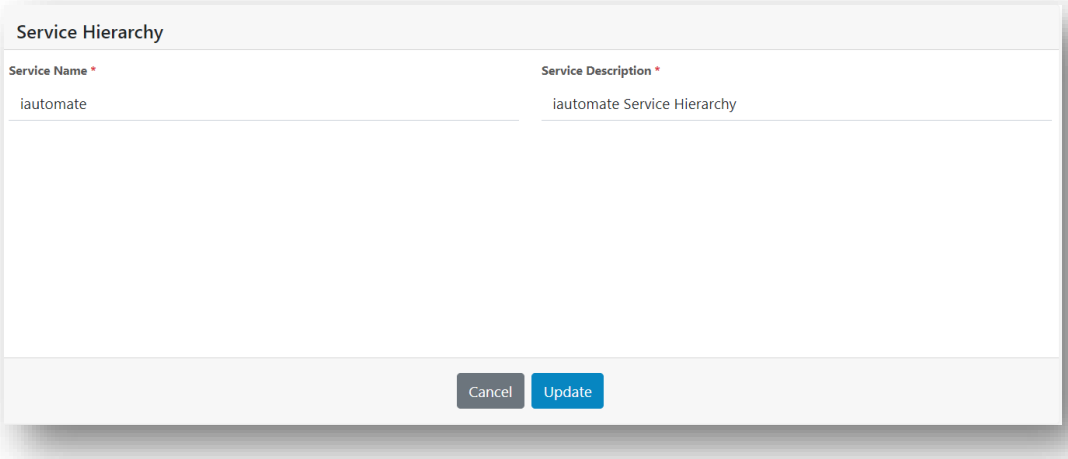

Figure 195 - Editing Service

4. Click Submit. On successful update the following popup message is displayed.

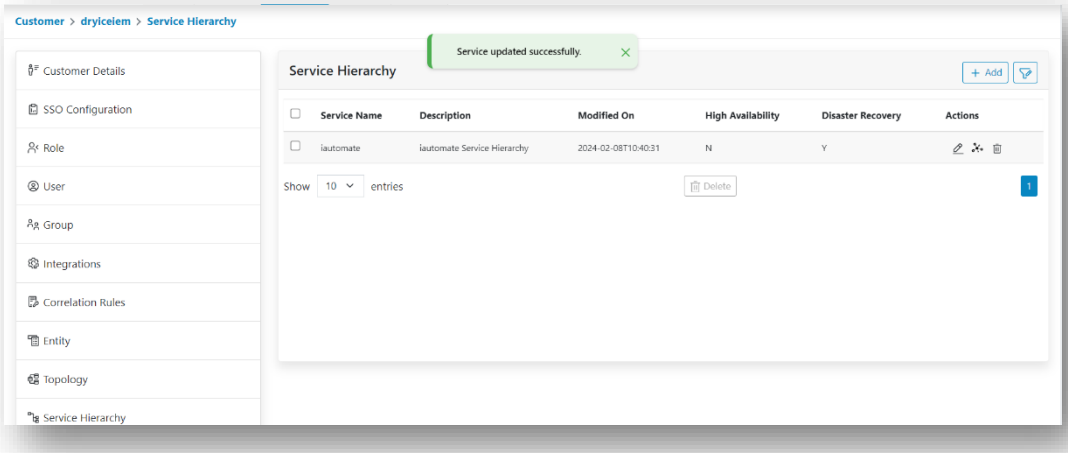

Figure 196 - Alert Message

Delete Service Hierarchy

1. Like with the entity and the topology screen, select the services that is to be deleted by selecting the check boxes next to their names in the grid view.

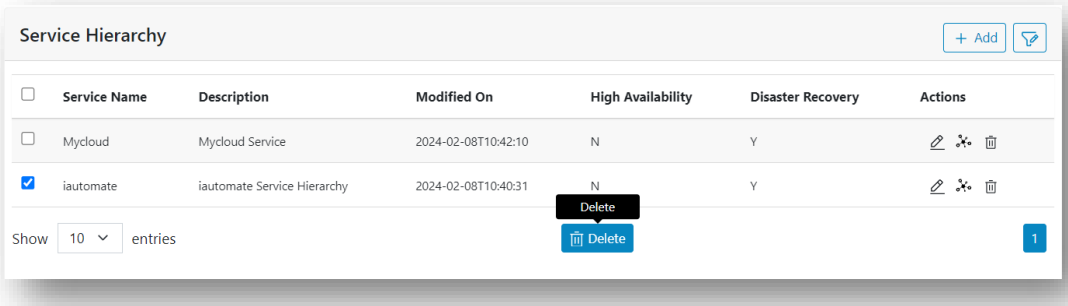

Figure 197 - Selecting Services

2. The icons will be enabled in the footer.

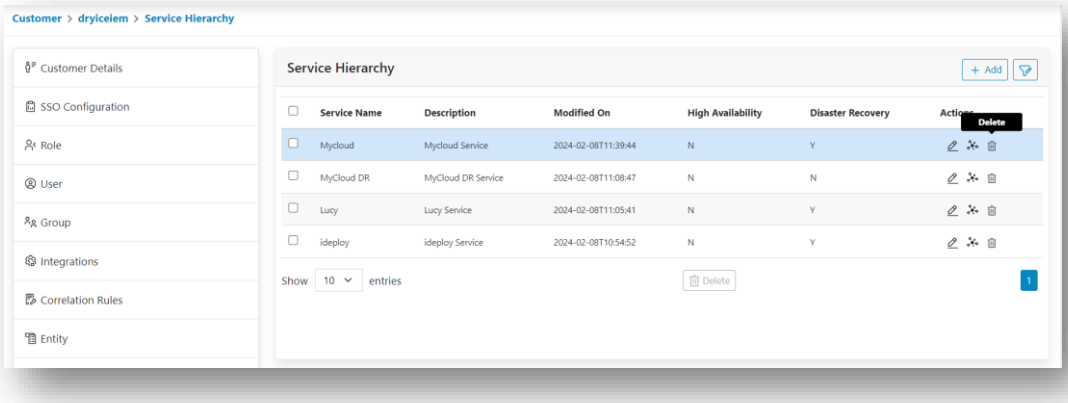

Figure 198 - Deleting Services

3. A Confirmation message box is prompted as shown.

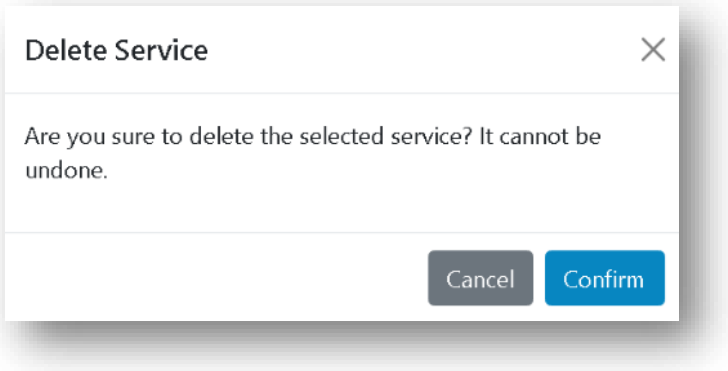

Figure 199 - Confirmation pop-up

4. Click on Confirm. On success the following popup is displayed.

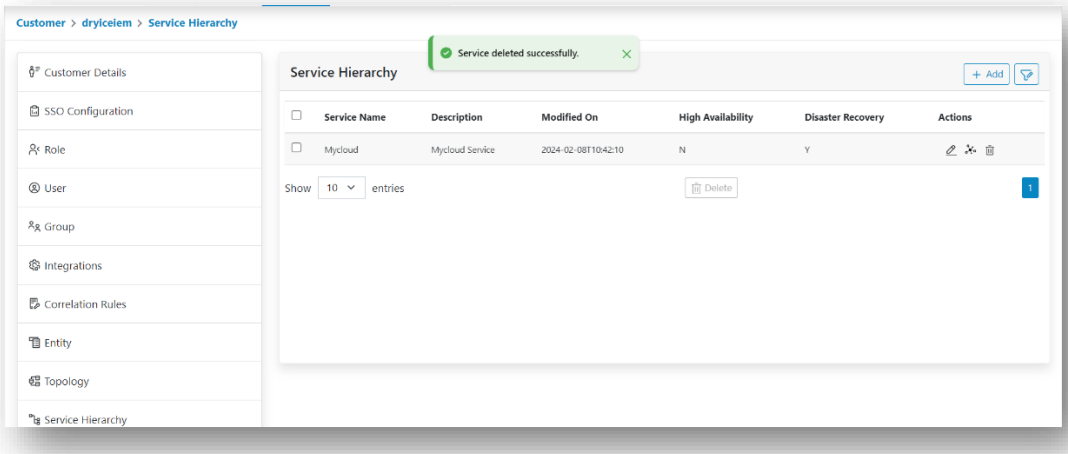

Figure 200 - Alert Message

Mapping Service Hierarchy

Mapping services in IEM involves the identification, visualization, and analysis of the relationships and dependencies between different services within an IT environment. This process is essential for understanding how services interact, detecting potential issues, and facilitating effective actionable management.

The relationship between the created services can be defined by clicking the Mapping icon below the actions field. By using this option, the mapping between the actual entities can be done.

1. Click on the service to see the details related to the service. There are three actions visible for a particular service: - Edit, Delete and Mapping.

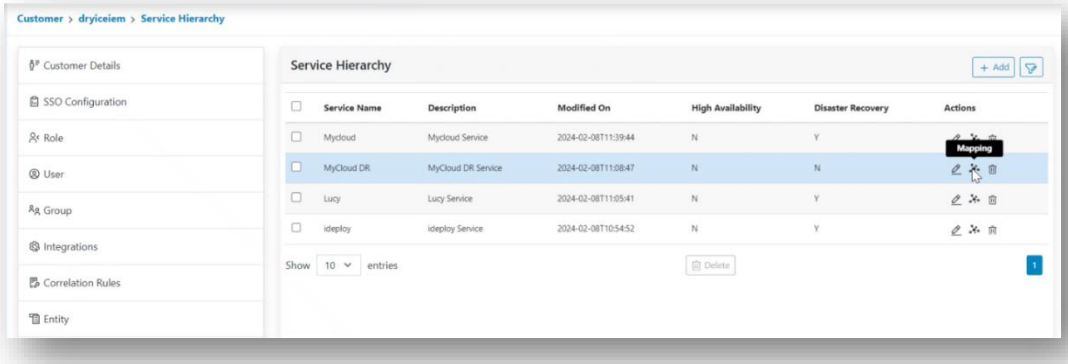

Figure 201 - Mapping Service

2. After clicking the **Mapping** icon on the service, user have the following two tabs: -
   - Define Topology
   - Map Entities

– **Define Topology** - This tab enables us to manage the relationship data. Let's click on the tab.

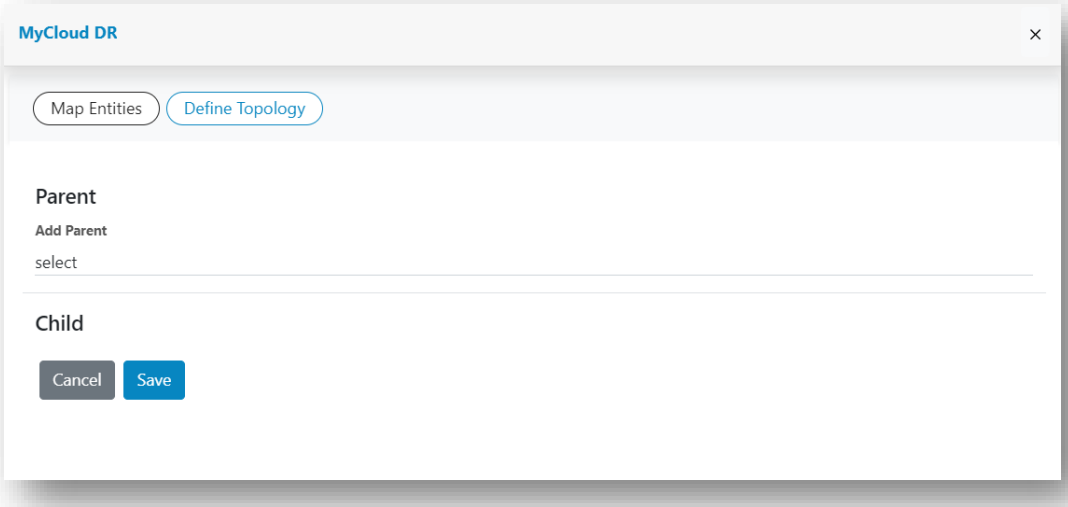

Figure 202 - Define Topology

a. It's divided into two sections:
   - **Parent** – In this section the mapping happens. Users specify the parent node here.
   - **Child** – This is a display only section. All the child services of the selected service will be displayed here.

b. Let's add a parent service. Click and select from the services available in the dropdown.

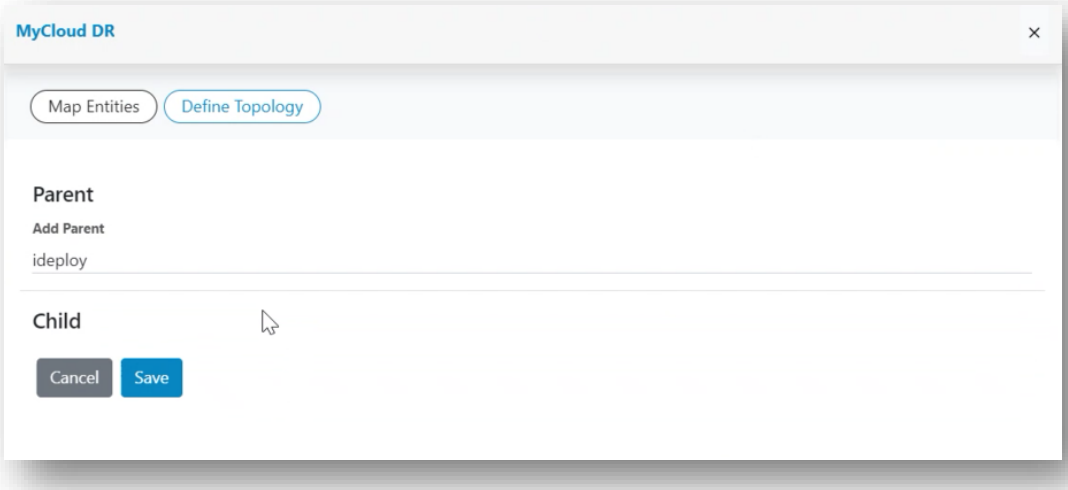

Figure 203 - Applying Parent Service

For example, let's select ideploy as Parent.

c. Click **Save**.

The following confirmation box will be displayed.

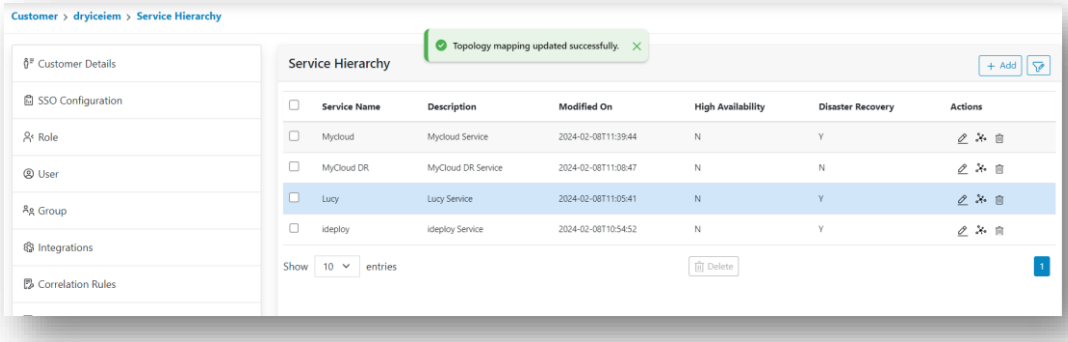

Figure 204 - Alert Message

d. Relationship has been created. Click on mapping icon of ideploy service and user can view the child of the service which the user has created above.

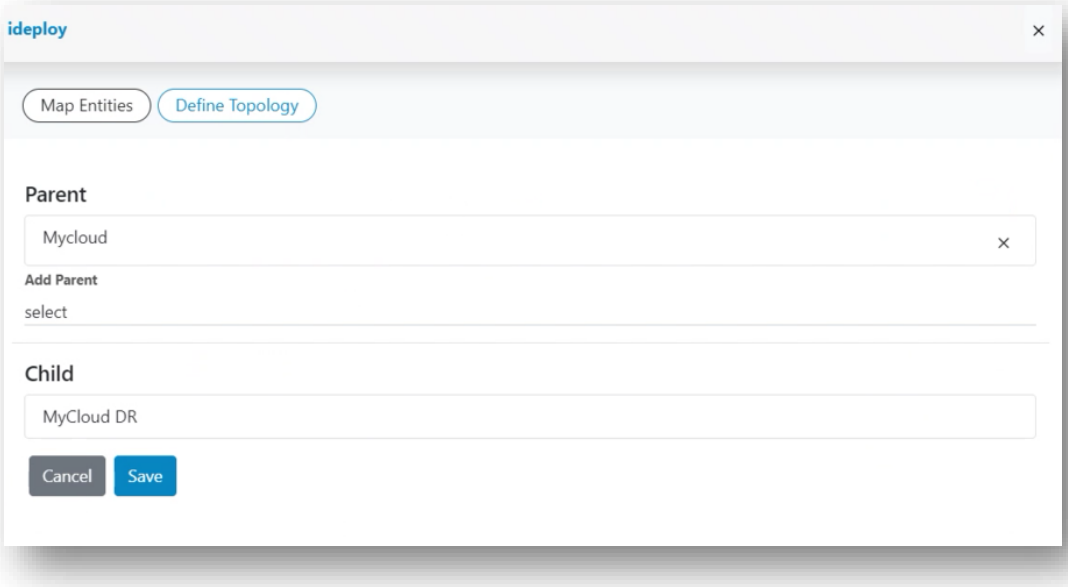

Figure 205 - Parent Service Name

e. A service can have multiple parents defined using the Add Parent drop down. Once a parent is added, it will start appearing underneath the Parent section.

User needs to save the parent one after the other.

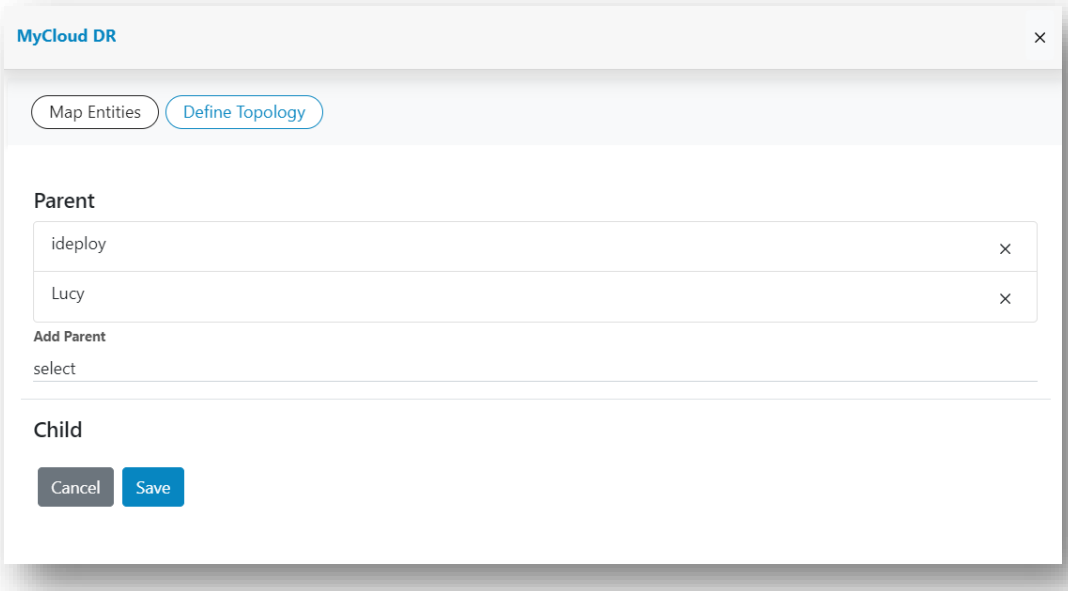

Figure 206 - Parent List Services

f. In case a relationship is wrongly created, click on the cross button next to the parent row to remove the relationship.

g. The row will disappear, click on Save button to save the changes permanently.

h. On successful save the following popup message will be displayed.

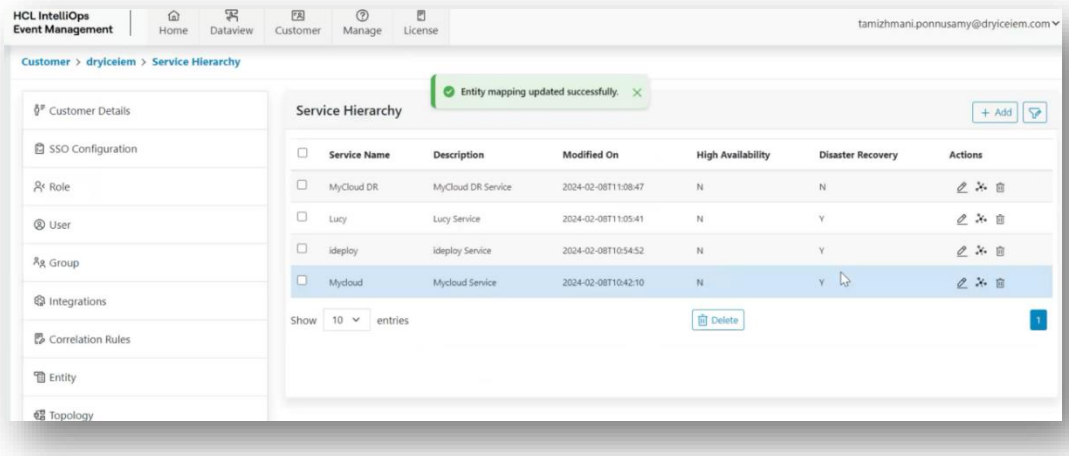

Figure 207 - Alert Message

– **Map Entities** – Here user maps the service to the actual entities. A service can be mapped to one or more entities.

If High Availability (HA) and Disaster Recovery (DR) both are disabled, at that time user can map only one entity to the service. Else if any of the HA and DR is enabled or both are enabled, user can map two or more than two entities to the service.

a. Clicking on the tab lists all the entities created for the selected customer.

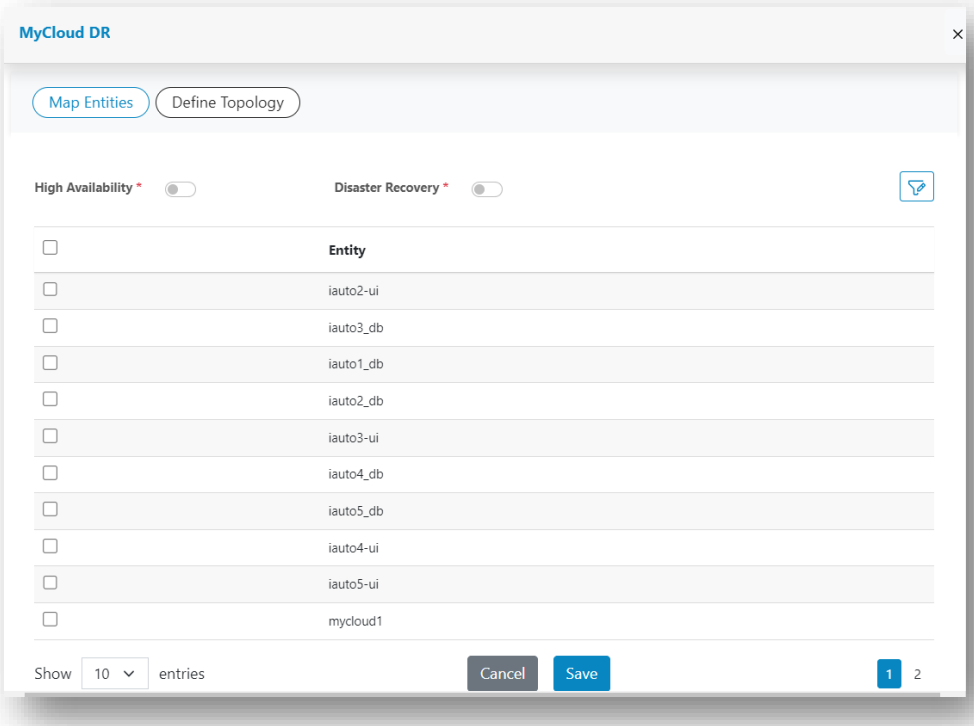

Figure 208 - Map Entities

b. Select the entities by clicking on the check boxes next to its name. For example, parse let's map iauto2-ui (as both HA and DR is disabled).

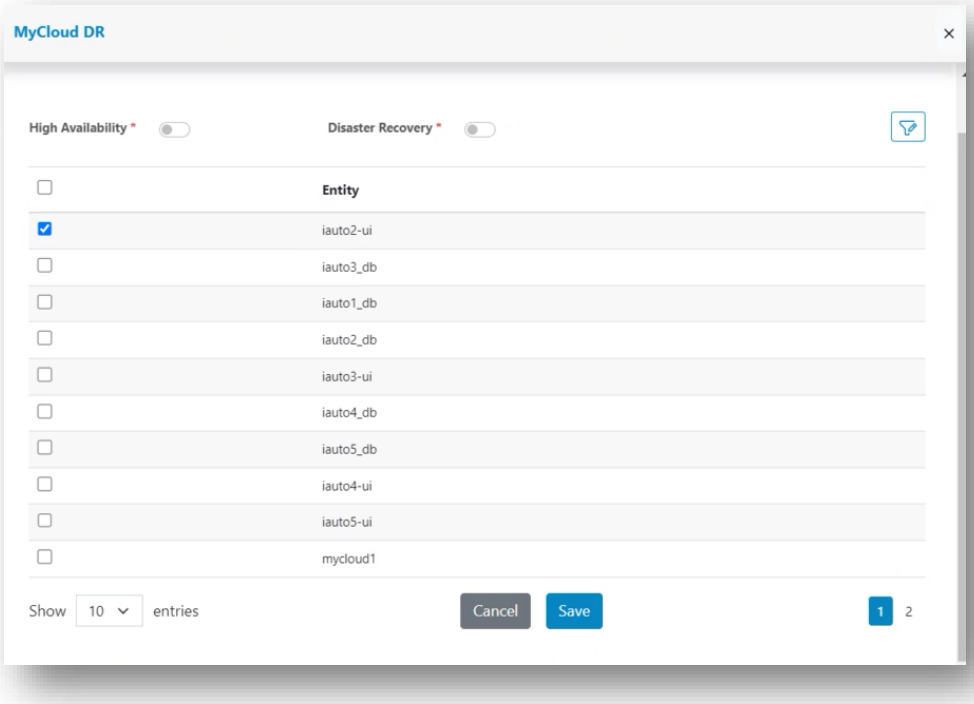

Figure 209 - Selected Entities for Service

Impact of mapping the service to the entities are, if an alert exists which is not closed, the node will be highlighted in the service view, and the flow will also propagate up in the view showing the impact on the parent nodes as well.

c. Click on **Save**.

d. On successful update, the following popup is displayed.

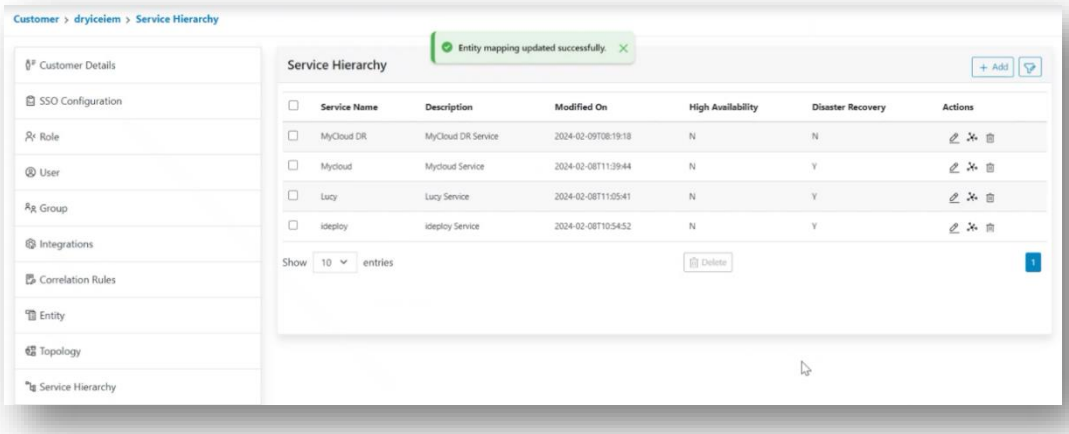

Figure 210 - Alert Message

e. Click **Ok**. The selected entities will start appearing at the top of the grid.

Apply Filters

The steps explain how to Apply filter to the Service Hierarchy Data.

1. Click on the **Apply Filters** action button present at the below header of the console.

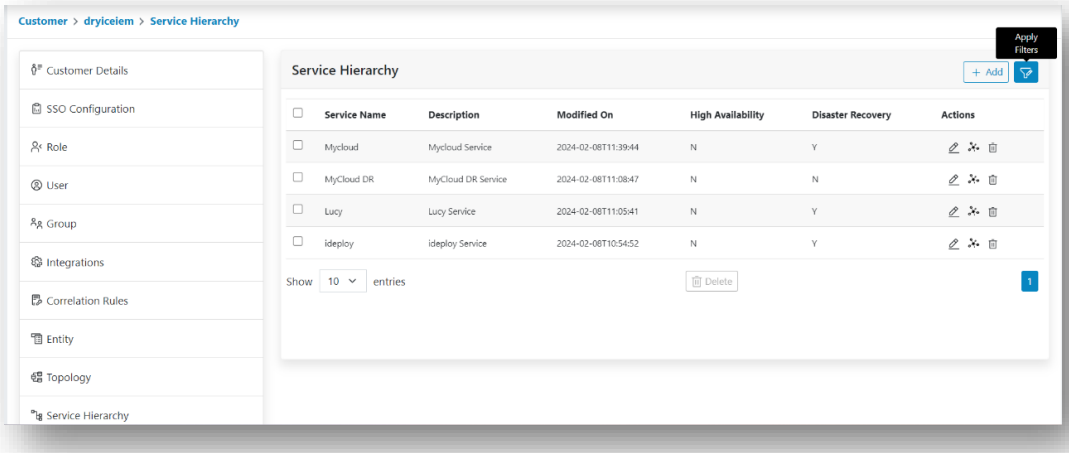

Figure 211 - Apply Filter Operation

2. The form will appear from there user can select Filed and operator from drop down list and must write value. Then click on the apply button.

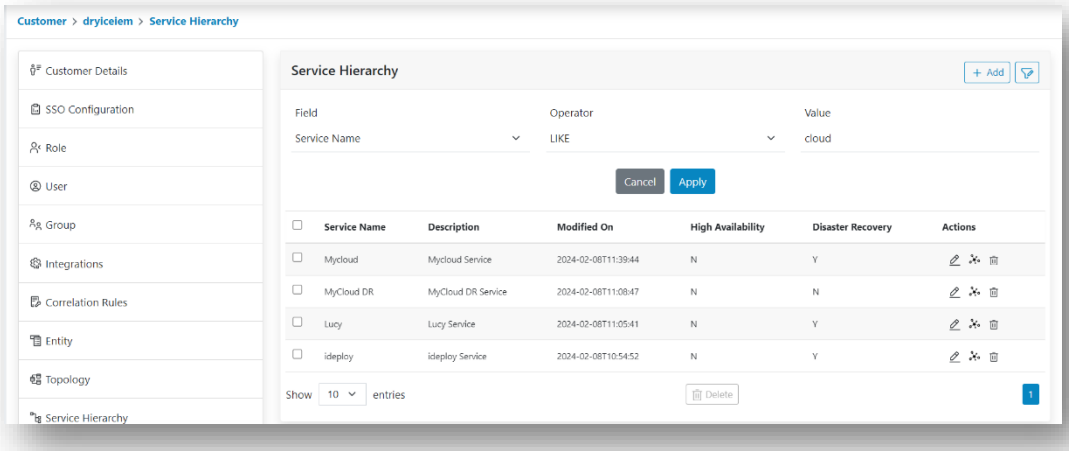

Figure 212 - Apply Filter Operation

3. User can see the result of applied filter.

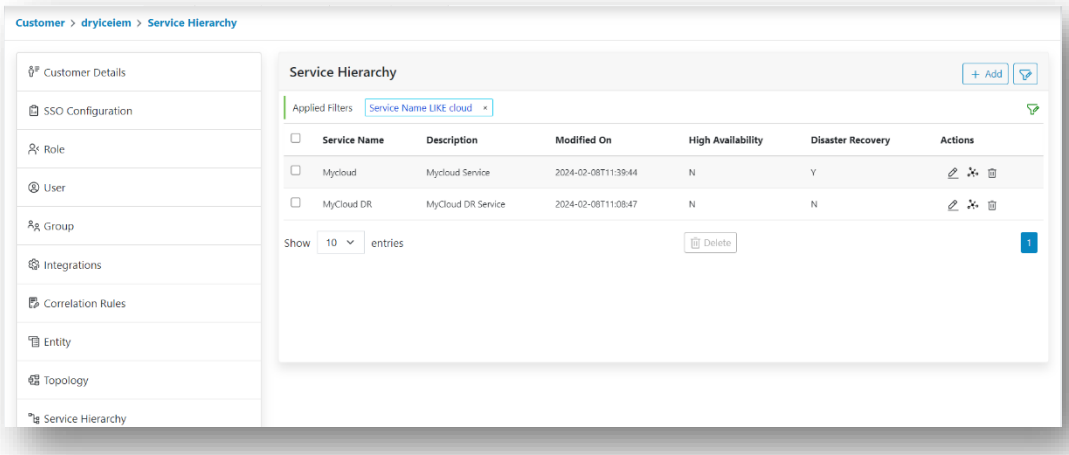

Figure 213 - Apply Filter Result

6.1.11.9 Noise Maintenance

Noise maintenance" refers to the ongoing process of managing and reducing the amount of irrelevant or non-actionable events, alerts, or data generated by the monitoring and detection systems. Noise, in this context, represents information that does not contribute to meaningful insights or indicate significant issues. Reducing noise is crucial for optimizing the efficiency of actionable detection, analysis, and resolution.

“Noise Maintenance Window" refers to a specific timeframe or scheduled period during which fine-tuning activities are performed to manage and reduce the noise generated by the monitoring and alerting systems.
This window allows IT teams to proactively address issues related to false positives, irrelevant alerts, or unnecessary noise in the event data.

This section enables user to define rules for filtering out events data at the beginning of event data processing. User can perform actions based on their role.

1. Click the customer onboard section, for particular customers click on customer action edit section. Click on the Noise/Maintenance window page, Records for the selected customer will be displayed in the grid view as shown.

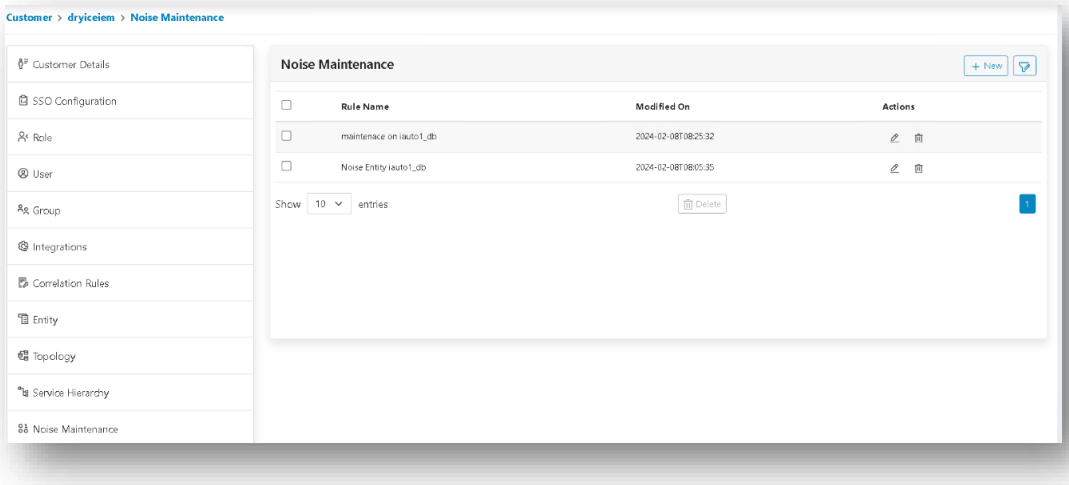

Figure 214 - Noise Maintenance Page

2. User can perform the following actions:
    - Add new
    - Edit
    - Delete
    - Apply Filter

Noise Rules can be created from the Entity screen as well. Refer to the Entity section. Those rules appear prefixed with the action i.e., whether it’s a Noise or a Maintenance configuration followed with the Entity name, user can create rule based on entity id only. In the Noise screen grid user can also see the rules that are configured from Entity screen and also the Noise Maintenance screen.

Add New Noise Maintenance

1. Click on the **+ New** button at the top of the grid to create a new rule.

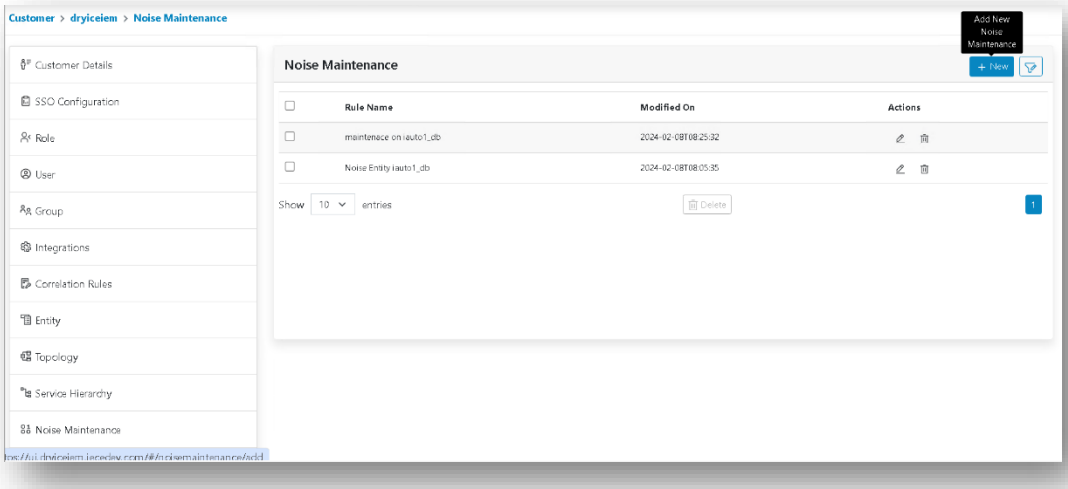

Figure 215 - New Noise Rule Creation

2. The following form is opened. Click on the **+Add** button.

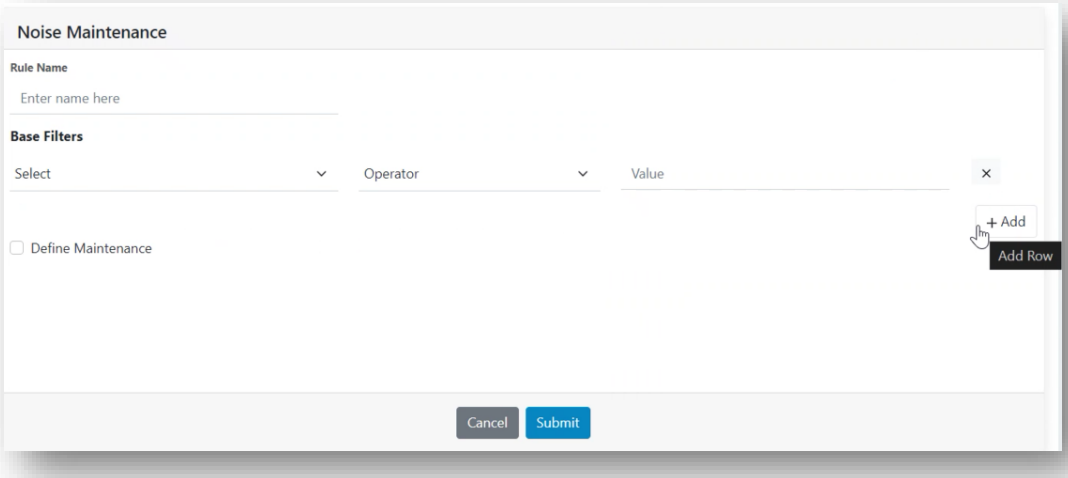

Figure 216 - Add Base Filters

3. The following page appears:

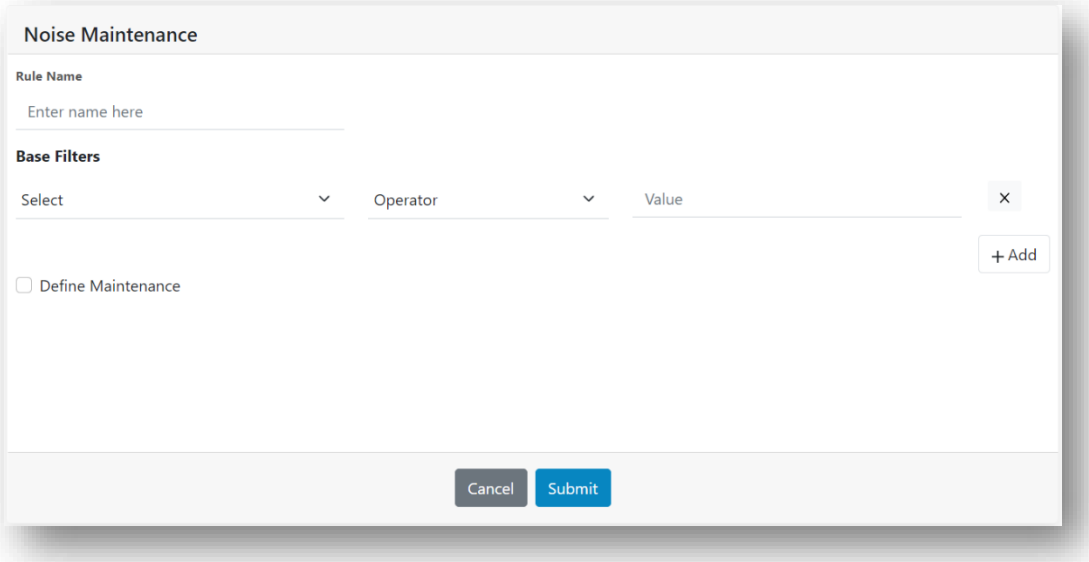

Figure 217 - Base Filters Menu

4. In **Base Filter** click on select field dropdown.

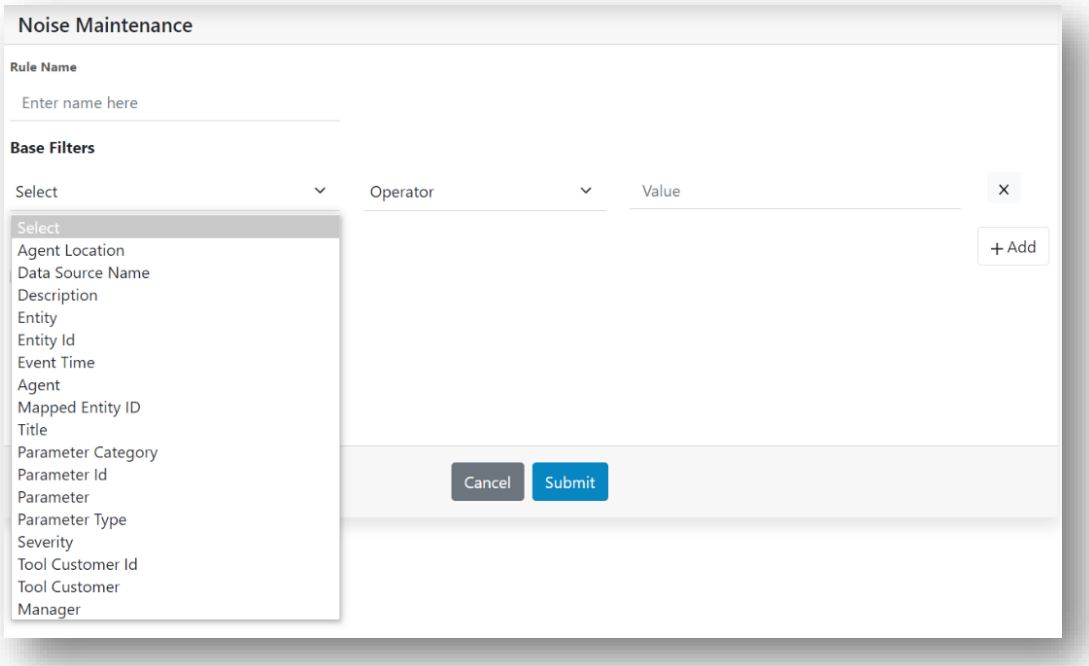

Figure 218 - Selection of The Field

5. Select any one of the fields like entity and select any operator from the dropdown.

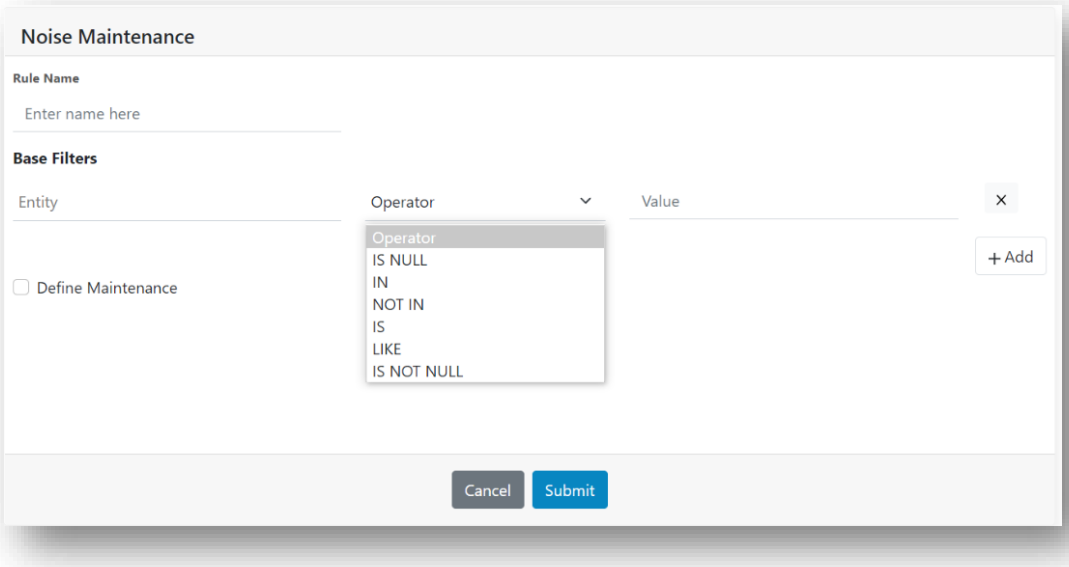

Figure 219 - Selection of The Operator

6. After selection of operator, specify the name of entity and add base filters.

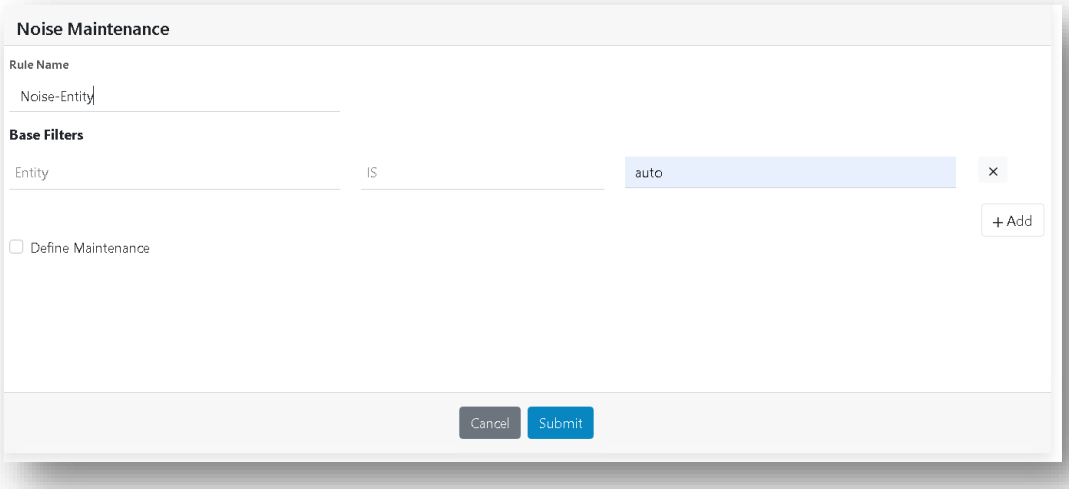

Figure 220 - Rule Name for Noise

7. In addition, like in Entity page, user can also specify maintenance window details. Refer the section Define Maintenance Window. The following screen appears:

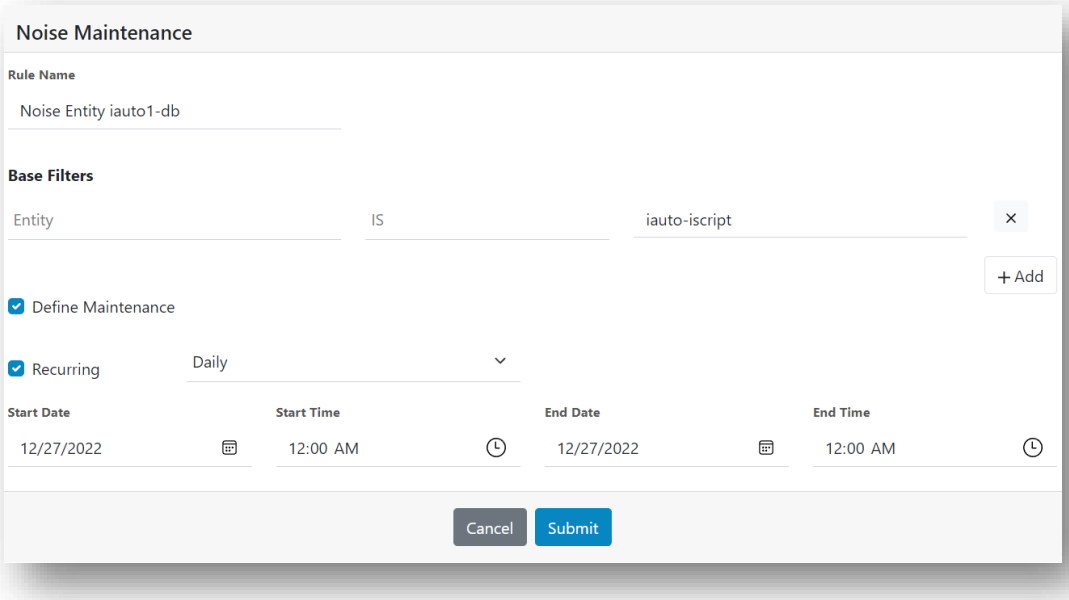

Figure 221 - Define Maintenance for Noise Rule

Reference- This section is like the one explained in Define Maintenance Window section.

8. In Entity screen, after selecting particular entity then user will click on the Noise button, Maintenance window will appear. Once user adds all the field data and on submission a Noise rule will be created for the particular entity in Noise Maintenance screen.
9. For Mark as Noise button in Entity screen, a noise rule will be created for the particular entity in the Noise Maintenance screen without any time constraints.
10. The recurring option shows the dropdown that contains Daily, Monthly, Weekly options for checking from the dropdown.

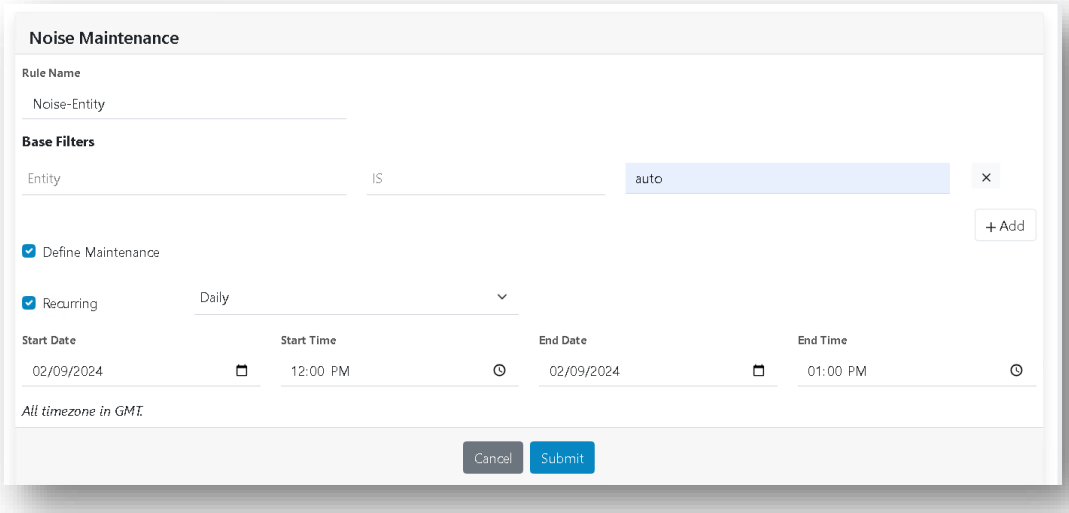

Figure 222 - Define Maintenance for Noise Rule

11. Click on **Submit**. A confirmation message is displayed.

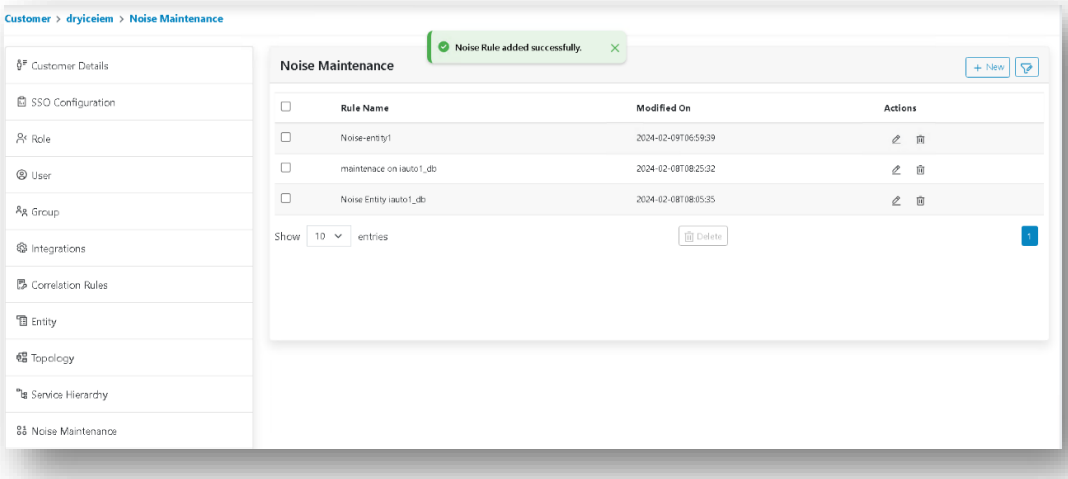

Figure 223 - Alert Message

12. The rule will start appearing in the gird view.
13. Let's next look at the way user can create time base (maintenance window) rule as well. Let's specify entity as auto and a one-time window as shown.

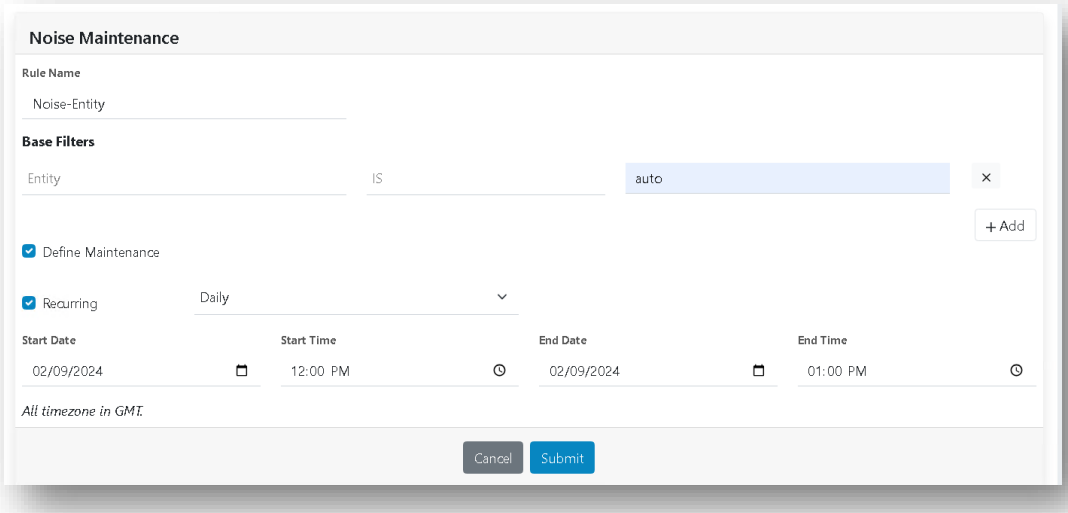

Figure 224 - Define Maintenance for Noise

14. This rule means that any data created on 9th February between 12PM to 1PM for the entity auto will be filtered out and will not process further. Events outside the window specified will be processed using the normal flow.
15. Like the previous rule, Clicking Submit, the rule will start appearing in the grid view.

Edit Noise Maintenance

Reviewing and modifying Maintenance window helps in adapting to changes in the environment and creating a window that clubs the events that are considered as noise within a specific timeframe and ensuring that alerts are relevant and indicative of actual issues.

User can edit the created noise rule also.

1. Click on the edit icon next to the rule which needs to be edited.

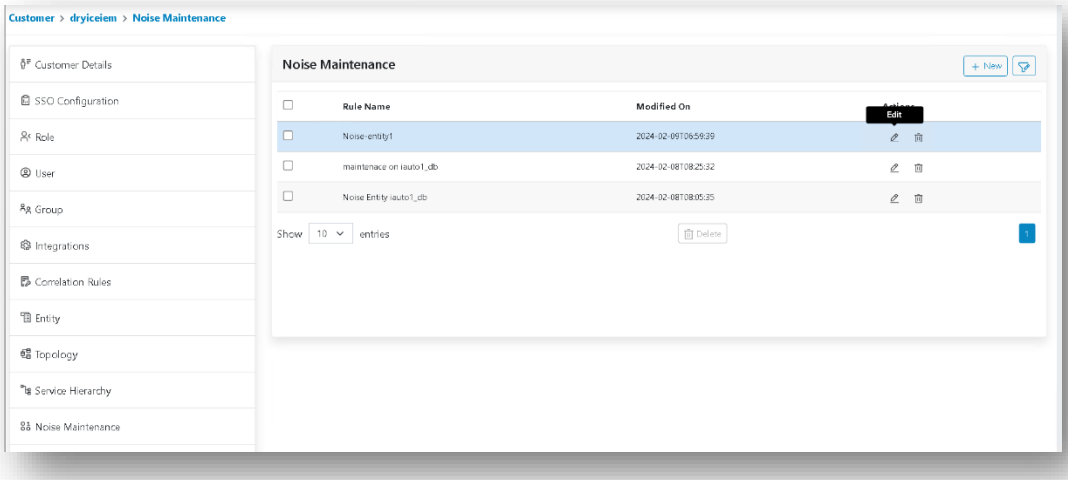

Figure 225 - Edit Option for Noise Rule

2. The Noise Maintenance window can be edited with the edit option. Base Filters can be added for the Noise Rule and after making the changes, click on the Submit button.

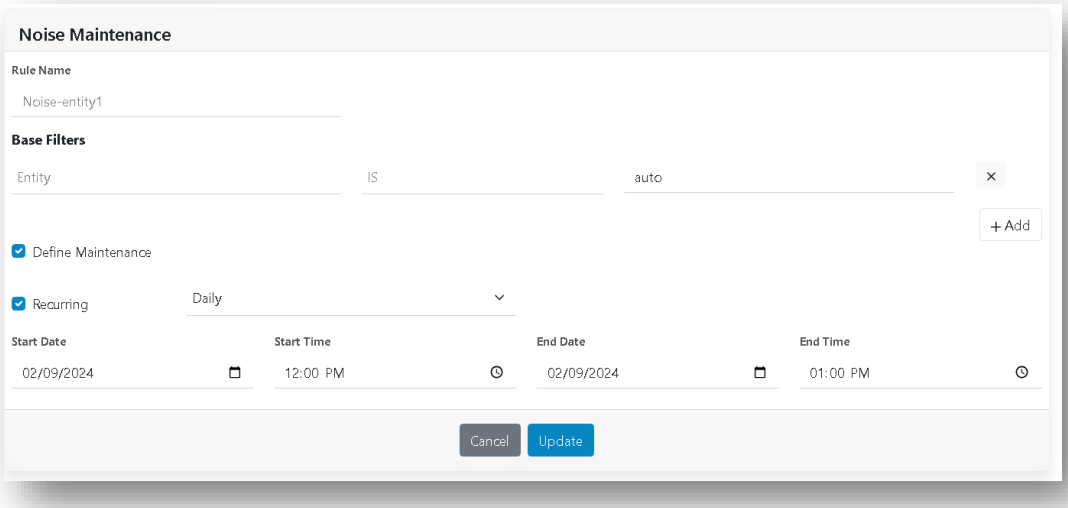

Figure 226 - Editing Noise Rule

3. A success message appears as shown below.

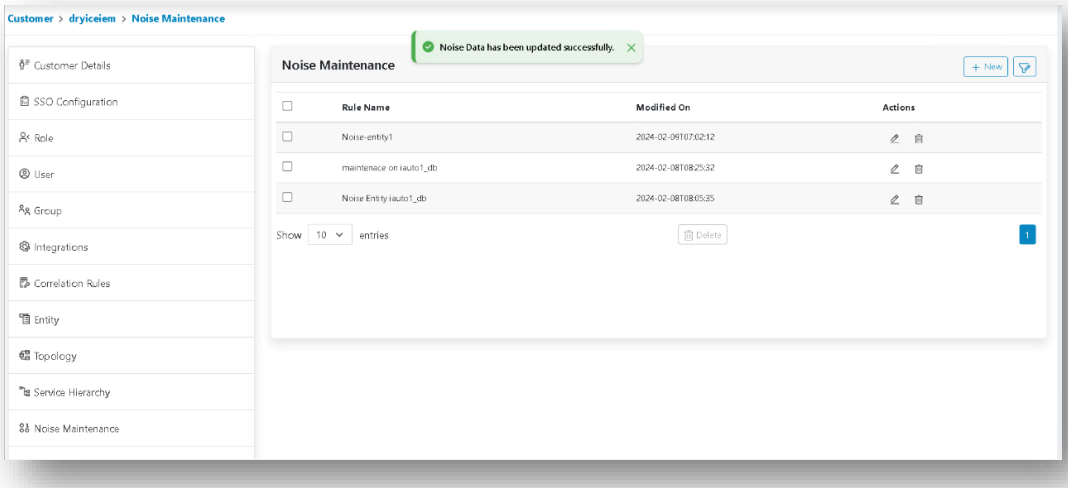

Figure 227 – Success popup.

Delete Noise Maintenance

This action enables user to delete the rules created.

1. Select the rules to be deleted and click on Delete icon in the footer row.

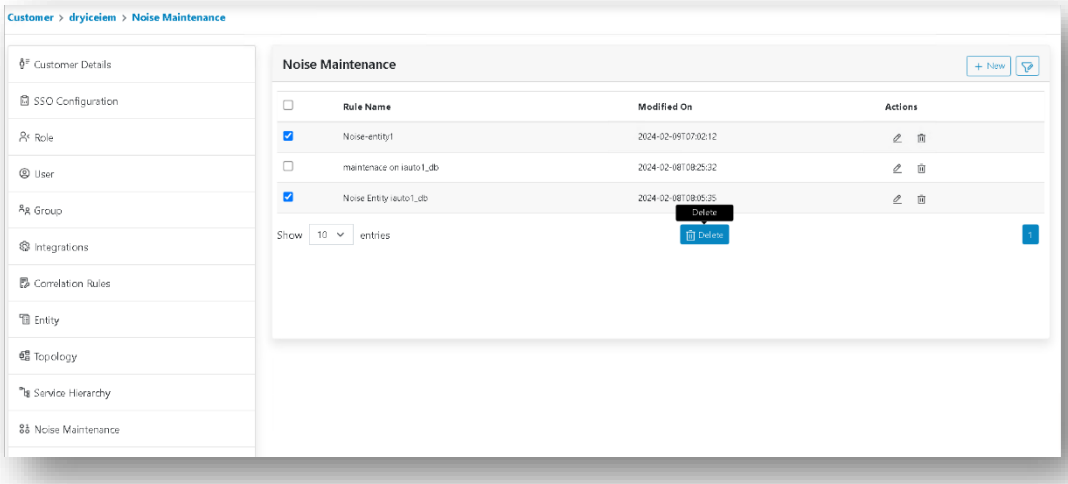

Figure 228 - Selected Noise Rules

2. A confirmation box is prompted.

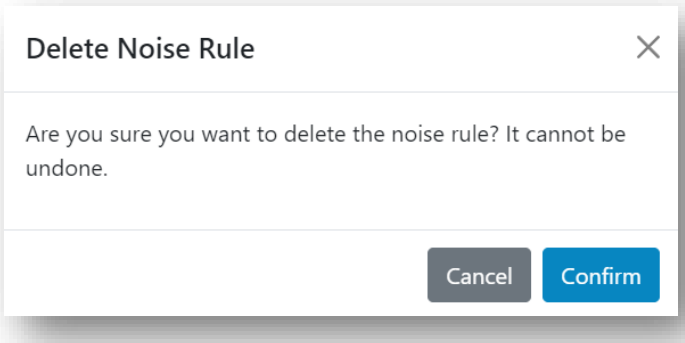

Figure 229 - Confirmation pop-up

3. Click on Confirm button to proceed for the deletion process.
4. On successful deletion, a confirmation message is displayed.

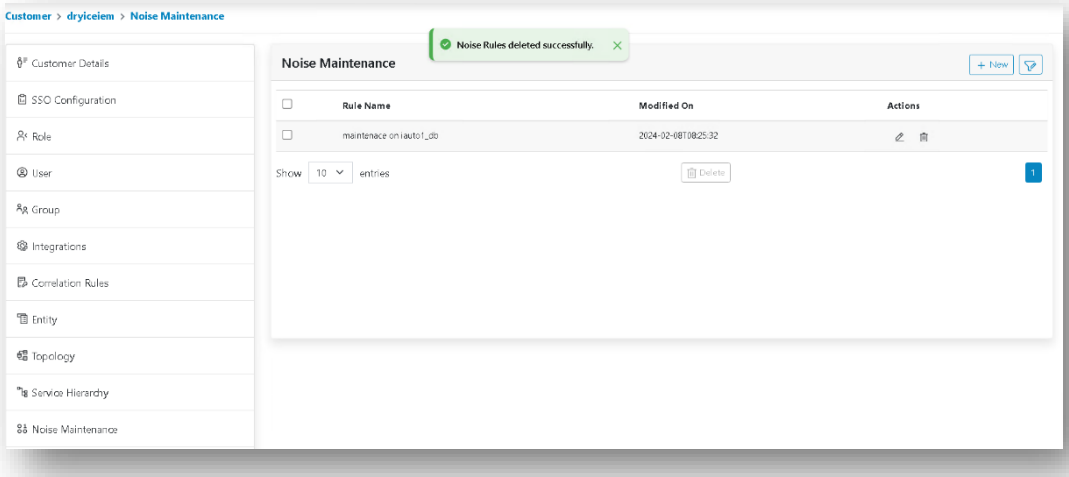

Figure 230 - Alert Message

5. Grid View will be refreshed, and the rules will be removed from the grid.

Apply Filters

The steps explain how to Apply filter, filters the Noise/Maintenance Window Data.

1. Click on the **Apply filter** action button present at the below header of the console.

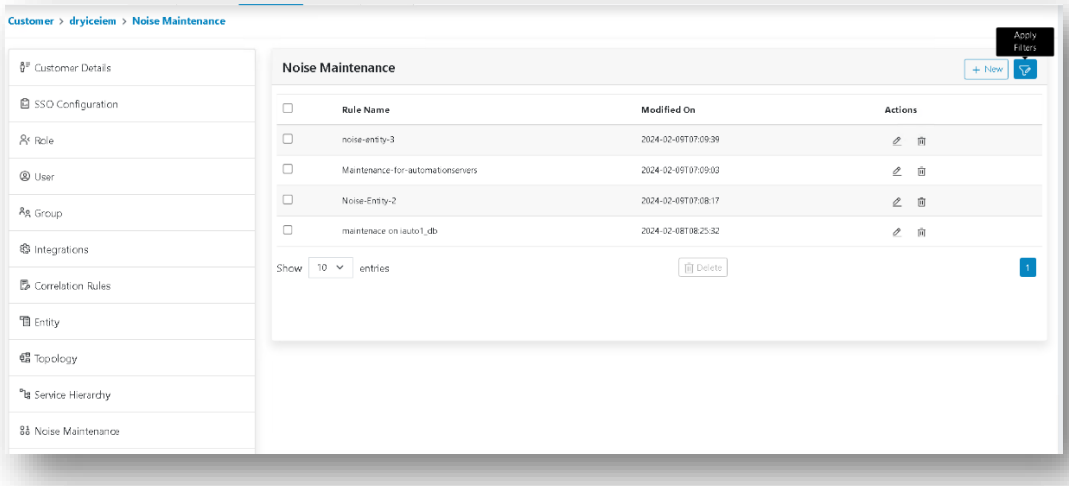

Figure 231 - Apply Filter Operation

2. The form will appear, from there user can select Filed and operator from drop down list and must write value. Then click on the apply button.

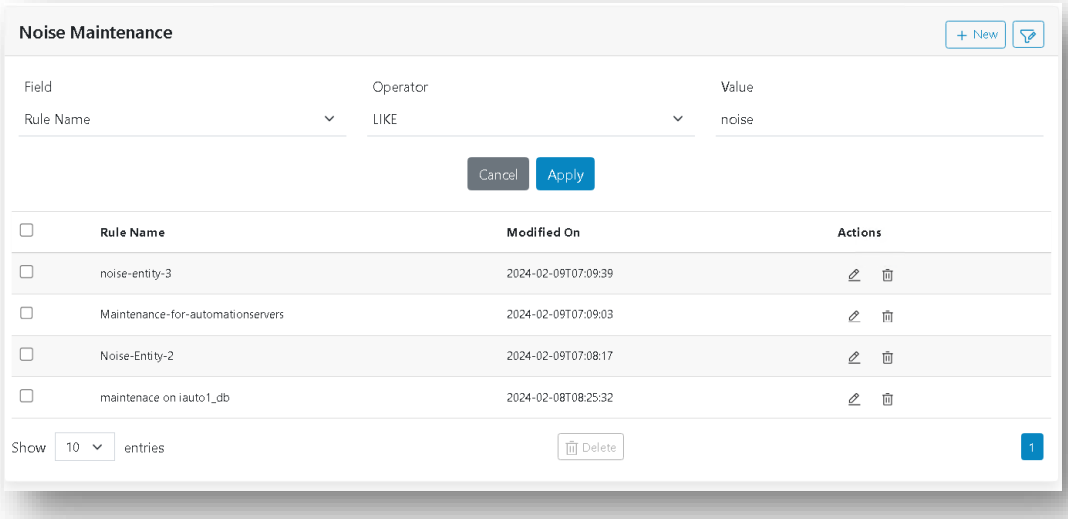

Figure 232 - Apply Filter Operation

3. User can see the result of applied filter.

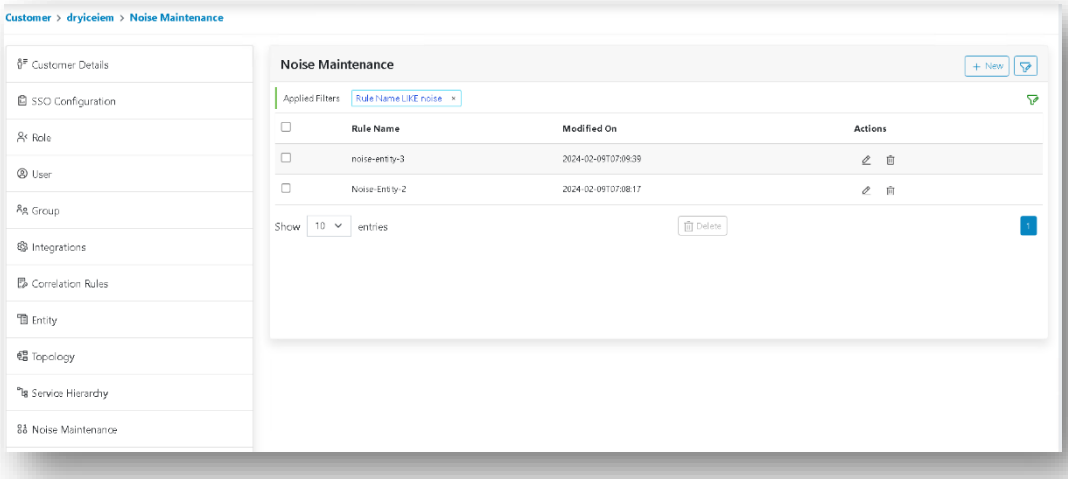

Figure 233 - Apply Filter Result

6.1.11.10 Correlation Rules

Correlation rules in IEM are predefined sets of conditions and logic used to analyze and associate multiple events or alerts to identify patterns, relationships, and potential root causes. These rules play a crucial role in minimizing noise, prioritizing incidents, and aiding in more accurate and efficient incident detection and response. Correlation rules define the criteria and logic for grouping or correlating related alerts based on certain conditions or characteristics. Conditions specify the criteria that must be met for events to be correlated.

When correlated alerts meet certain criteria, correlation rules can trigger the automatic creation of actionable to streamline the actionable response process.

IEM Supports Topology based alert correlation and Temporal based alert correlation.

- **Topology based alert correlation**:

  Topology-based alert correlation helps in identifying root causes, reducing noise, and providing a more comprehensive view of incidents.

By considering the topology of the infrastructure, HCL IntelliOps Event Management can correlate alerts from different sources and determine their impact on the overall environment. This enables faster and more accurate incident resolution, as well as proactive problem identification.

- **Temporal-based Correlation with feedback system**

  A technique implemented in HCL IntelliOps Event Management, allows for the analysis and correlation of alerts based on their time-related attributes. It helps in identifying patterns, trends, and dependencies among events over time. By incorporating temporal-based correlation into event correlation, we can gain insight into the temporal relationships among alerts. This allows for more accurate and timely actionable detection, helping to improve overall operational efficiency and responsiveness**.**

Topology Based Alert Correlation – OOB Correlation Rules

- **There are OOB default correlation rules for a tenant present in the environment**.

  Out-of-the-box correlation rules refer to predefined logic/rules that analyze and correlate incoming alerts or events from various sources to identify actionable.

  - **Time & Location Based Cross Domain Correlation Rule**- This correlation rule groups and filters alerts based on environment. There is a filter applied for production environment. The rule will be triggered and will stop grouping alerts into actionable when a specific metric (location) breaches a predefined location/region.
  - **Time Based Cross Domain Correlation Rule**-This correlation rule groups and filters alerts **based on** environment. There is a filter applied for production environment. The rule will be triggered and will stop grouping alerts into actionable when a specific metric (time) exceeds a predefined threshold.
  - **Network Topology Based Correlation Rule**- This correlation rule groups and filters alerts based on environment. There is a filter applied for production environment. There is predefined topology and the alerts having same entity following similar topology will be grouped into an actionable.
  - **Entity and Time-Based Cross Domain Correlation Rule**- This correlation rule groups and filters alerts based on environment. There is a filter applied for production environment. The rule will group the alerts based on entity name. The rule will be triggered and will stop grouping alerts into actionable when a specific metric (time)exceeds a predefined threshold.
  - **Noise and Incident Reduction Due to System Load**- This correlation rule filter alerts **based on** parameters (which should contain -CPU, memory or Swap). The alerts with the same entity will be clubbed into actionable.

This section enables us to define the correlation rules within environment as per the requirements. Correlation rules are user-defined rules which correlate the incoming alerts, identify causal and the impacting alerts within a correlated group and enable actionable creations. In addition to enablement of actionable creation, this enables user to define automated actions on the actionable ’s created by the rule for e.g., auto resolution actions based on criteria’s such as occurrence of a resolving event.

1. Navigate to the **Customer** page. Click on the edit icon corresponding to the customer for whom the Correlation Rules are to be added.
2. The following screen appears. Select **Correlation Rules** option from the left navigation pane**:**

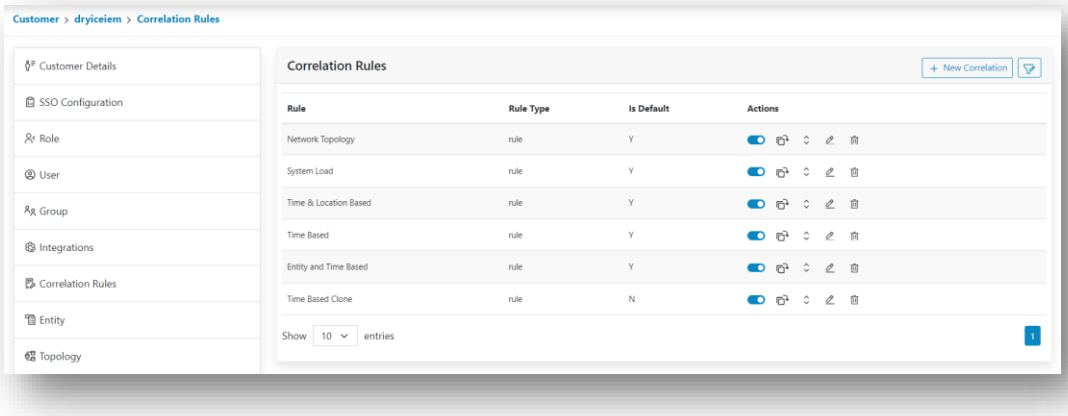

Figure 234 - Correlation View

3. Following are the actions users can perform on this screen based on their assigned roles.
   - Add New
   - Edit Existing
   - Delete
   - Change Rule Priority
   - Clone Correlation Rule
   - Enable/Disable Correlation Rule
   - Apply Filters

Add New Correlation Rules

1. Click on the +**New Correlation** button.

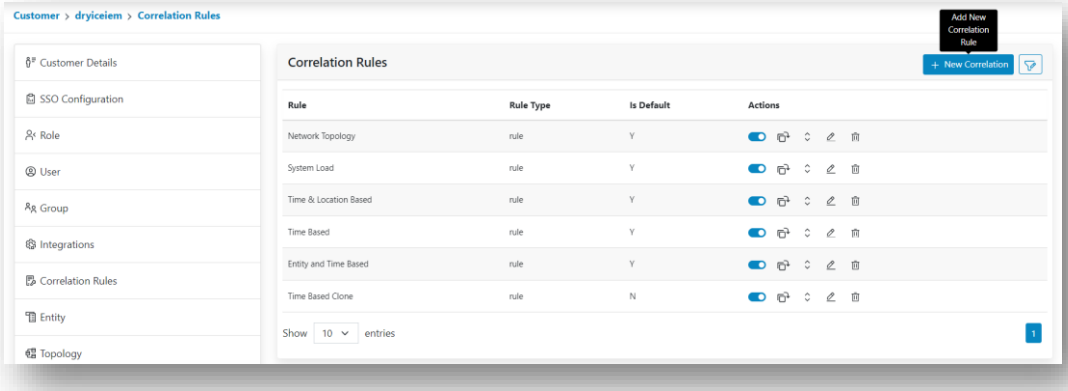

Figure 235 - Creating New Correlation Rule

2. The following form appears for the correlation screen:

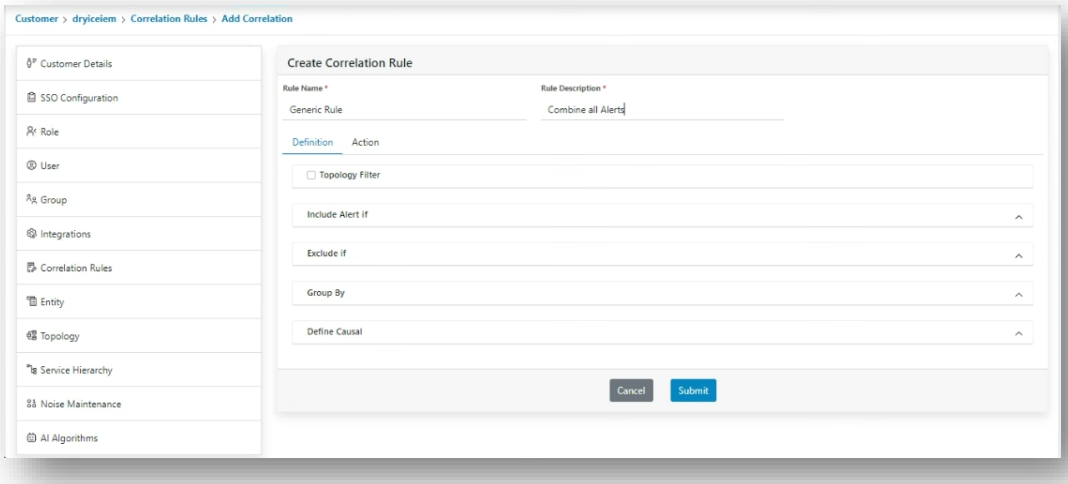

Figure 236 - Correlation Page

3. The correlation creation is divided into three sections:
   - General
   - Definition
   - Action

– **General** section enables user to specify the following:
   - **Rule Name** – Name of the rule
   - **Rule description** – Brief description of the rule

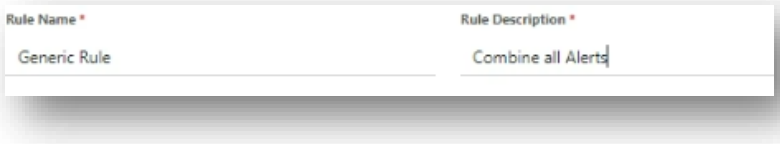

Figure 237 - Create New Name

– **Definition** section is where the user defines the way the alerts data are correlated and is further divided across the following sections:
   - Topology Filter Check Box
   - Include if
   - Exclude if
   - Group by
   - Define Casual

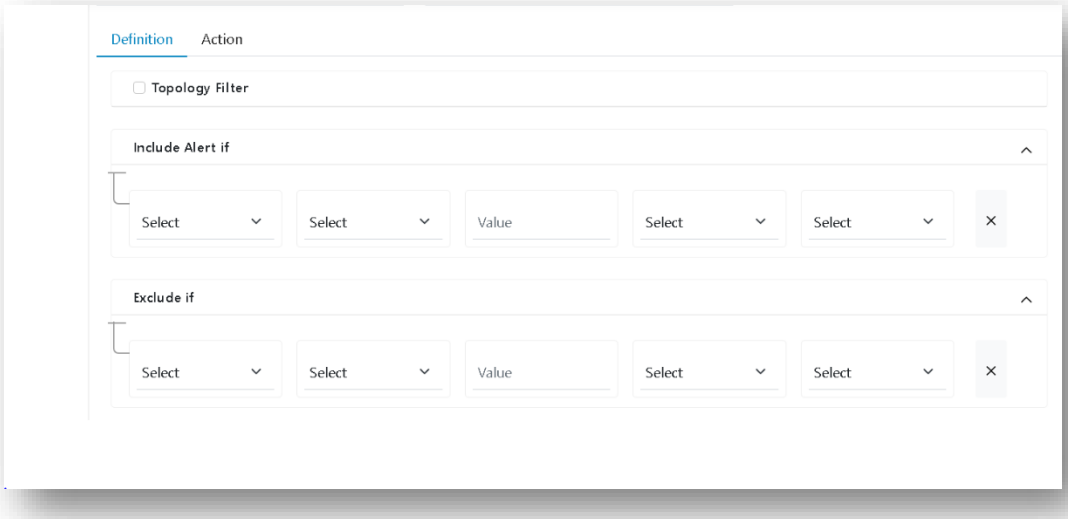

Figure 238 - Definition Section

- **Topology Filter**: This lets the user decide whether the topology details are to be taken into consideration. If selected, the alerts for which the entities topology details are available will only be taken into consideration.

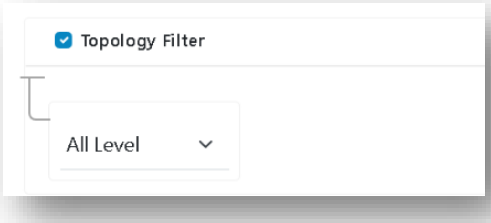

Figure 239 - Topology Filter

a. Topology filters are selected from the dropdown.

b. The user then selects the levels to be considered, i.e., whether all the levels of the tree to be considered or limited levels.

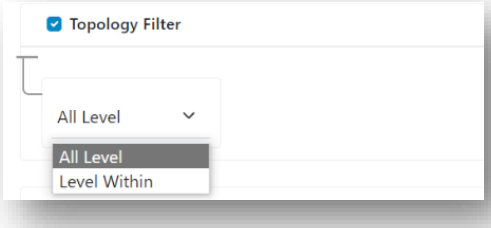

Figure 240 - Selecting Topology Level Types

c. By Default, **All Level** option is selected.

d. If user selects **Level Within**, he next needs to specify the number of levels to be considered and while grouping the data, the user needs select the methodology to group between **Tumbling** or **Sliding**. Tumbling means no overlap will happen in the level grouping of alerts whereas sliding implies overlapping will happen in the level grouping of alerts.

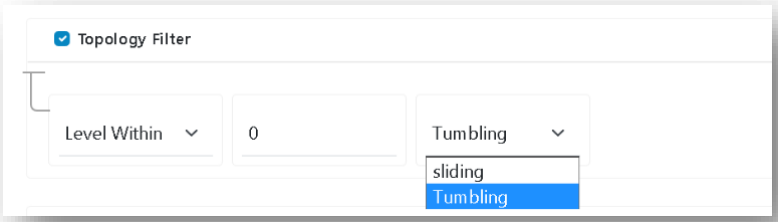

Figure 241 - Selecting Sliding and Tumbling

e. Based on the selection, entities which topology details match the criteria are taken into consideration for this rule.

– **Include Alert if Filter**: User specifies here the alerts data to be considered based on its field's values. E.g., alerts where parameter is CPU or memory or disk. Refer Table 3 – Include Alert If Filter Fields to understand the fields of this filter.

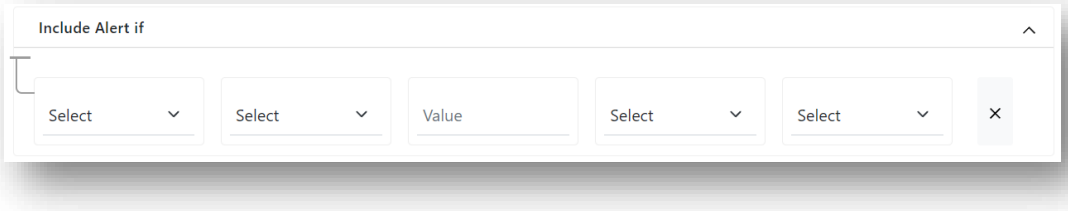

Figure 242 - Include Alert If

Table 3 – Include Alert If Filter Fields

Fields	Description
Fields	Enables users to select the field which user want to consider while applying the filter and it comprises of Alerts direct fields, its custom keys, associated entities master key data defined.
Operator	Based on the fields datatype the operators are populated
Value	Users need to specify the value to be compared to the field selected based on the operator chosen
Condition	Users choose to specify nested Sub And/Sub Or condition or Main And/ Or conditions

With the data filled in the section looks as below: -

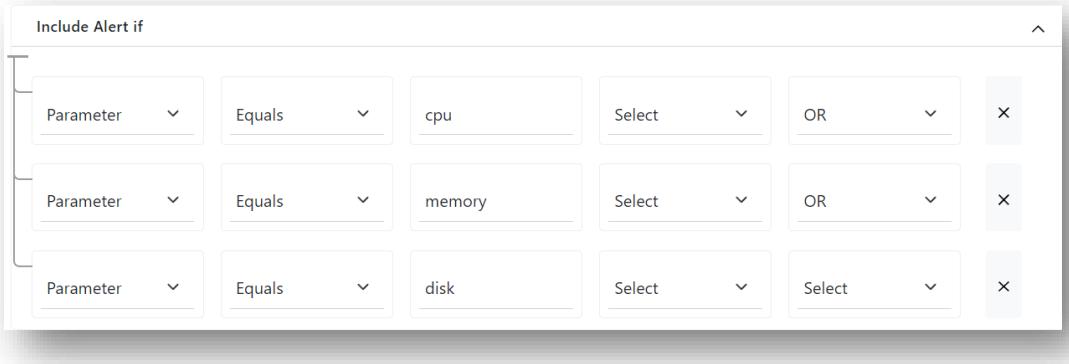

Figure 243 - Selecting All Fields

- **Exclude if Filter** - User specifies here the criteria based on which incoming alerts data to be excluded if applicable, e.g., alerts where agent heartbeat belongs to a specific location. The condition is defined the same way it is defined for include filter. With the details filled in, the section looks as below:

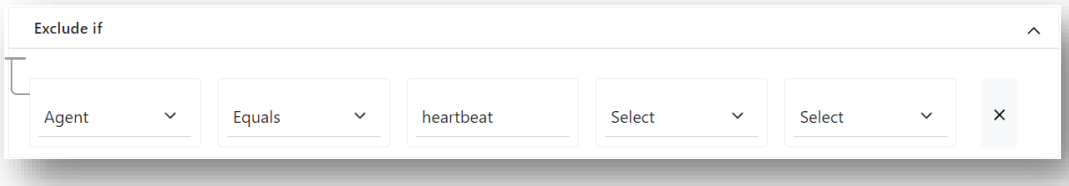

Figure 244 - Exclude Alert If

By the end of this section, users have alerts data which qualifies to be correlated by this rule.

- **Group By**: Once user have the alerts which qualifies for this rule, user decides how to group those, e.g., group all the alerts by its entity id. This means all the incoming alert data will further be segregated by their entity id and will form that many groups.

  a. In this section, user chooses the fields based on which the incoming alerts are to be grouped.

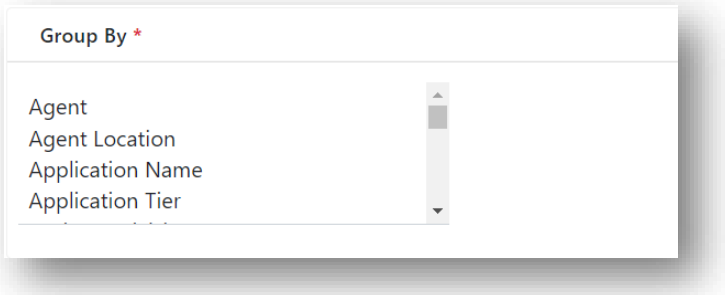

Figure 245 - Group By

  b. The fields are listed is same way as it is displayed in the included filter section. User can select one or more fields. With the inputs selected, the field looks as below.

  c. In case of tumbling & Sliding topology, the user needs to group by Hierarchy ID & Sub Entity ID as a mandate.

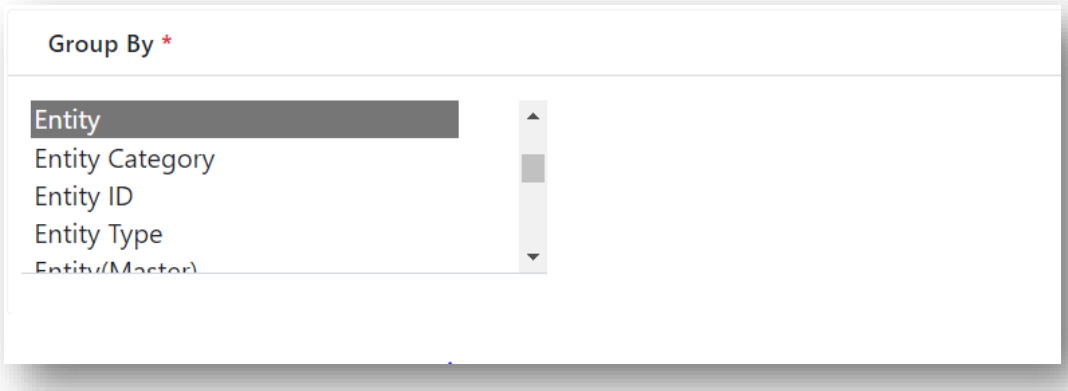

Figure 246 - Selecting Group By

– **Define causal**:

With the groups identified, user next determines the following:

- **Process for** – Define windows within the group. for e.g., user wants to create hourly windows within the groups so that 10-11, 11-12 alerts data are grouped together and actionable are created accordingly. For this, you specify the interval and period as shown below. Default is set to 1 Hour.

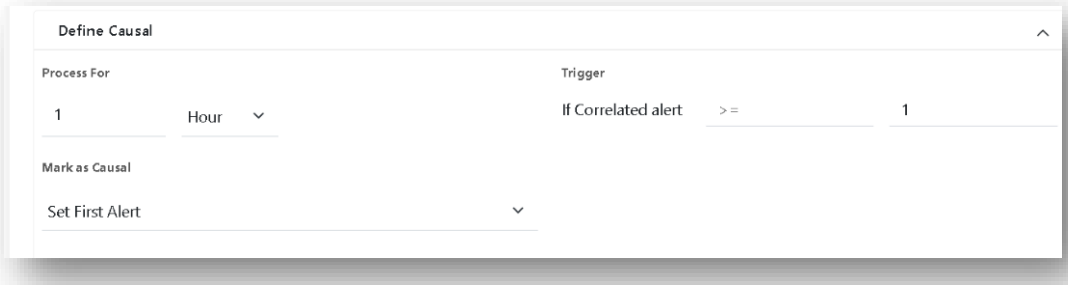

Figure 247 - Process For

- **Trigger** – Defines when the grouping to be marked as actionable. This is based on the correlated alert count which is by default set to 1 as shown below.

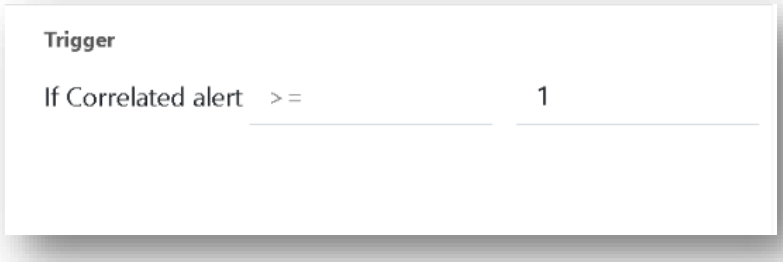

Figure 248 – Trigger

User can specify the count based on their trigger criteria.

- **Mark as Causal**: With the groups identified this section helps determine out of all the alerts within a group which one is to be tagged as causal. For this, user have the following options.
  - Based on Time user have two options enabled: -
    - **Set First Alert** – First occurring alert within the group, the one with the minimum first occurrence.

- **Set Last Alert** – This is the alert which occurred latest in the group i.e., the alert with maximum alert time (first occurrence).

- Based on Topology level user have two options enabled: -
  - Set First level
  - Set Last level

    These options are enabled in case user have selected topology data to be considered. As the name suggest first level is the first one and Last level is as the level comes in last. In case of conflict the time of occurrence is taken into consideration for determining the causal.
  - **Set using expression** – This enables user to identify causal based on an expression.

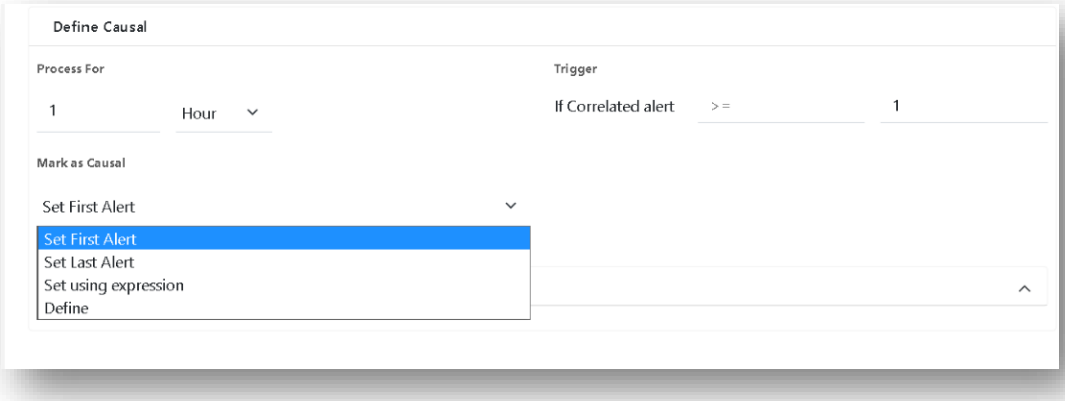

Figure 249 - Mark as Casual

- **Define** an order of events based on which the alerts meeting the criteria will become causal.

- Criteria are defined in a similar manner as user did for include criteria. Multiple criteria can be specified by Clicking on +Criteria(case).
- As the +Criteria(case) is clicked new rule section is created as shown below.

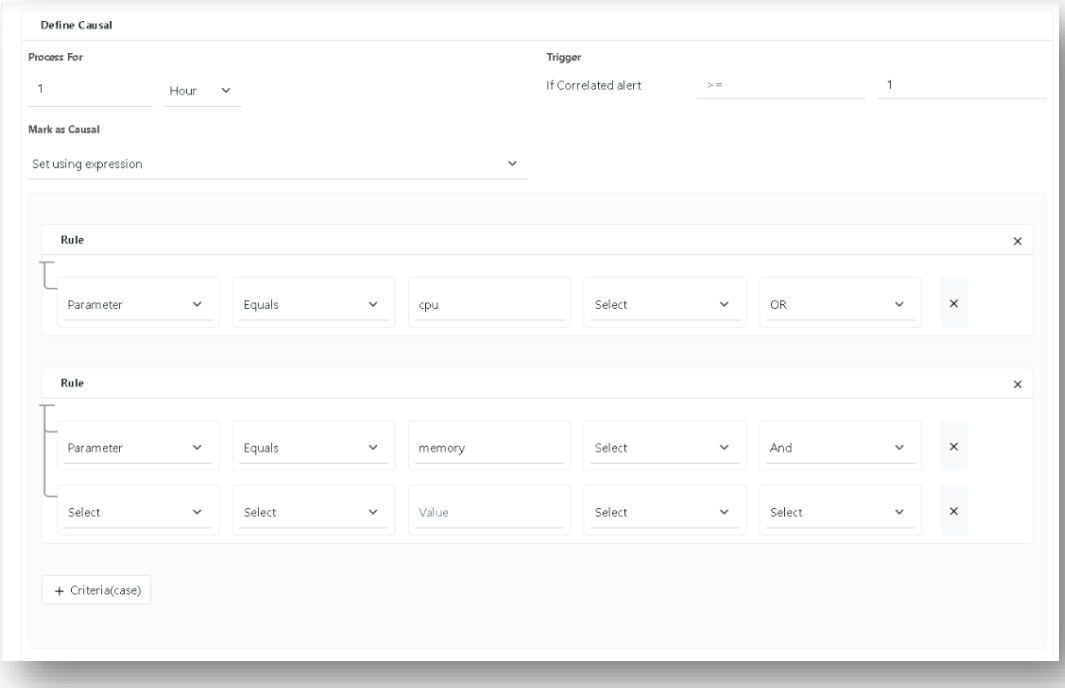

Figure 250 - Click on +Criteria

- The order of the section determines the causal priority with the first one having the highest priority.
- At any time, user can delete criteria, by clicking on delete icon on its section as shown below.

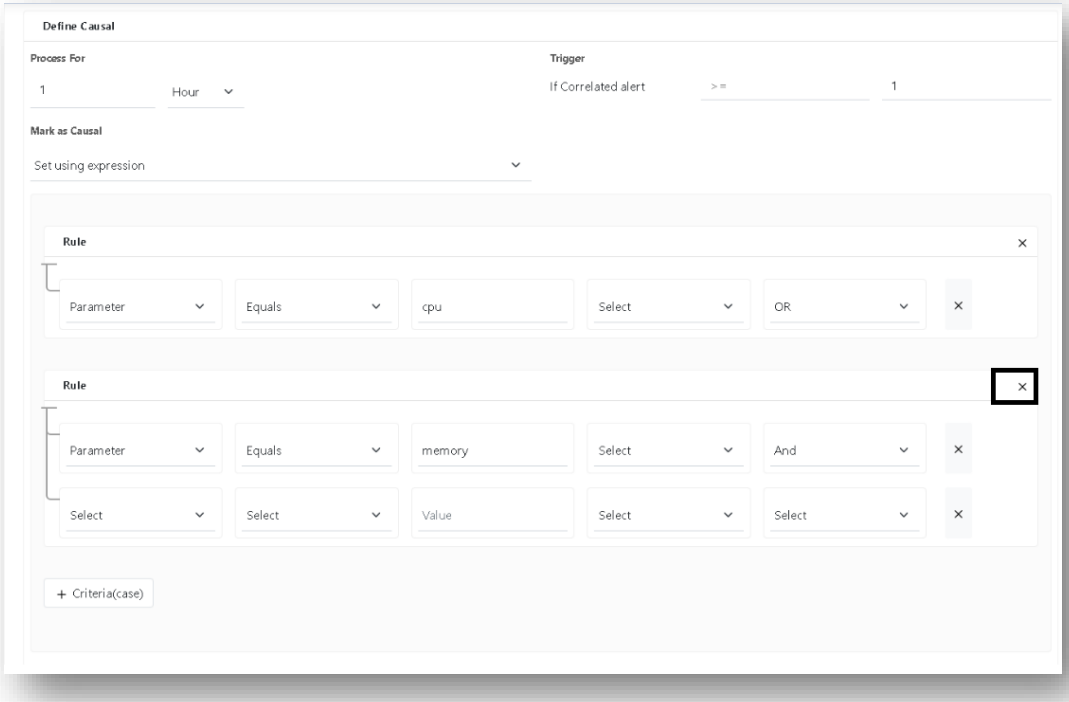

Figure 251 - Delete of Extra Criteria

- With the details filled in the section looks as below.

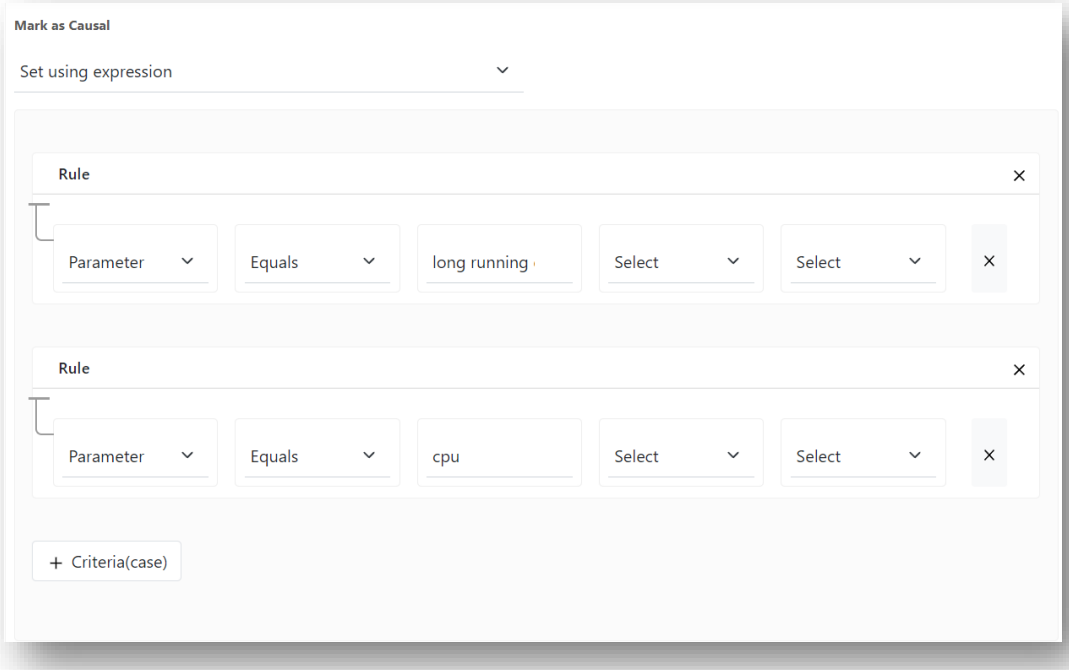

Figure 252 - Set Using Expression

- This implies in the group if user have long run query coming in its priority of becoming a causal alert is higher than the CPU alert. This can help user override the time of occurrence case, scenarios where user might have possibility of causal delayed and received after the impacted once.

- Define – This enables user to group the incoming alert and define a higher cause which is not dependent on any alert, but which is the reason behind the alert's occurrences.
  - Specify Actionable Details – helps user to work and resolve the causal actionable created.
  - Enter the specific actionable details as mentioned.

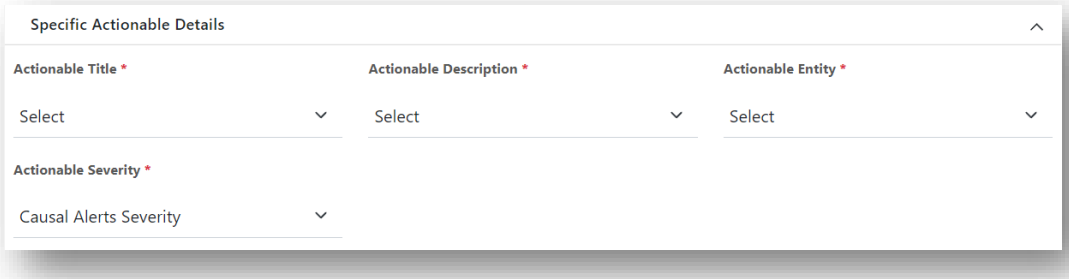

Figure 253 - Specific Actionable Details

- **Title** – Brief description about the actionable. User can choose to specify any alert field e.g., Title as shown below or create its own title using combination of alerts fields or its associated master fields as shown below or create its own title using combination of alerts fields or its associated master fields as shown below.

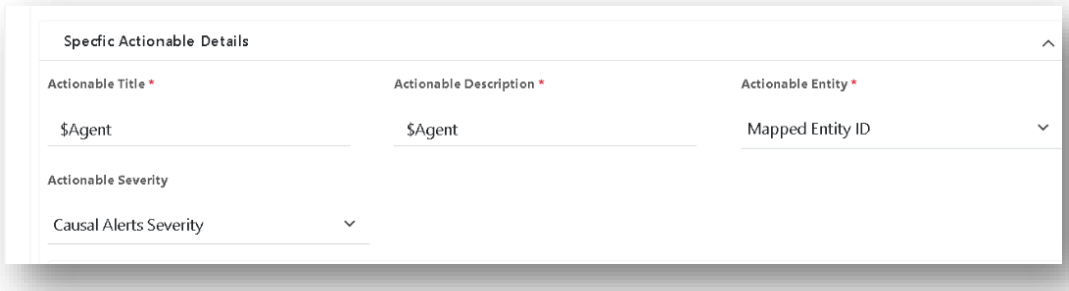

Figure 254 - Actionable Title

- Create its own title using combination of alerts fields or its associated master fields.
- As mentioned, the fields can be accessed by using $ sign as shown below: -

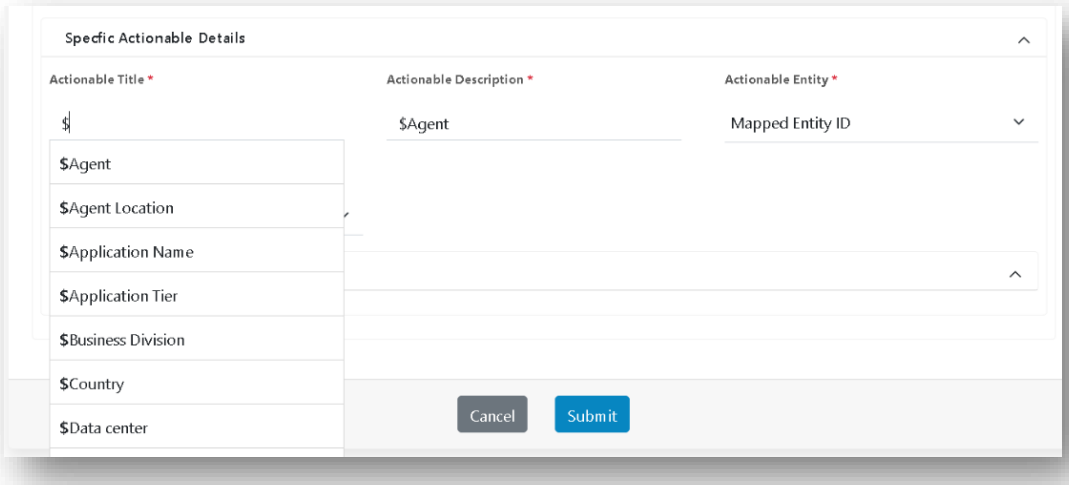

Figure 255 - Actionable Title Drop-down

- Description – Detailed description about the actionable wherein user can add additional details which will help the operation user to better work on the actionable. Like Title either a single field can be specified, or a combination of texts and fields can be specified. With the values filled in the field looks as below

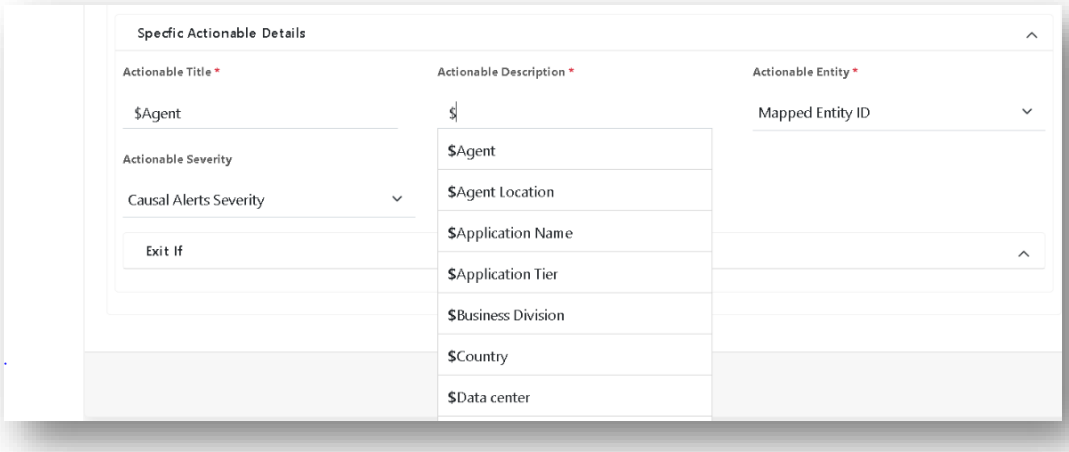

Figure 256 - Actionable Description

- **Entity** – This is default set to the causal alert's entity id as shown below.

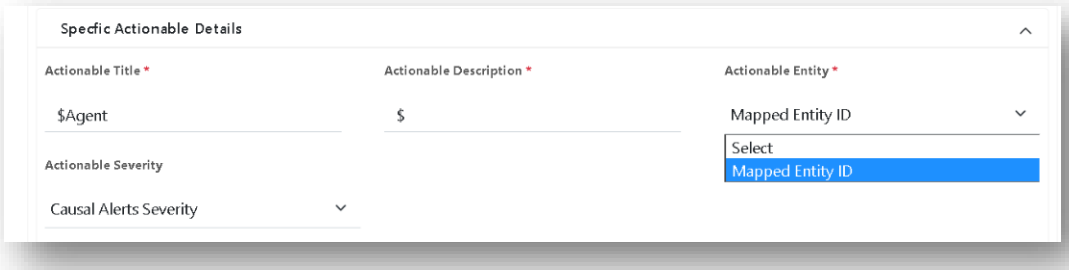

Figure 257 - Actionable Entity

- In the case of Define, this is based on Group in which the alerts data is grouped which requires the action to be taken upon the group by field itself e.g., Datacenter. With defined option the Actionable entity looks as below.

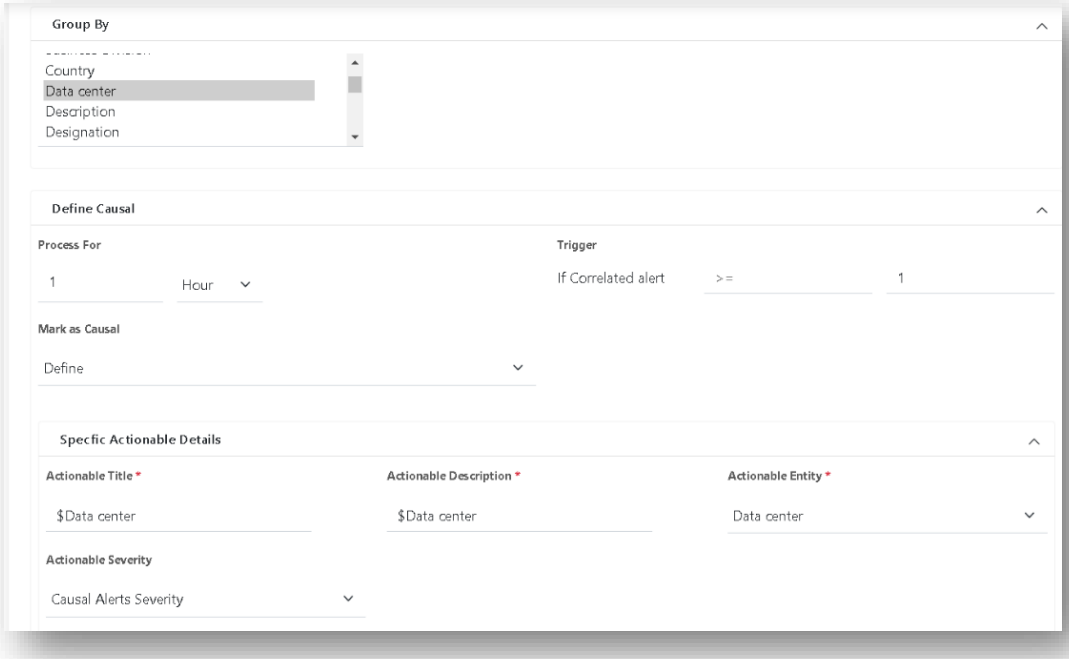

Figure 258 - Enter all Fields

- Severity – Sets the actionable severity. Possible options are:

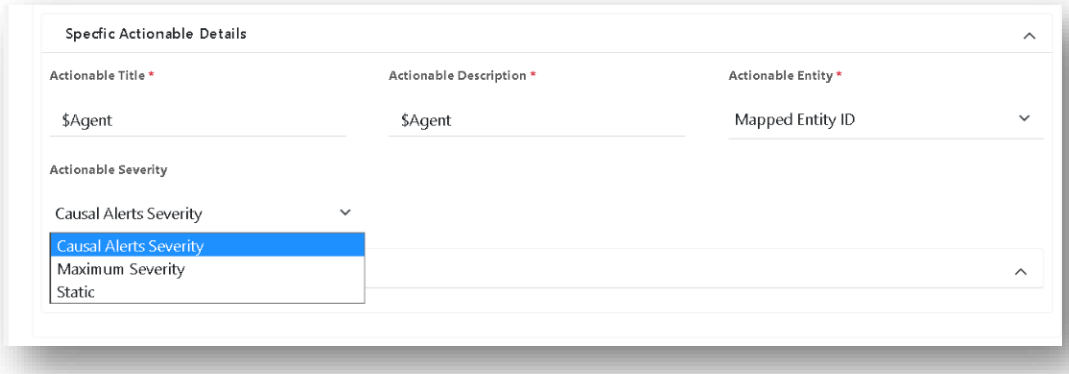

Figure 259 -

- Causal severity – if selected the severity is set to be same as the causal alert severity on grouping.
- Maximum severity – if selected the severity is set to maximum severity of all the grouped alerts.
- Static severity – if selected, user choose to specify the severity of actionable as shown below.

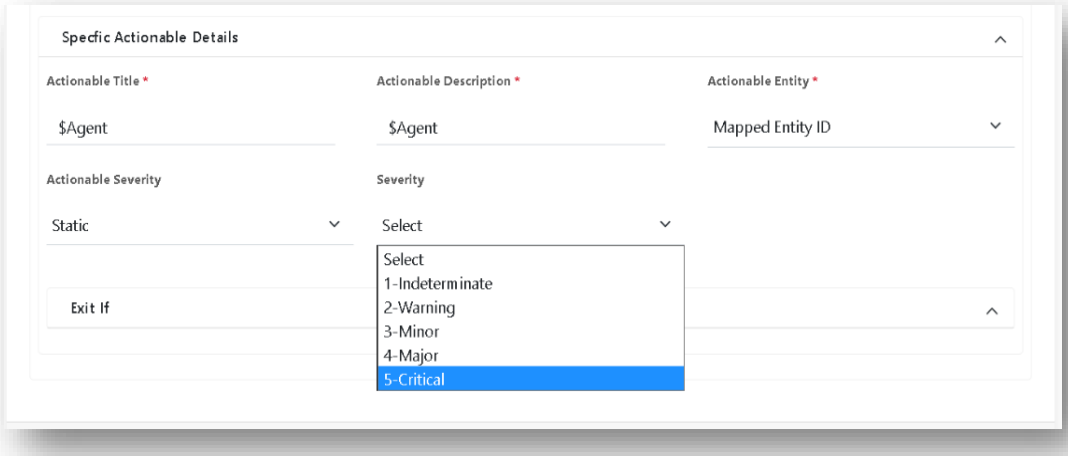

Figure 260 - Actionable Severity

- Exit if – with the details specified next user determine when the actionable grouping will be emitted from the state, and it has the following three options.

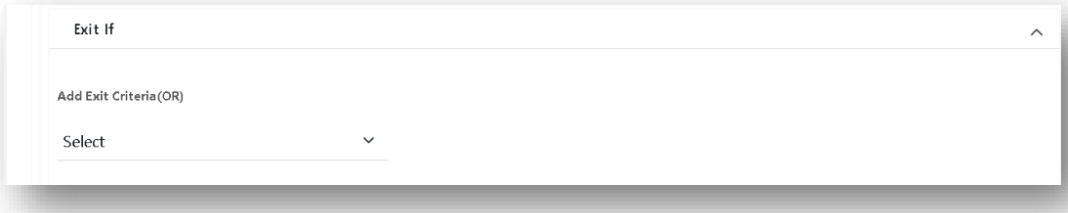

Figure 261 – Exit if

To close actionable, it is mandate to add exit criteria of the correlation rules as "Exit If, clear is received for Causal Alert".

- If clear received for the Causal – As the name suggests if the causal alert clear severity is received, this actionable will be emitted from the state.
- If the following record appears – This section helps user to specify conditions and when it is met, leads to actionable being emitted from the state e.g., incoming alert parameter contains *up or* any alert is received within the group where severity is clear.
- If the flow of new records is paused for specified duration – When it is selected it emits the actionable from the state if incoming data is stopped for the mentioned duration.

All these options are available as shown below: -

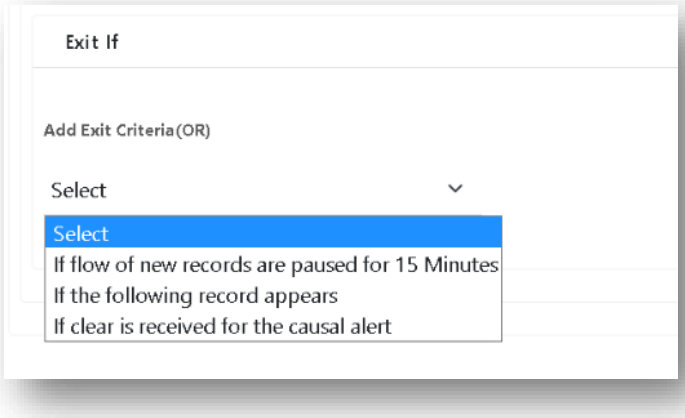

Figure 262 - Exit If

- Choose to specify either one or all the conditions. Select, individual sections are added for each which captures the relevant input as required.
- Figure shows the section which appears when “If flow of new records is paused for” is selected: -

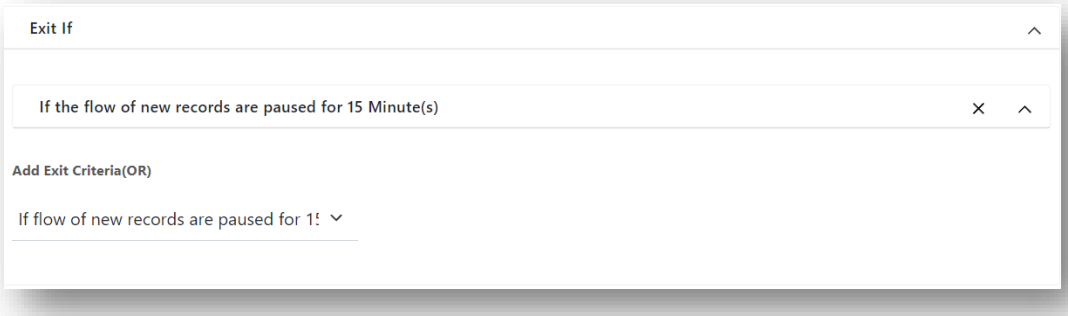

Figure 263 - Exit If Condition

- 4 min default is selected, expand the added section, user has the option to provide the interval and duration as shown below.

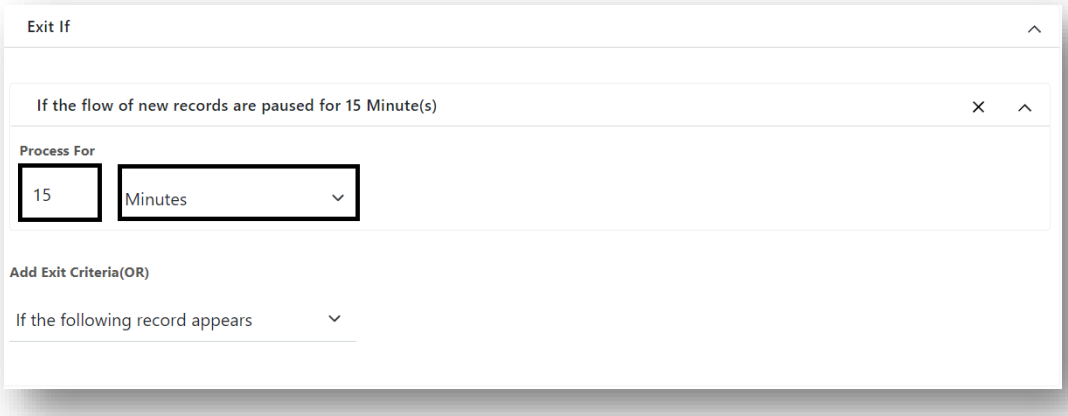

Figure 264 - Process For

- Figure below shows section which appears when the option “If the following record appears” is selected.

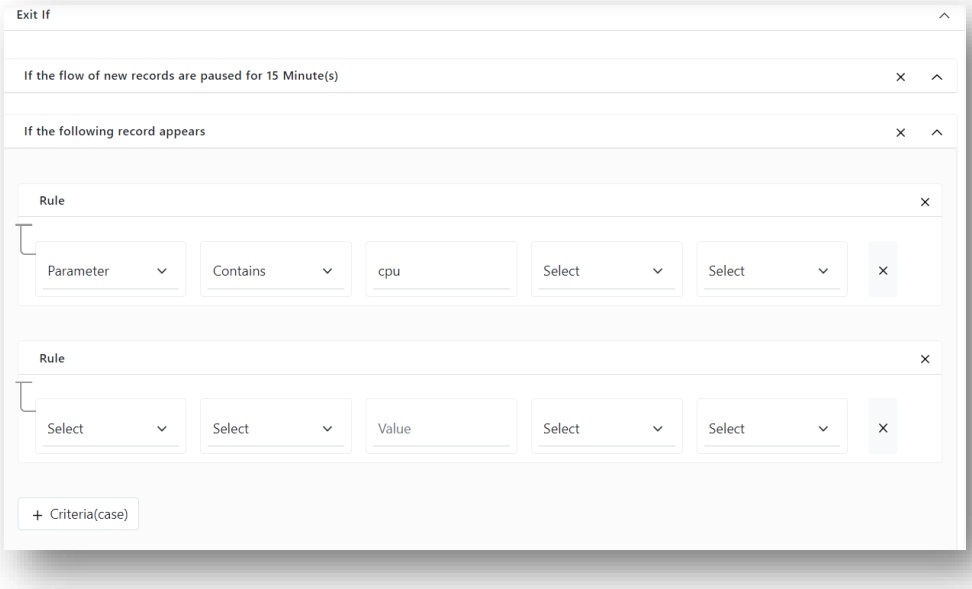

Figure 265 - Entity Fields

- Expression Criteria is defined in similar manner as user did for include criteria. Multiple criteria can be specified by Clicking on +Criteria(case).
- Figure shows the section which appears when “if clear is received for the causal” is selected. In this section there’s no input to be captured.

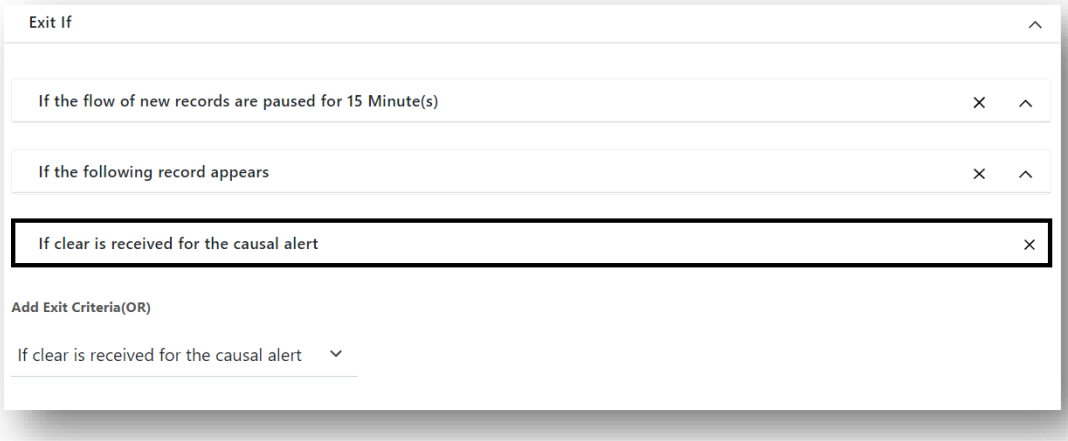

Figure 266 - Select Condition

- All the criteria can be added only once. User can choose to delete any section (if not applicable) by clicking the delete icon next to the section as shown below.

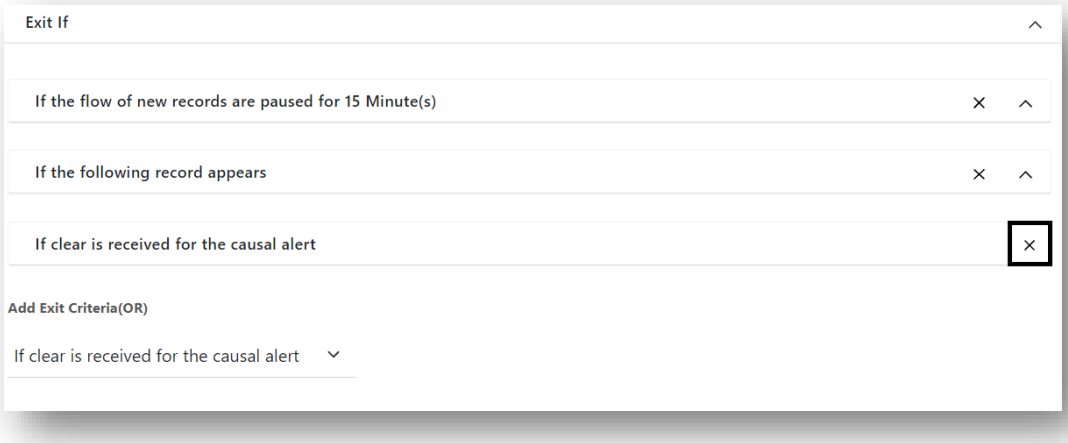

Figure 267 - Delete Condition

- **Action**: With the actionable creation rule defined in the *Definition* section next user can specify automated actions on the actionable' s created by the said rule using the *Action* section.

  a. Actions are defined using If *<Condition>* Then *<Action>* expressions as shown.

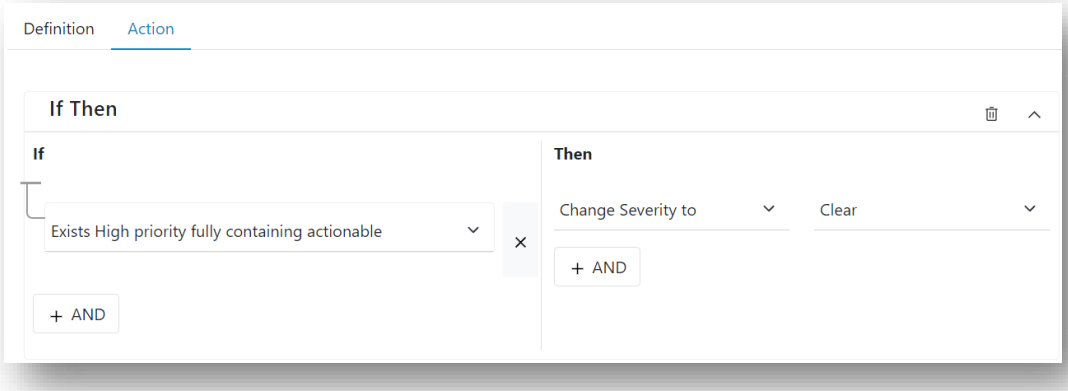

Figure 268 - Action

  b. User can define 1 or more such expressions. This can be added by clicking on **+Action Rule** button.

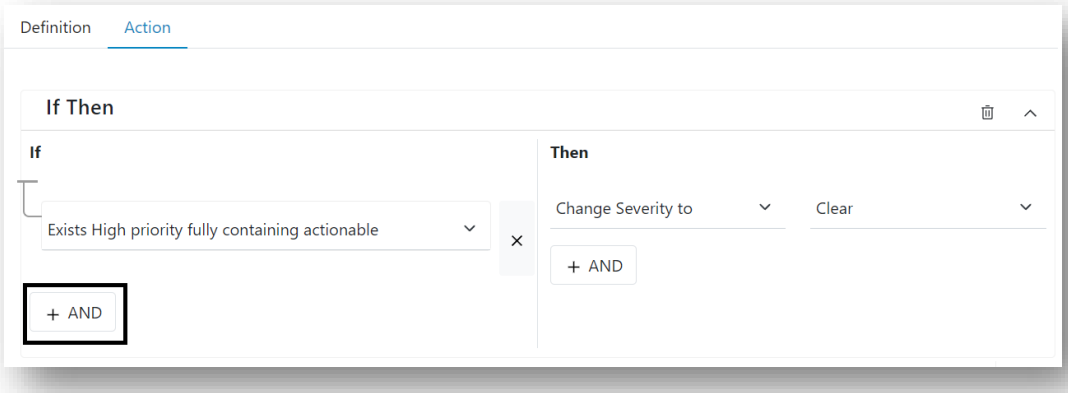

Figure 269 - Click on +Action Rule

  c. As the button is clicked a new section appears as shown below.

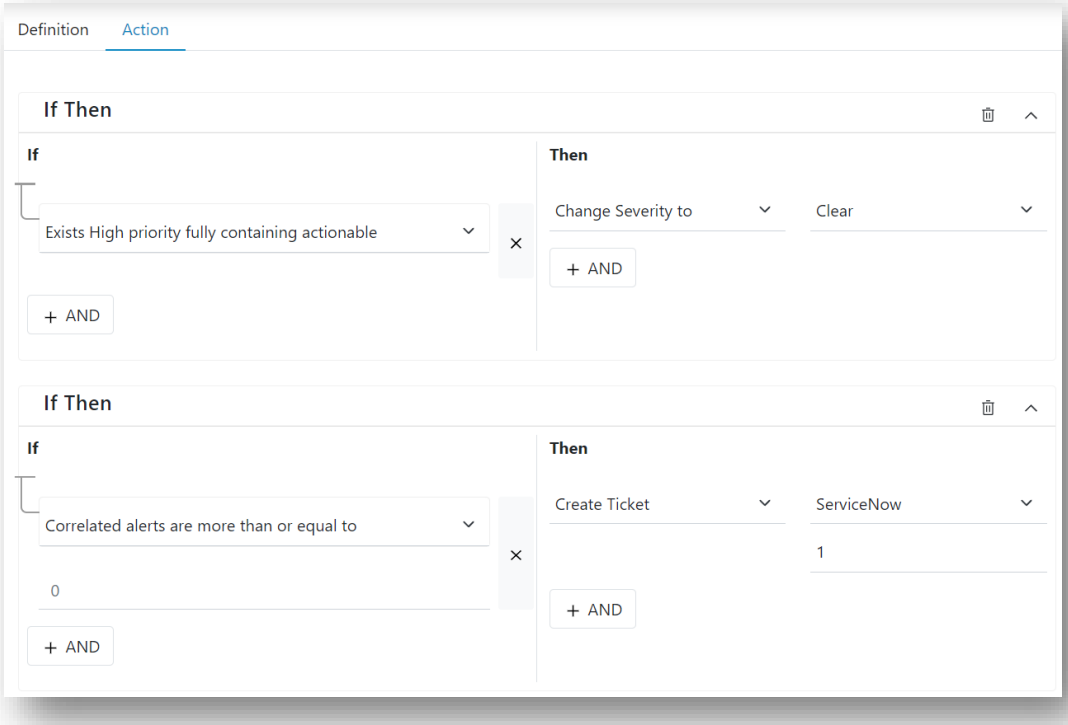

Figure 270 - Action Rules

- The section can be deleted by clicking on the delete icon next to it as shown below.

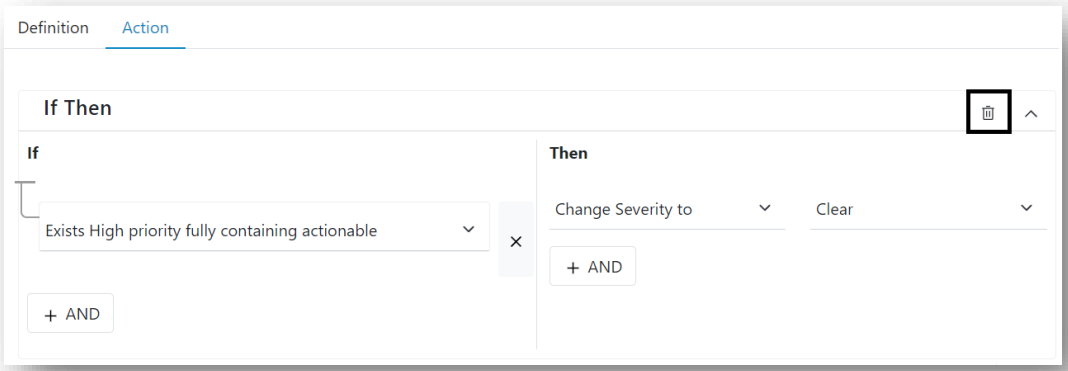

Figure 271 - Delete Action Rule

- Within a section an expression condition (if) section can be defined as combination of one or more conditions. A new condition within a section is added by clicking +AND button.

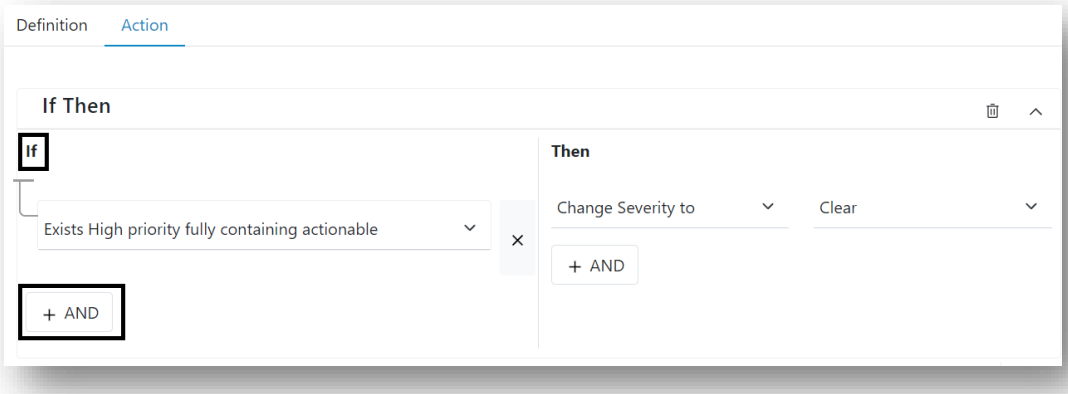

Figure 272 - Click on +AND

- As the button is clicked a new dropdown appears for user to choose the condition from as shown below.

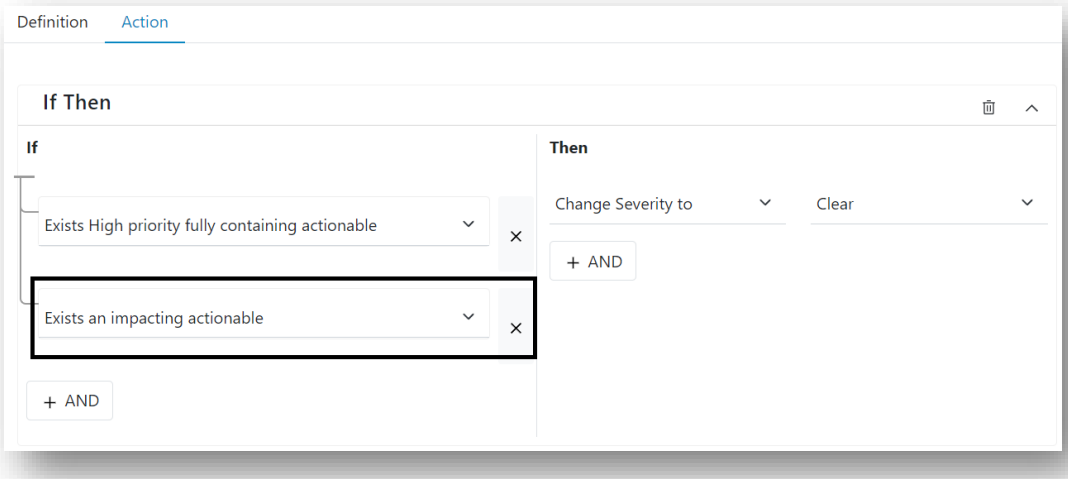

Figure 273 - Selecting the Rule

- Condition expression can be made of one or more of the following available options.
  - Exists an impacting actionable- This means there exists actionable' s whose impacted alert list comprises of the causal alert of actionable created by the rule.
  - Exists a high priority fully containing actionable-This means exists an actionable created by a high priority rule which comprises of all alerts of the actionable created by the rule.
  - Correlated alerts are more than or equal to-This means the count of alerts grouped is greater than or equal to the mentioned number.
- As this option is selected a text box appears next to the dropdown as shown below, enabling user to specify the count. The default is set to 1.

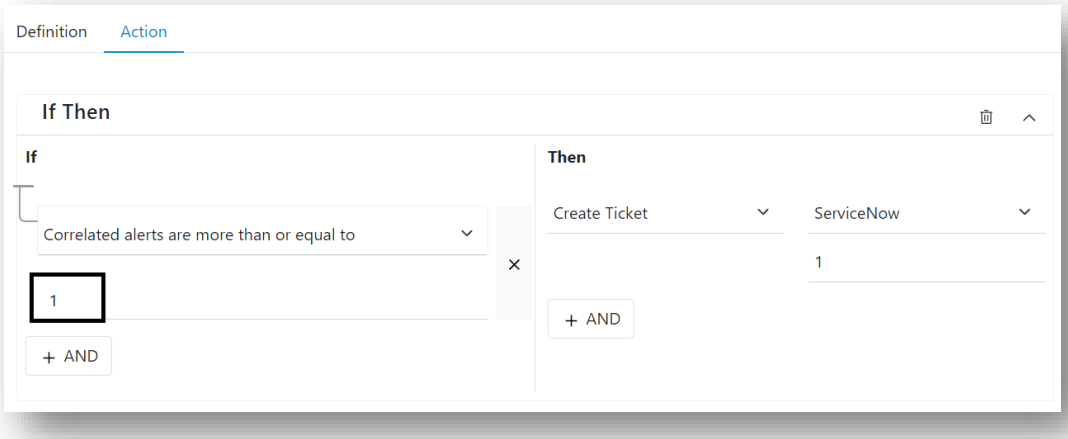

Figure 274 – Count

- Resolving event occurred- This means that actionable is emitted from the state due to either causal alert clear event occurrence or specified alert criteria occurrence (specified using “if the following record appears” clause)
- Actions that are to be taken when a condition is met are defined in the Action section of the expression.

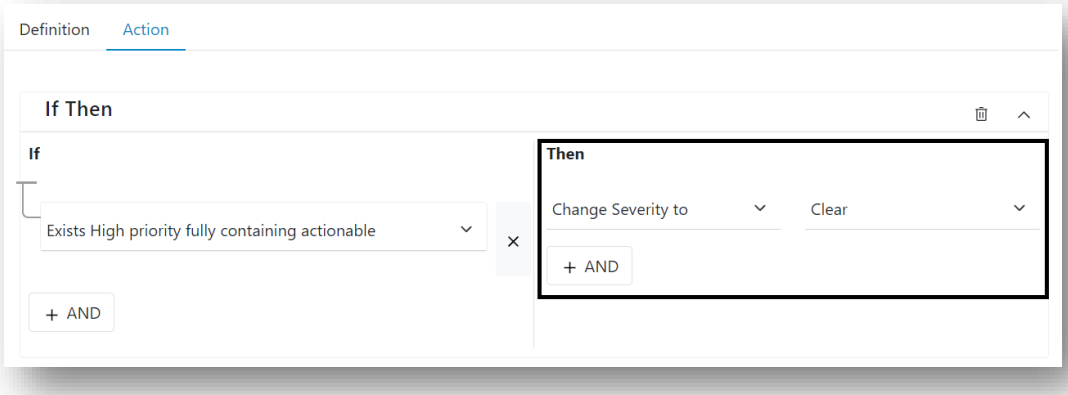

Figure 275 - Change Severity

- Like the condition(if) section, one or more actions can be defined for a particular condition expression by clicking on the +AND button in the Then section.

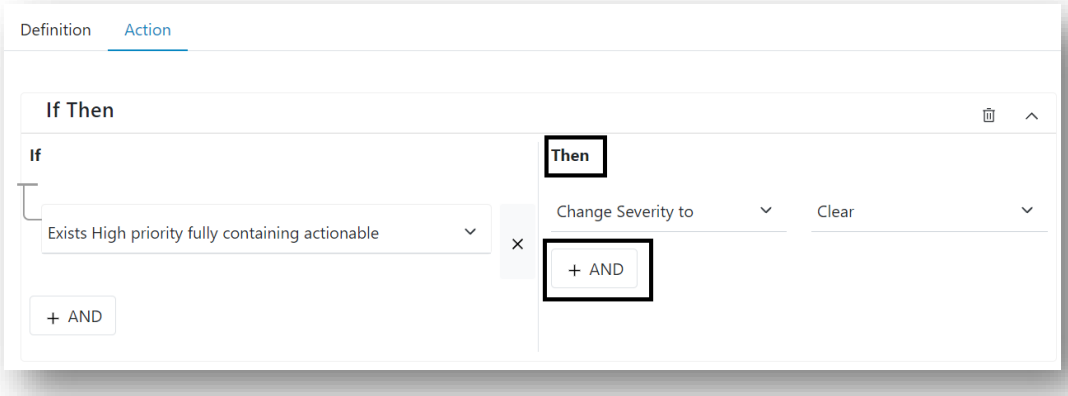

Figure 276 - Click on +AND

- Clicking +AND adds a new row with the Action dropdown within the section as shown below.

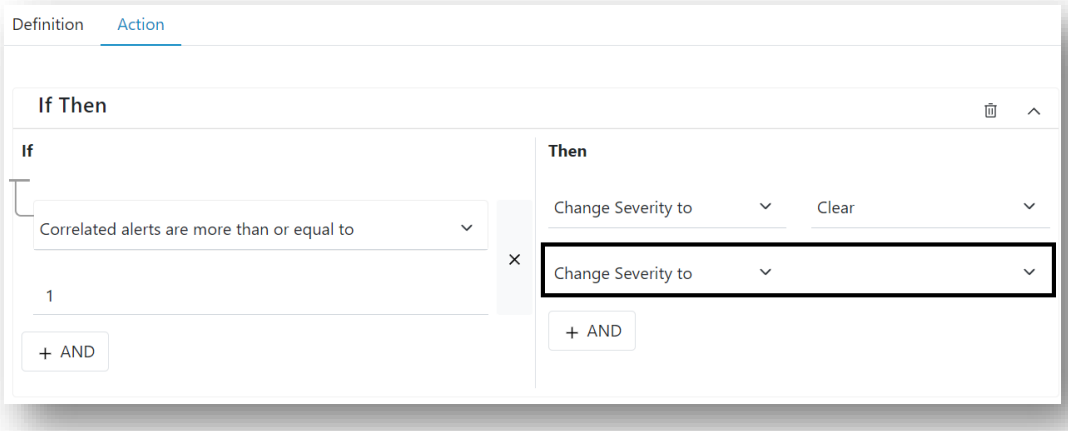

Figure 277 - Change State

- Possible Actions can be any of the following available options: -
  - Change Severity To - Set severity of the actionable to the specified value. As this option is selected, severity dropdown appears for the user to choose from as shown below.

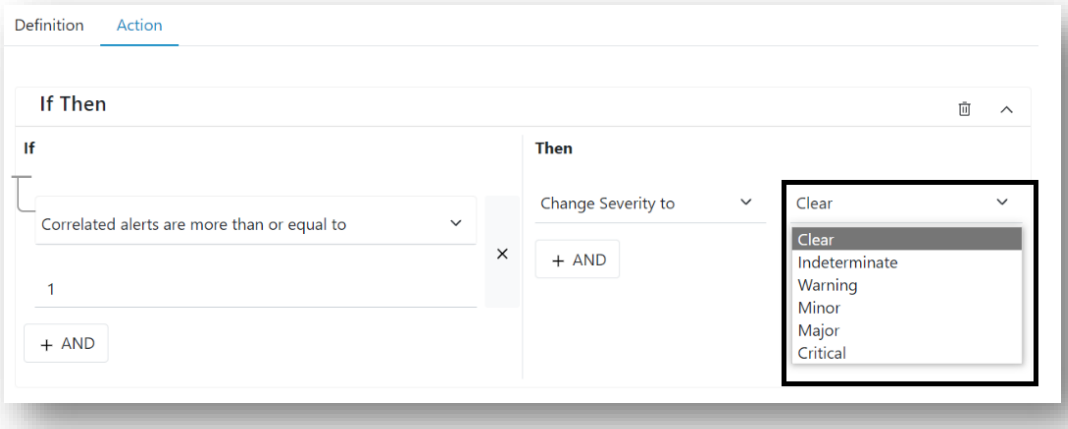

Figure 278 - Select the Fields

  - Change State To - Set State of the actionable to the specified value. As this option is selected, a state dropdown appears for the user to choose from as shown below.

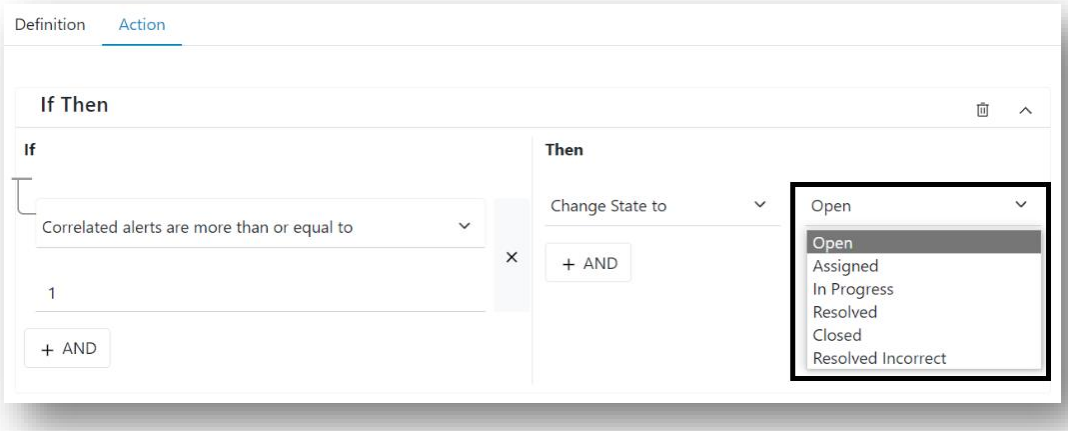

Figure 279 - For Change State Select

- Change Title - Set title of the actionable to the specified value. As this option is selected, text box appears for user to specify the title for the actionable as shown below.

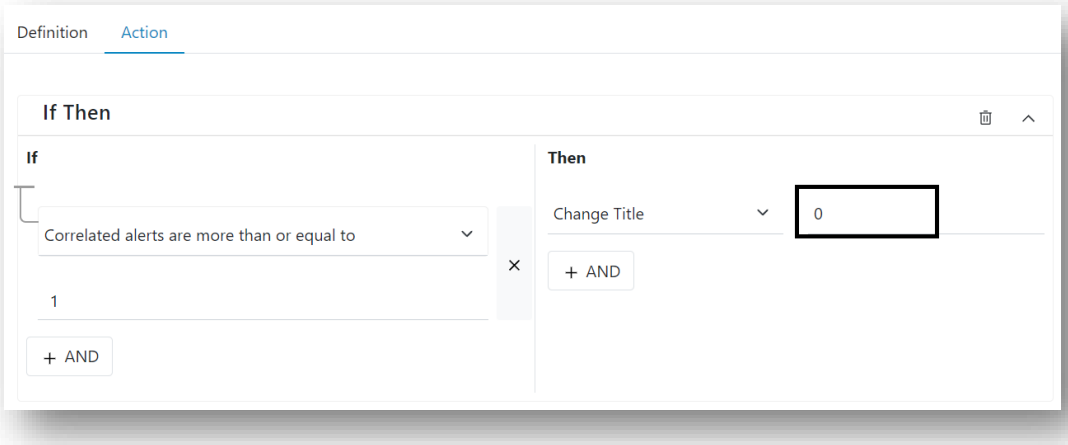

Figure 280 - Change Title

- Create Ticket – Enables ticket creation in the specified tool after specified interval in minutes. As the option is selected a dropdown appears enabling user to select from the available tool list along with a text box for user to specify the lag duration in minutes. The lag by defaults is 0 which implies immediate creation of ticket as the corresponding condition is met.

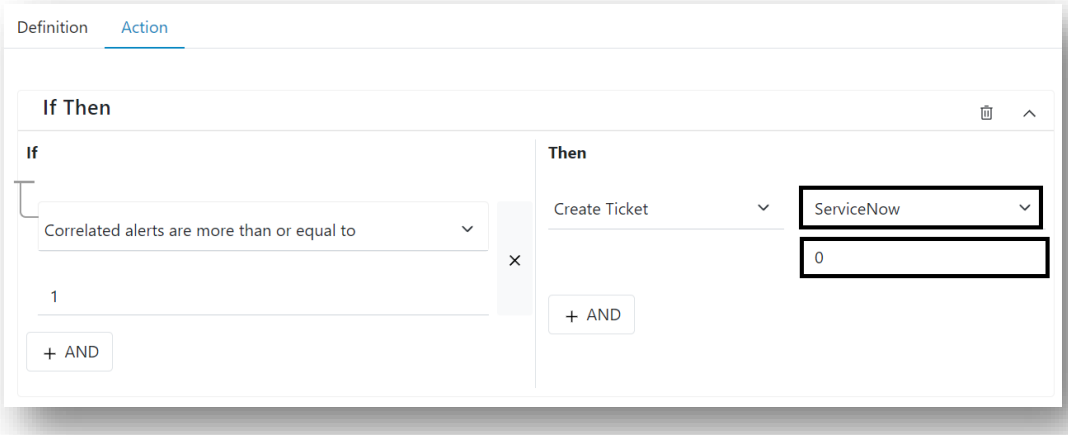

Figure 281 - Creation of ticket

- Users need to note that the ticket will only be created for the actionable if the associated customer's integration is defined.
- By default, the following expressions are preconfigured.
- Change state to resolved if exists an impacting actionable or exists a high priority fully containing actionable, or a resolving event has occurred.
- The below figure shows the actions configured.

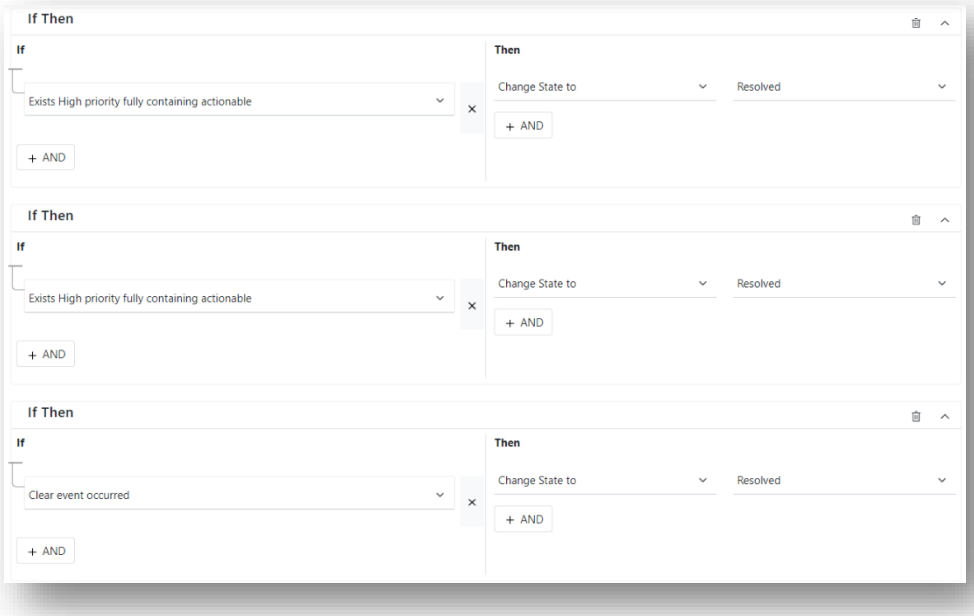

Figure 282 - Actions Rules

- User can choose to update the existing actions or create new actions.
- With all the details filled in click on the Submit button to Save the rule and create the associated processing details.

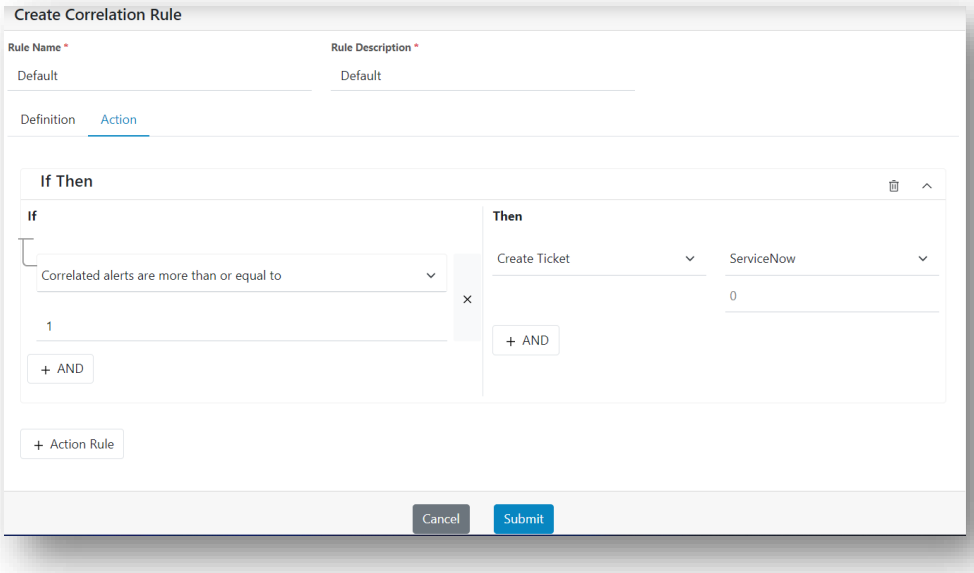

Figure 283 - Click on Submit

- As the Submit button is clicked, control is redirected to the grid view page listing the rule created as shown below.

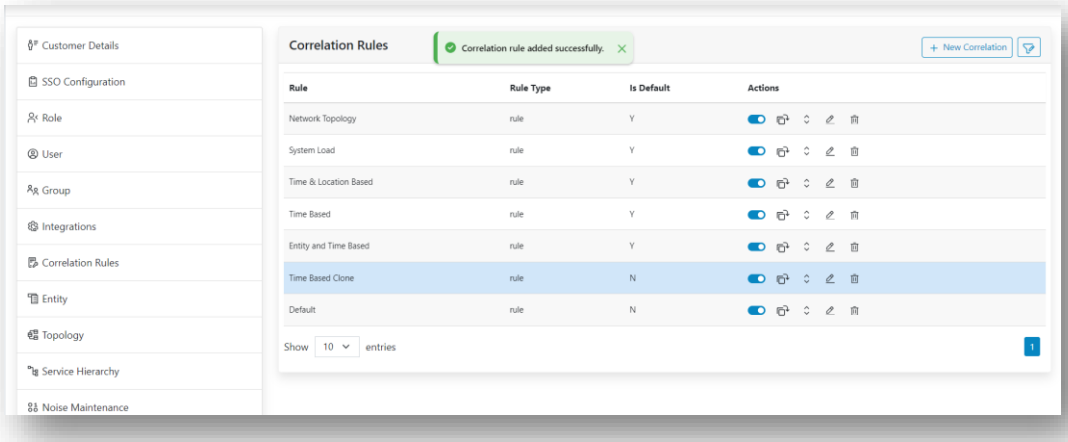

Figure 284 - Grid View for Correlation Rules

Edit Correlation Rules

1. Click on the Edit icon next to the rule that is to be edited.

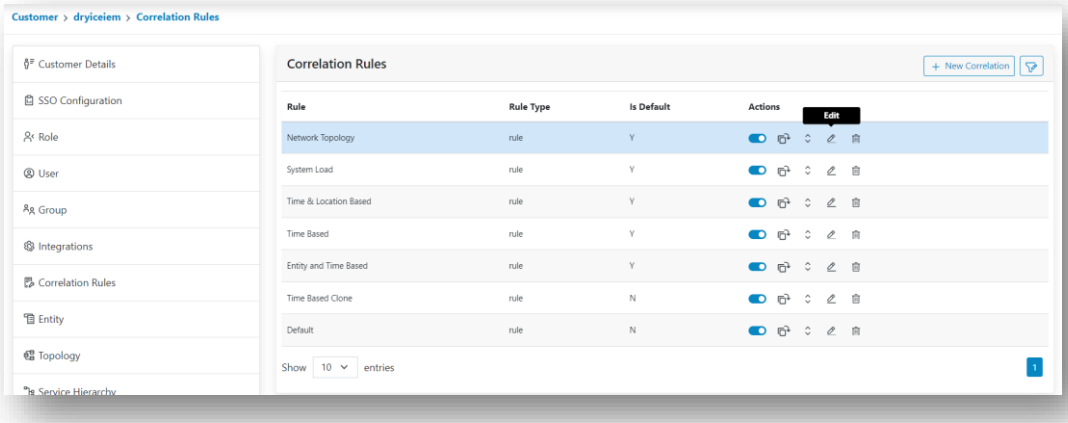

Figure 285 - Edit Correlation Rule

2. The form appears with all the details filled in.

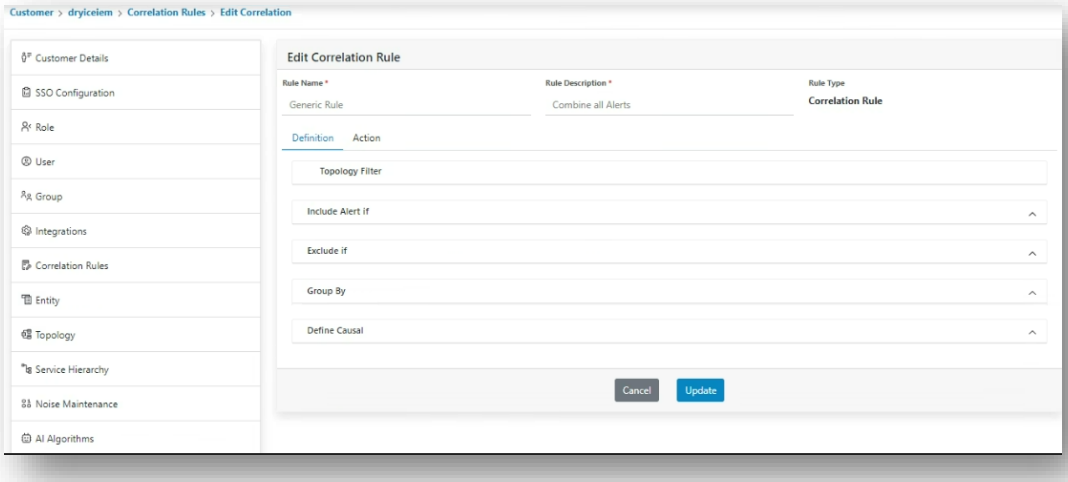

Figure 286 - Edit Correlation Rule (Cont.)

3. Once saved, the user can only perform the following action on the saved data.
   - **Manage Automated Actions** – Add, Update, or delete action expressions in the action section.

4. All the other sections will appear in read only mode as shown in the following figure:

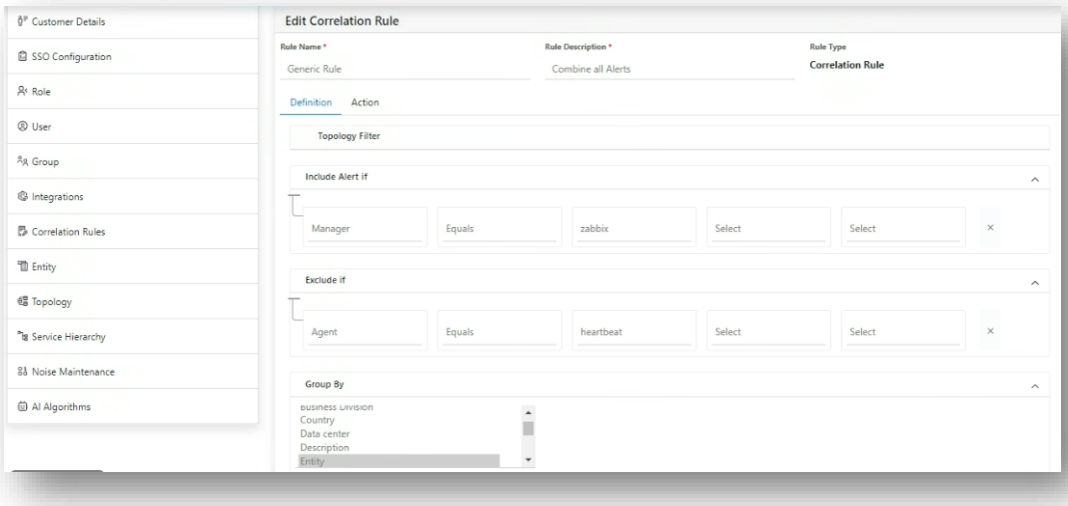

Figure 287 - Updated Correlation Rules

5. Make the required changes and click on Update for the changes to be applicable.
6. A prompt is displayed as shown below.

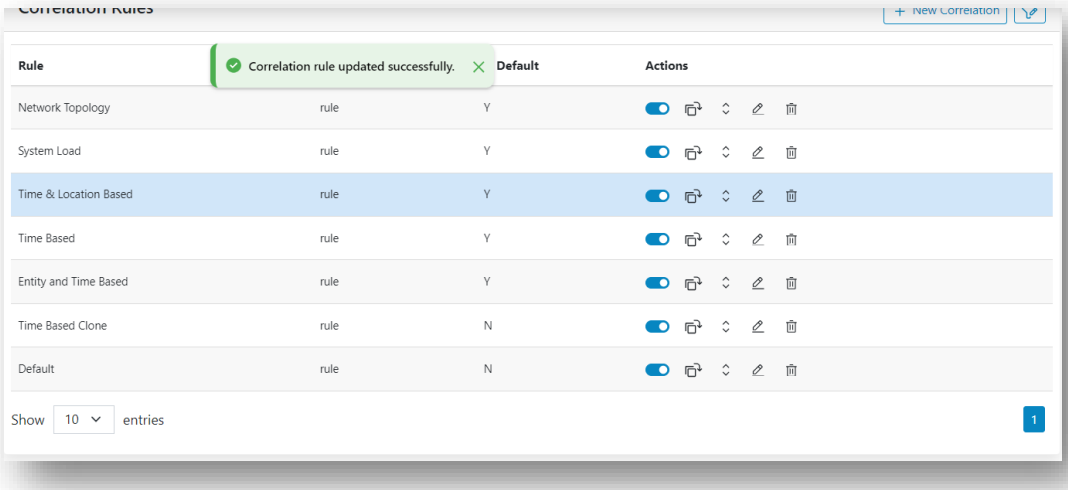

Figure 288 - Alert Message

Delete Correlation Rules

1. Click on the Delete icon next to the rule that is to be deleted.

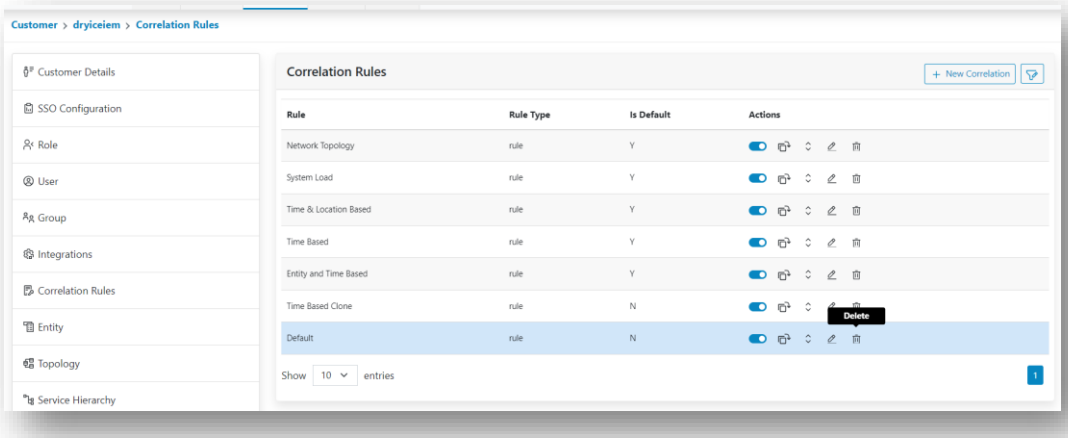

Figure 289 - Delete Correlation

2. A prompt is displayed as shown below.

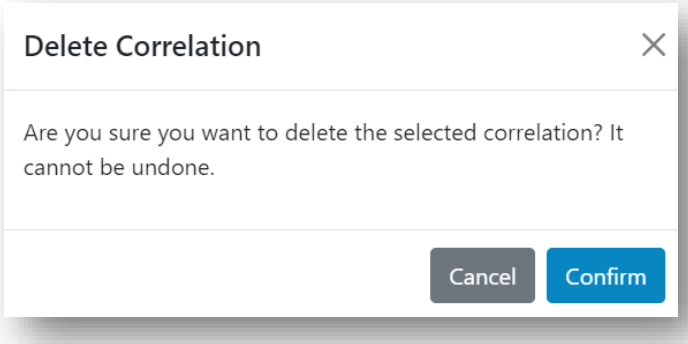

Figure 290 - Confirmation pop-up

3. On confirmation the rule and the associated processes will be deleted.
4. On successful deletion the following message will be displayed.

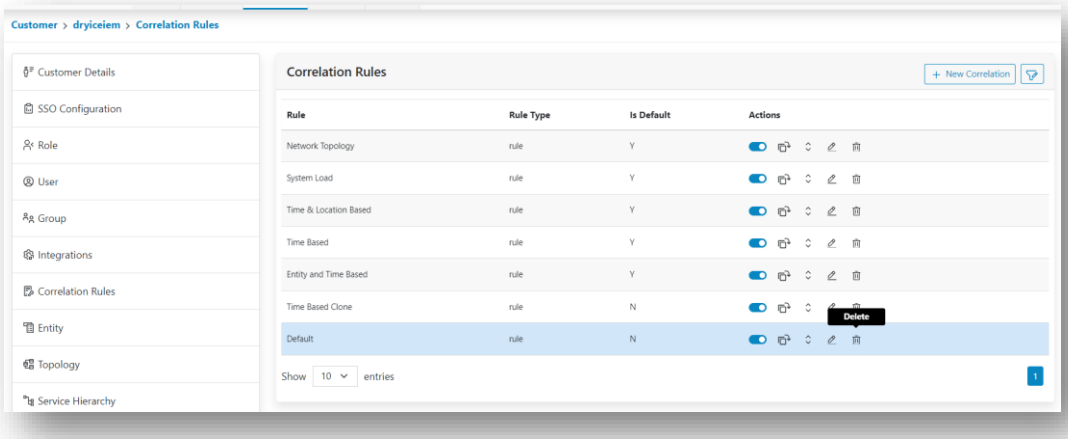

Figure 291 - Alert Message

5. The rule no longer appears in the grid and the data table is updated.

Change Rule Priority

The grid view page enables user to adjust the rule priority. Rule priority helps prioritize the actionable created by different rules and enables us to take actions or define automated actions based on the priority ordering.

Users need to note that the rules are displayed in descending order of their priority in the grid. The topmost rule has the highest priority with the priority decreasing as user go down in the grid.

1. Click on the drag icon next to the rule for which the priority needs to be adjusted.

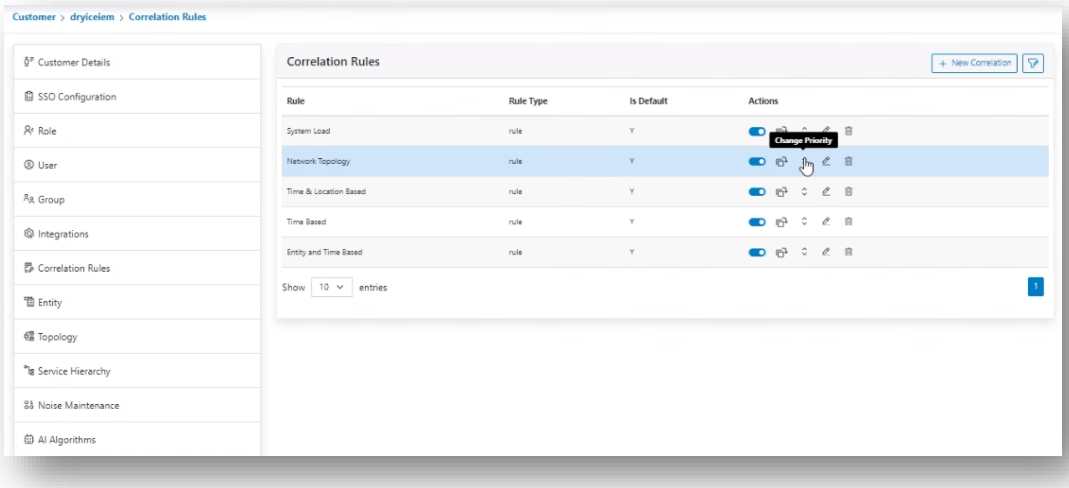

Figure 292 - Change the Priority

2. Select and drag the rule.

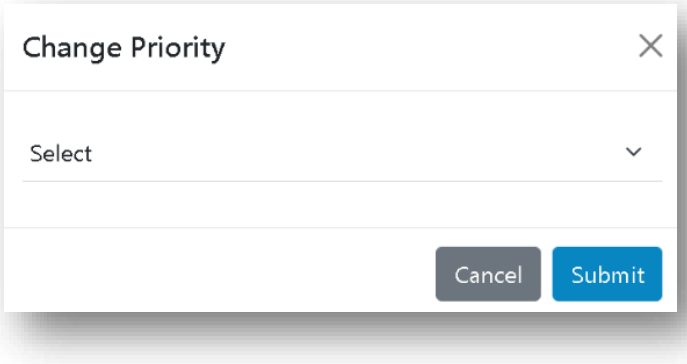

Figure 293 - Select the Change Priority Dropdown

3. Position the dragged rules at the desired position. As the ordering is changed, a **Save Priorities Button** appears at the bottom of the grid.

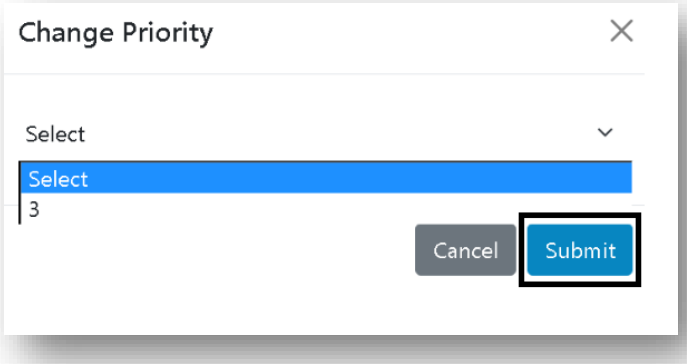

Figure 294 - Select the Change Priority Dropdown

4. Click on the **Submit** button to update the rule priorities.

5. On successful update the following message is displayed

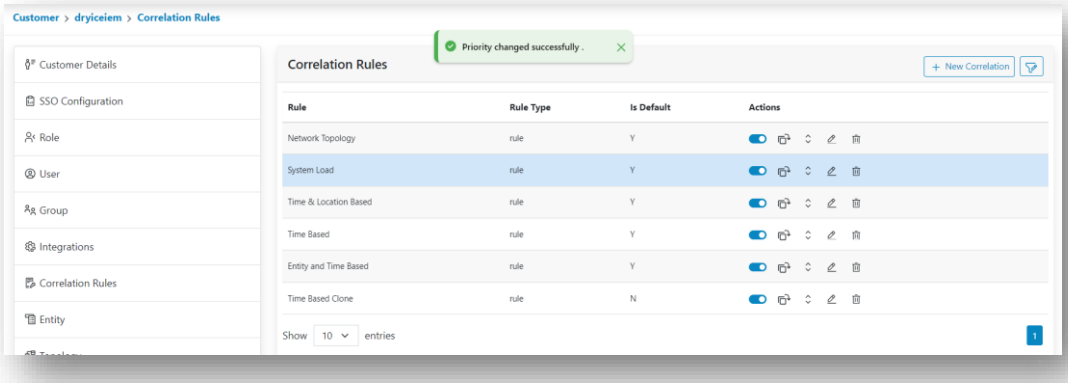

Figure 295 - Alert Message

6. The priority is saved; grid is refreshed showing the changed ordering.

Clone Correlation rules

1. Click on the **Clone** button next to the correlation rule that is to be cloned.

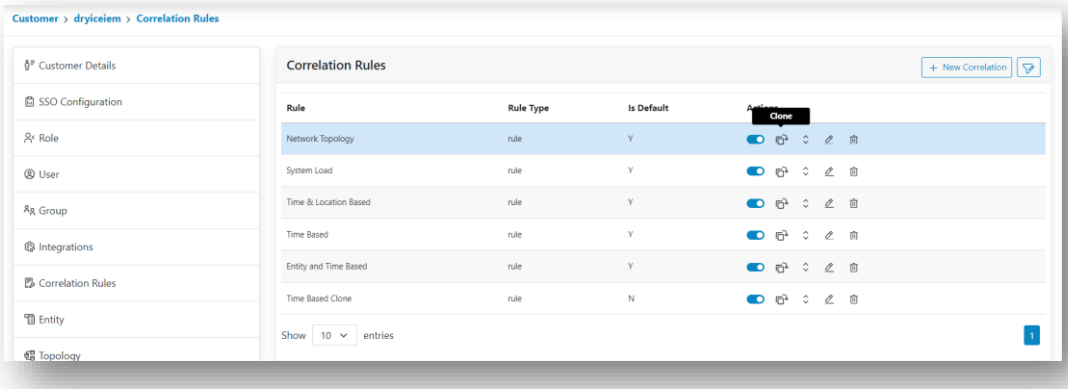

Figure 296 - Clone Action

2. This will prompt for confirmation as shown:

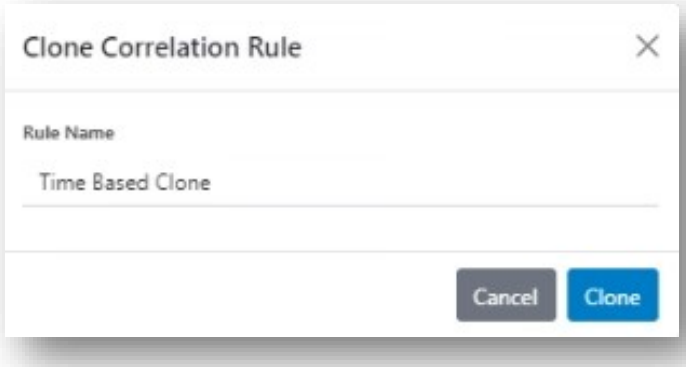

Figure 297 - Clone Connection Integration

3. On successful cloning the following message is displayed

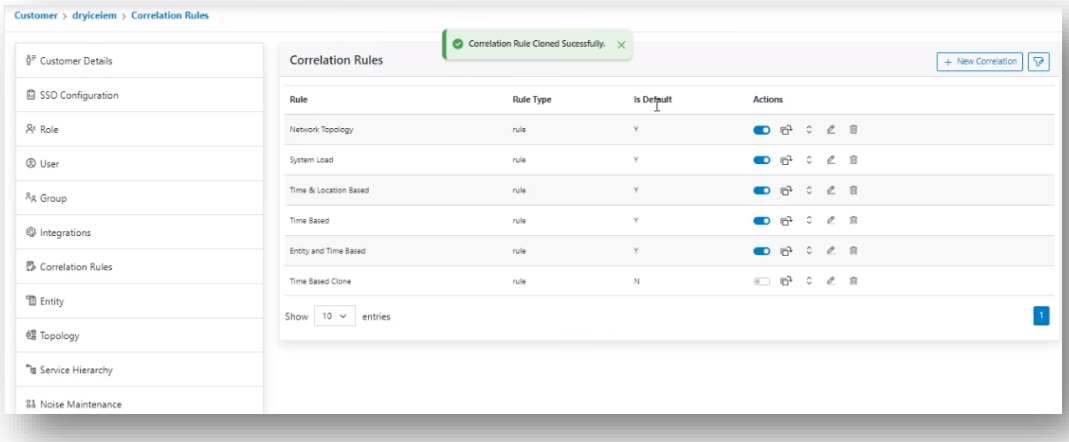

Figure 298 - Alert Message

Enable/Disable Correlation Rule

1. Click on the Enable/Disable toggle button next to the correlation rule that needs to be Enabled/Disabled.

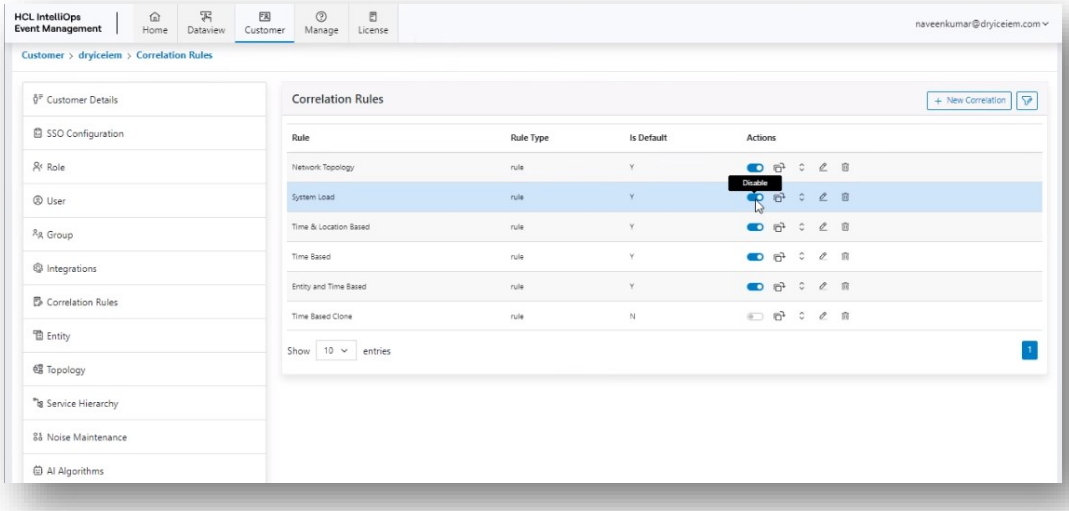

Figure 299 - Enable /Disable Correlation Rules

2. Click on **Enable/Disable** icon, on success a confirmation pop-up message is displayed.

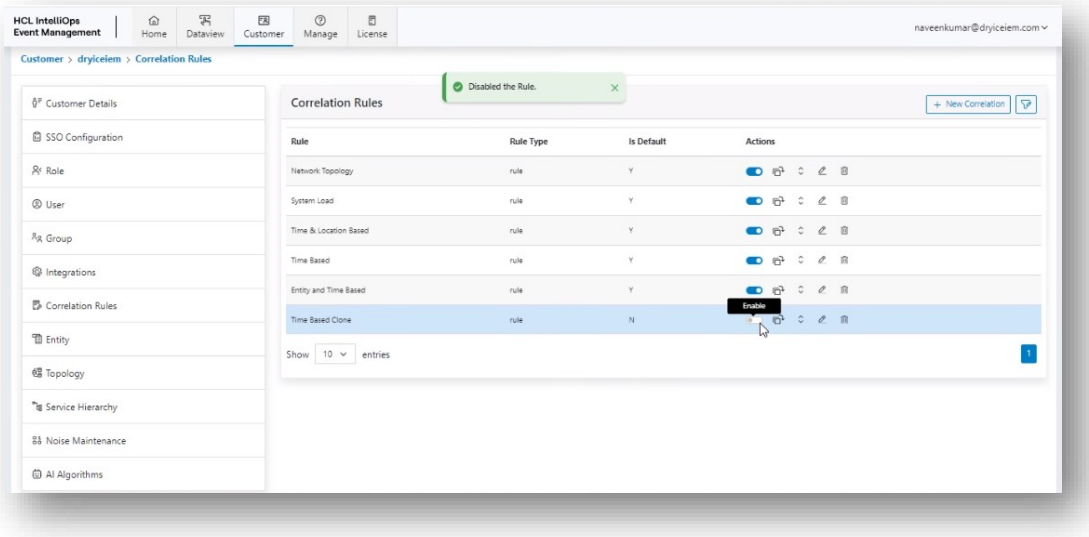

Figure 300 - Alert Message

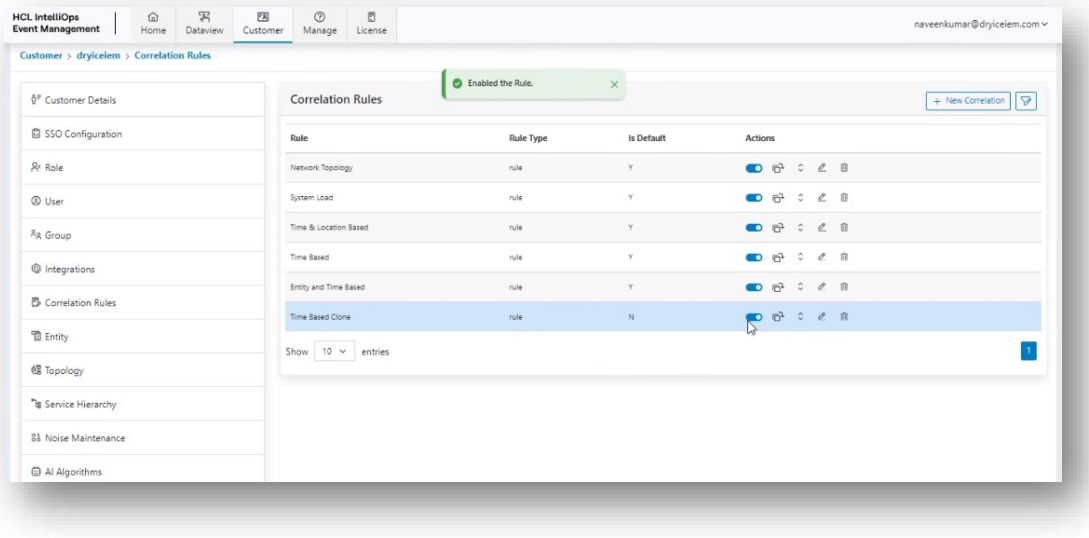

Figure 301 - Success Pop-up for Enable

Apply Filters

The section involves the steps to Apply filter to the Correlation Rules Data.

1. Click on the Apply filter action button present at the below the header of the console.

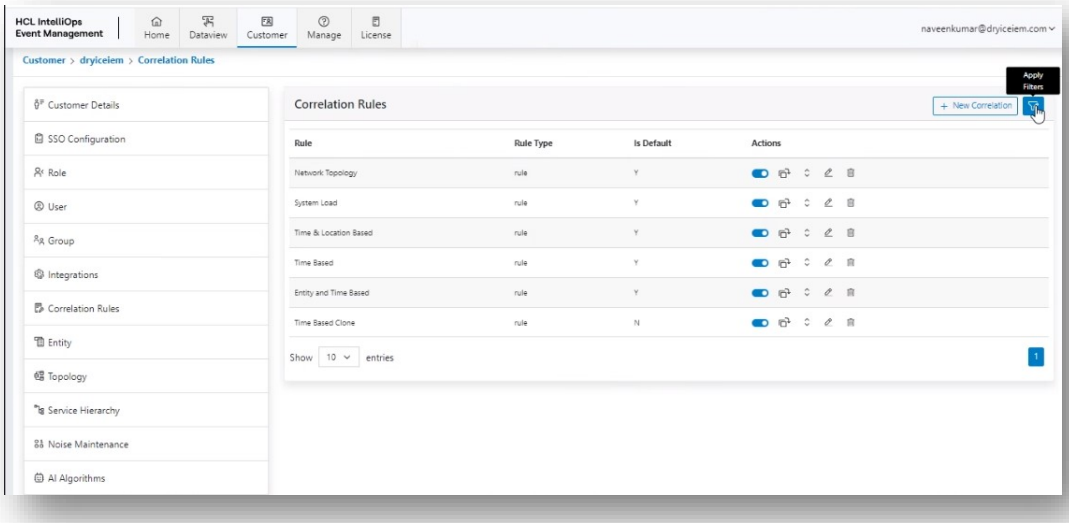

Figure 302 - Apply Filter Operation

2. The form appears. From there, select **Field** and **Operator** from drop down list and provide **Value**. Then click on the **Apply** button.

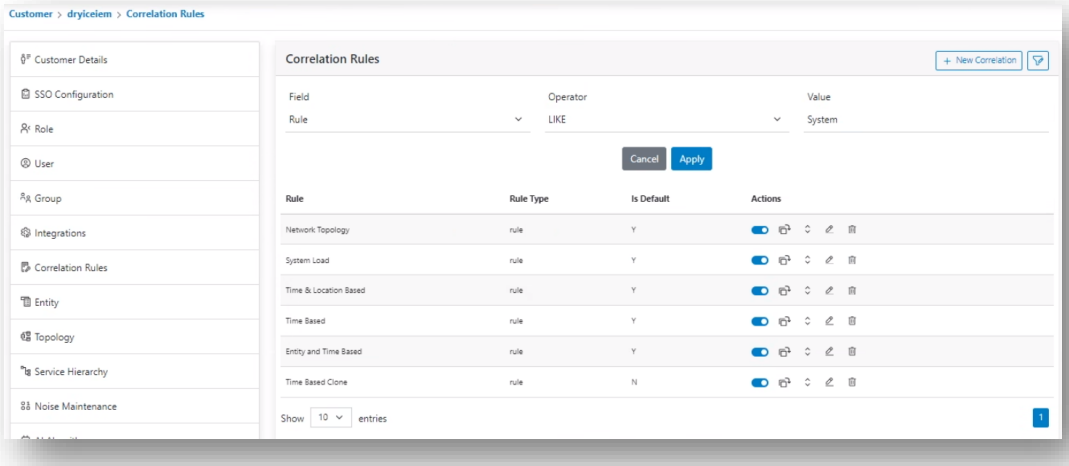

Figure 303 - Apply Filter Operation

3. The result looks as shown in the following figure:

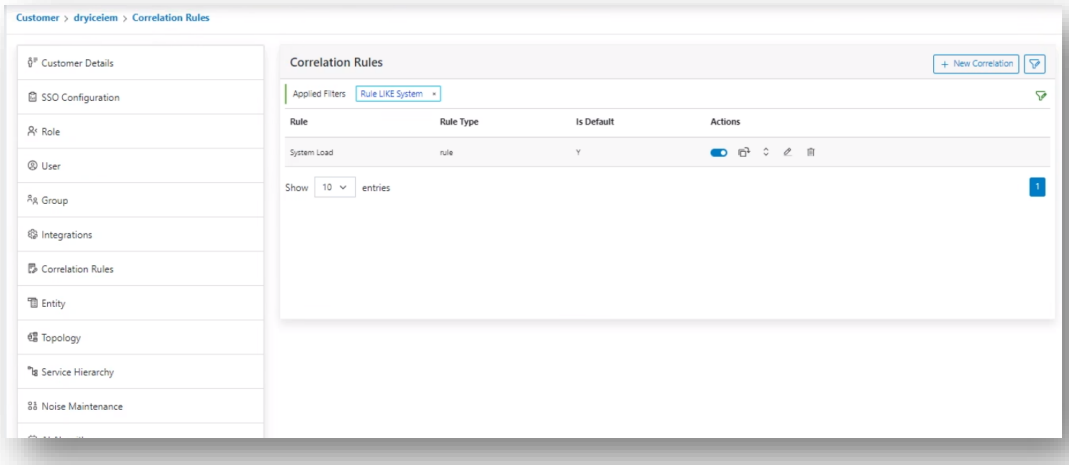

Figure 304 - Apply Filter Result

6.1.11.11 Integrations

Integration with third-party tools is a crucial feature for IEM. IEM leverage external tools and services to enhance their capabilities, providing a more comprehensive and effective solution for effective Event Management.

IT Service Management (ITSM) Integration:

- Integrate ITSM platforms for seamless collaboration between Event Management and IT service workflows.
- Facilitates the creation of tickets, automated incident resolution and related changes and problems updates for effective Root Cause Analysis.

Currently IEM has integrat**ion** with two tools:

- ServiceNow
- ServiceXchange

Both the tools are responsible for Incident Management, Automated Ticket creation, ITSM Collaboration providing a cohesive approach efficiently.

This section enables a user to define the external tool integrations within our environment e.g., if user needs to create a ticket in Service Now or update a ticket in ServiceNow, this is where user will define the integration details.

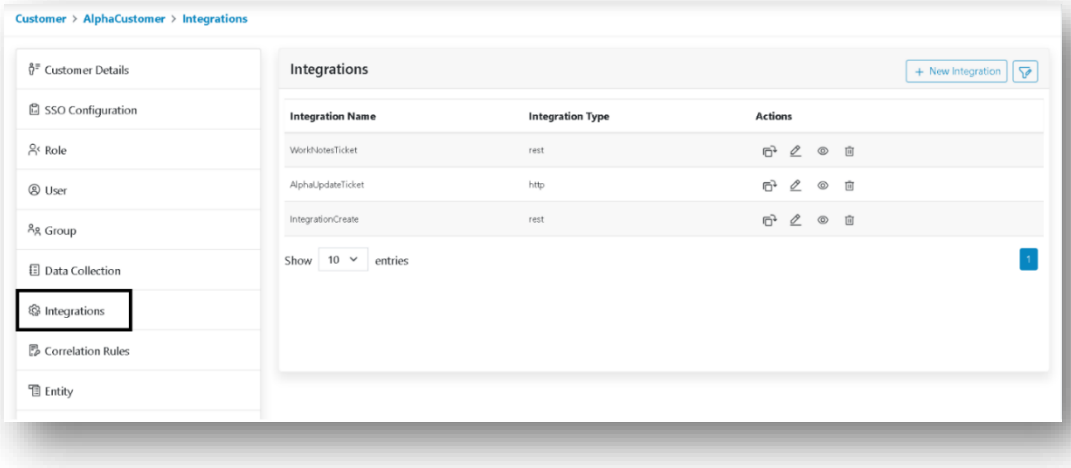

Figure 305 - Integration Page

1. Click the customer onboard section (“**Customer**”→ ”**Customer Name**”→ “**Integrations**”)
2. Click on the **Integration** page. Available integrations are displayed in the grid. Following are the actions, the user can perform on this screen based on their roles.
   - Add New
   - Clone Existing
   - Edit Existing
   - View Existing
   - Delete
   - Apply Filters

Add New Integration

1. If there’s no integration defined, then click on **“+ New Integration**” button shown on the top of the Integrations Screen, as in the below image:

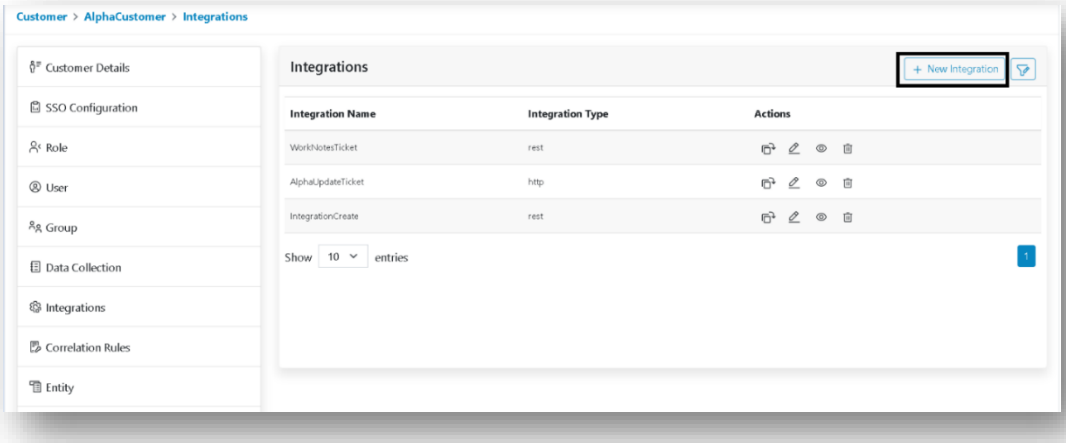

Figure 306 - Creating New Integration

2. The user is redirected to the Integration form, which is divided into 3-Steps.
   - **General** (Step 1)
   - **Connection** (Step 2)
   - **Definition** (Step 3)

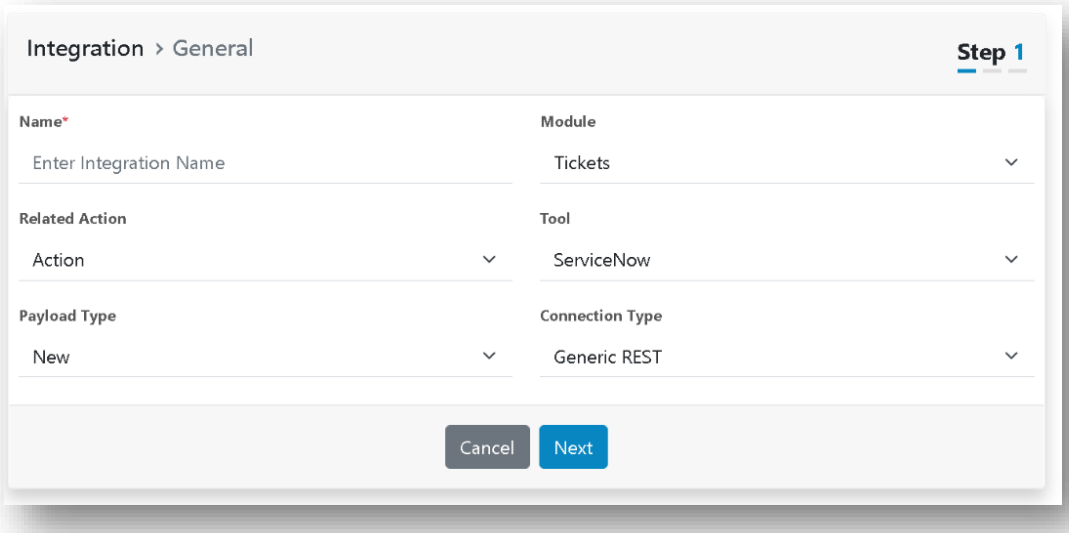

Figure 307 - Create an Integration

3. In **General** Section fill in the below details:
   - **Name**: Name of Integration
   - **Module**: Module for which the integration is to be defined like Tickets.
   - **Tool**: Tool related to the selected module e.g., for Tickets user have ServiceNow.
   - **Payload Type**: Payload Type default set to New.
   - **Connection Type**: The way user integrates with the selected tool. Two integration types are supported:

- **Generic REST** with basic authentication (pull based)
- **HTTP Push Request** with Token based authentication.

- **Related Action**: Type of action for which the integration is being defined like Create Ticket, Update Ticket etc.

4. Once user fills in the above details and click on Next, control is redirected to the second step.

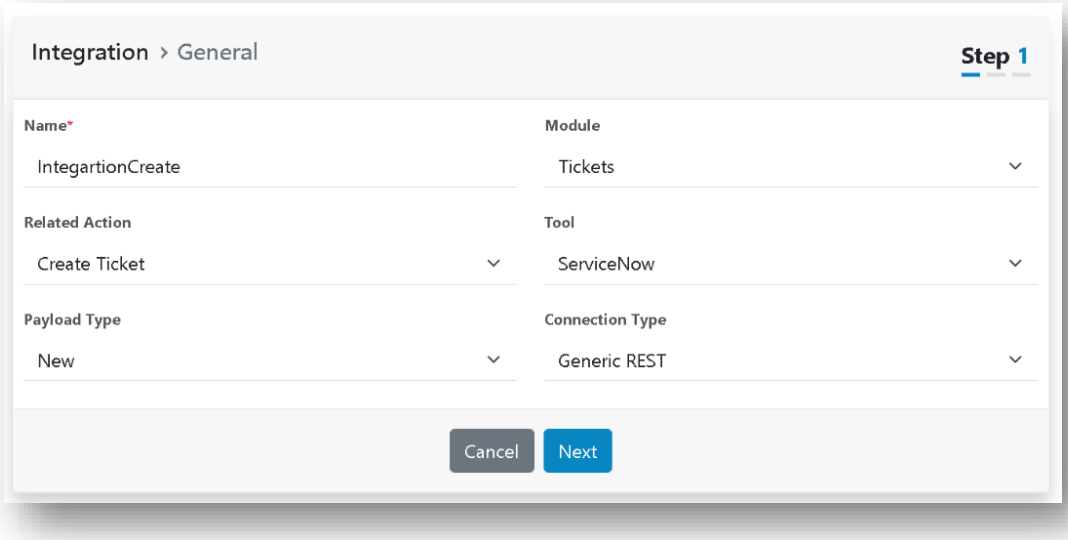

Figure 308 - Create an Integration

5. **Connection** Section – In this section, users can select an existing connection or create a new connection.

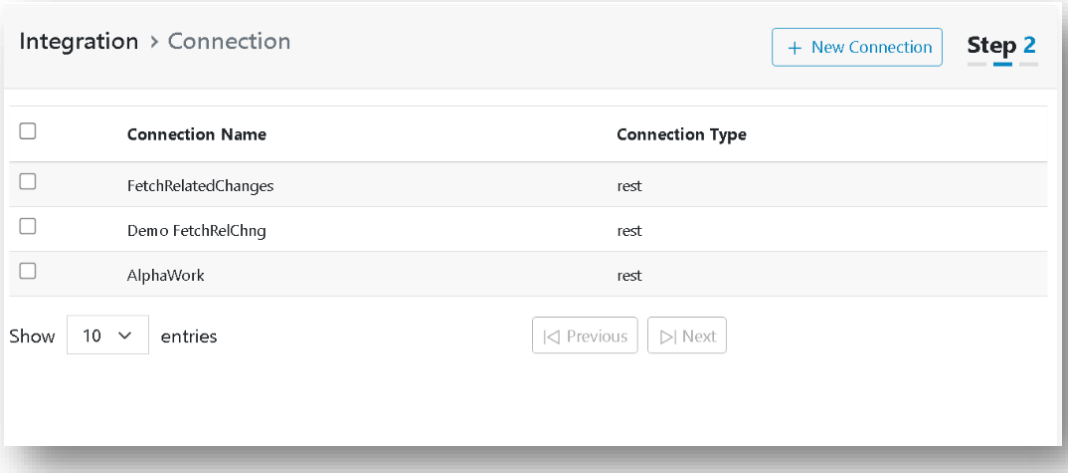

Figure 309 - Existing Connection

6. For selecting from the existing list of connections, user must select the checkbox from existing connection and click on **Next** button.

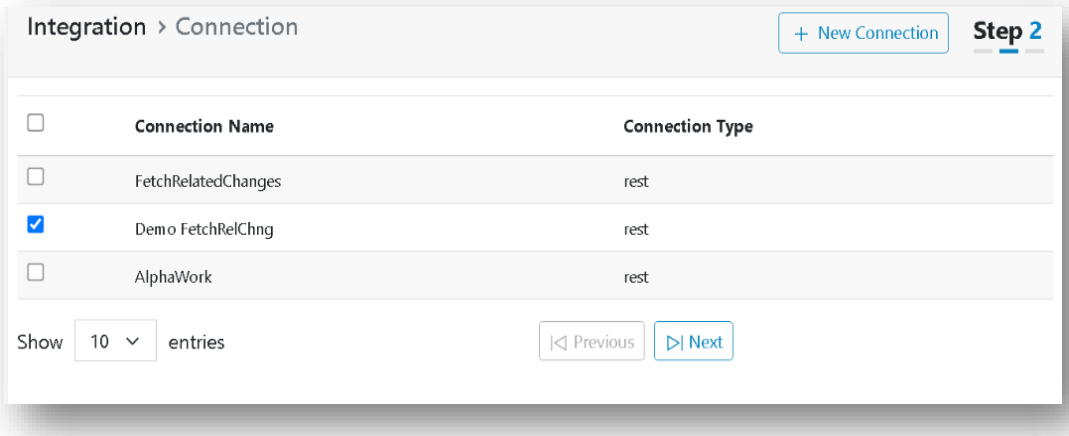

Figure 310 - Existing Connection

To create a new connection, the **New Connection** button is to be clicked, and user will be redirected to the Manage connection form.

7. The input being asked for in this section depends on the **Connection Type** selected.
8. Refer to the “Manage Connection section” to understand the steps for creating a REST based connection.
9. For the Generic REST Pull Based Connection Type in the General section, the following options need to be filled in.
   - Connection Name
   - Base URL

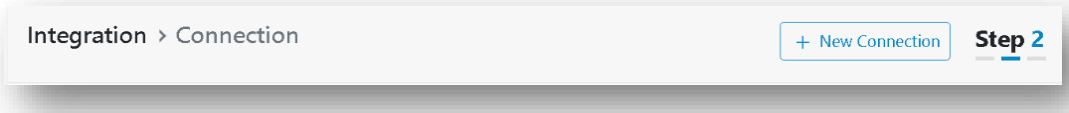

Figure 311 - Navigation Bar for Create a New Connection

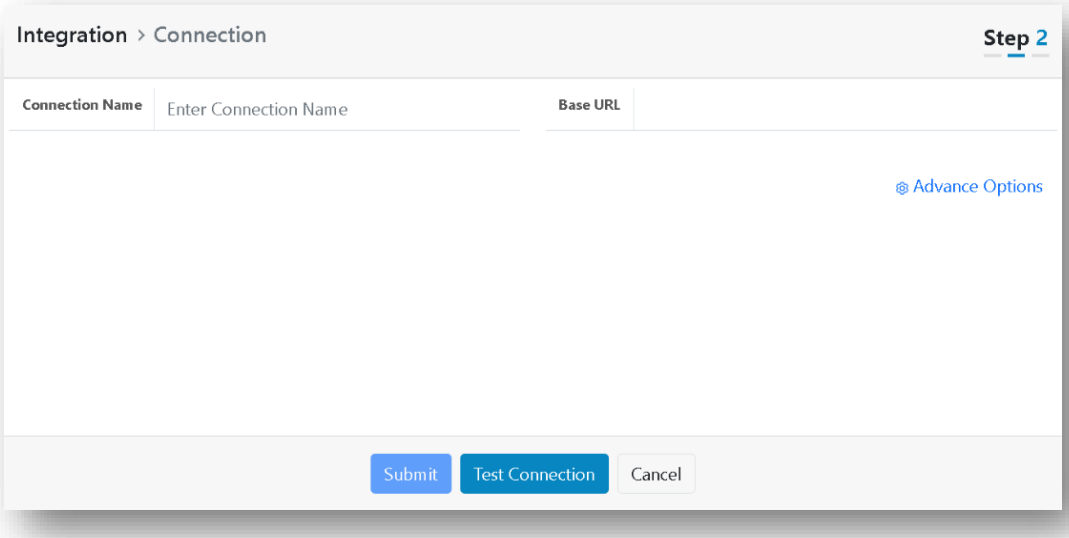

Figure 312 - Creating New Name for Connection

10. If the user clicks on the **Advance Options** button, it displays the following options to fill in.
    - Authentication Type
    - Username

- Password

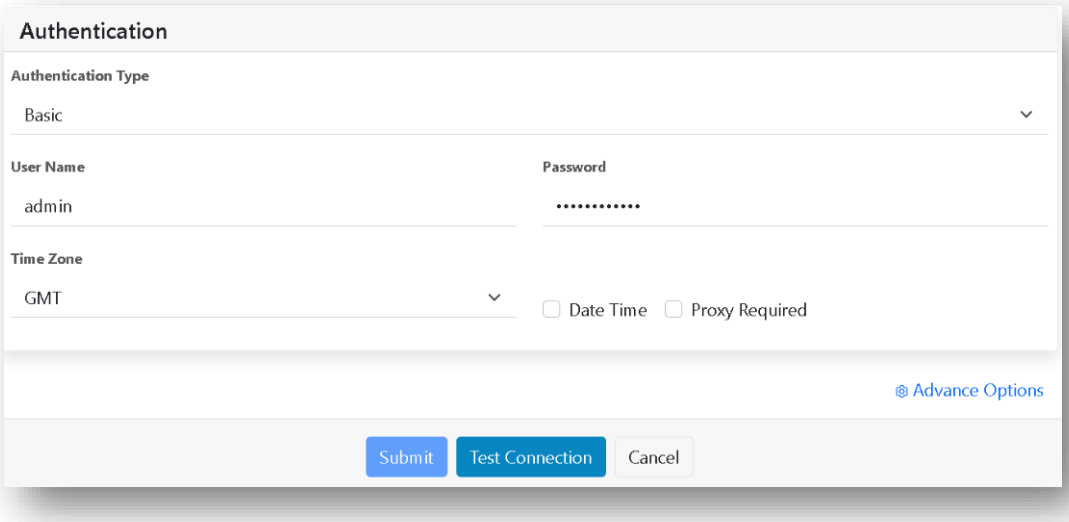

Figure 313 - Advance Options

11. After all fields are filled, click on the **Test Connection** to check the URL Connection. It displays the message as shown below:

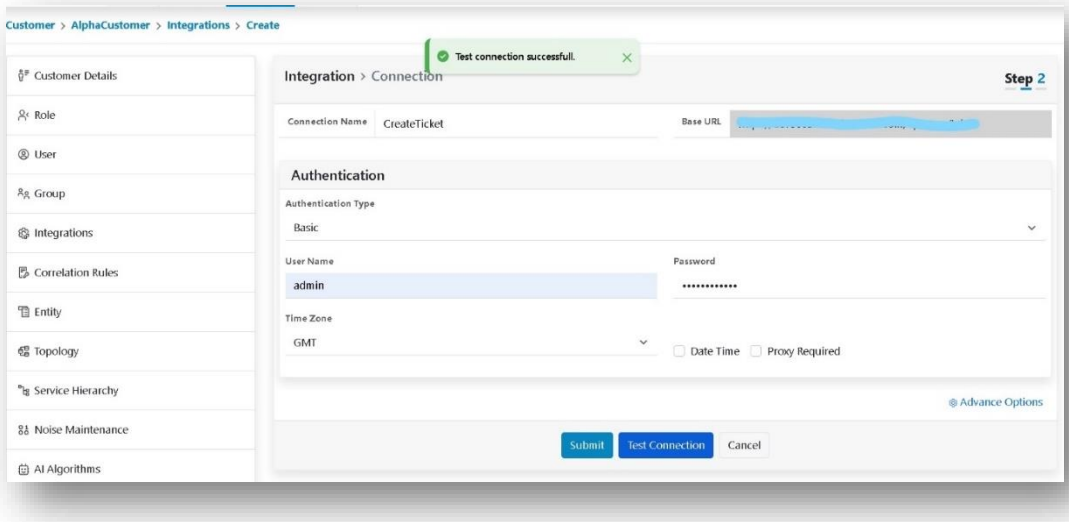

Figure 314 - Alert Message

12. After successful Test connection, click on **Submit** Button. It displays the New Connection added pop-up as below.

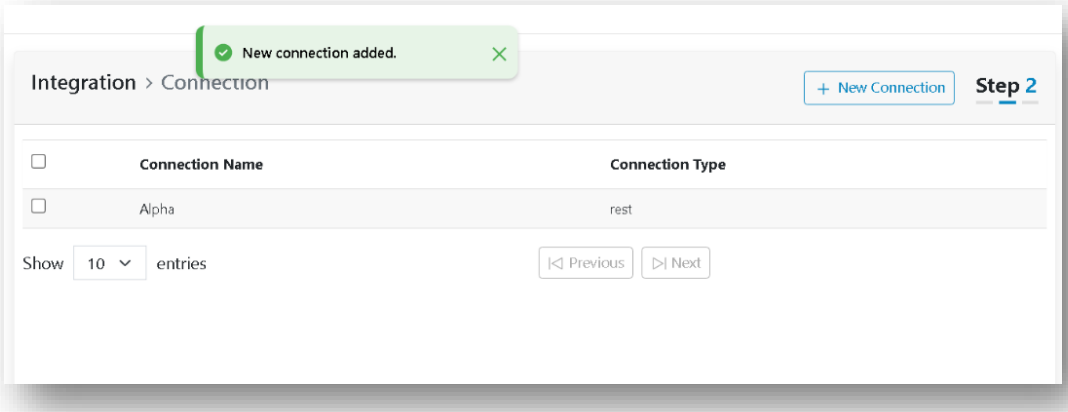

Figure 315 - Alert Message

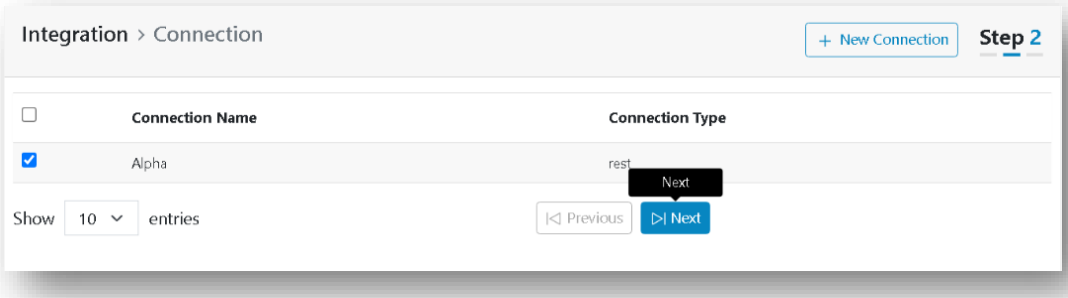

Figure 316 - Existing Connection

13. If a user selects HTTP Request Push Based Connection Type in the General section, the following fields need to be filled.
    - Connection Name
    - Base URL
14. Specify the **Connection Name**, a Token is populated, and the URL is ready to be used for integration by the external tools.

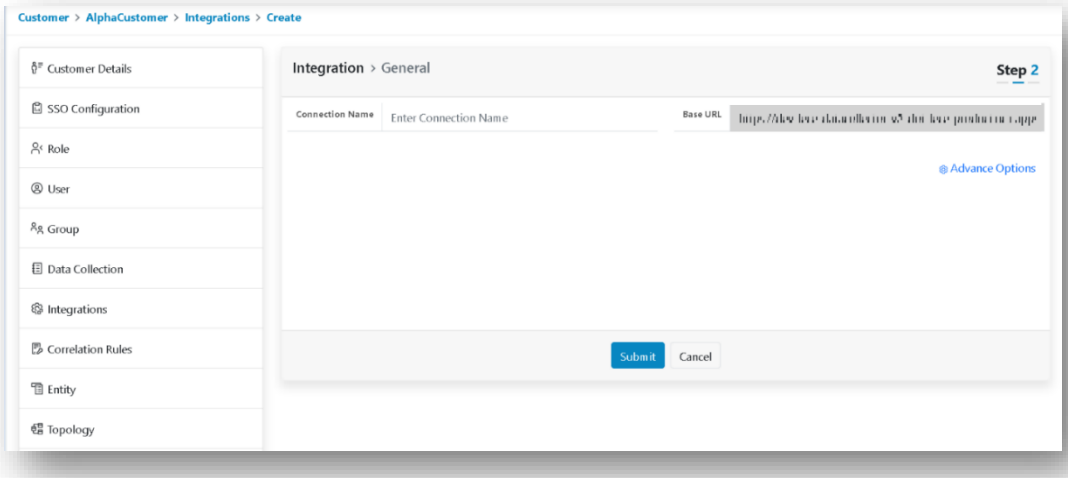

Figure 317 - Create New Connection

15. Copy the URL and click on the **Submit** button.

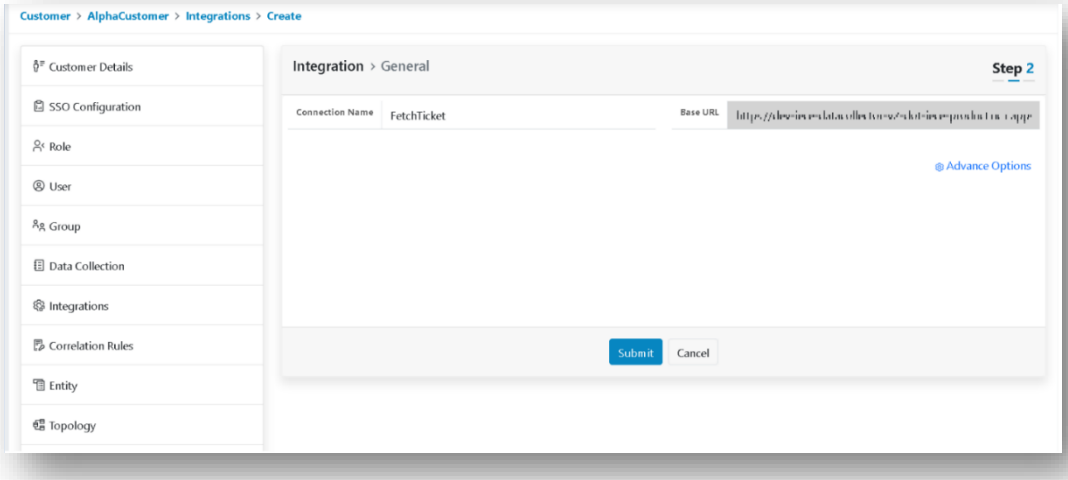

Figure 318 - Create New Connection

16. Clicking on the **Submit** button takes the user to the **Definition** tab.

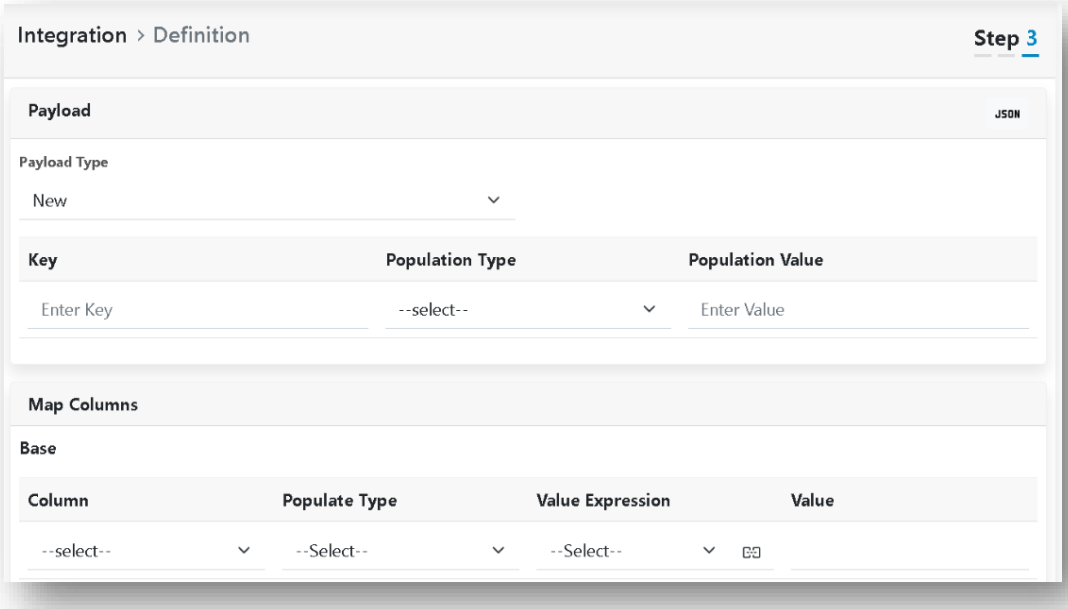

Figure 319 - Definition Section

17. **Definition** (Step 3) is where user defines the request details. This section is further divided into the following subsections.
    - Method
    - Table Name
    - Request Body
    - Response
    - Payload
    - Map Columns

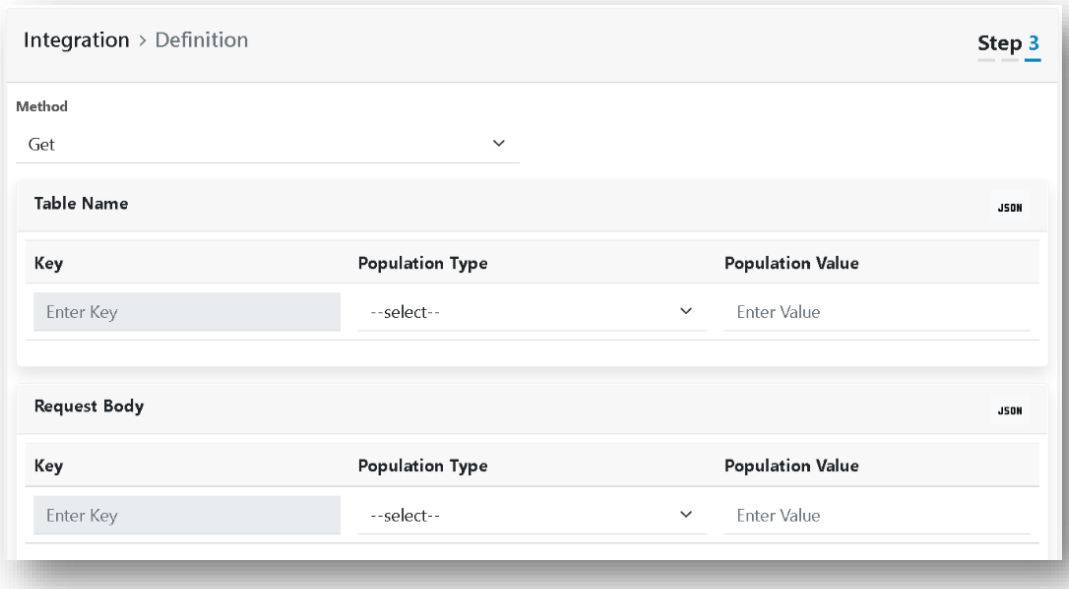

Figure 320 - Definition Section

These sub-sections depend on the **Connection Type** selected.

a. **Method**: In this section the user needs to select **Method Type** from the dropdown list.

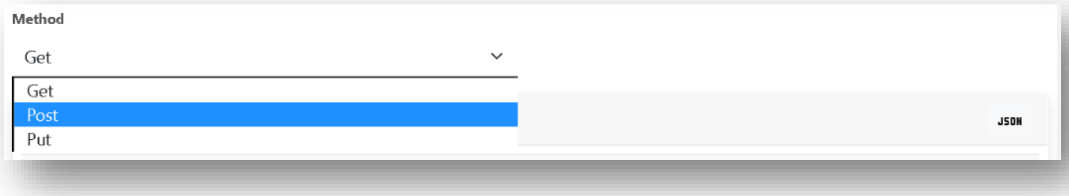

Figure 321 - Method Type

b. **Table Name**: In this section, the user needs to add the **Table Name**. First, the user needs to click on JSON button which is on right side top. A form appears in which user needs to add JSON data.

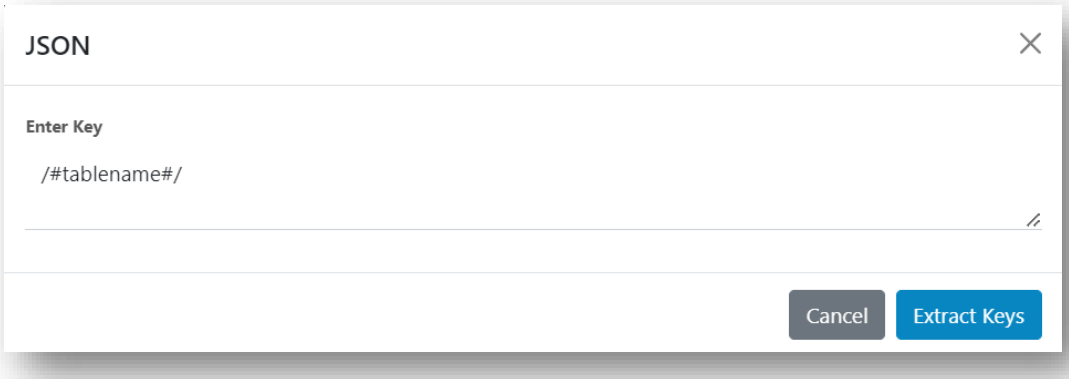

Figure 322 - Table Name

c. Click on the **Extract Keys** button. It displays the screen below. Select the *Population Type* and **Population Value**.

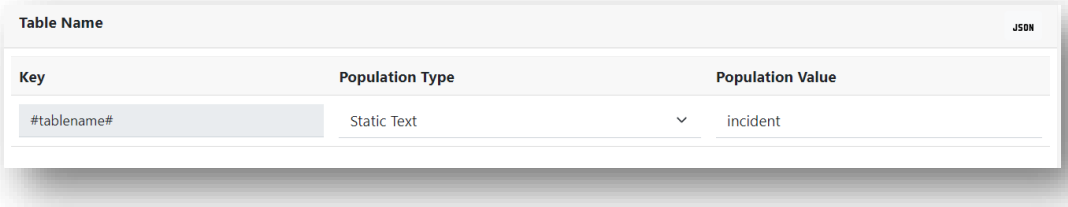

Figure 323 - Extract Keys

d. **Request Body**: In this section adds table name. First, select JSON button which is on right side top, a form appears in which the user adds JSON data.

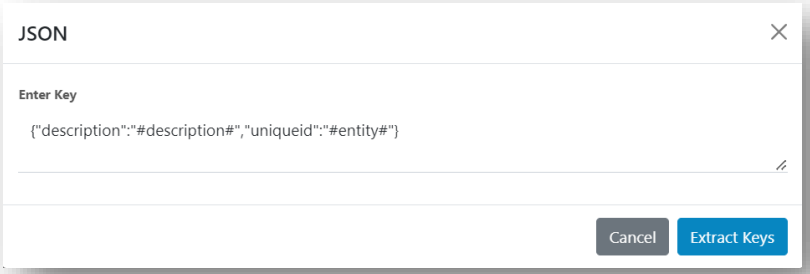

Figure 324 - Request Body

In Request body, against unique ID we should be able to map multiple or 2 fields, namely entity and parameter. Add Entity and parameter under JSON in a single tab.

e. Click on the **Extract Keys** button. The following screen appears. Select the **Population Type** and **Population Value**.

In case of problem & Change Integration, state mapping values from service Now need to be taken from customer service now team.

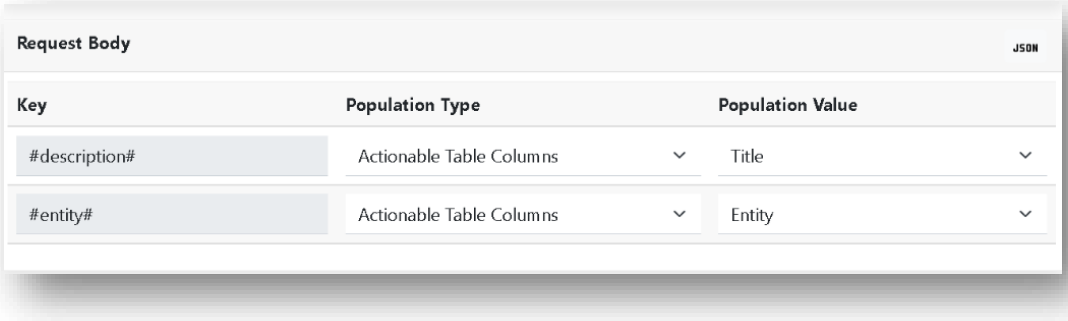

Figure 325 - Extract Keys

f. **Response**: User needs to fill the following fields.

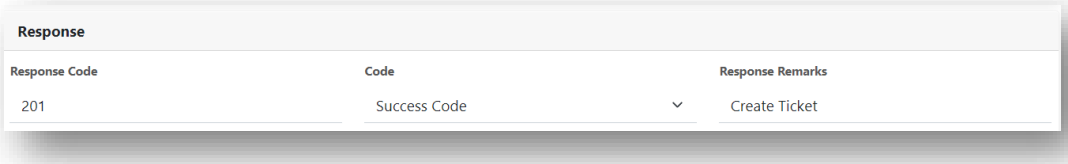

Figure 326 - Response

g. **Payload**: Next, user needs to define the payload json. This section is applicable for both Generic REST as well as HTTP. Specify the JSON and click on Extract Keys. This populates all keys and values of that response JSON.

Figure 327 - Define Payload Json

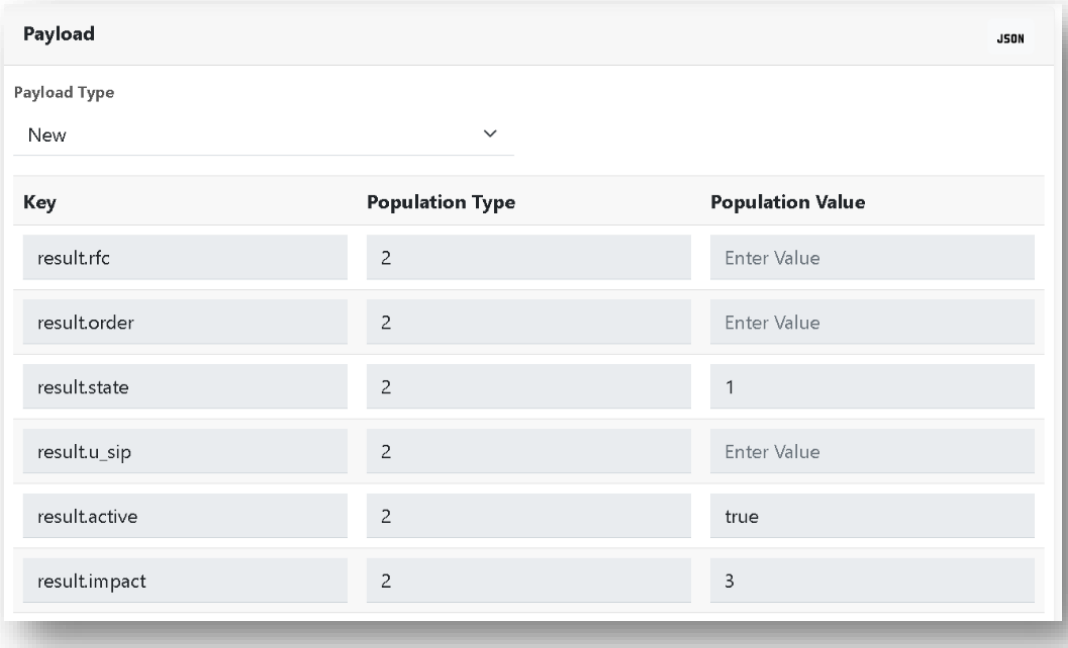

Figure 328 - Extract Payload Json

h. **Map Columns**: This section is applicable for both Generic REST as well as HTTP, once the Payload JSON is extracted, user then maps the source columns to IEM columns using the following Population Type:

- **JSON key**: the columns are mapped with the Payload JSON Keys.

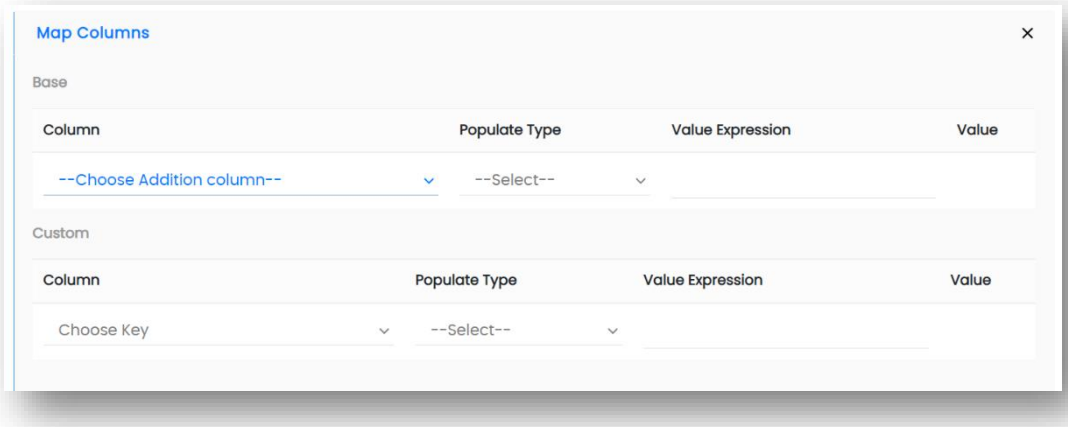

Figure 329 - Map Columns

- In the **Columns** section, select the IEM column or create a new custom key in the **Custom** section. In the **Population Type**, select JSON key and the value expression populates with the JSON keys extracted. Choose the relevant key. As the key is selected, its values are displayed underneath the value column.

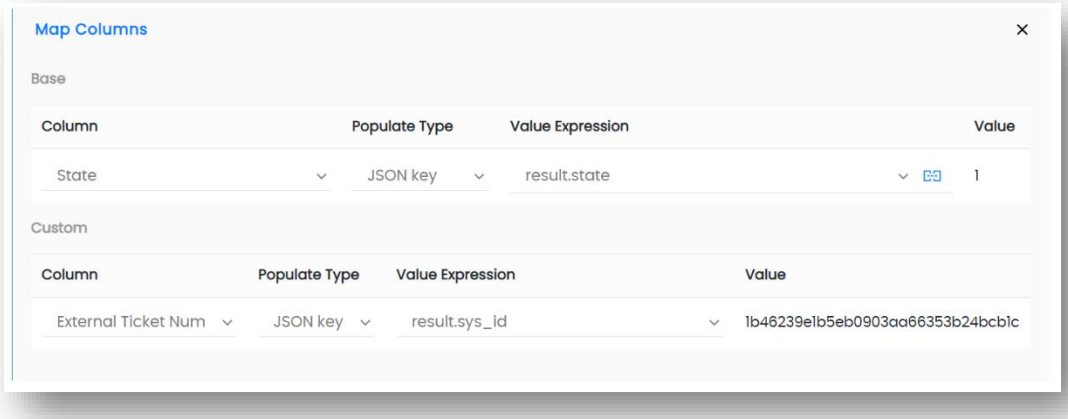

Figure 330 - Map Columns

- There are a few columns, for which it is must to specify the value mapping. For e.g., for State column user need to specify mapping of the incoming values to state values as shown below.

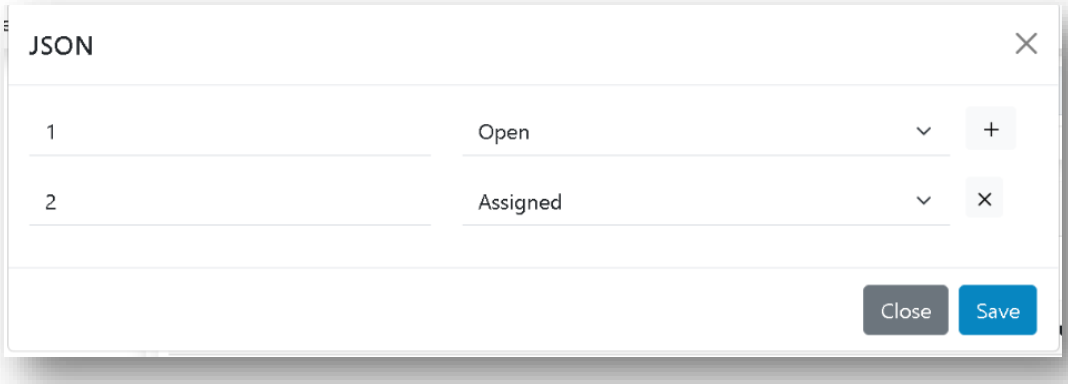

Figure 331 - Mapping State Column

- After clicking on the **Save** button, the following will appear.

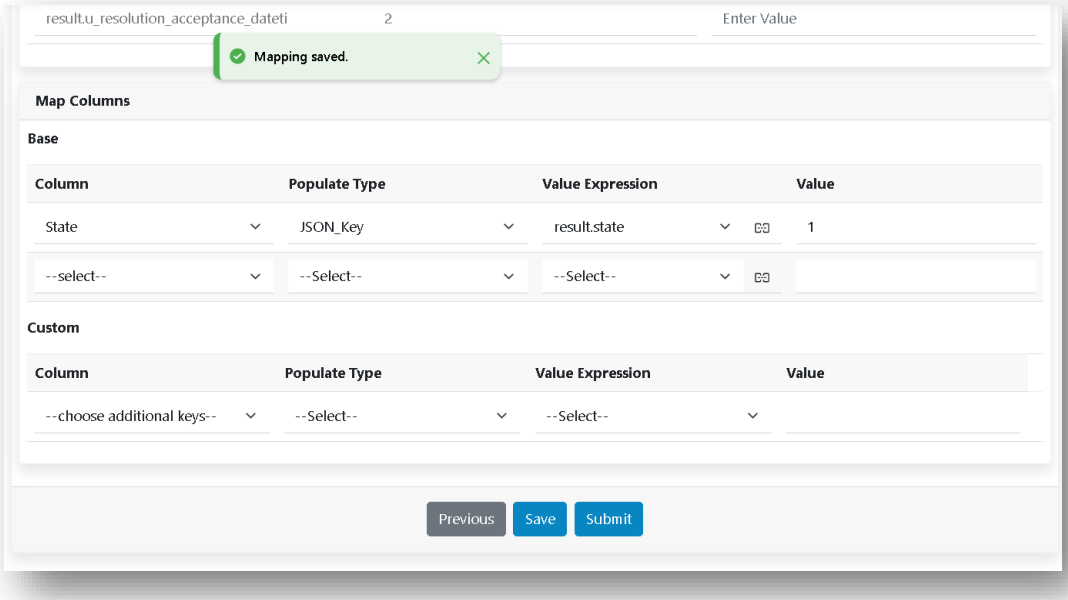

Figure 332 - Alert Message

It's important to capture all important fields from the source which might later be used for modification purposes or creating a bidirectional integration. E.g., in the case of ServiceNow along with Incident Number it's important to capture sys id which is their unique identifier as it enables easy update flow between the two tools i.e., ServiceNow and IEM.

i. Once all the details are specified, user have two options for Saving its details.

- **Save** – Saves the configurations details. Once saved user can edit the configurations.
- **Submit** – Submits not only save the details but it also enables all the related processing's for the associated integration and is the final submission of the details. Post submission the processing details cannot be edited. Refer to the edit section to understand the possible edit allowed post Final submission.

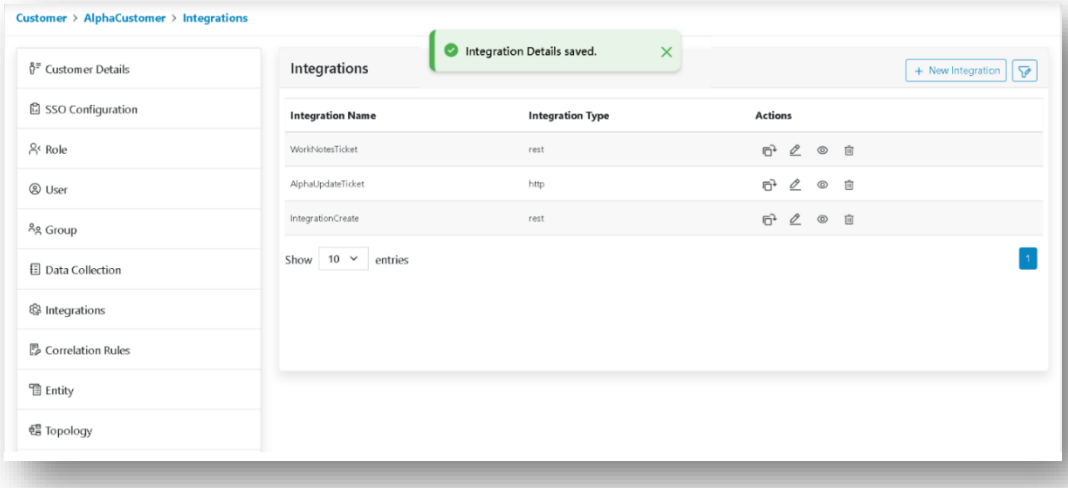

Figure 333 - Alert Message

Clone Integration

1. Click on the **Clone** button next to the integration that is to be cloned.

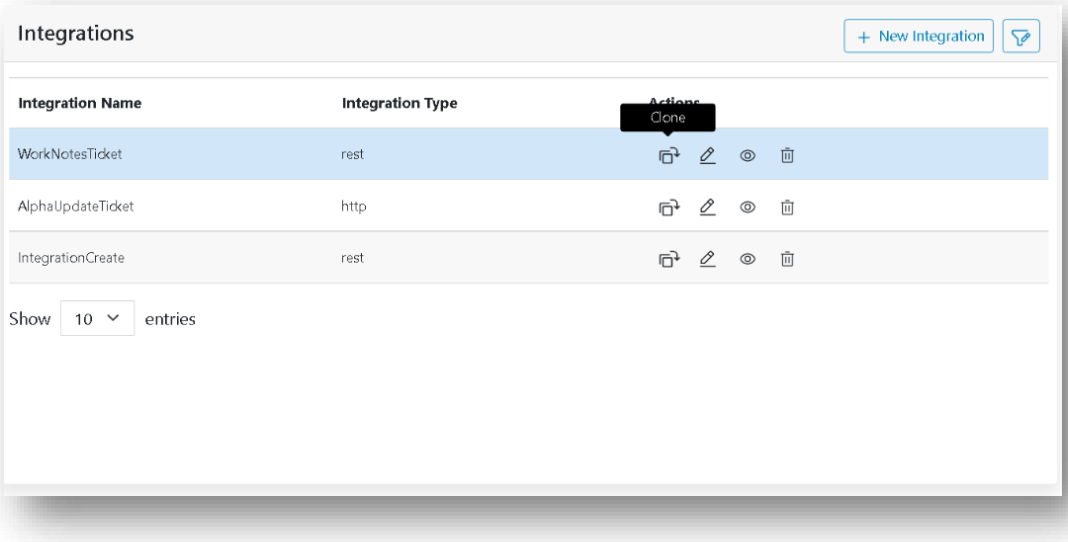

Figure 334 - Clone Action

2. This prompts for confirmation as shown:

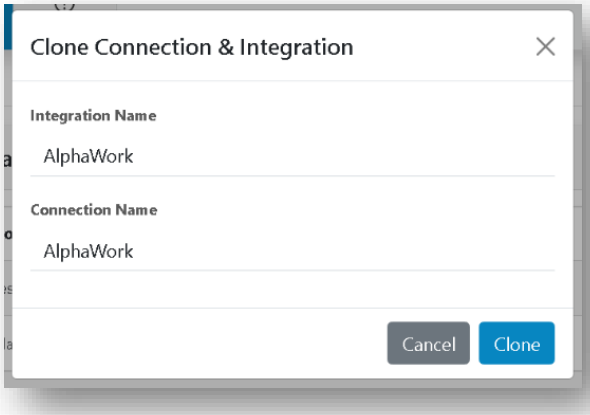

Figure 335 - Clone Connection Integration

3. On successful cloning the following message will be displayed

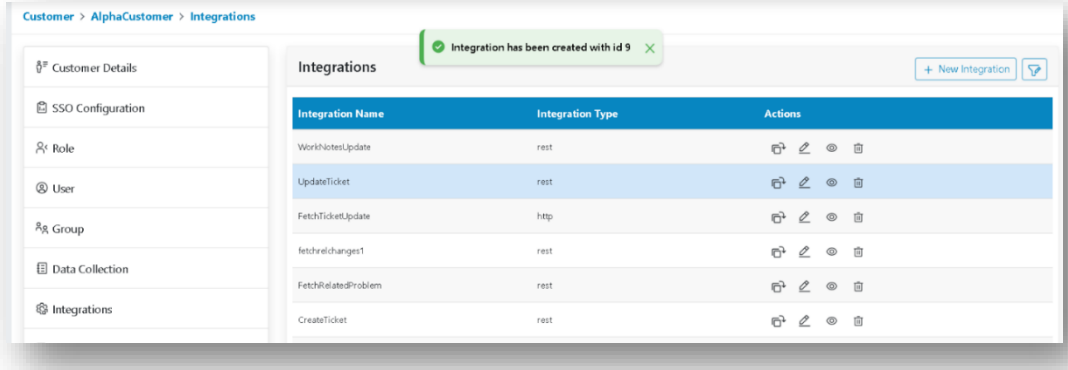

Figure 336 - Alert Message

Edit Integration

1. Click on the Edit icon next to the integration that is to be edited.

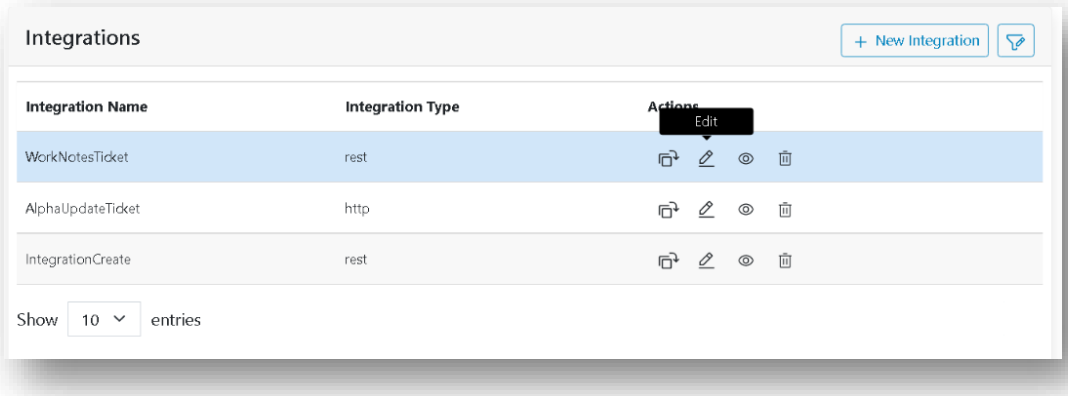

Figure 337- Edit Action

2. This populates all the sections user discussed while creating new connection with the Saved Values.

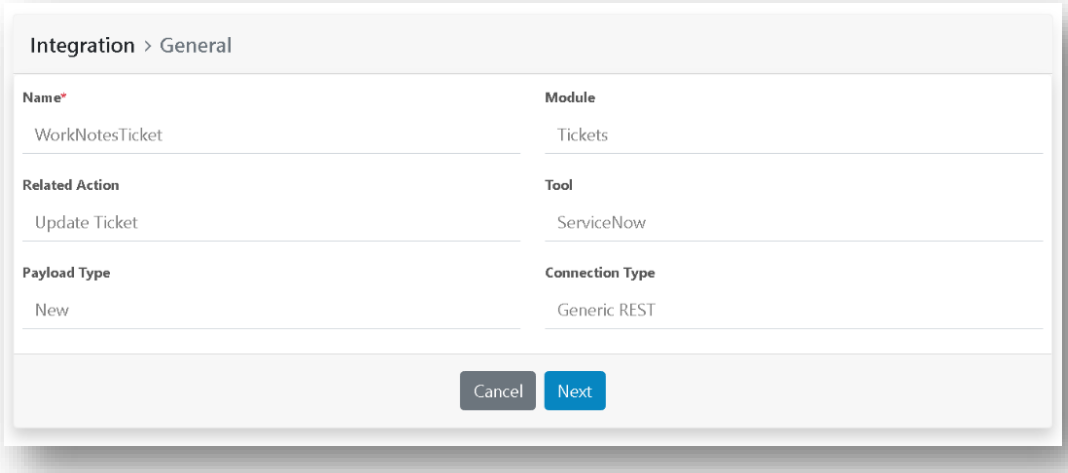

Figure 338 - Edit General Section

If user only Saves the integration, then inputs are enabled for the user to update its values, however if user edits post Submitting the integration, he can only update credentials\Tokens.

3. Make the necessary changes and click on **Save/Submit** as applicable.

Once the Integration is submitted, the only option available is “Submit”, If the integration is saved only then both **Save** and **Submit** options are available.

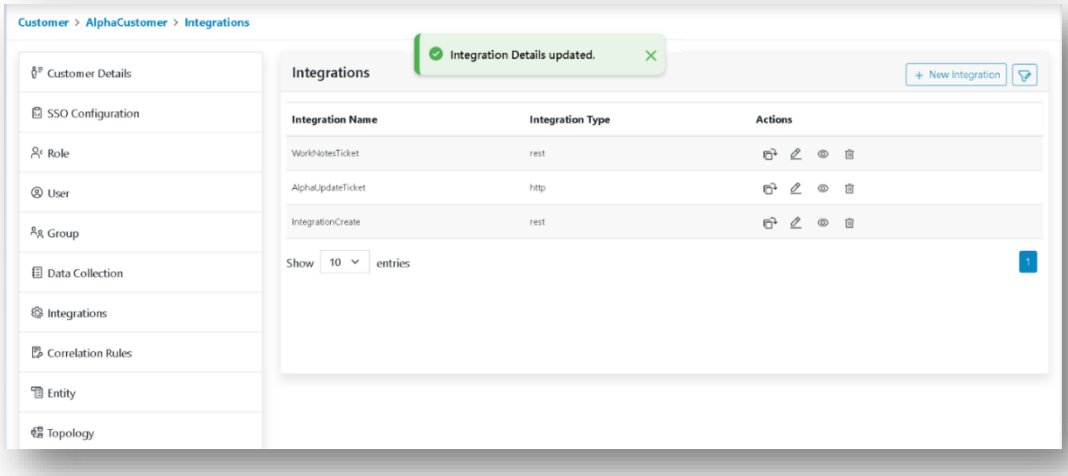

Figure 339 - Alert Message

View Integration

1. Click on the View icon next to the integration that is to be viewed.

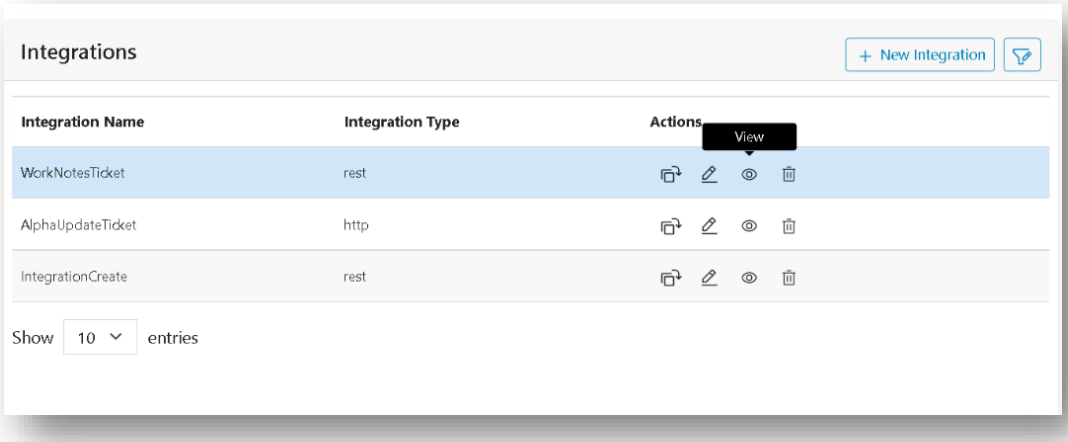

Figure 340 - View Integration

2. This opens all the sections in Read Only mode with the saved value.

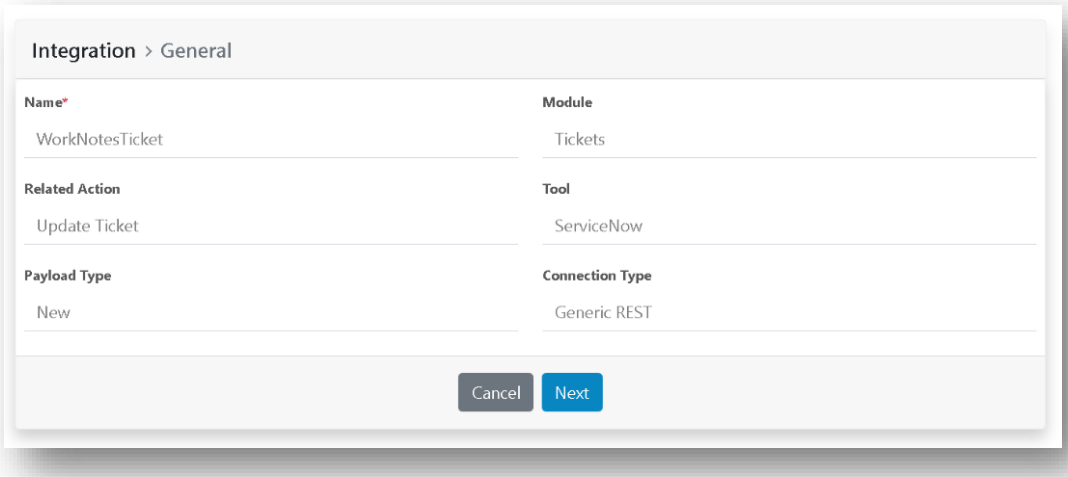

Figure 341 - View Integration

1. Click on the Delete button next to the integration that is to be deleted.

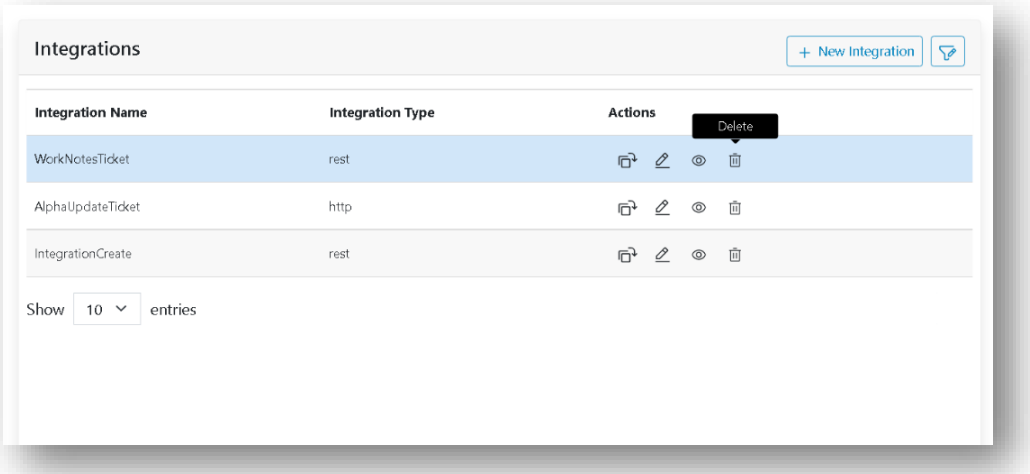

Figure 342 - Delete Integration

2. This will prompt for confirmation as shown.

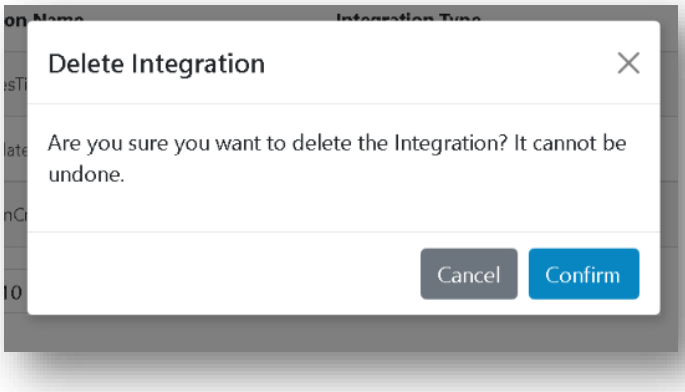

Figure 343 - Confirmation pop-up

3. On successful deletion the following message will be displayed.

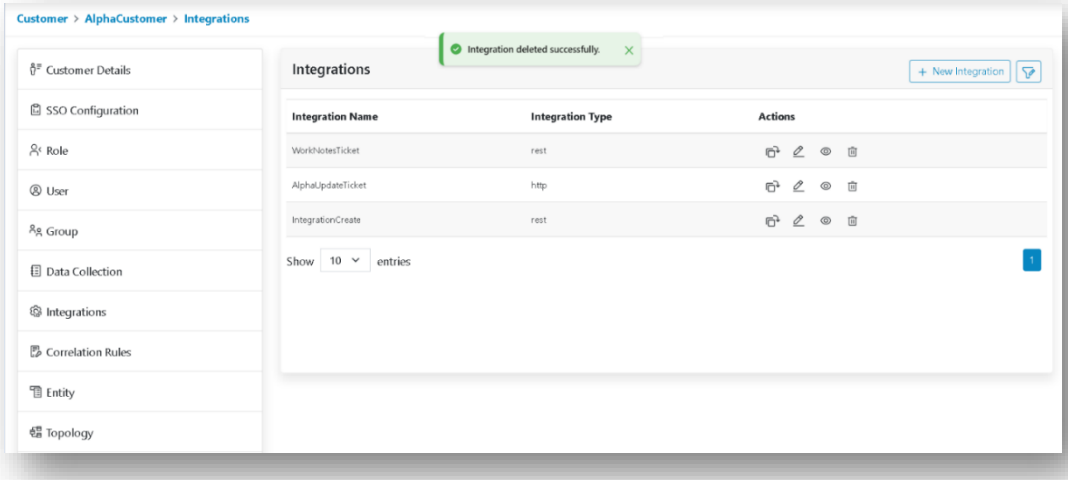

Figure 344 - Alert Message

The steps involved how to apply filter to the Integration Data.

1. Click on the Apply filter available action button present at the below header of the console.

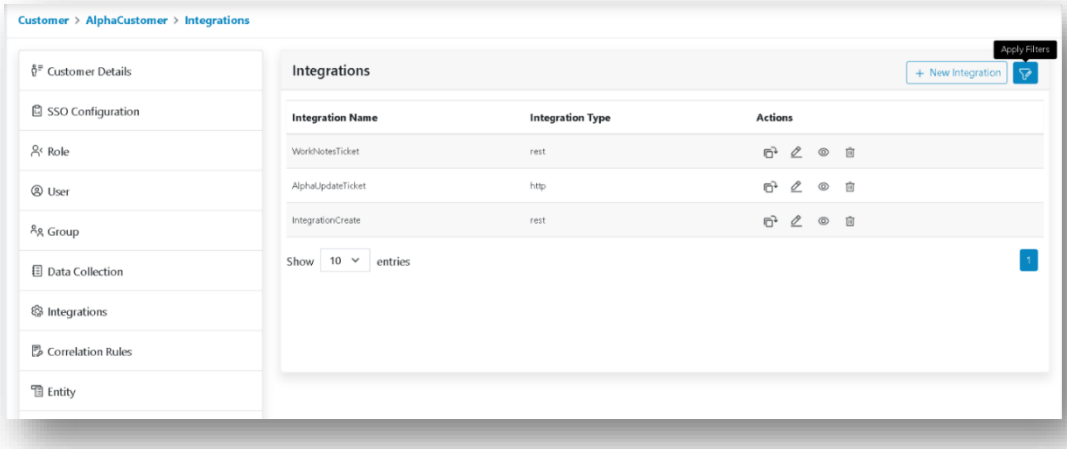

Figure 345 - Apply Filter Operation

2. The following form appears. Select **Field** and **Operator** from drop down list and provide the values. Then click on the **Apply** button.

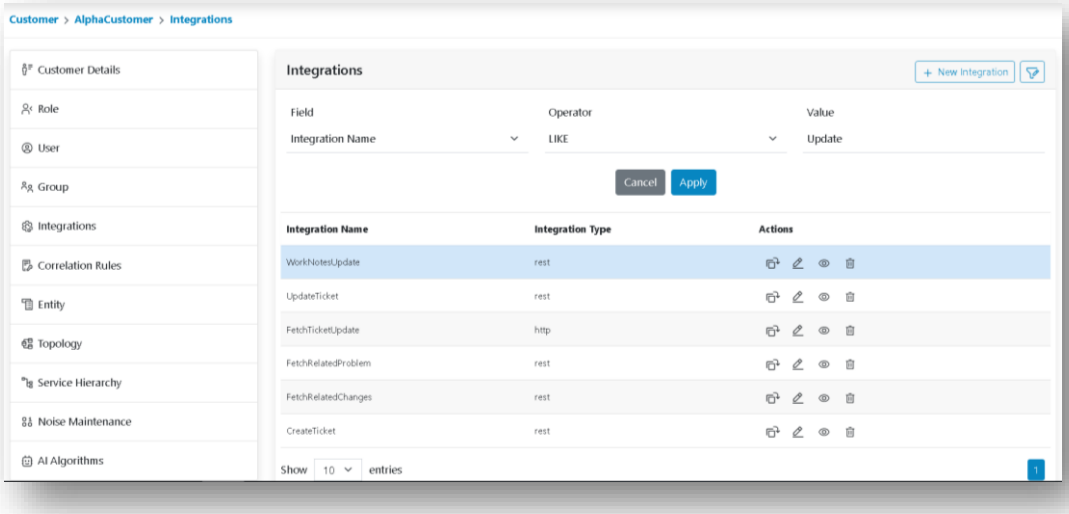

Figure 346 - Apply Filter Operation

3. The result of applied filter looks as shown in the following figure:

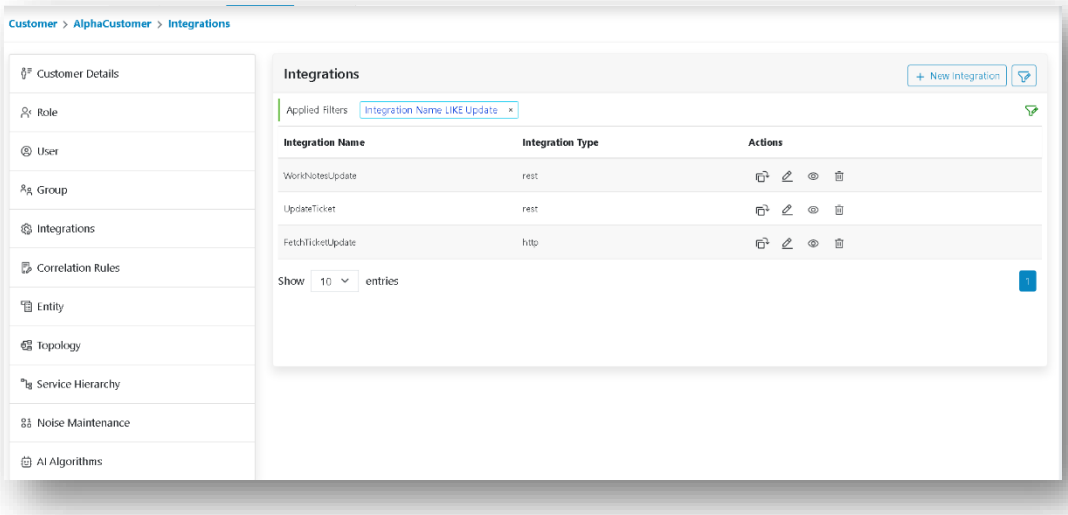

Figure 347 - Apply Filter Result

6.1.11.12 AI Algorithms

AI algorithms excel at identifying anomalies or deviations from normal behavior in large datasets. Early detection of abnormal patterns helps in proactively identifying potential issues or security threats before they escalate. AI algorithms can recognize patterns and trends in historical and real-time data. It automates the process of identifying the root cause of incidents. AI algorithms correlate alerts from various sources to identify relationships and dependencies. AI Algorithms in IEM enable Temporal-based alert Correlation.

IEM leverages in-house AI Toolkit which has Out-of-Box features and it can be accessed based on roles and permission. Customer administrator then can create objectives over IEM and post that training of model is implemented on the data ingested via IEM and model is used in prediction for AI-Use cases.

AI-Driven Use-Cases for IEM includes,

- Enables user / system to select relevant algorithm for the use cases.
- Metric anomaly system to identify anomalous metric point.
- Temporal-based Alert Correlation.
- Feedback system for temporal-based correlation to avoid irrelevant alert to actionable grouping.

This section enables us to configure the AI Algorithms in IEM.

1. Click on the “Customer”→ “Customer Name”→”AI Algorithms” (On the Navigation page)
2. The Following page will be displayed:

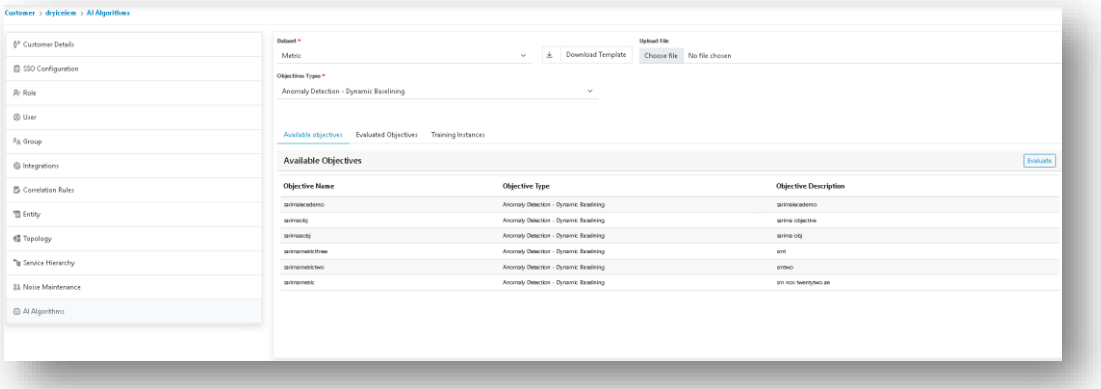

Figure 348 - Algorithms Available objectives

3. Objectives created in the environment will be listed in the grid view.

AVAILABLE Objectives

1. Select the dataset from the Dataset dropdown. The following options are available:
   - Metrics
   - Correlation Data
   - Correlation Feedback Data

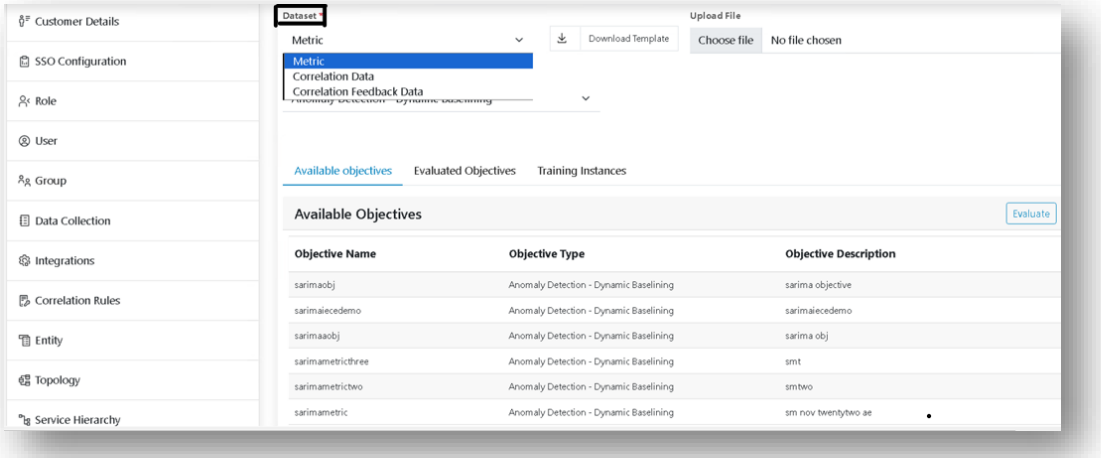

Figure 349 - Selecting Dataset type for Available Objectives

2. In Al Algorithms, Available Objectives contains all the objectives that are in the Objective AIML tool kit of the IEM.

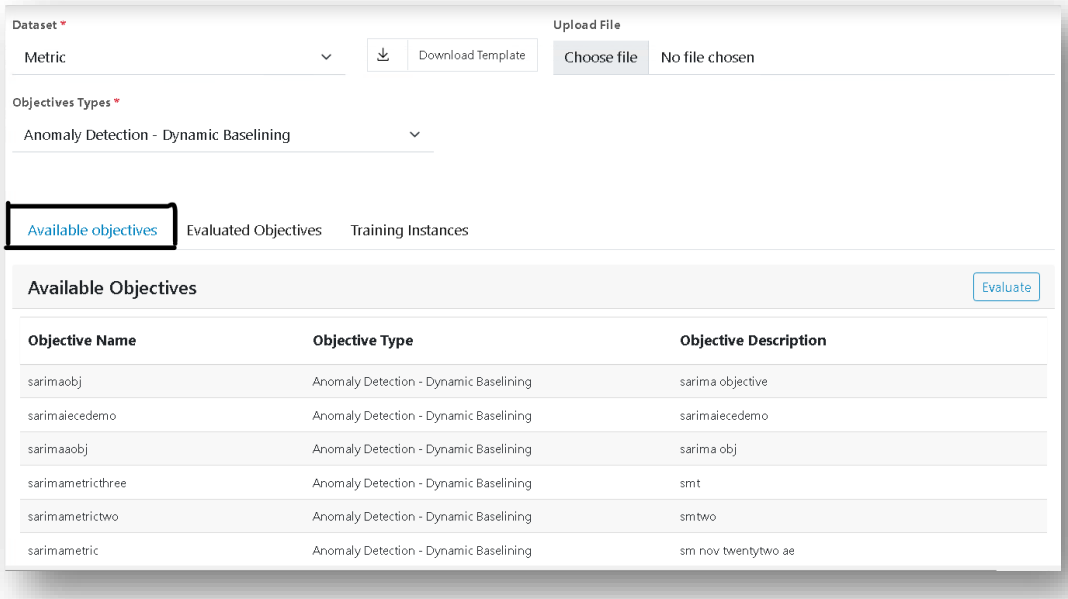

Figure 350 - Algorithms available objectives

3. If any objective is already populated, it will start appearing in the grid below.

Evaluate Action in AI ALGORITHM (Upload CSV File).

1. Select the dataset from the Dataset dropdown.
2. Click on **Download Template** (This will download the template specific to the selected dataset to upload its sample data)

Prior to running Evaluate, user must upload the sample dataset.

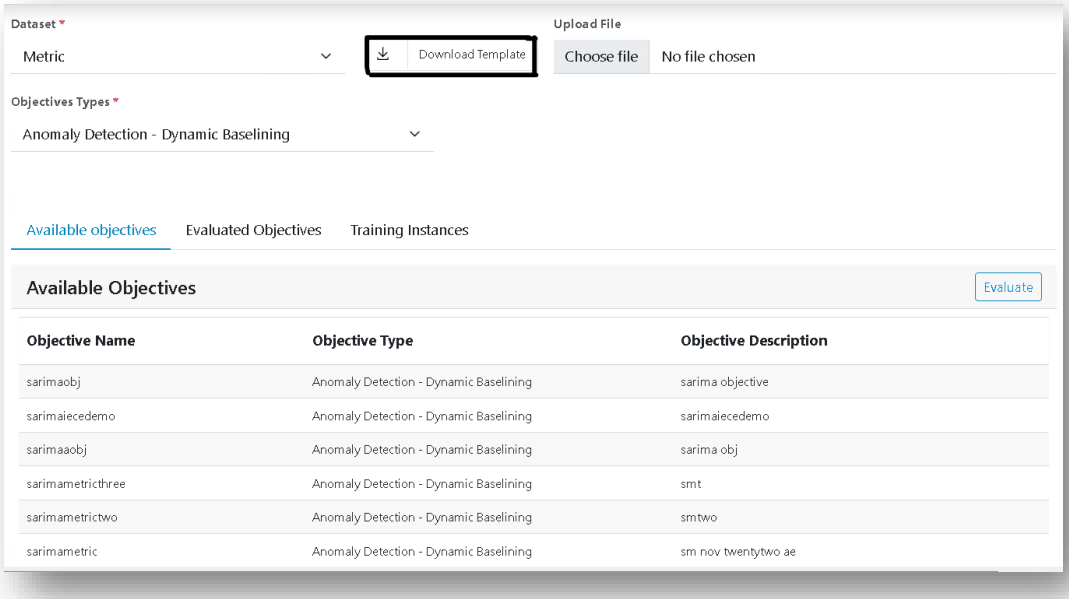

Figure 351 - Bulk Upload AI Algorithm Objectives

3. Click on the **Download Template** button. The following template is downloaded.

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	subentityname	agentlocation	entityid	datasum	entity	datacount	iperfid	subentitytype	datasourceid	datasourcename	entitytype	tooluniqueid	toolcustomername
2													

Figure 352 - Template for Bulk AI Algorithm Objectives

4. “Source entity id” is the mandatory column, rest are the additional\Optional details available in the environment.
5. user can choose to provide values of the additional details or can add more details in the columns as per the requirements.
6. The new additional details will be added in the repository post the data is uploaded.
7. Upload the filled excel file by clicking on **Upload CSV**.

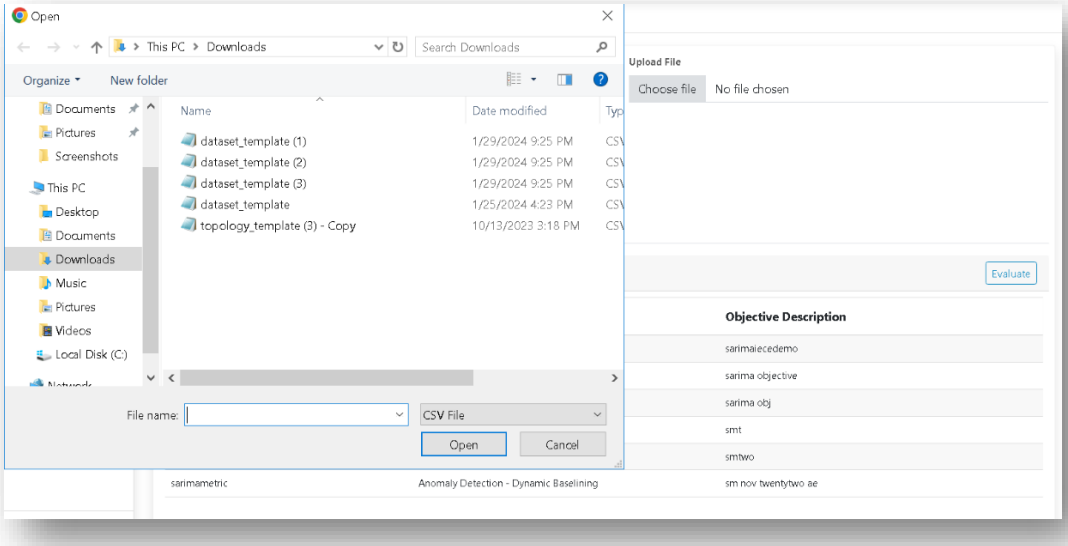

Figure 353 - Upload csv from Local Directory

8. Browse to the local directory where the data file is saved and select the file.
9. Once the file is selected it appears as shown in the below images.

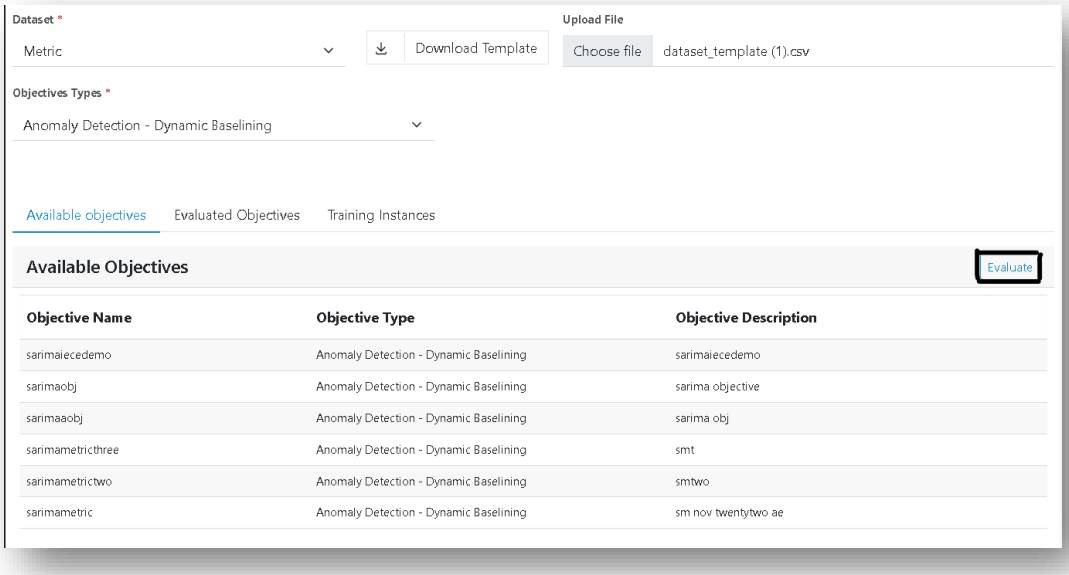

Figure 354 - Evaluate

10. Click **Evaluate**. Evaluation pop-up will be displayed as shown below.

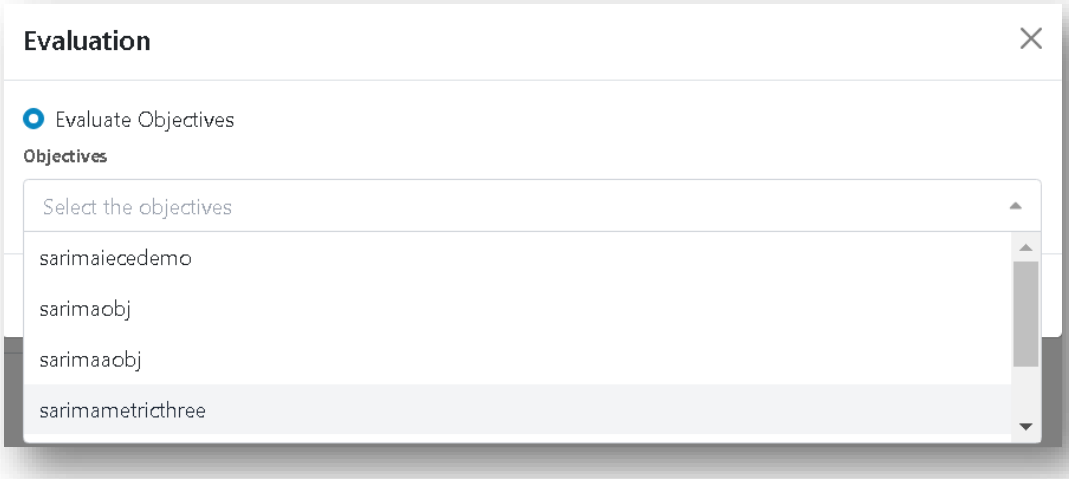

Figure 355 - Evaluate All

- **Evaluate Objectives**: Evaluate Objectives Option explains about the Objectives which users can select from the options in the dropdown as shown in below:

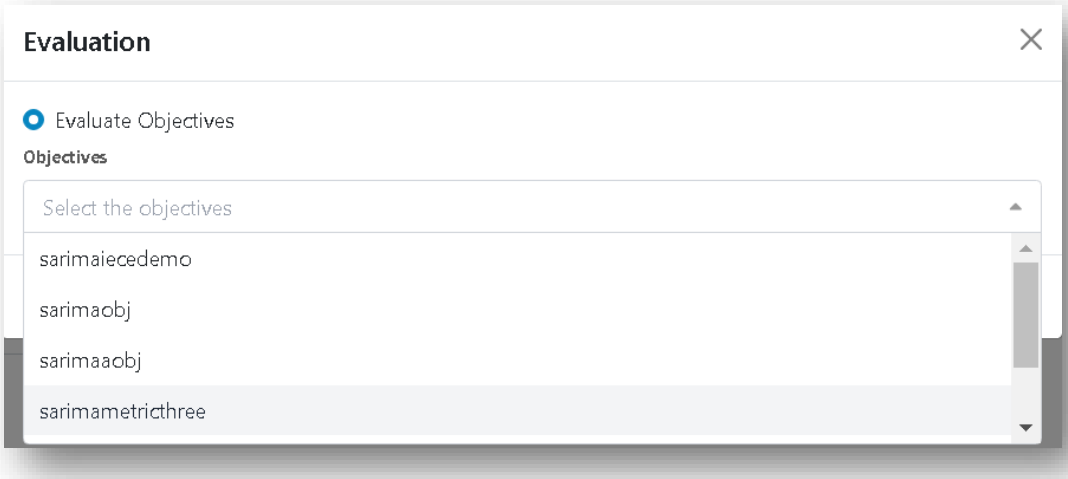

Figure 356 - Evaluate Objectives Dropdown

a. Select an **Objective** and click on **Submit** button.

b. Once done, the following confirmation box is displayed.

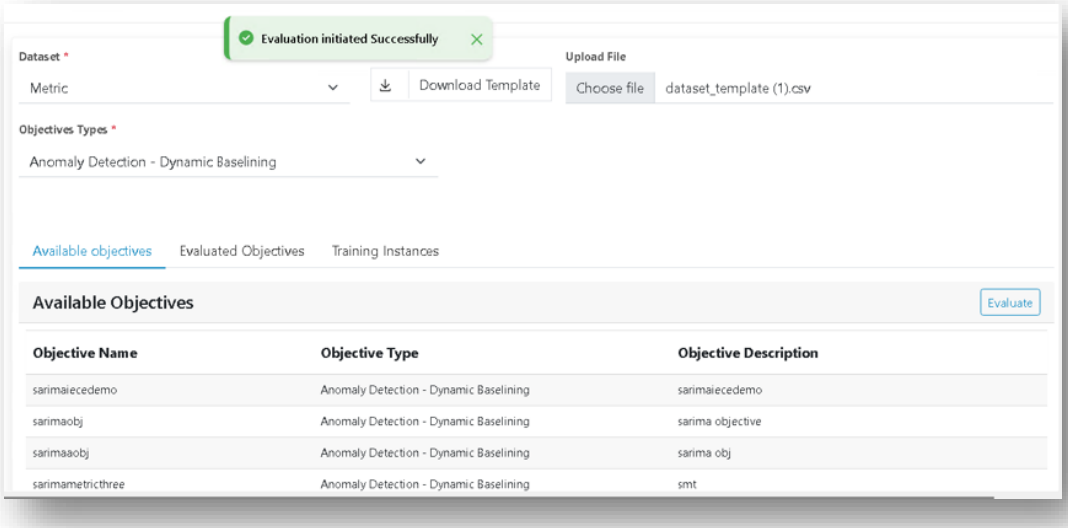

Figure 357 - Alert Message

After submitting the Evaluate Objective, all the Evaluated Objective job type will run in processing screen as shown below.

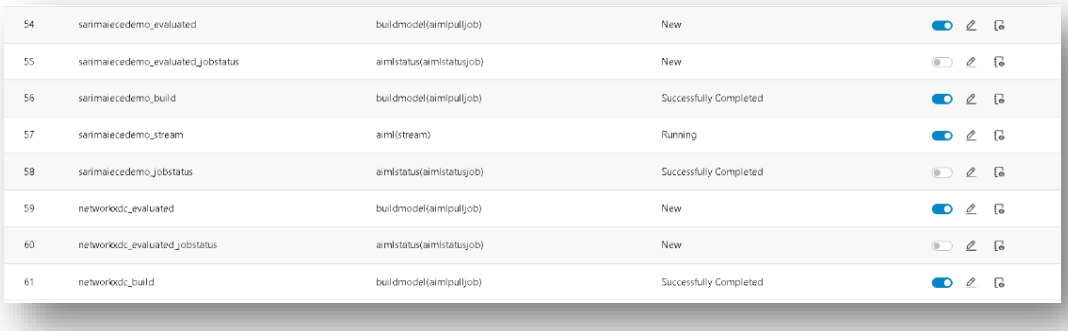

Figure 358 - Evaluate Objective job on Processing Screen

1. Select the dataset from the Dataset dropdown.
    - Metrics
    - Correlation Data
    - Correlation Feedback Data

15 days Metrics data will be considered as a baseline for model training.

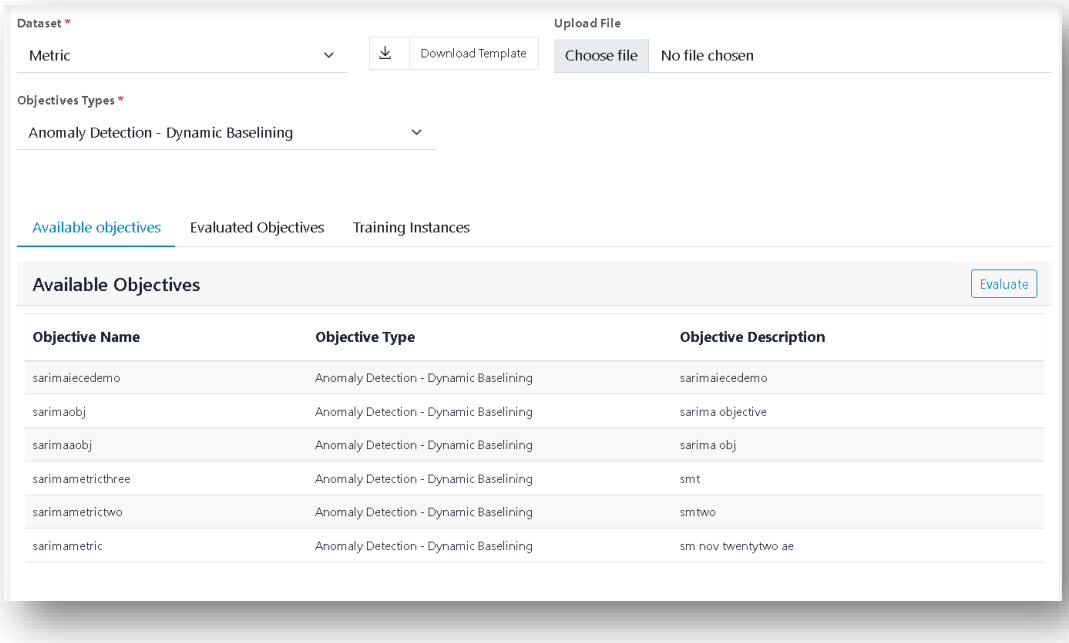

Figure 359 - Select Dataset Type for Evaluated Objectives

2. If any objective is already populated, it will start appearing in the grid below.
3. Click on the **Evaluated Objectives** of datasets, then evaluated objectives grid will be shown below.

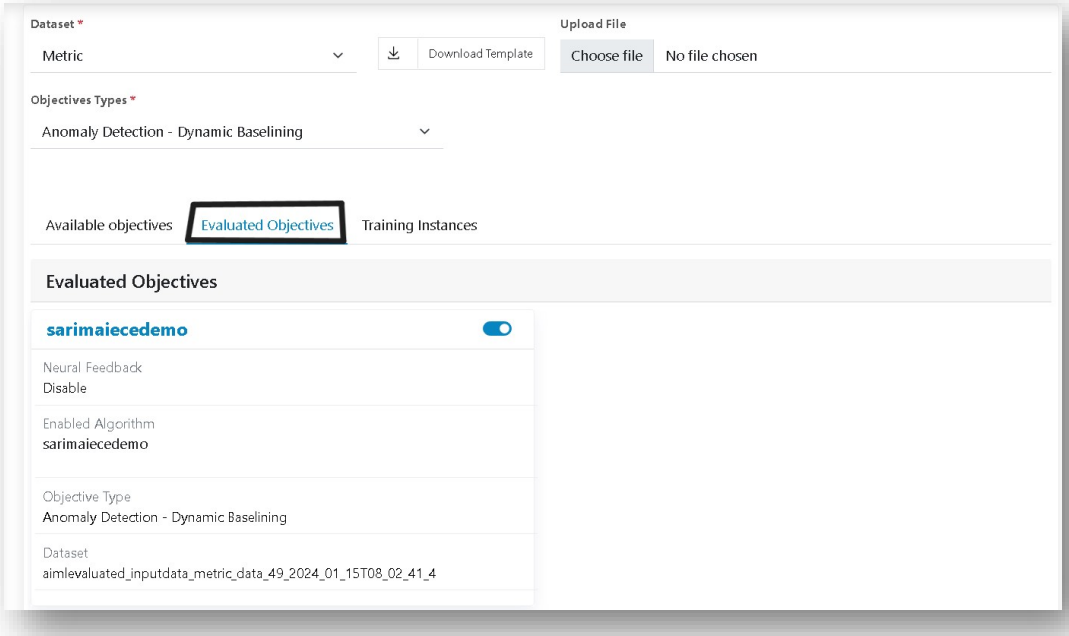

Figure 360 - Evaluated Objectives

Enable/Disable Objective

1. Click on the **Enable/Disable** icon corresponding to the **Evaluated Objective** which is to be Enabled/Disabled.

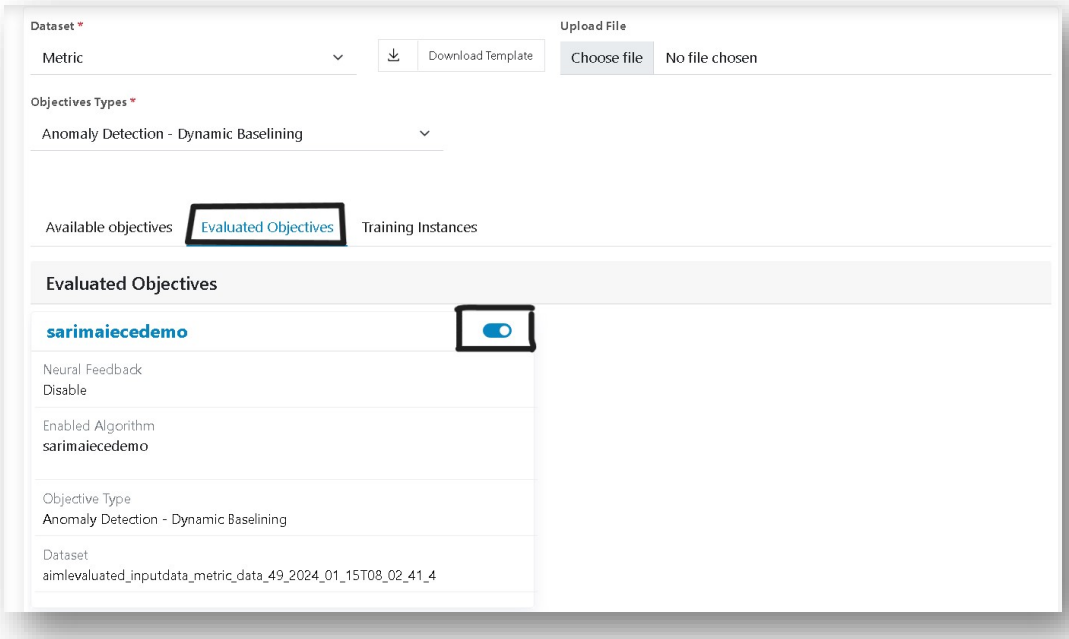

Figure 361 - Enable / Disable Evaluated Objectives

2. On success, a confirmation pop-up message will be displayed.

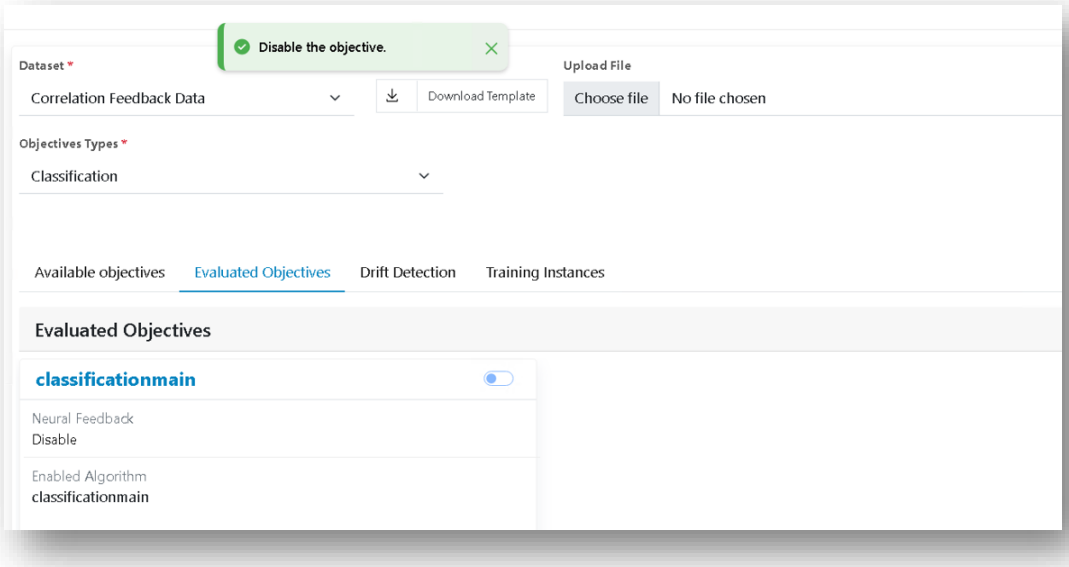

Figure 362 - Alert Message

Enable Feedback

1. When user clicks on Enable feedback button in Evaluated Objectives, Dropdown will be visible for selecting the options.

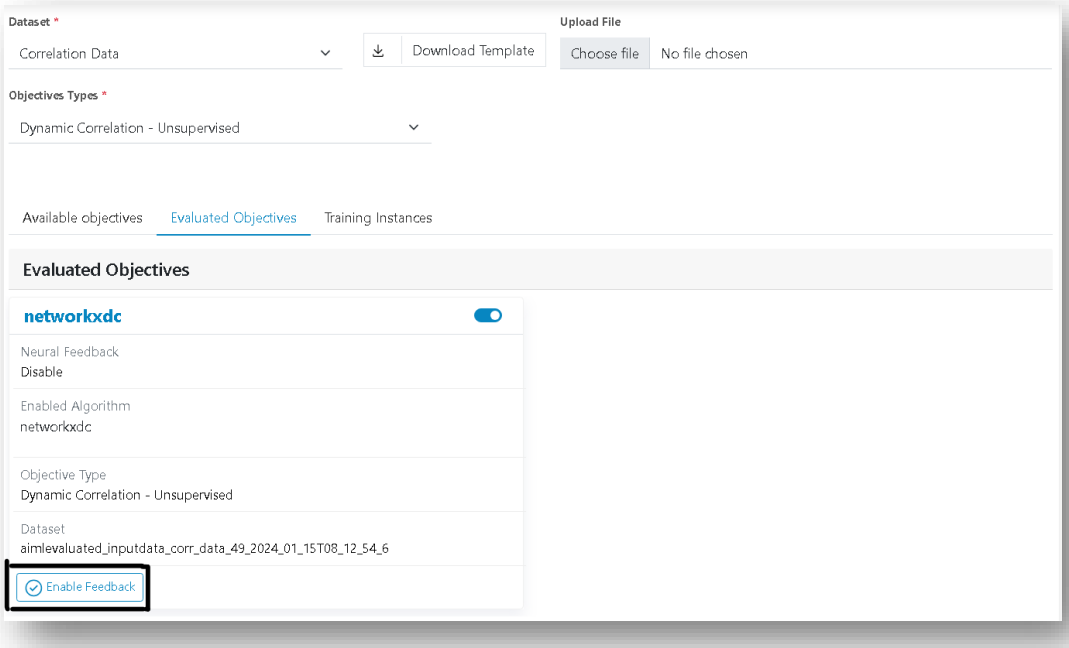

Figure 363 - Enable Feedback in Evaluated Objectives

2. Enable feedback drop down will be displayed. Select the feedback according to the objective as shown below.

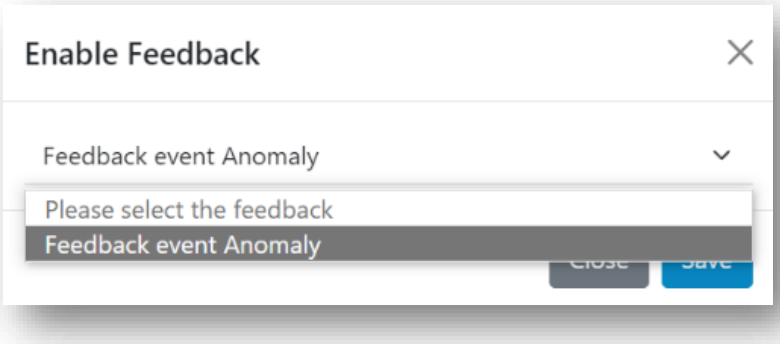

Figure 364 - Enable Feedback Dropdown

3. After selecting the option for enabling feedback from the dropdown, Click on **Save**.

View More Action

1. In **Evaluated Objectives** tab, click on **View More** action button.

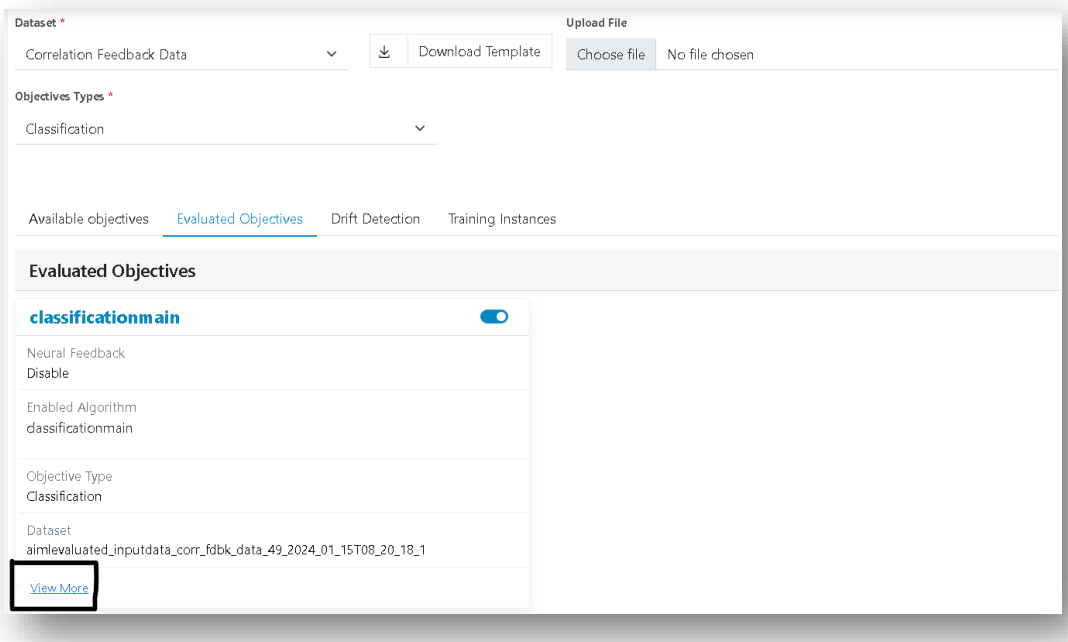

Figure 365 - View More action for Evaluated Objectives

2. The following screen appears:

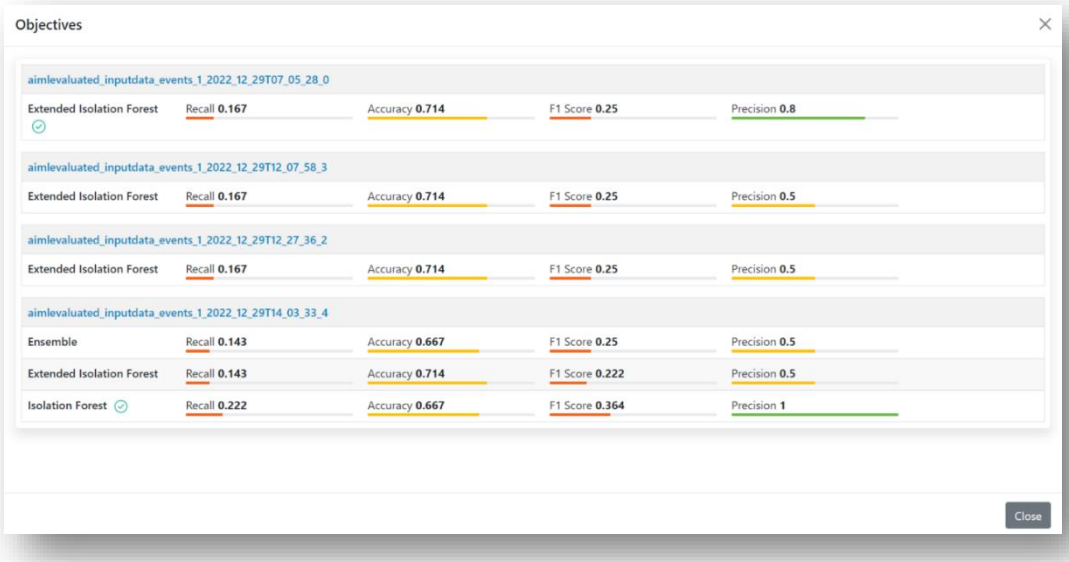

Figure 366 - View More

3. Click on the **Close** button, it will navigate to evaluated Objectives.

Training Instances

1. Select the dataset from the Dataset dropdown.
   - Metrics
   - Correlation Data
   - Correlation Feedback Data

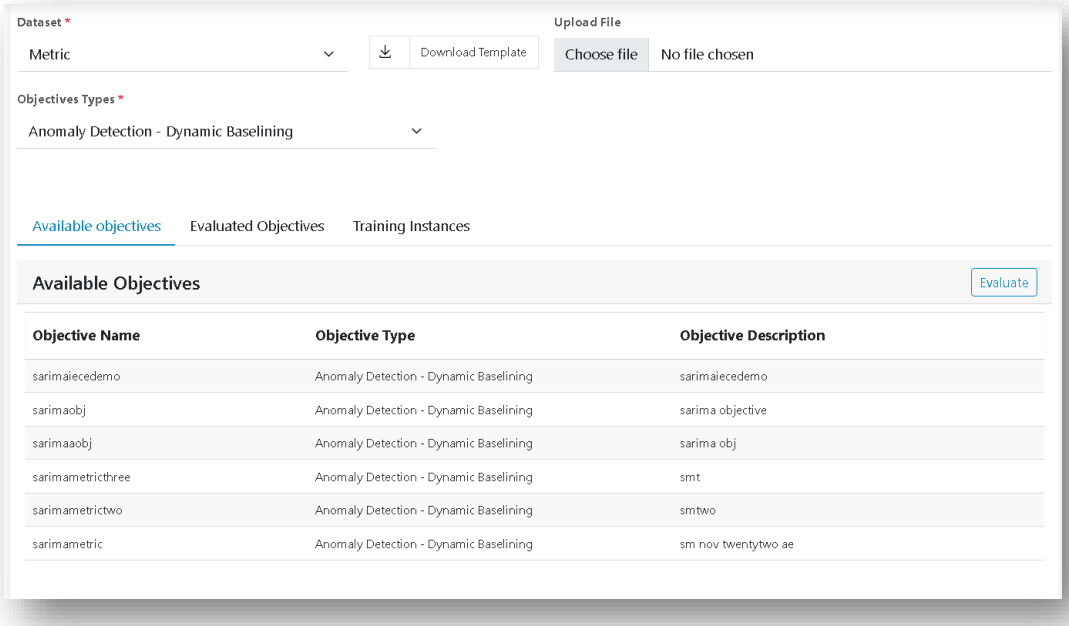

Figure 367 - Select Dataset Type for Training Instances

2. If any objective is already populated, it will start appearing in the grid below.
3. Click on the Evaluated Objectives of datasets, then the training instances grid will be shown below.

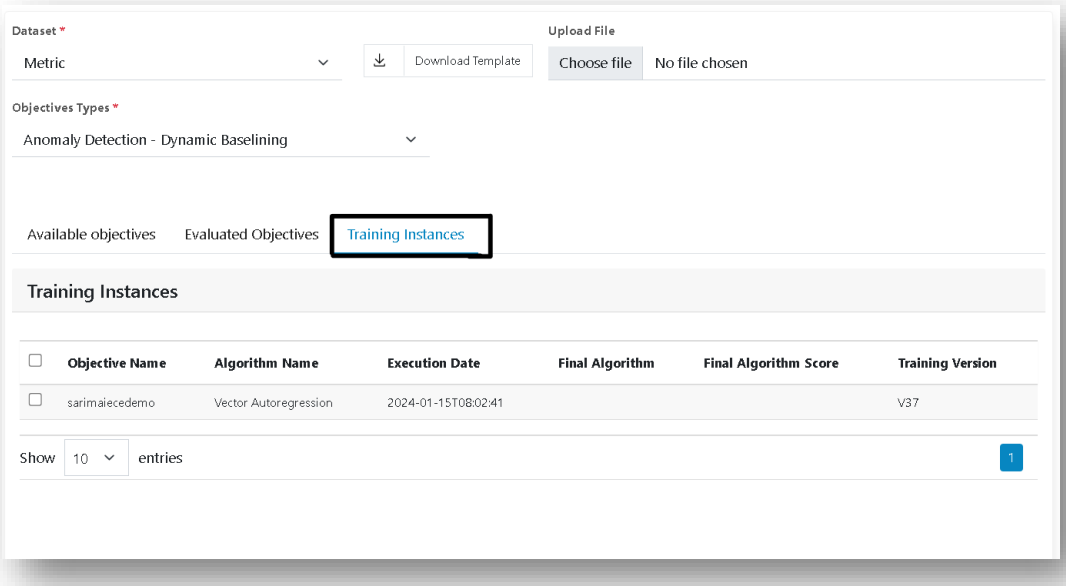

Figure 368 - Training Instances

Refresh Objectives

1. Click on Refresh Objectives icon.

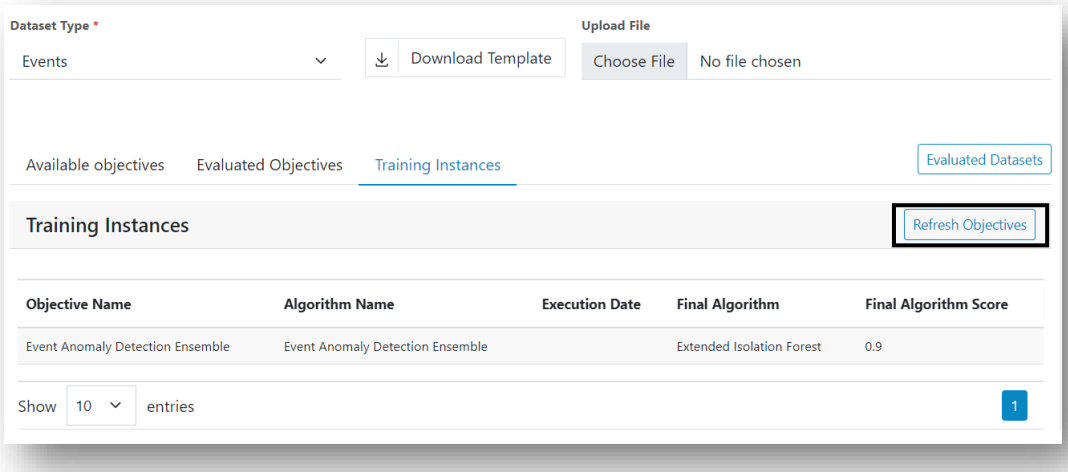

Figure 369 - Refresh Objectives

2. On success, the following pop-up message will be prompted.

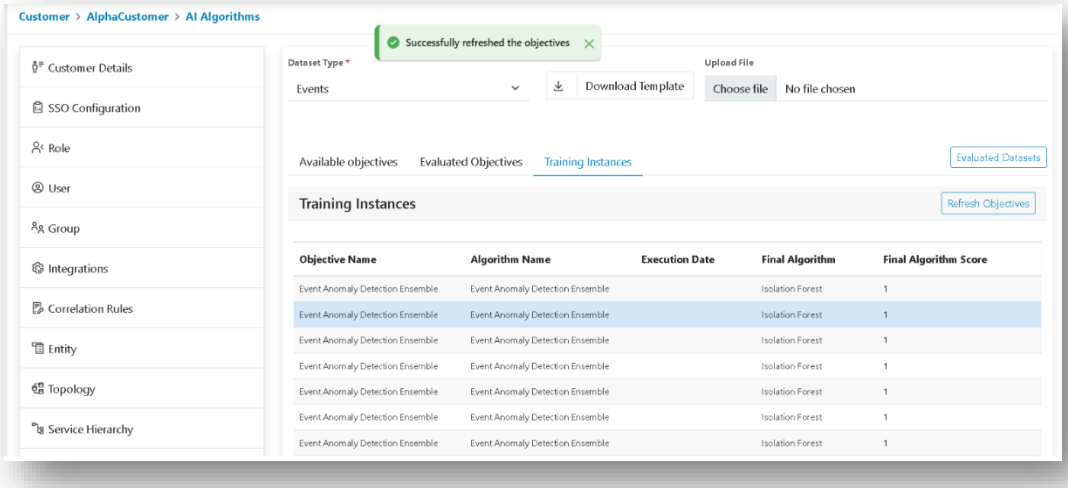

Figure 370 - Alert Message

3. This action populates on the grid with the objectives created in the AIML toolkit for the selected dataset.

6.1.11.13 Cost Configuration

Cost Configuration Feature" for actionable in IEM refers to the ability to assign and track costs associated with managing and resolving actionable within the IT environment. This feature is valuable for organizations as it allows them to measure and analyze the financial impact of actionable, helping in cost allocation, budgeting, and overall financial management. This action enables us to configure the average cost of actionable.

1. The side Navigation bar contains **Cost Configuration** option, click on the option and the screen will get opened.
2. Add the currency from the dropdown and add the average cost of actionable.

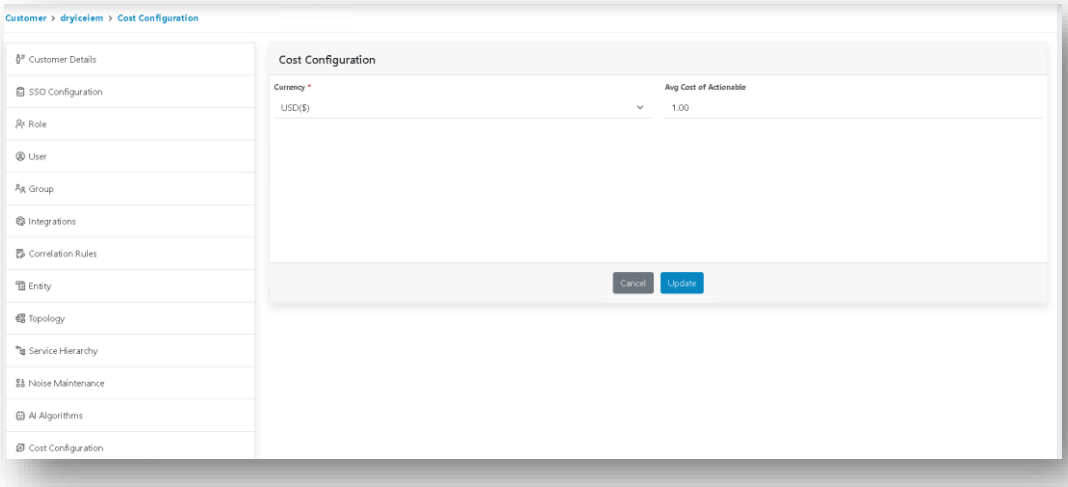

Figure 371 - Cost Configuration

3. The average cost of actionable saved in the configuration will help in generation of average savings in the currency selected in configuration.

7 IEM Interface

The interface presents a unified views like Metric View, Topology View and Service View to facilitate Event Management helping IT Professionals understand the relationships between different entities and services to make informed decisions to manage and troubleshoot complex IT environments more efficiently.

7.1 Login to HCL IEM

To login to the system, perform the following steps:

1. Launch a user browser and provide HCL IEM User Portal URL. The HCLIEM Login Page appears.

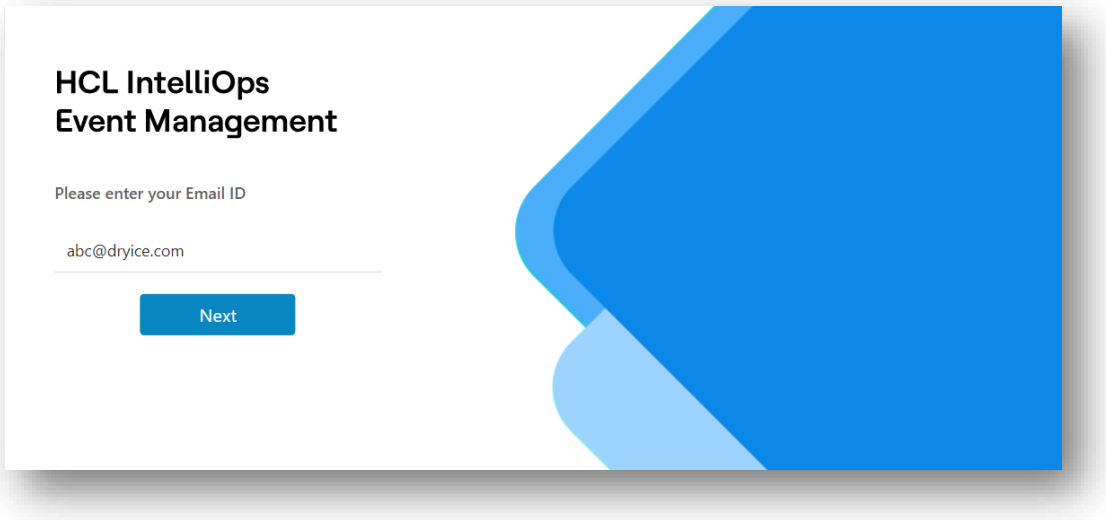

Figure 372 - HCLIEM Login Page

2. On the HCL IEM Login Page, type the **Login ID**. The user is redirected to the **Password** page.

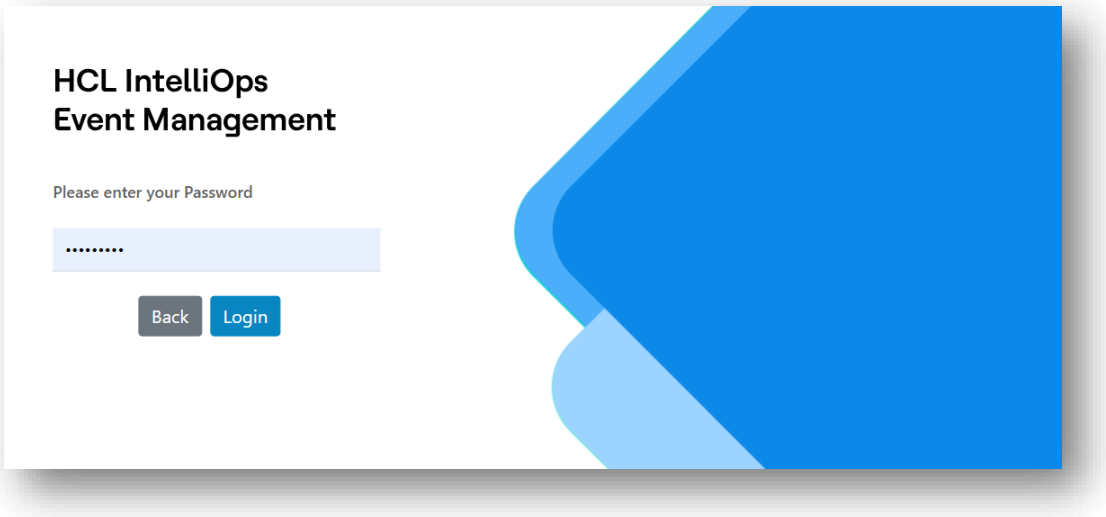

Figure 373 – Login Authentication

3. Enter the **Password** and click on **Login**.
4. The HCL IEM home page dashboard appears. This Home page is the landing page of IEM.

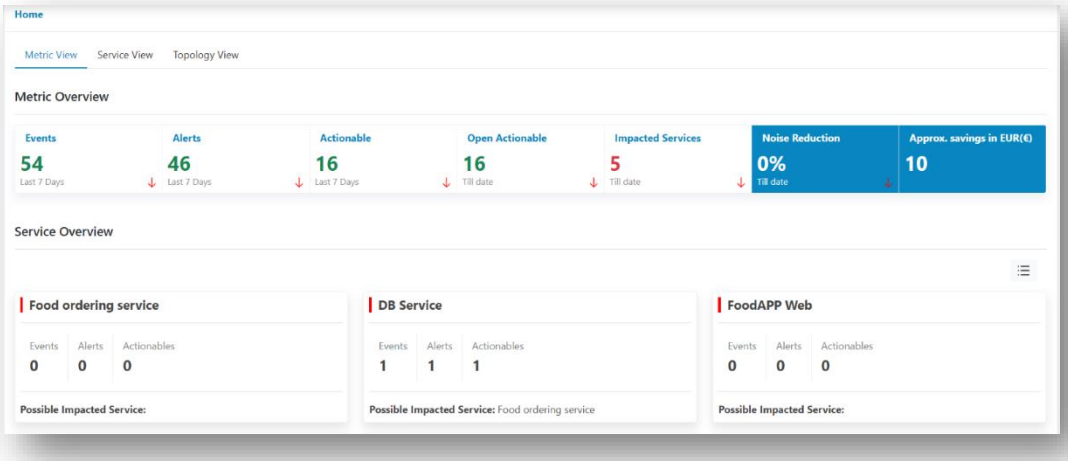

Figure 374 - FIGURE – Home Page Dashboard

Home Screen shows three different views to user.

- Metric View
- Service View
- Topology View

Metric Overview and Service Overview card club to form a dashboard to show the numbers that user can view to create an overall perspective of the system configured.

7.1.1 Metric View

A metrics dashboard is one kind of the data dashboard, it is a tool that collects, integrates, and displays key performance indicators in a single place to analyze and project quality status of the KPIs in real-time.

Metric Overview shows the metric analysis of Events, Alerts, Actionable for a customer. It gives a view of open actionable and impacted services. In addition, Noise Reduction % calculated shown in the metric view.

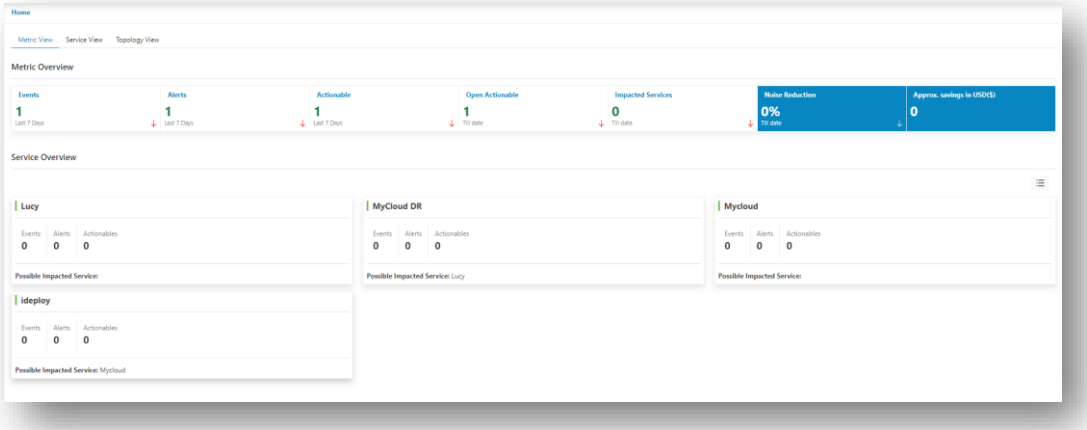

Figure 375 – Metric View

7.1.2 Service View

Service dashboards visualize the Service relationship data in a way that can be understood easily. Service View shows the service tree for a customer. Parent and Child nodes are depicted in the Services chart for a customer configured. The color coding shows the Service Impact.

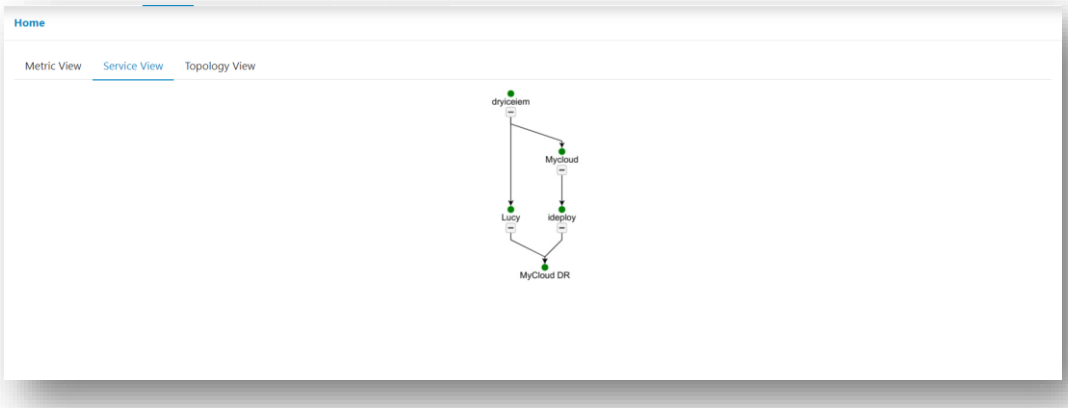

Figure 376 – Service View

7.1.3 Topology View

Topology view involves creating a visual representation of the dependencies between various IT components, showcasing which components rely on others for proper functioning. This mapping helps in assessing the potential impact of a failure or performance issue in one component on others within the system.

Topology view dashboard provides a visual representation of the relationships and dependencies between different servers, applications, and other infrastructure components. It allows for quick identification of bottlenecks, potential issues, or areas of concern, facilitating efficient troubleshooting and proactive management of IT events.

Topology views can be dynamic, providing real-time updates on the status and health of components and their connections.

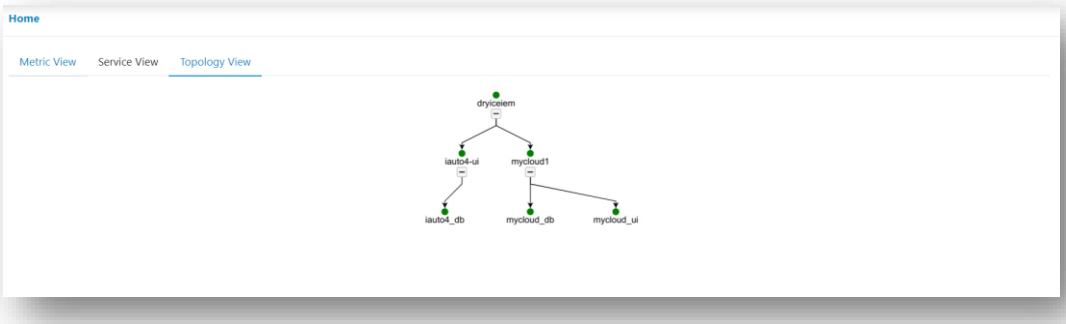

Figure 377 - Topology View

7.2 Data View

Based on the configurations, three data types are displayed over Data View Console:

- All Events
- Noise Events
- Events
- Alerts
- Actionable

7.2.1 Events

An "event" refers to a significant occurrence or incident within an IT environment that is detected, monitored, and logged by various systems and tools. Events are typically generated by hardware, software, applications, or network devices, and they serve as a key source of information for monitoring and managing the performance and health of IT systems. Events can be diverse and may include activities such as system errors, warning messages, user interactions, configuration changes, or security-related incidents.

7.2.1.1 Events View

The steps explain how to view the events data.

1. In the top navigation bar, click on Data View and click on Events.
2. Events data will be displayed for the selected customer.

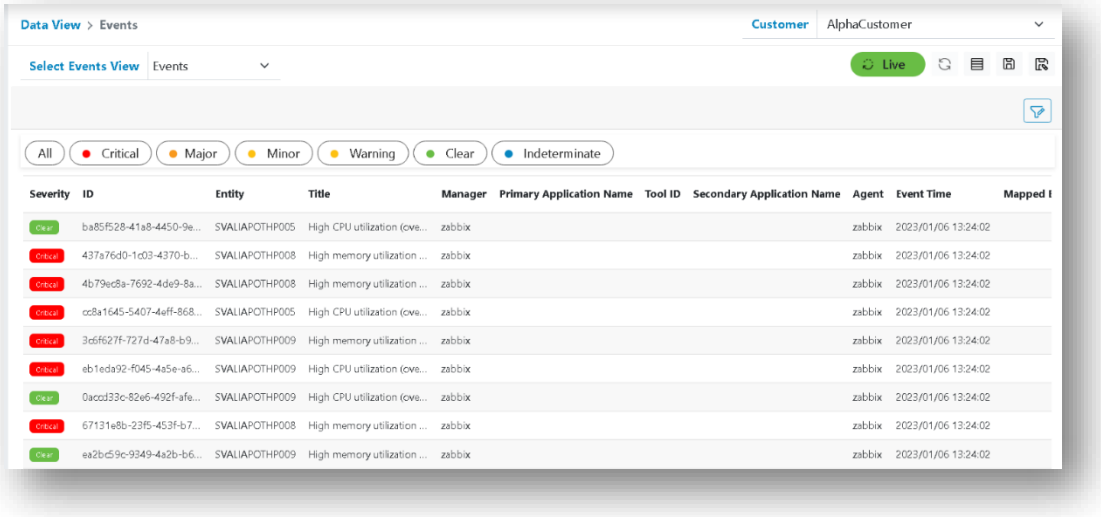

Figure 378 - View Events

7.2.1.2 Add Column

The steps explain how to add column to event data:

1. In the top navigation bar, click on Data View and click on Events.
2. Click on the Add Column action button present at the header of the console.

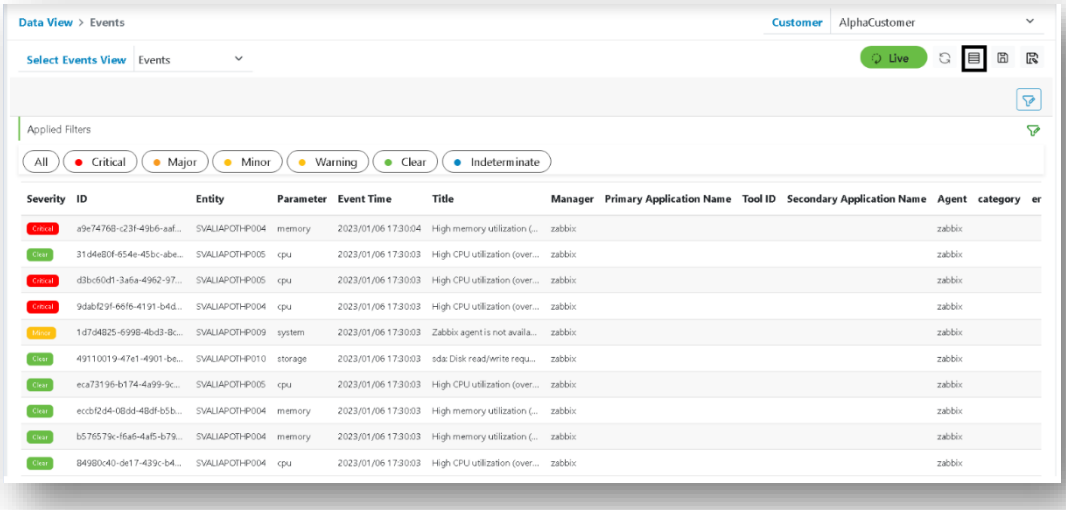

Figure 379 - Add Column

3. The form will appear from there user can select from drop down list. Then click on the save button.
4. The form will appear from there user can select from drop down list. Then click on the save button.

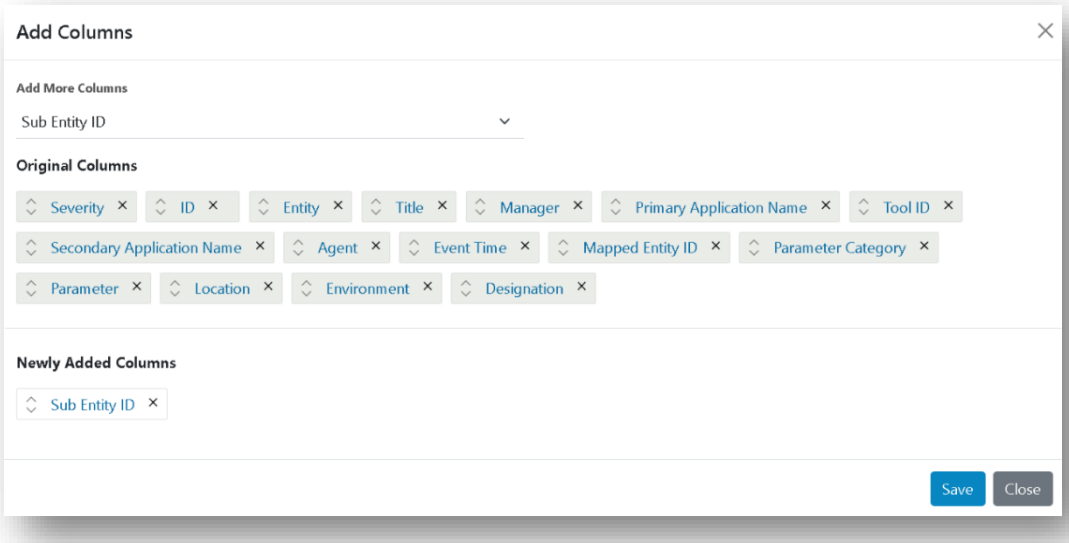

Figure 380 - Add Column

7.2.1.3 Save View

The steps explain how to save the events data:

1. In the top navigation bar, click on Data View and click on Events.
2. User can click the save button.

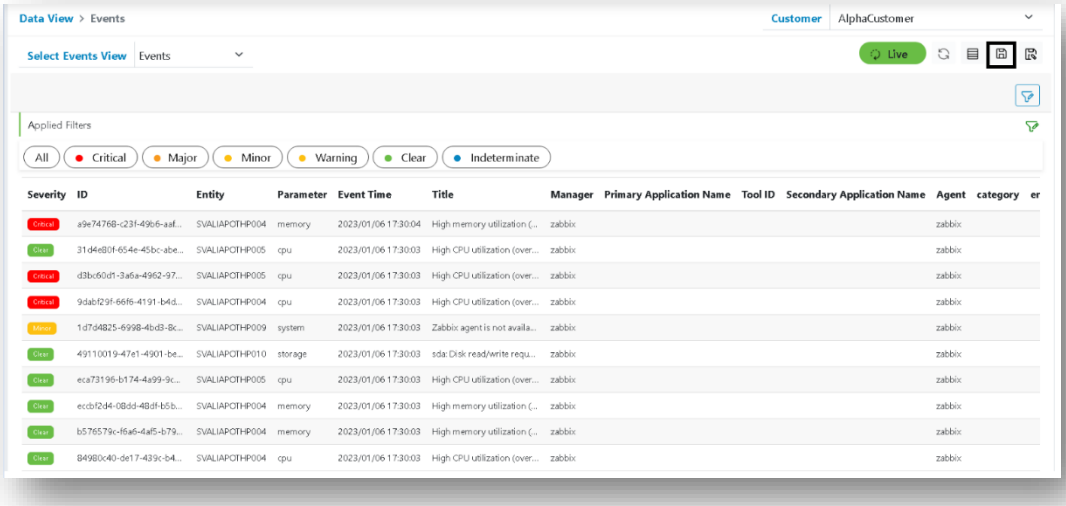

Figure 381 - Save View

3. A confirmation pop-up message will appear.

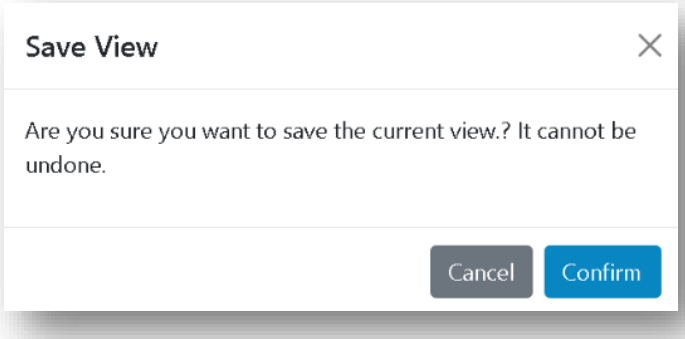

Figure 382 - Save View Events

4. Click on **Confirm** button, a success pop will appear and the grid changes.

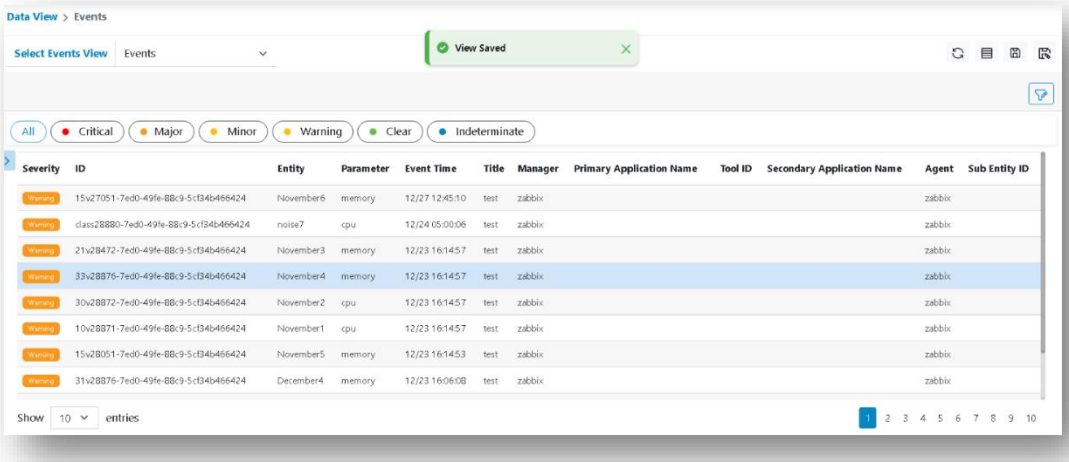

Figure 383 - Popup confirmation

7.2.1.4 Save As Events

The steps explain how to save the events data as view.

1. In the top navigation bar, click on Data View and click on Events.

2. User can click the save as events button.

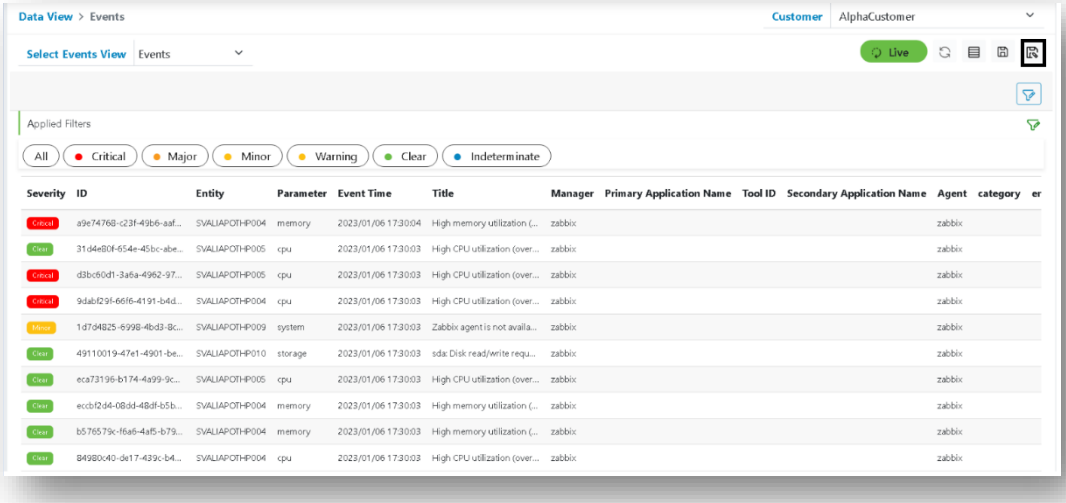

Figure 384 - Save As Events

3. A confirmation pop-up message will appear.

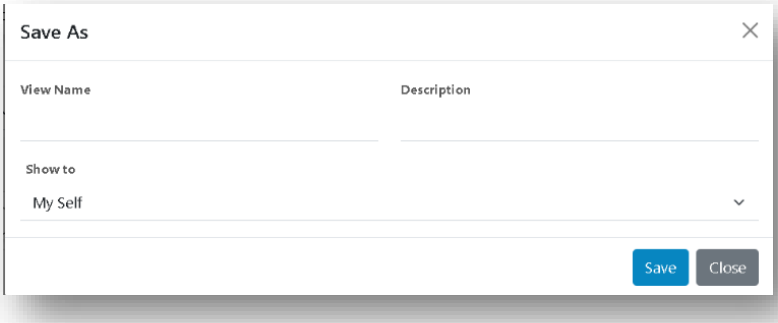

Figure 385 – Save as Events

4. As all fields are entered click on save button, success popup message will appear.

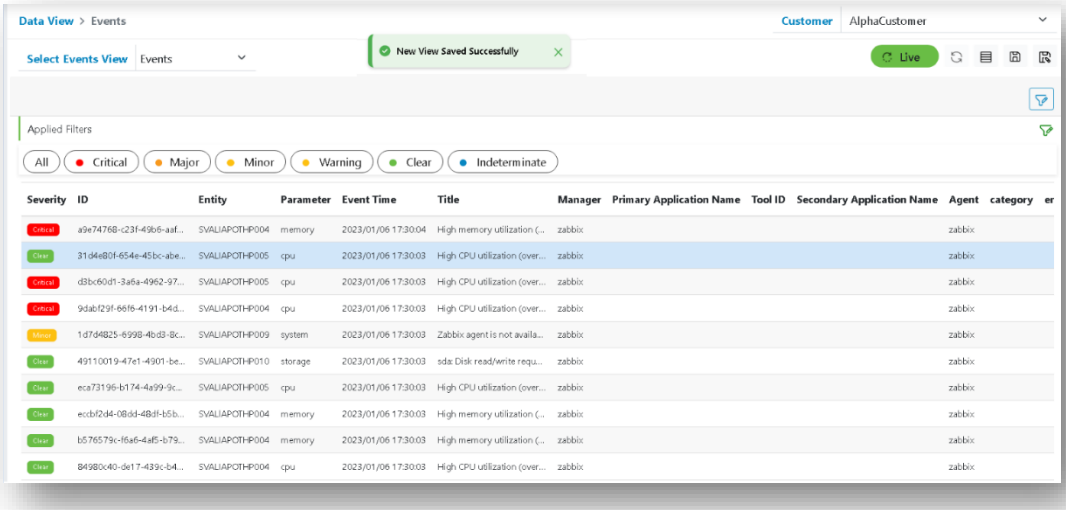

Figure 386 - Alert Message

5. Then user can select Events view from the dropdown list in which user can created before this step.

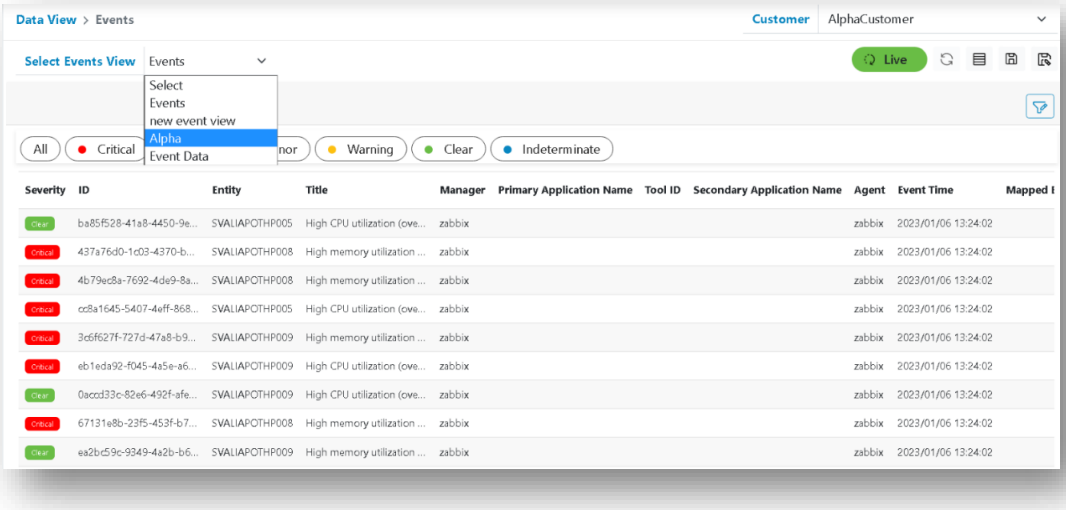

Figure 387 – Select Events View Dropdown

7.2.1.5 Live Events Data

The steps explain how to refresh the events data.

1. In the top navigation bar, click on **Data View** and click on **Events**.
2. User can see the Live Events Data updating every 4 seconds in Grid view.

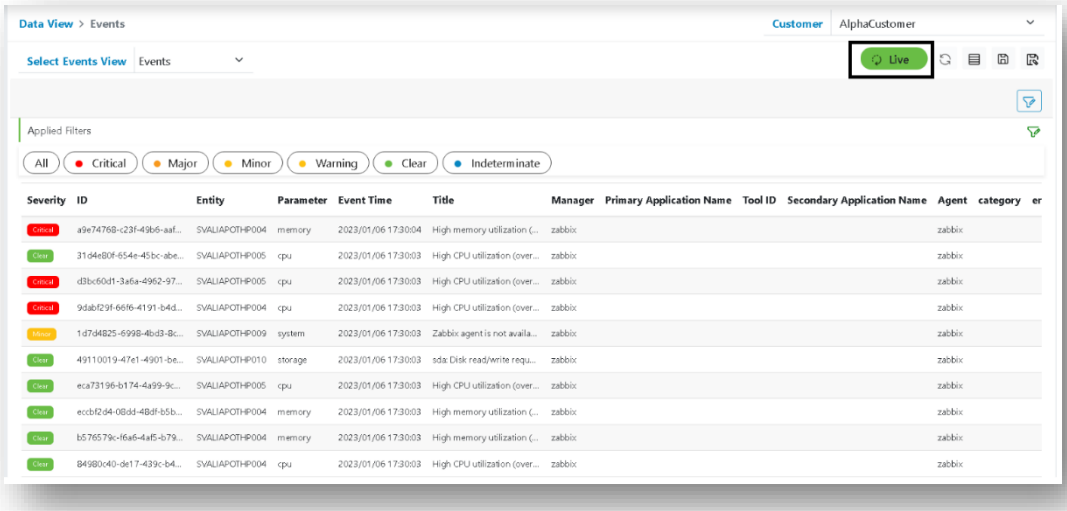

Figure 388 – Live Events Data

3. To stop the auto-refresh, click on the **Live Events Data** button, a confirmation pop up message will appear.

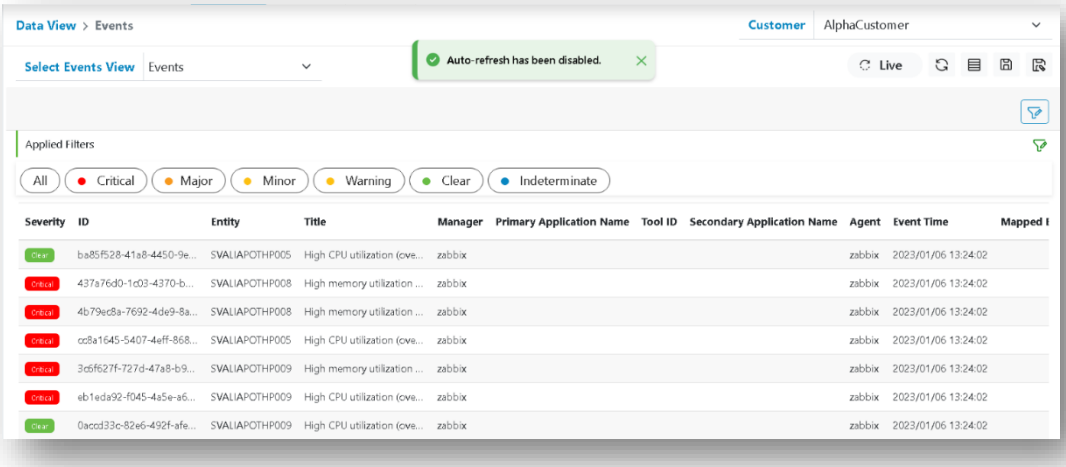

Figure 389 – Live Events Data Disabled

7.2.1.6 Refresh Events

The steps explain how to refresh the events data view.

1. In the top navigation bar, click on Data View and click on Events.
2. Click on Refresh Events button if Live Events Data is disabled only.

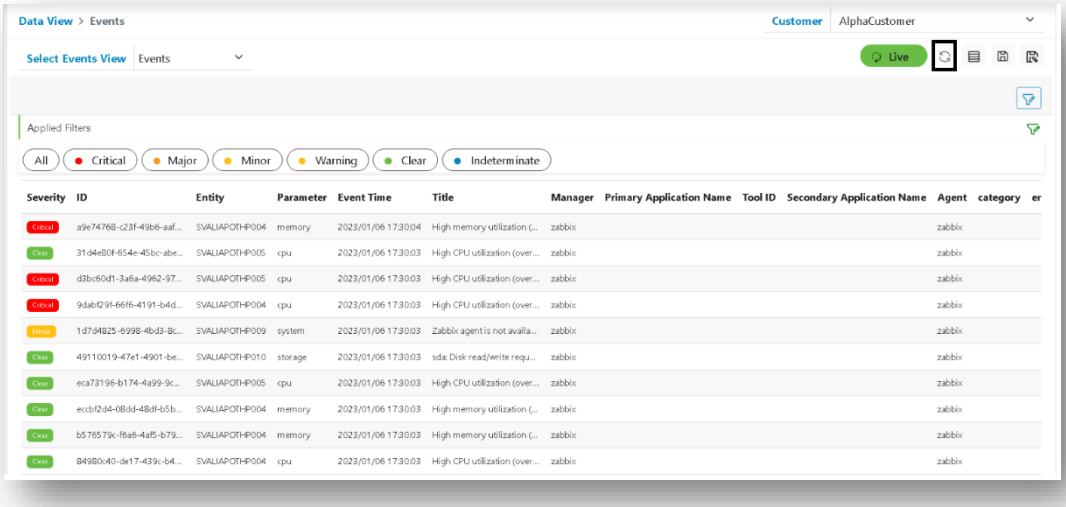

Figure 390 – Refresh View Data Events

3. A confirmation pop up message will appear.

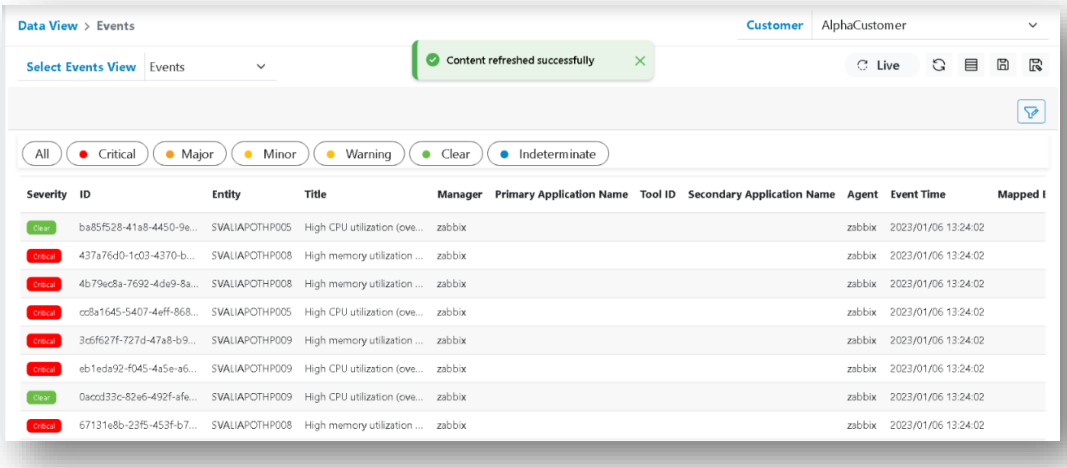

Figure 391 – Alert Message

7.2.1.7 Apply Filters

The section provides details on how to apply filters to the event data.

1. In the top navigation bar, click on **Data View** and click on **Events**.
2. Click on the **More Filter**  action button.

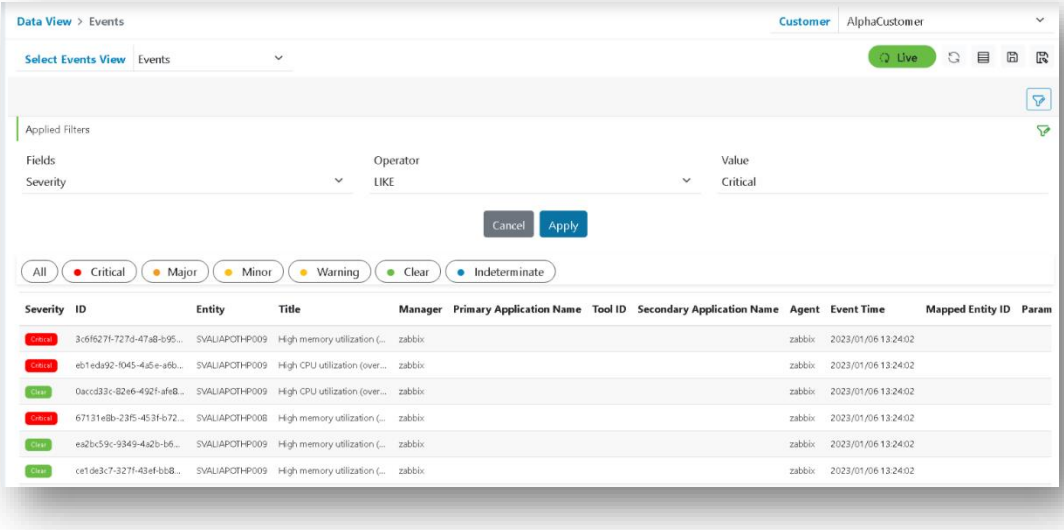

Figure 392 - More Filter Operation

3. A form will appear. Select **Field** and **Operator** from drop down list and write a value. Then click on the **Apply** button.

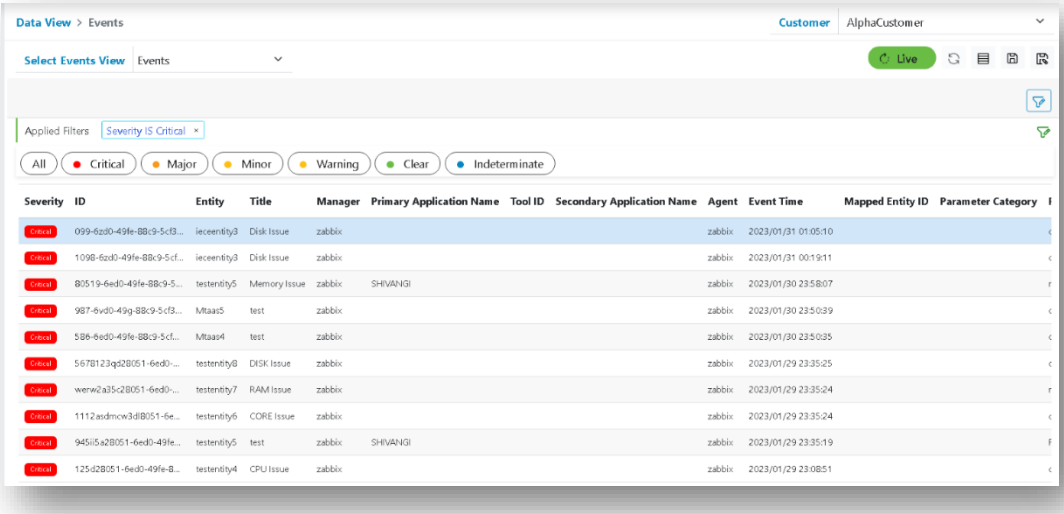

Figure 393- More Filter Operation

7.2.2 Alerts

"Alerts" refer to notifications or warnings generated by monitoring systems or tools when significant events or issues are deviating from normal system behavior. Alerts play a crucial role in proactively identifying potential problems, anomalies, or security incidents within the IT environment. Alerts are triggered by a monitoring system to indicate the occurrence of a specific event or condition that requires attention. Alerts are typically generated based on predefined rules, thresholds, or conditions associated with events. Multiple alerts may be correlated to identify patterns or relationships between different events, helping in understanding the broader impact.

Well-designed alerting view provides IT teams with crucial information, enabling them to respond proactively to potential issues and minimize the impact on operations.

7.2.2.1 Alerts View

The steps explain how to view the alerts data.

1. In the top navigation bar, click on Data View and click on Alerts.
2. Alerts data will be displayed for the selected customer.

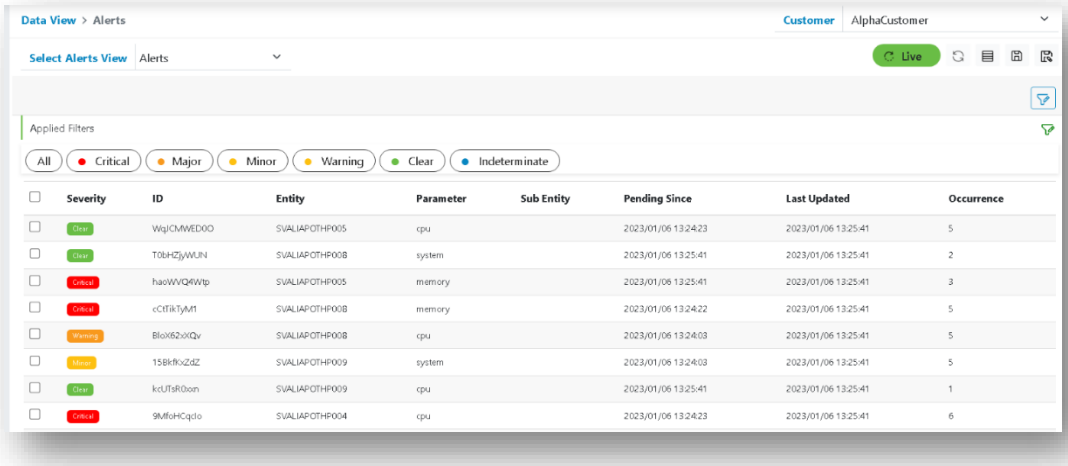

Figure 394– Alerts View

7.2.2.2 Delete Alerts

The steps explain how to delete the alerts data:

1. In the top navigation bar, click on Data View and click on Alerts.
2. Alerts can be selected by clicking on the checkbox. (Single select/Multi select)

The auto-refresh feature automatically updates data (including events, alerts, noise, actionable items, and all events) in the grid. Consequently, any previously checked items will be unchecked. If you intend to delete something, it is advisable to disable the auto-refresh feature first and then proceed with deletion operations.

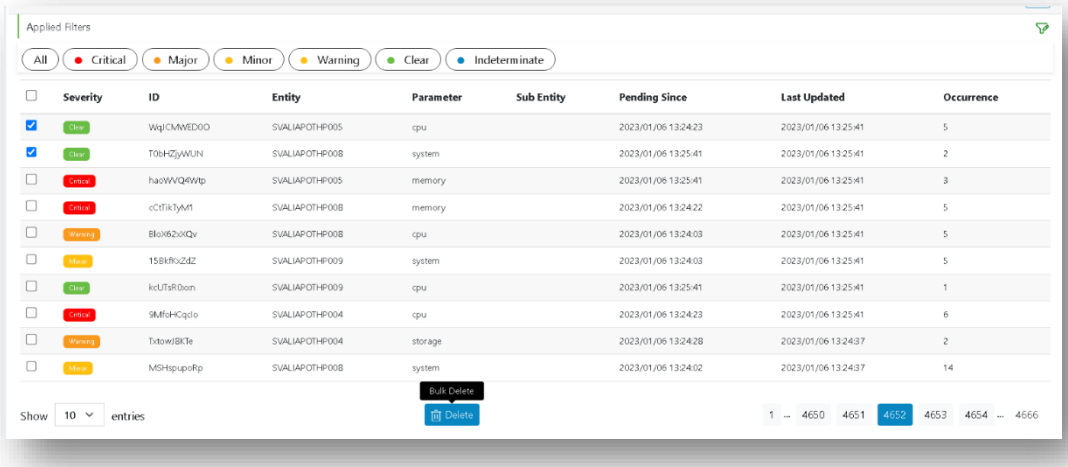

Figure 395– Deleting Bulk Alerts

3. Click on the **Delete** action button present at the bottom.
4. A confirmation dialog box appears to confirm the deletion.

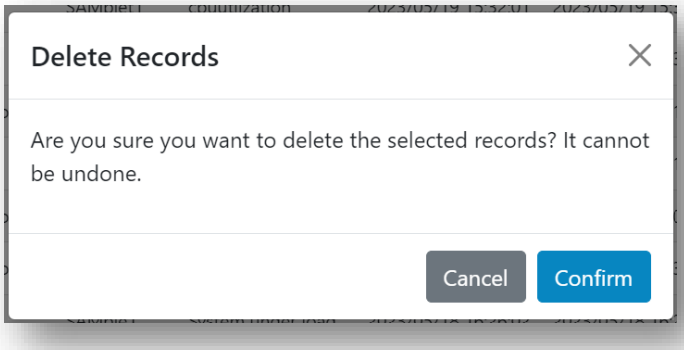

Figure 396- Confirmation pop-up

5. Click on **Confirm** button, a dialog box would appear for successful deletion of alerts.

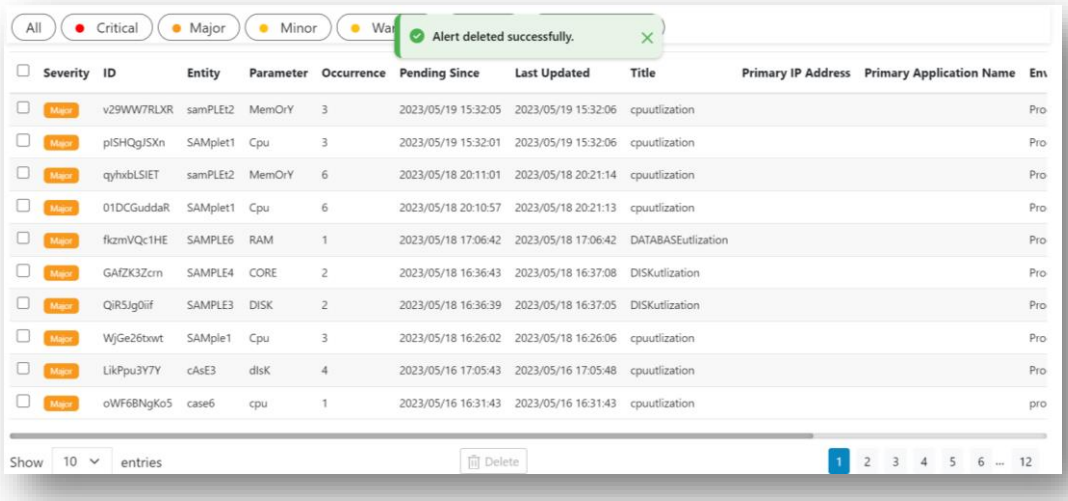

Figure 397– Alert Message

7.2.2.3 Save Alerts

The steps provide information on how to save alert data.

1. In the top navigation bar, click on Data View and click on Alerts.
2. User can click the save button.

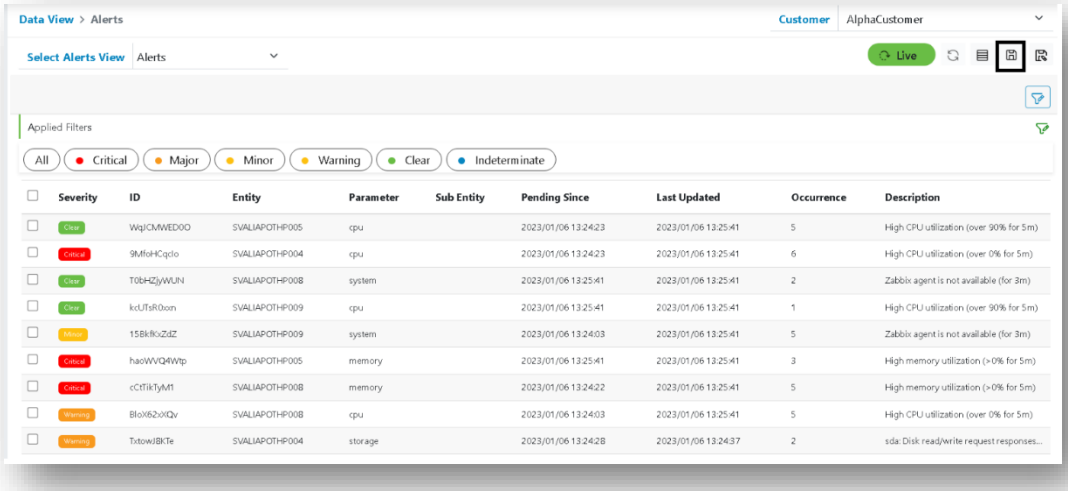

Figure 398- Save Alerts

3. After saving, the event data appears in the grid and a success popup appears.

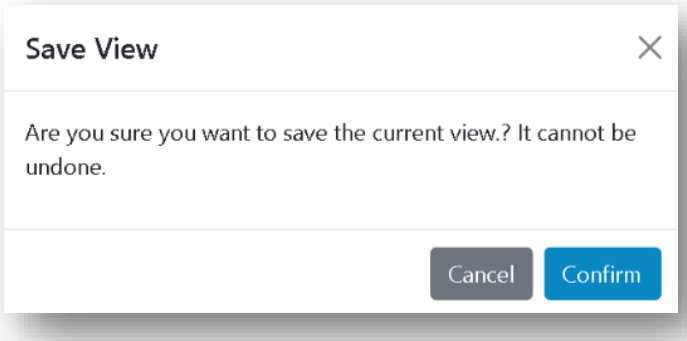

Figure 399- Save Alerts

4. On clicking the **Confirm** button, a success pop up will appear.

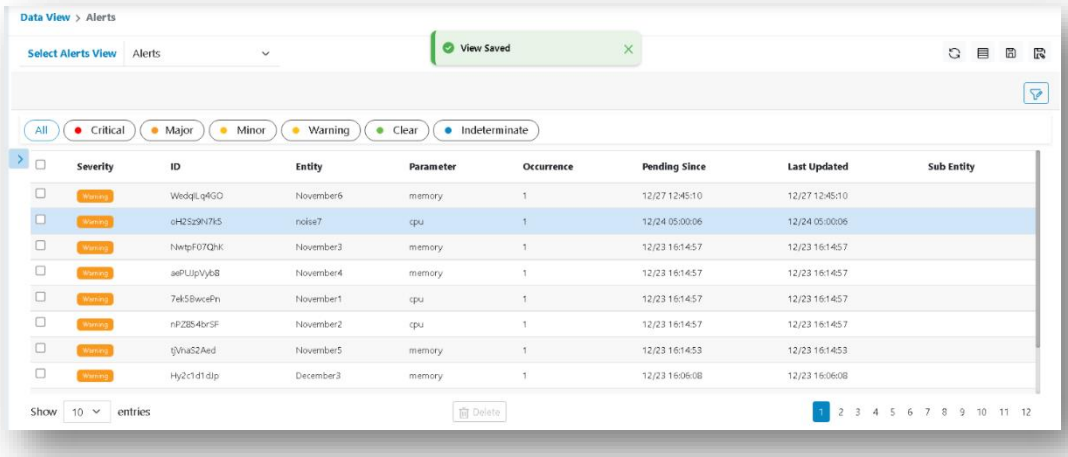

Figure 400- Alert Message

7.2.2.4 Save As Alerts

The section explains the steps to Save a personalized view of Alert data as per the requirement:

1. In the top navigation bar, click on **Data View** and click on **Events**.

2. Click **Save as Alerts** button.

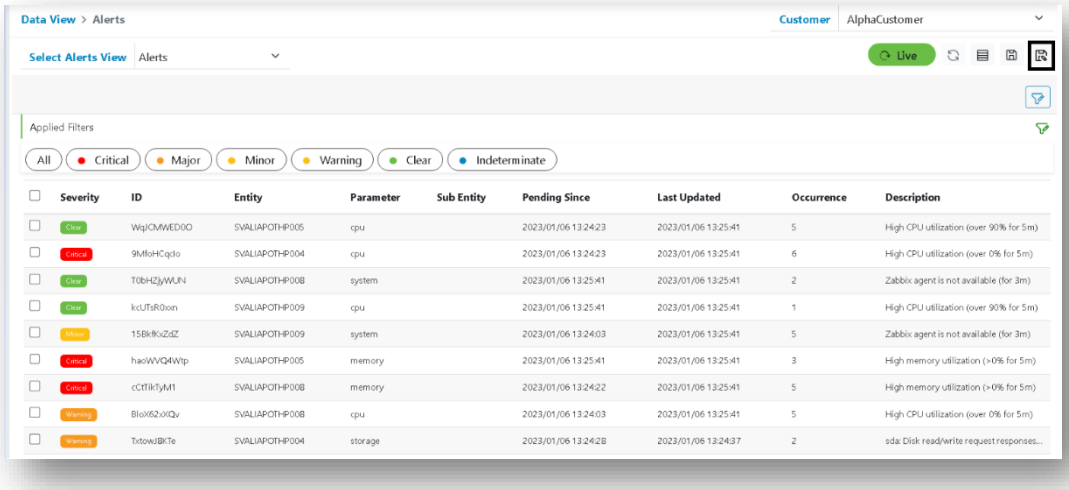

Figure 401– Save As Alerts

3. The following form appears:

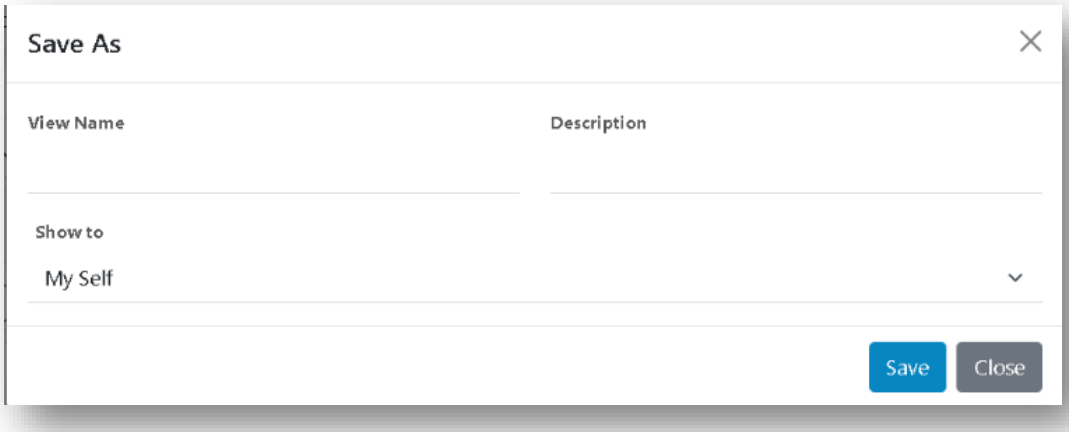

Figure 402– Save As Alerts

4. Once all the fields are entered, click on **Save** button.

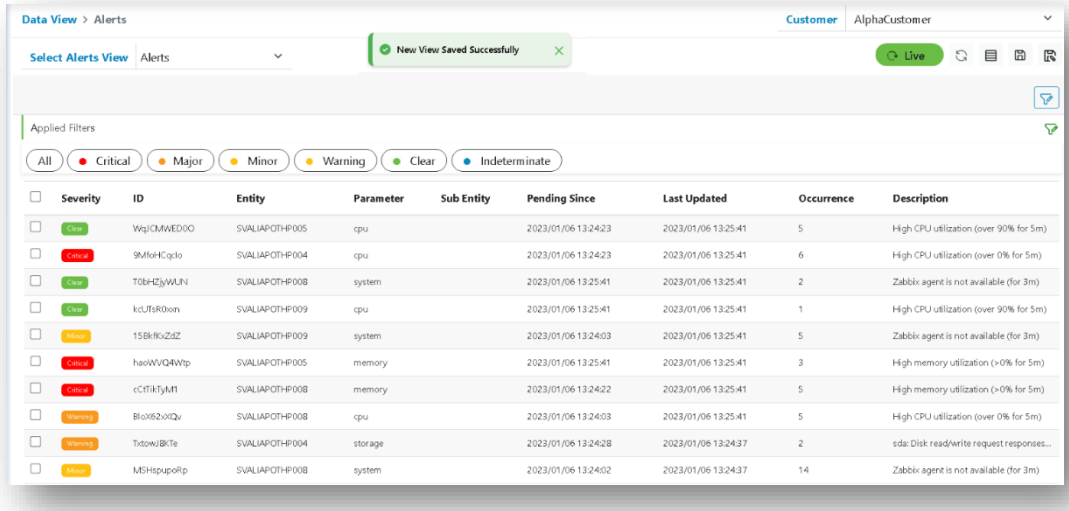

Figure 403– Alert Message

5. The newly created view is now available in the list of available views. The user can select Events view from the dropdown that lists all the existing views.

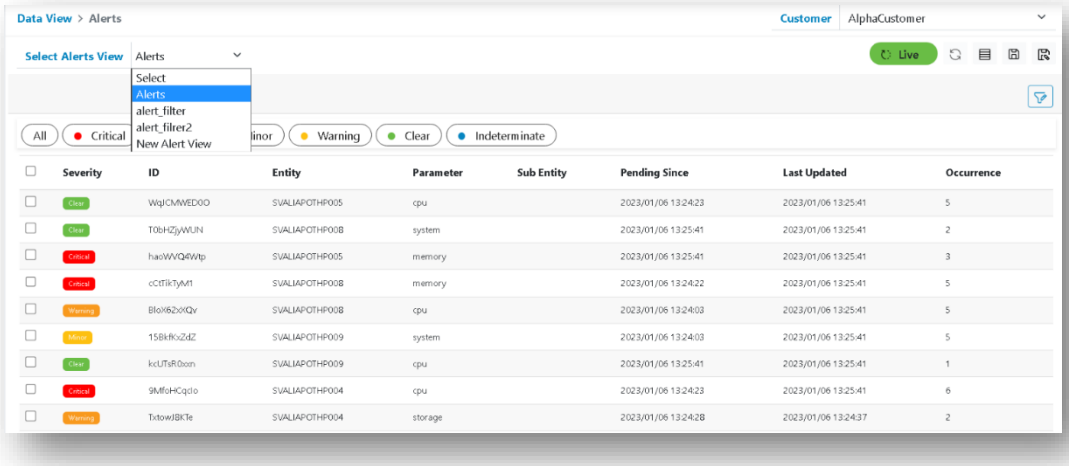

Figure 404– Select Alerts View Dropdown

7.2.2.5 Add Column

The section explains how to Add Column to alerts data:

1. In the top navigation bar, click on Data View and click on Alerts.
2. Click on the Add Column action button present at the header of the console.

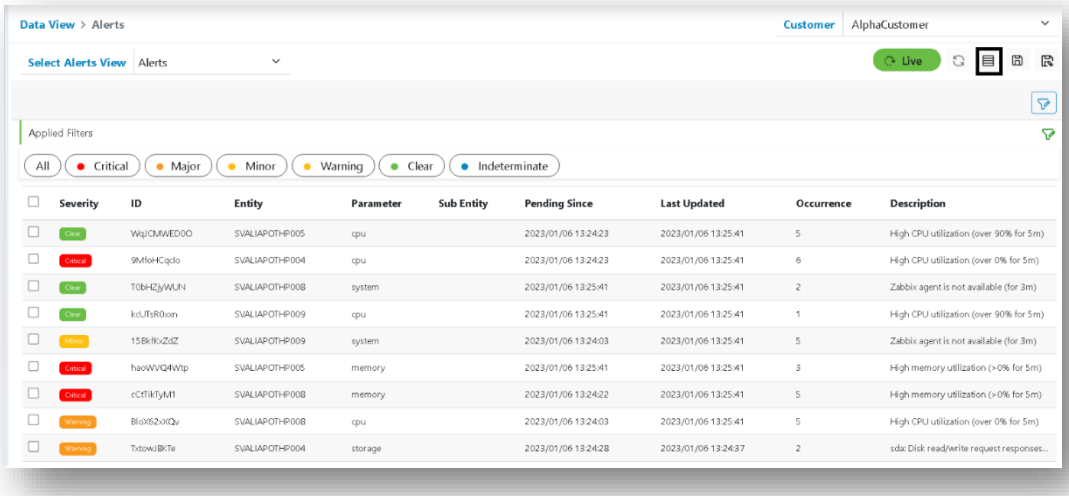

Figure 405– Add Column

3. The following form will appear. The user can select values from the drop-down lists.
4. Once done, click **Save**.

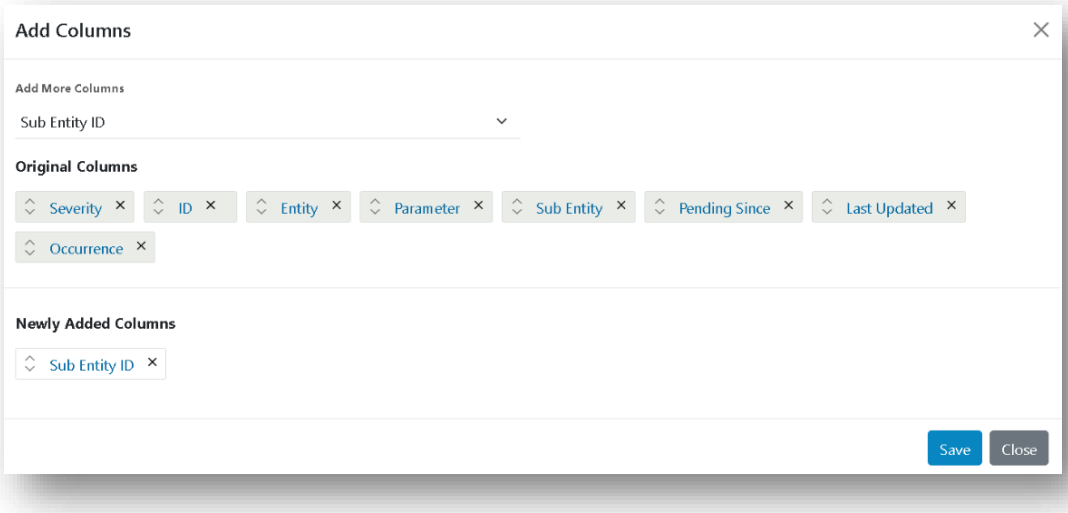

Figure 406– Add Column

7.2.2.6 Events Mapping (Alerts)

The steps involved to see events in alerts data:

1. In the top navigation bar, click on Data View and click on Alerts.
2. Click on an alert on Data View-Alert screen, then go to the pop up opened for the alert. Events for the selected alert are visible.

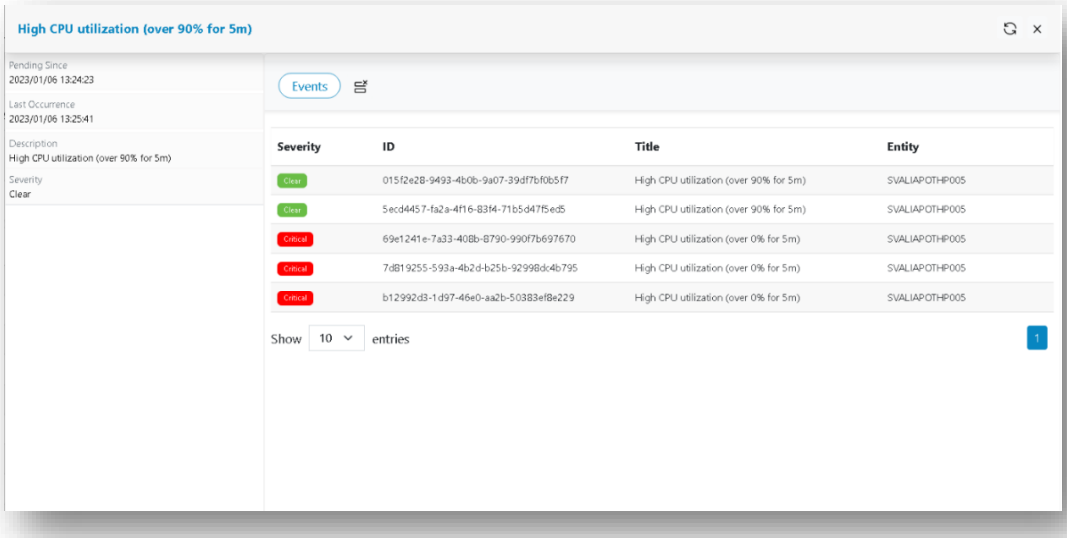

Figure 407 - Alerts Related Events

3. User can mark alerts as incorrect by clicking Mark as Incorrect button.

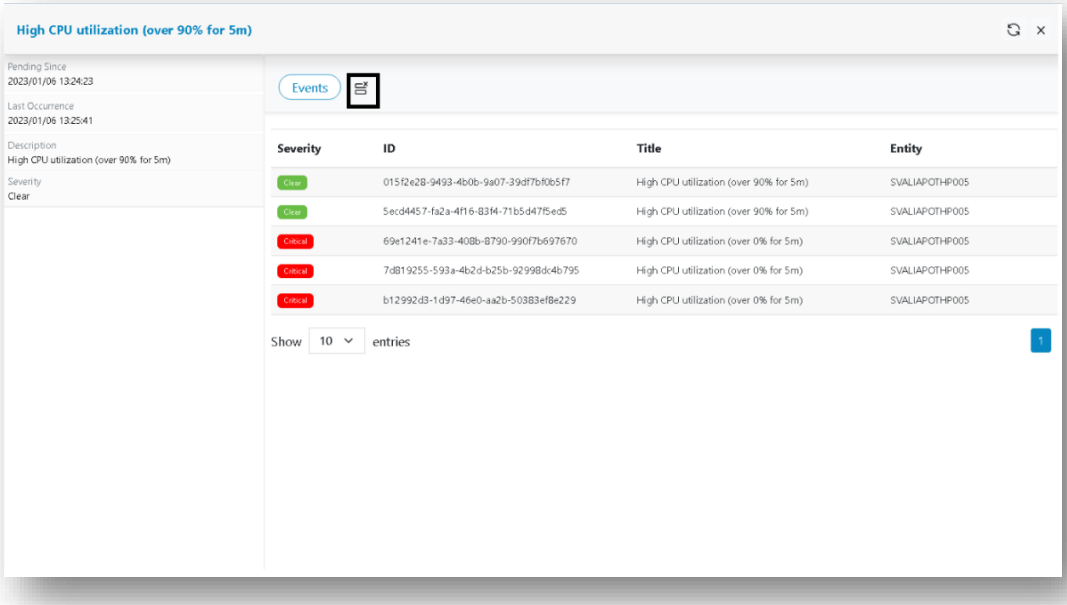

Figure 408- Mark as Incorrect

4. On successful marking the alert as incorrect, the following message will be displayed:

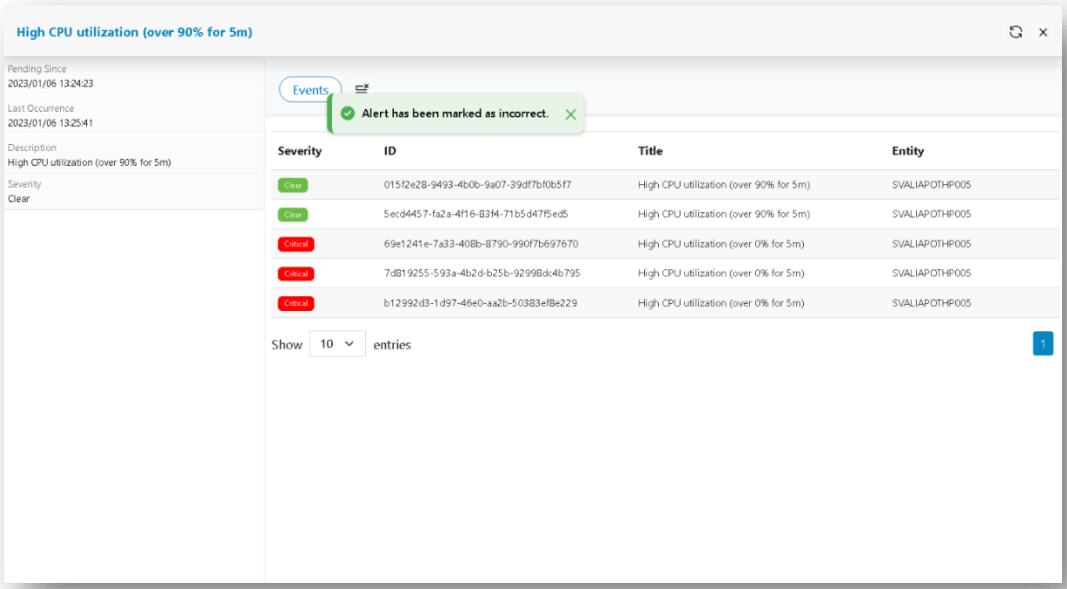

Figure 409– Alert Message

7.2.2.7 Live Alerts Data

The section helps users to view Live Alert Data.

1. In the top navigation bar, click on Data View and click on Alerts.
2. User can see the Live Alert Data in Grid view. The data gets auto refreshed every 4 seconds.

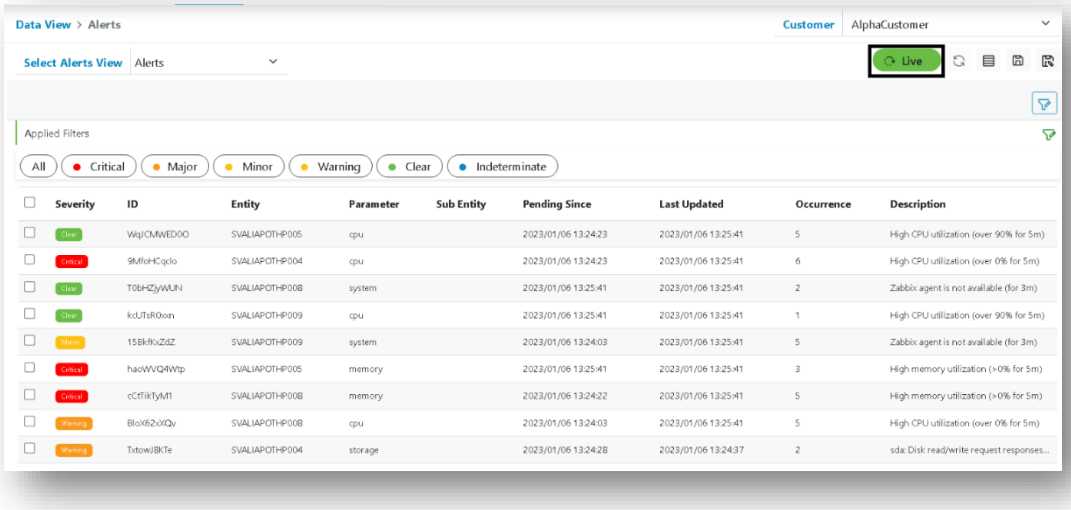

Figure 410 – Live Alerts Data

3. On clicking the **Live Alert Data** button, the auto refresh gets disabled and the following confirmation message pops-up.

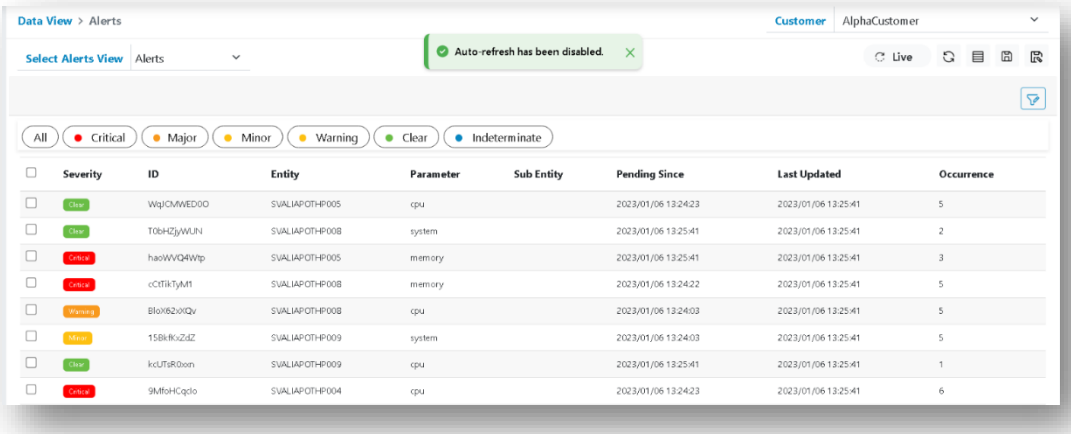

Figure 411 – Live Alerts Data Disabled

7.2.2.8 Refresh Alerts

The steps to apply **Refresh Time View** to alert data:

1. In the top navigation bar, click on Data View and click on Alert.
2. User can click on **Refresh** button only if the Live Alert Data is disabled.

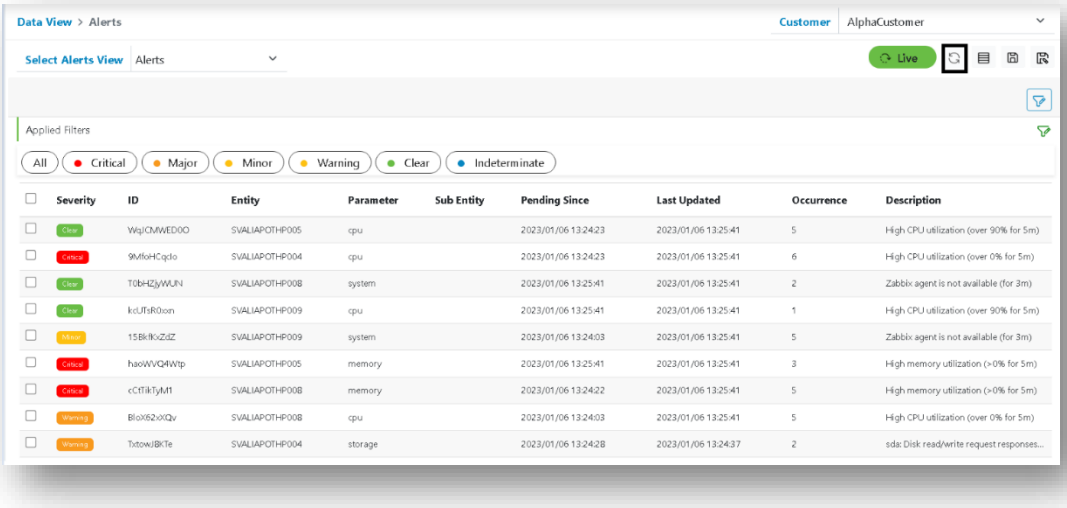

Figure 412- Refresh Data View Alerts

3. A confirmation pop-up message will appear.

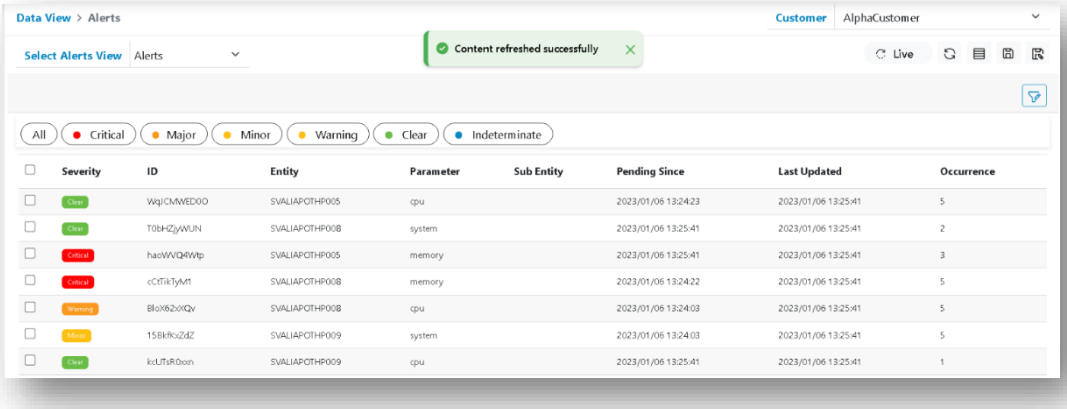

Figure 413 - Refresh Data View Alerts

7.2.2.9 Apply Filters

The steps explain how to apply Filter to the alerts data.

1. In the top navigation bar, click on Data View and click on Alerts.
2. Click on the **Apply Filter** action button present at the below header of the console.

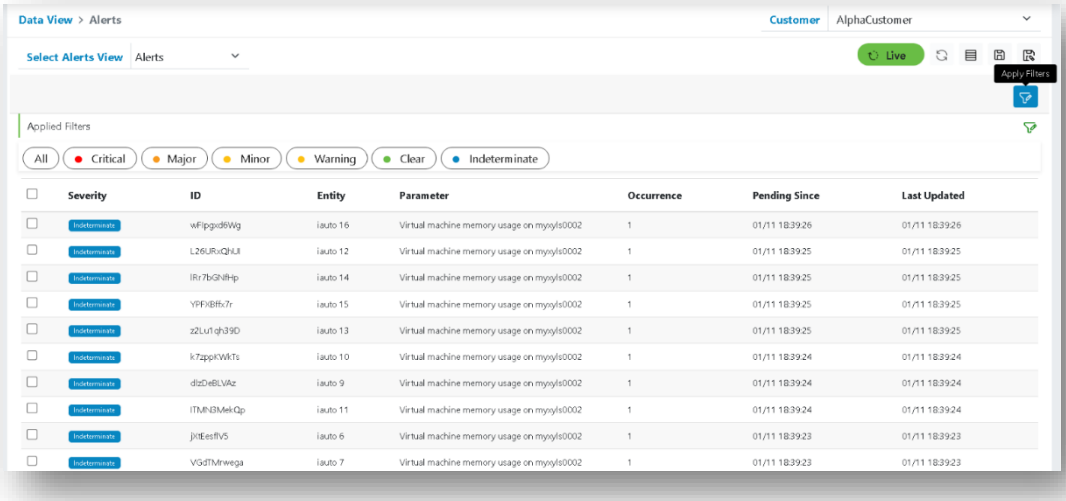

Figure 414 - More Filter Operation

3. A form will appear. Select **Field** and **Operator** from drop down list and write **Value**. Then click on the **Apply** button.

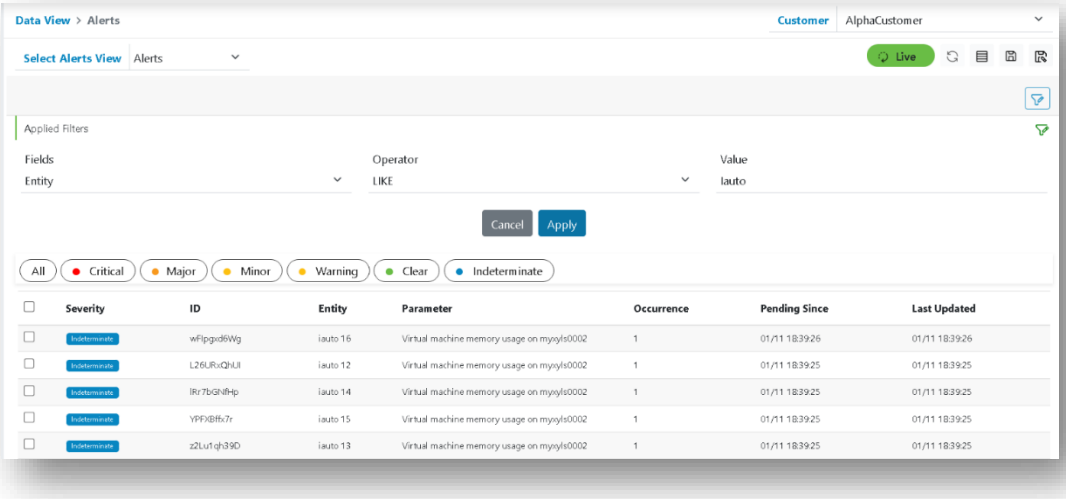

Figure 415 - More Filter Operation

4. User can see the result of applied filter.

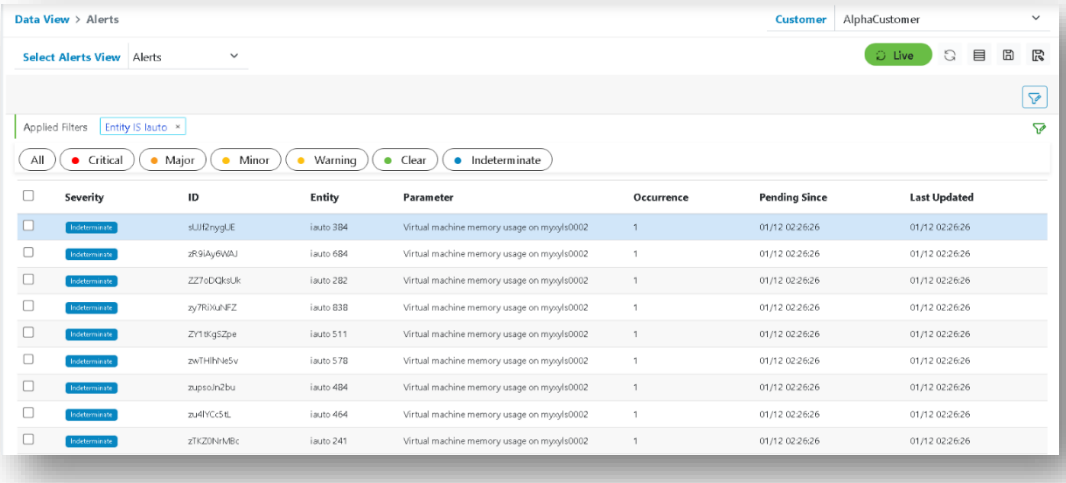

Figure 416 - More Filter Operation

7.2.3 Actionable

“Actionable" refers to a specific occurrence or situation that disrupts normal IT operations and requires attention, investigation, and resolution. Actionable are typically identified based on events or alerts generated by monitoring systems, and their management involves a structured and coordinated response to minimize the impact on the organization's IT services. Actionable are identified through the correlation and analysis of alerts, or anomalies detected by monitoring systems over IEM. Efficient Actionable creation depends upon how effective alert correlation is happening over the system.

Actionable progress through various stages in their lifecycle, including detection, identification, classification, investigation, resolution, and closure. It includes root cause analysis to identify the underlying factors that led to the actionable, helping in preventive actions.

7.2.3.1 Actionable View

The following steps help users in viewing the actionable data

1. In the top navigation bar, click on Data View and click on Actionable.
2. Actionable data will be displayed for the selected customer.

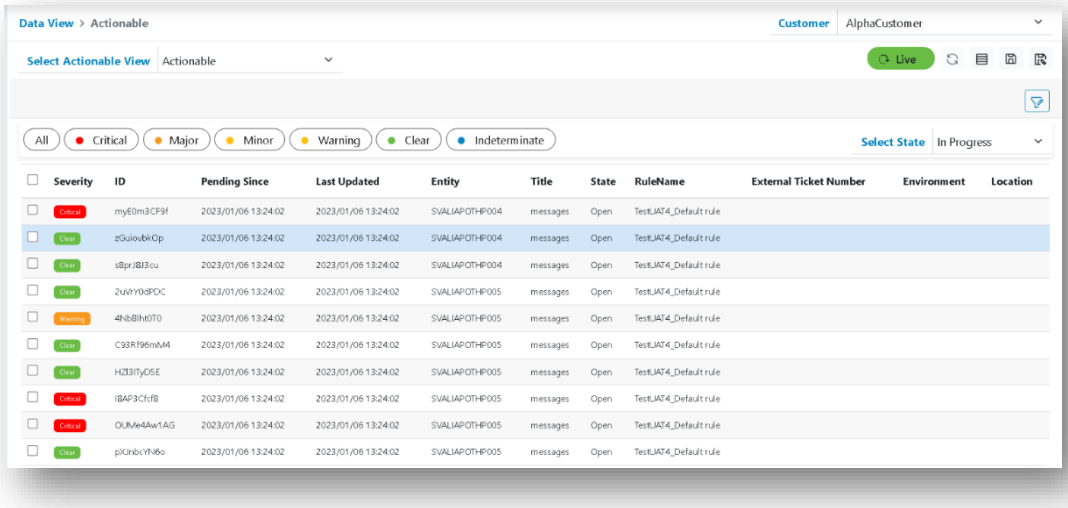

Figure 417 - Actionable View

7.2.3.2 Delete Actionable

The section contains the steps of deletion of the Actionable data.

1. In the top navigation bar, click on Data View and click on Actionable.
2. Alerts can be selected by clicking on the checkbox. (Single select/Multi select)

The auto-refresh feature automatically updates data (including events, alerts, noise, actionable items, and all events) in the grid. Consequently, any previously checked items will be unchecked. If you intend to delete something, it is advisable to disable the auto-refresh feature first and then proceed with deletion operations.

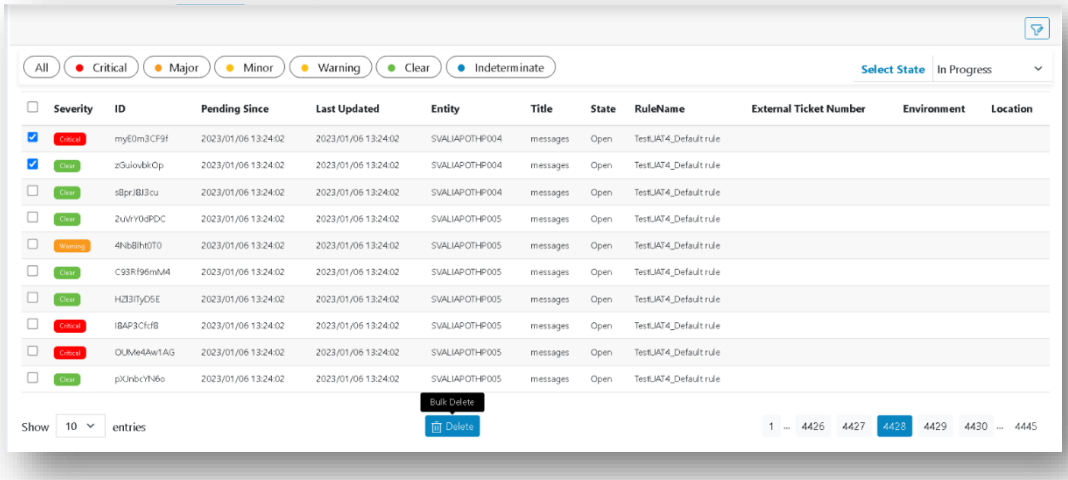

Figure 418 – Deleting Bulk Actionable

3. Click on the **Delete** action button present at the bottom.
4. A confirmation dialog box appears to confirm the deletion of alerts.

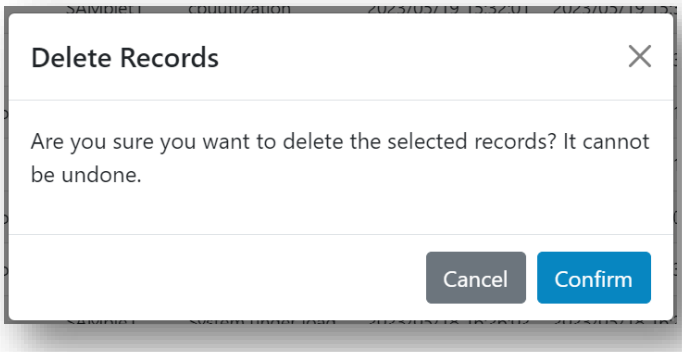

Figure 419 - Confirmation Pop- up

5. Click on Confirm button, a dialog box would appear for successful deletion of alerts.

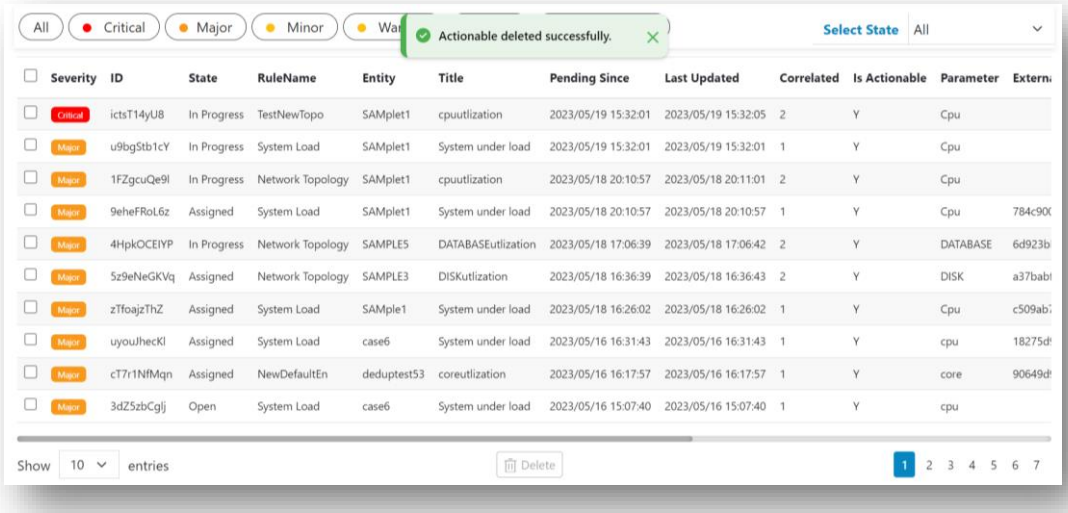

Figure 420 - Alert Message

7.2.3.3 Add Column

The steps explain how to add column to alerts data.

1. In the top navigation bar, click on Data View and click on Alerts.
2. Click on the Add Column action button present at the header of the console.

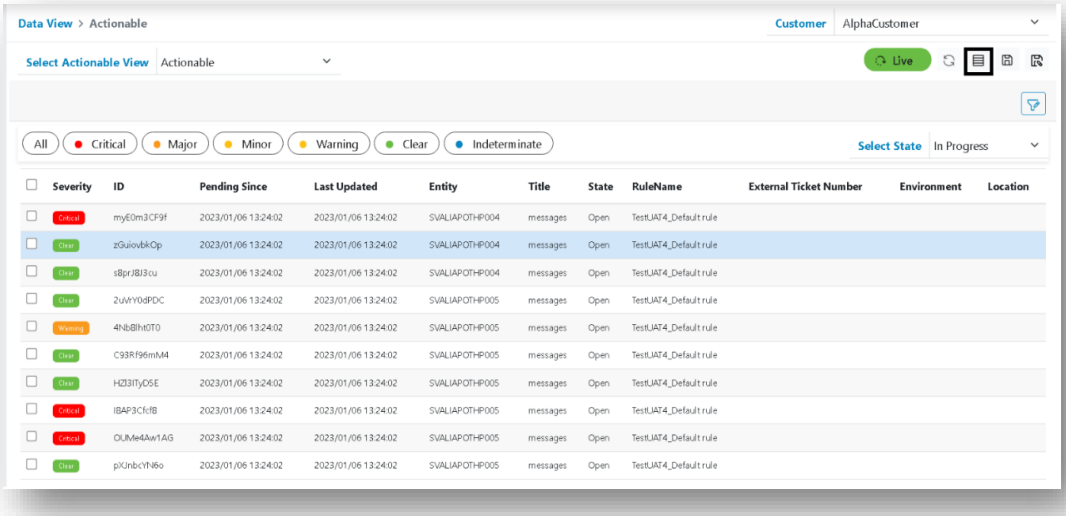

Figure 421 – Add Column

3. A form appears. Select the values from drop down lists and click **Save**.

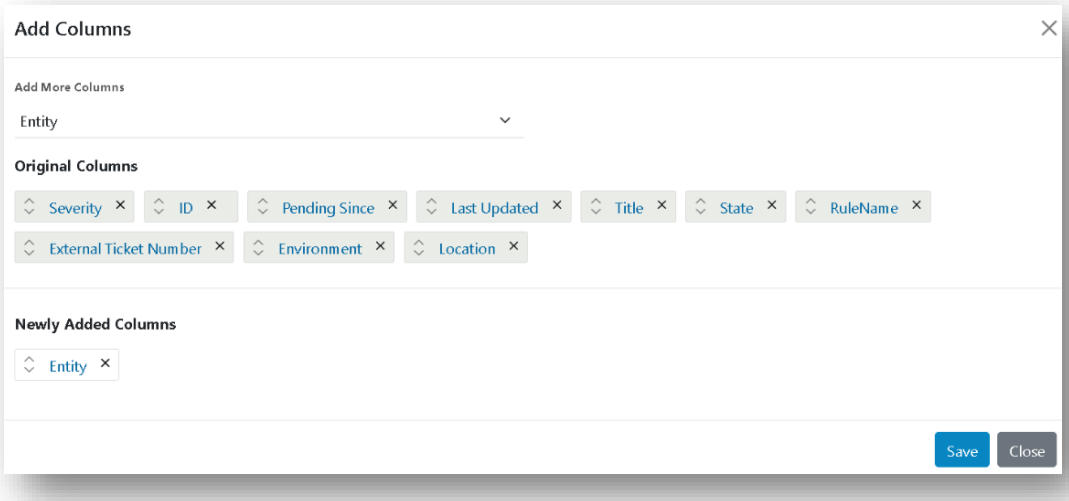

Figure 422 – Add Column

7.2.3.4 Related Changes and Related Problems

The steps explain how to view Related Changes and Related Problems for an actionable:

1. Click on an actionable on Data View-Actionable screen, then go to pop up opened for the actionable.
2. Click on **Related Changes or Related Problems** icon present over the header of the actionable popup.
3. A pop up displaying **Related Changes and Related Problems** details will be opened.

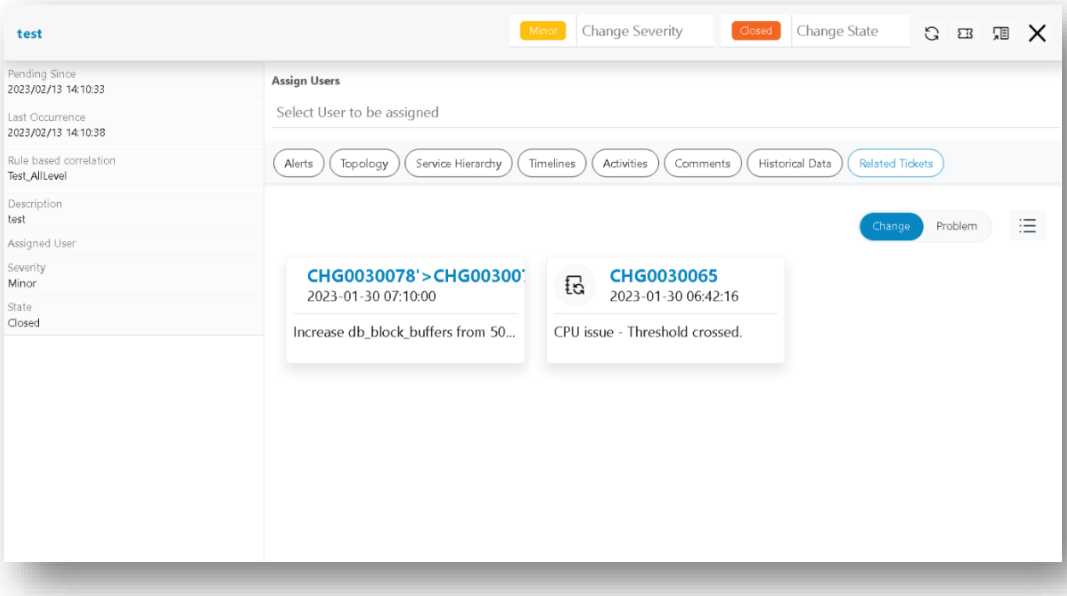

Figure 423 - Related Changes or Related Problems

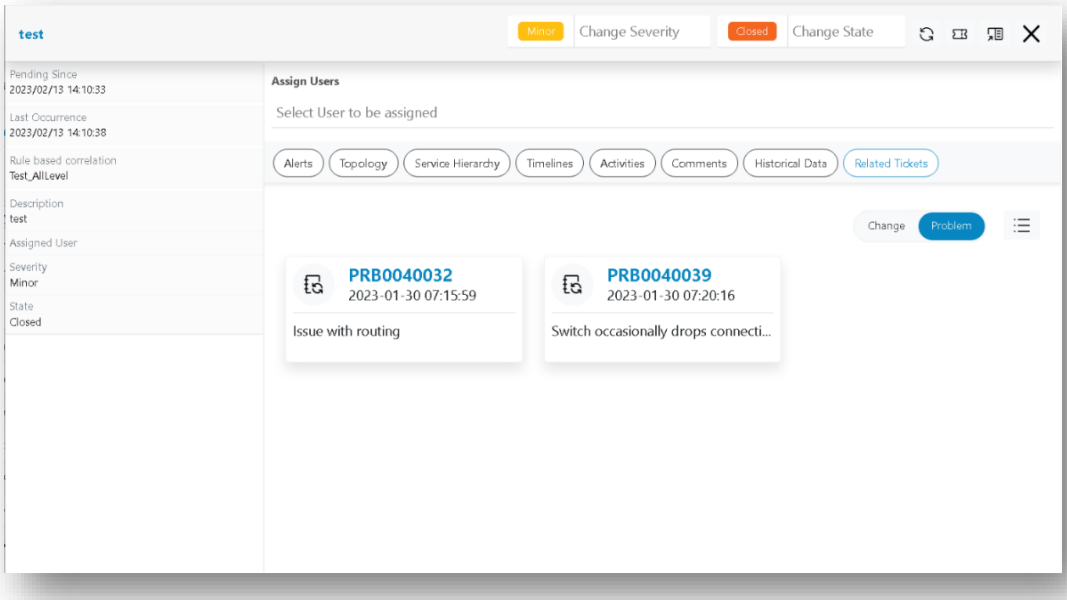

Figure 424 – Related Problems & Related Changes

7.2.3.5 Chat Bot

These steps enable user to initiate chat with a particular user over chat window.

1. Click on an actionable on Data View-Actionable screen, then go to pop up opened for the actionable.
2. Click on the chat icon present over the header of the actionable popup.
3. Actionable ID is mentioned over the chat window. User can initiate chat with the invited user as shown.

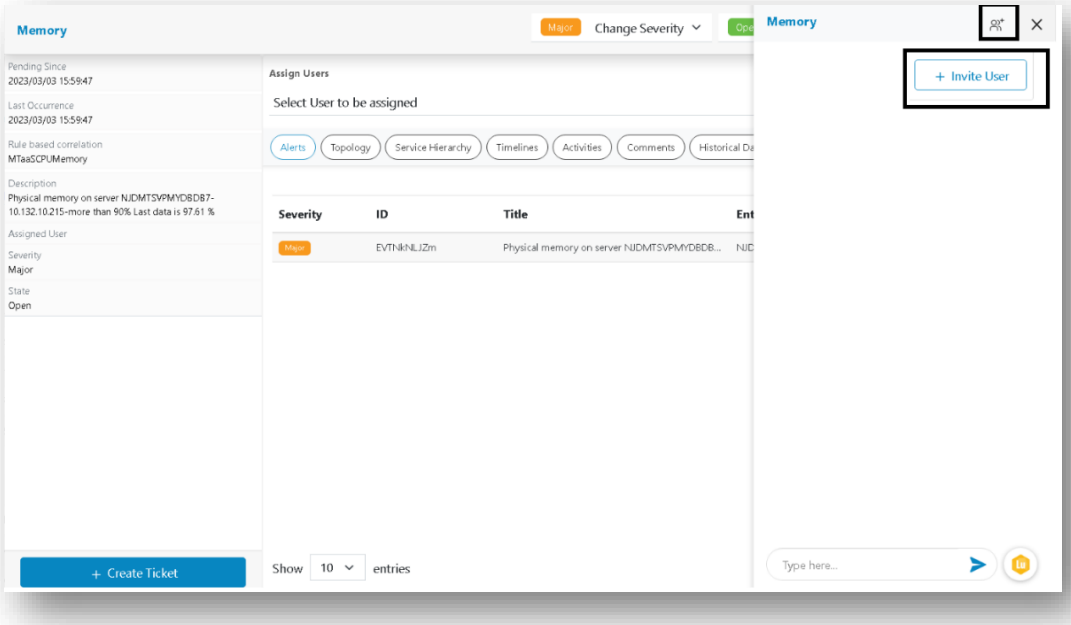

Figure 425 - Invite user

4. On clicking + Invite User, user can select the user from the dropdown as shown in the image below:

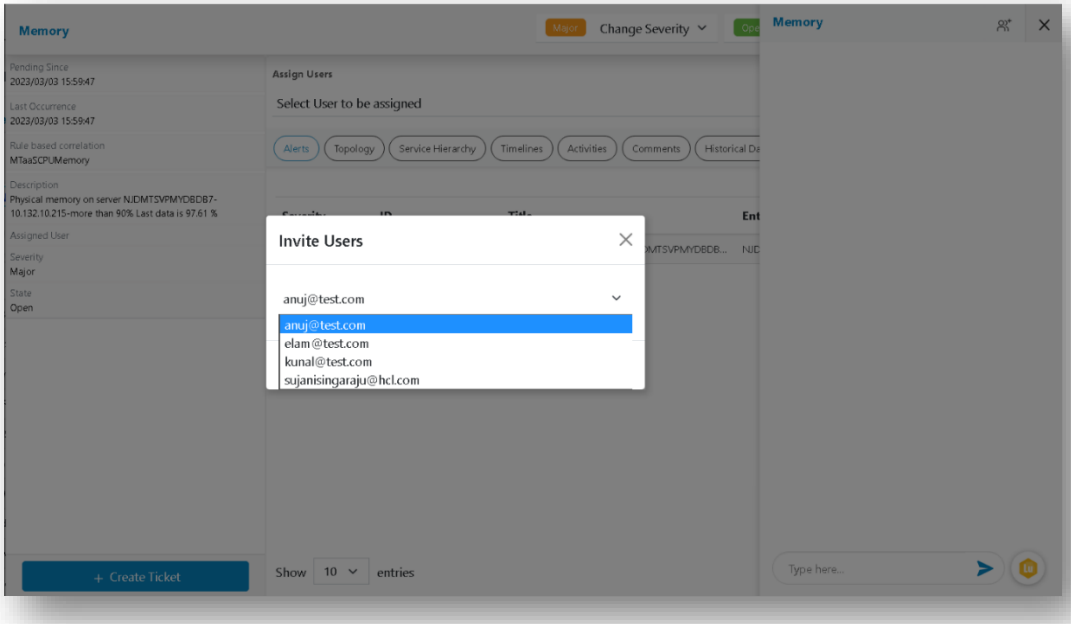

Figure 426 - Select Users

5. Once Inviting a user for the selected actionable is completed, a confirmation message is prompted.

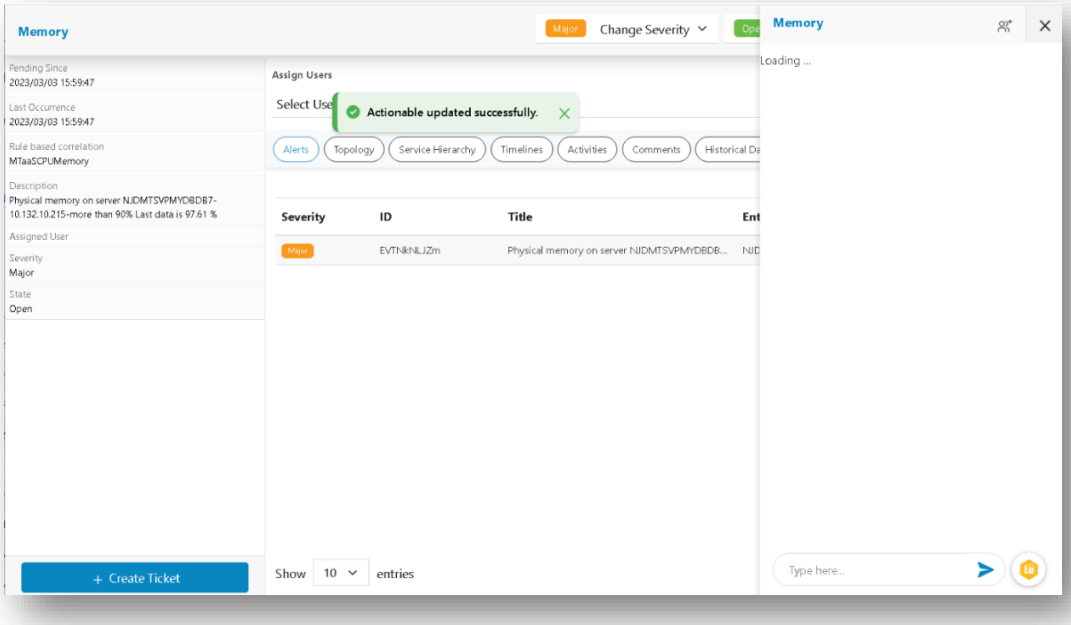

Figure 427 - Confirmation popup

6. Lucy chatbot icon is also present in the chat window to find some knowledge articles related to resolving queries for actionable.
7. Red Dot /Green Dot show if the chat window is inactive/active.

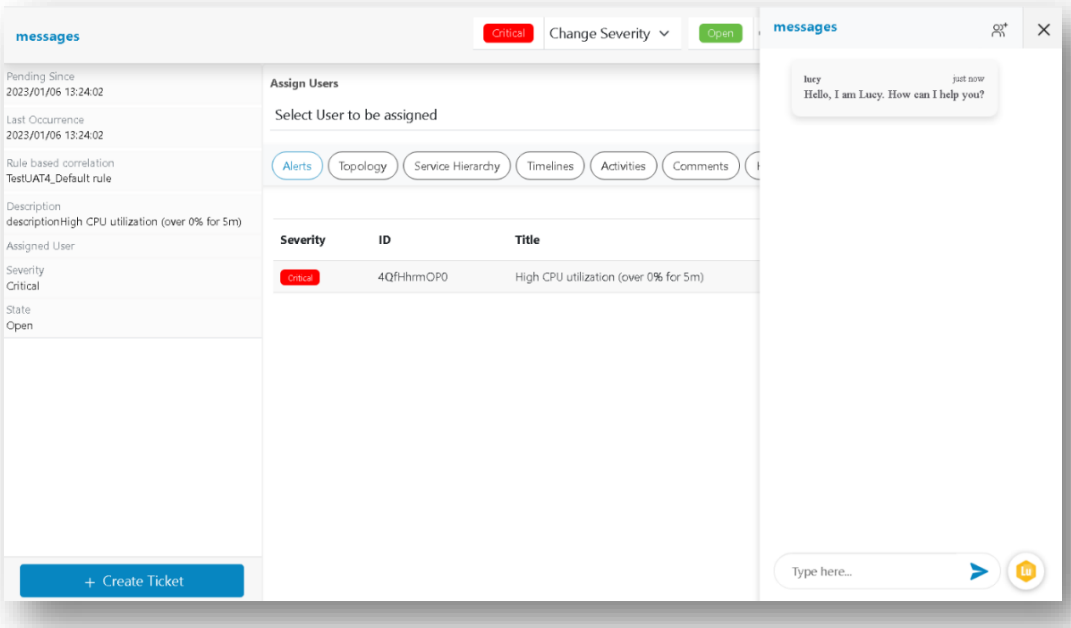

Figure 428 – Chat Bot

7.2.3.6 Add Comments

The steps explain how to add comments for selected actionable.

1. Click on an actionable on Data View-Actionable screen, then go to pop up opened for the actionable.
2. Click on the Comments header present in the actionable popup.
3. Detailed view of users along with time and comments will be visible as shown.

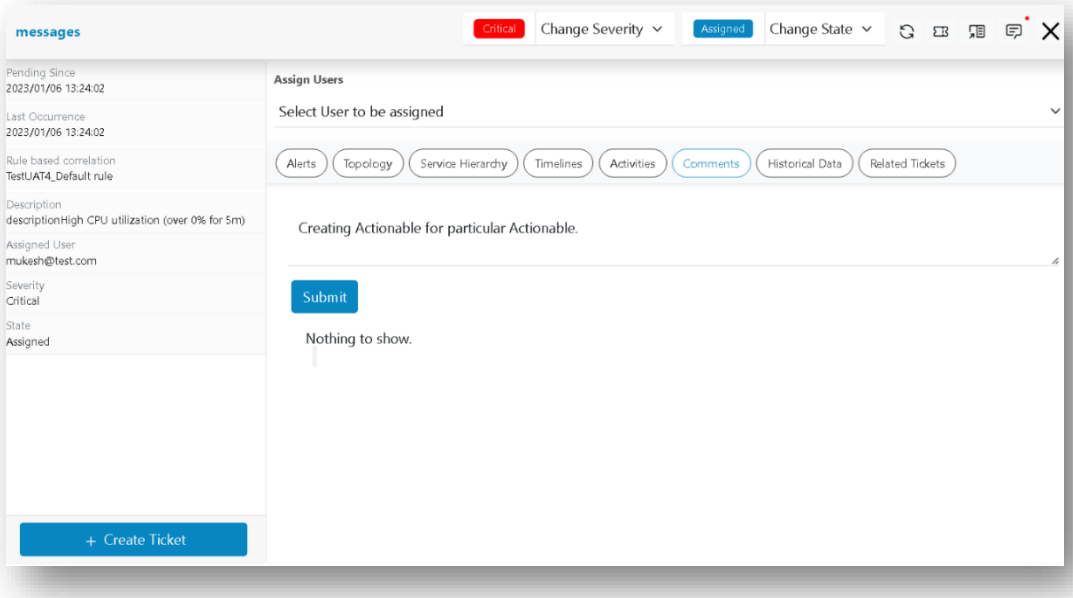

Figure 429 – Add Comments to Actionable

4. Write the comment and click on **Submit** button. Once submitted the comment is displayed for that actionable as shown in the image below:

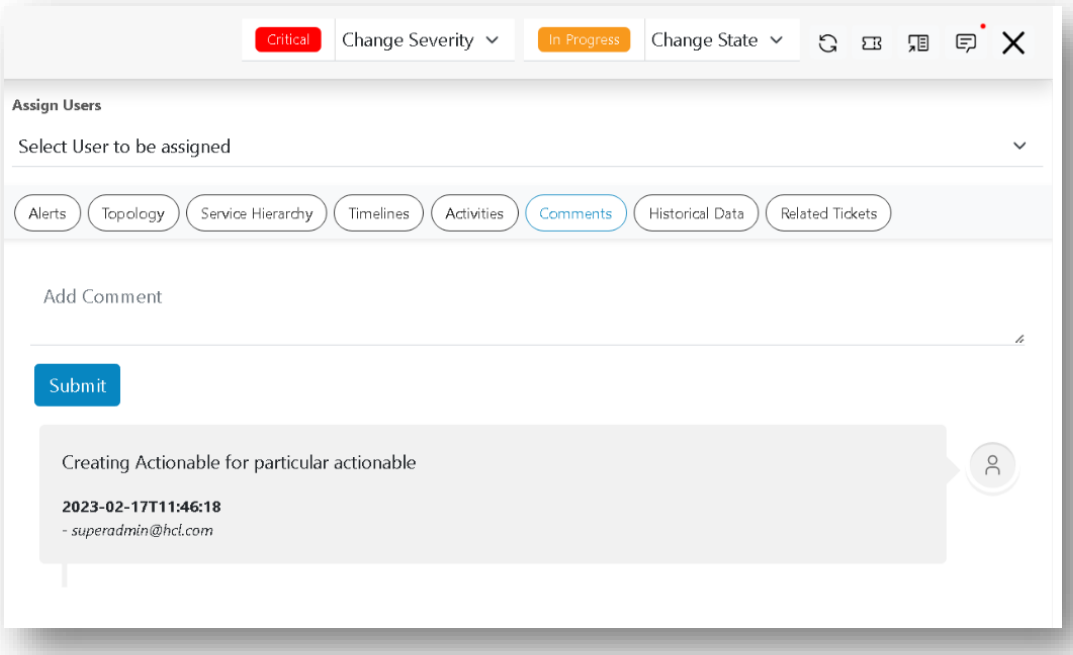

Figure 430 – Add Comments to Actionable

7.2.3.7 Activities

On this section, the users see activities for actionable data.

1. Click on an actionable on Data View-Actionable screen, then go to pop up opened for the actionable
2. Click on the Activities header present in the actionable popup.
3. Detailed view of changes in the logs for that actionable and its related alerts will be visible as shown.
4. Search tab is present to search for a specific log present in the activity view.

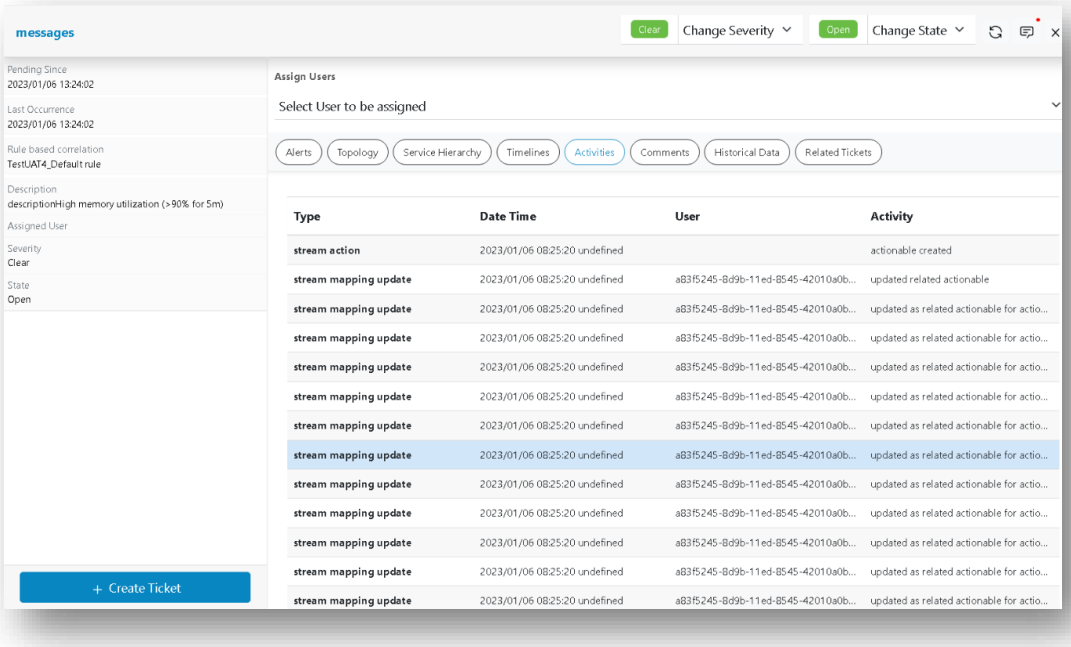

Figure 431 – Activities

7.2.3.8 Similar Actionable

The steps explain how to view similar actionable for actionable data.

1. Click on an actionable on Data View-Actionable screen, then go to pop up opened for the actionable.
2. Click on the **Historical Data** present in the actionable popup.
3. Historical Data containing details will be displayed and details can be seen while scrolling from left to right for similar actionable.

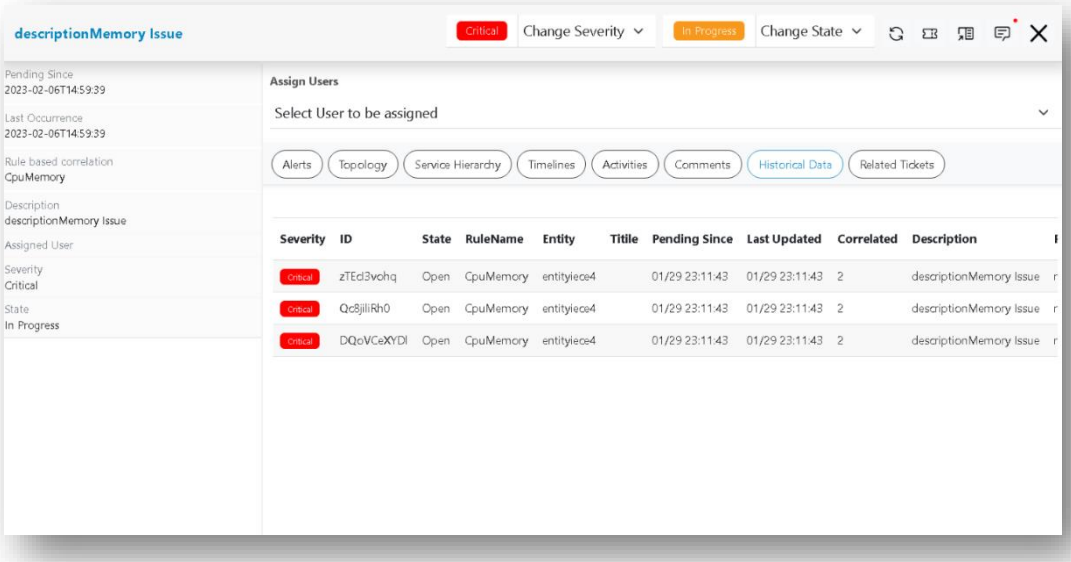

Figure 432 – Similar Actionable

7.2.3.9 Service Hierarchy

The steps explain how to view service hierarchy for actionable data.

1. Click on an actionable on Data View-Actionable screen, then go to pop up opened for the actionable.

2. Click on the **Service Hierarchy** header present in the actionable popup.
3. Service Hierarchy would be visualizing the relationship between the various services and their downstream / upstream impact due to any issue for a specific entity.
4. Impacted services can be highlighted as per custom logic (based on color-coding).

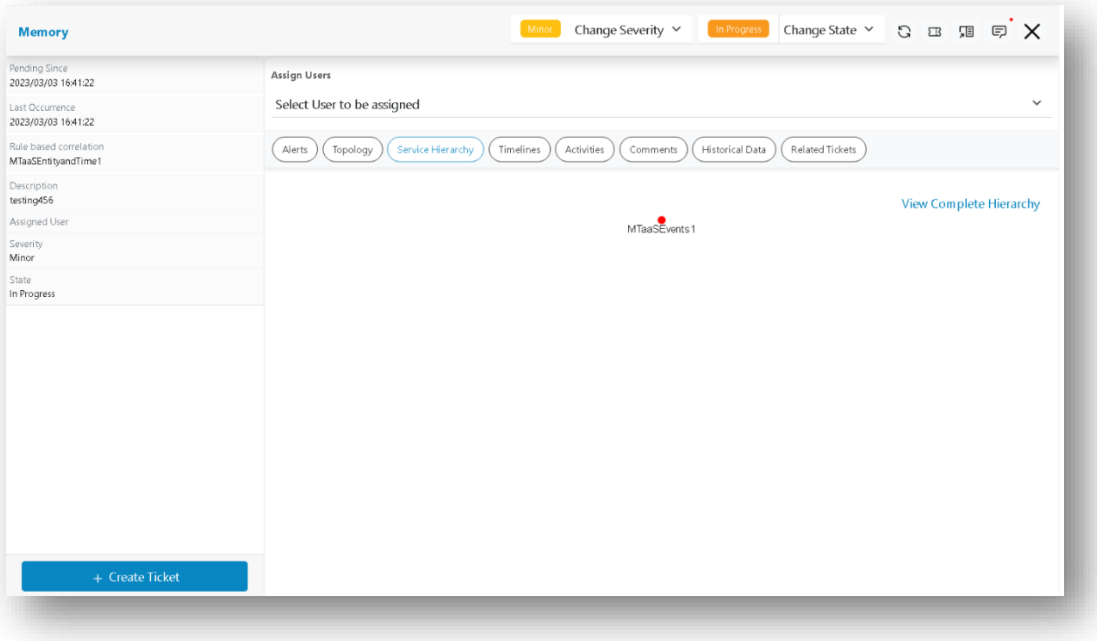

Figure 433 – Service Hierarchy

7.2.3.10 Timelines

The steps explain how to view timeline for actionable data.

1. Click on an actionable on Data View-Actionable screen, then go to pop up opened for the actionable.
2. Click on the **Timelines** header present in the actionable popup.
3. Timeline view is visible under the header and details can be seen while scrolling from top to bottom to check the timestamp of events and alerts for that actionable.
4. Entity, Parameter, Description and Timestamp are displayed for the selected Events/Alerts/ Actionable in the timeline view.
5. There are different icons present in timeline for displaying events, alerts and actionable details and their color would display the severity.

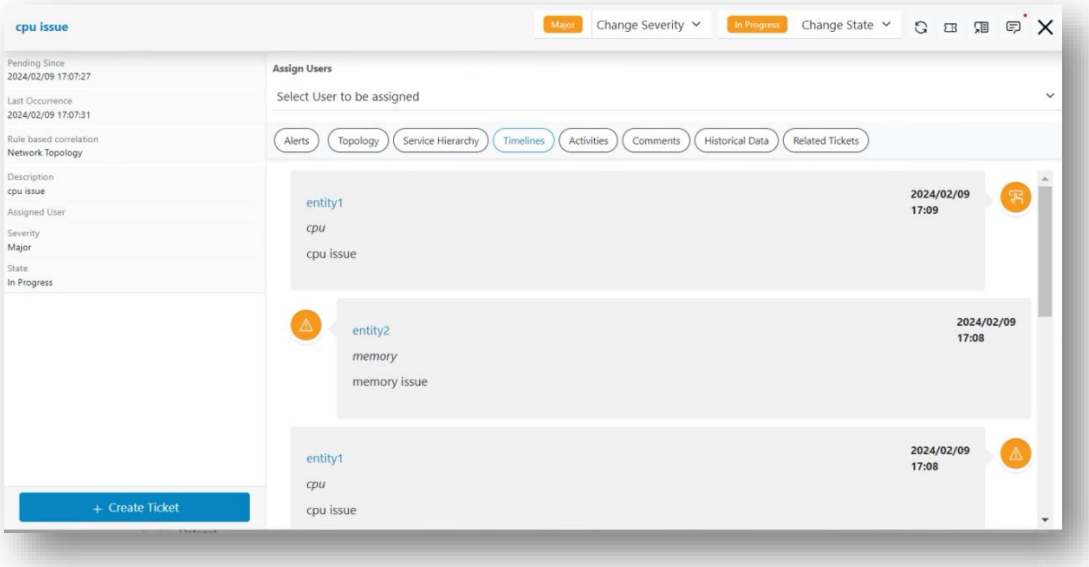

Figure 434 – Timelines

7.2.3.11 Change Severity

The steps explain how to change severity for actionable data:

1. Click on an actionable on Data View-Actionable screen, then go to pop up opened for the actionable.
2. Change the severity of the actionable using the drop-down as shown in the image below:

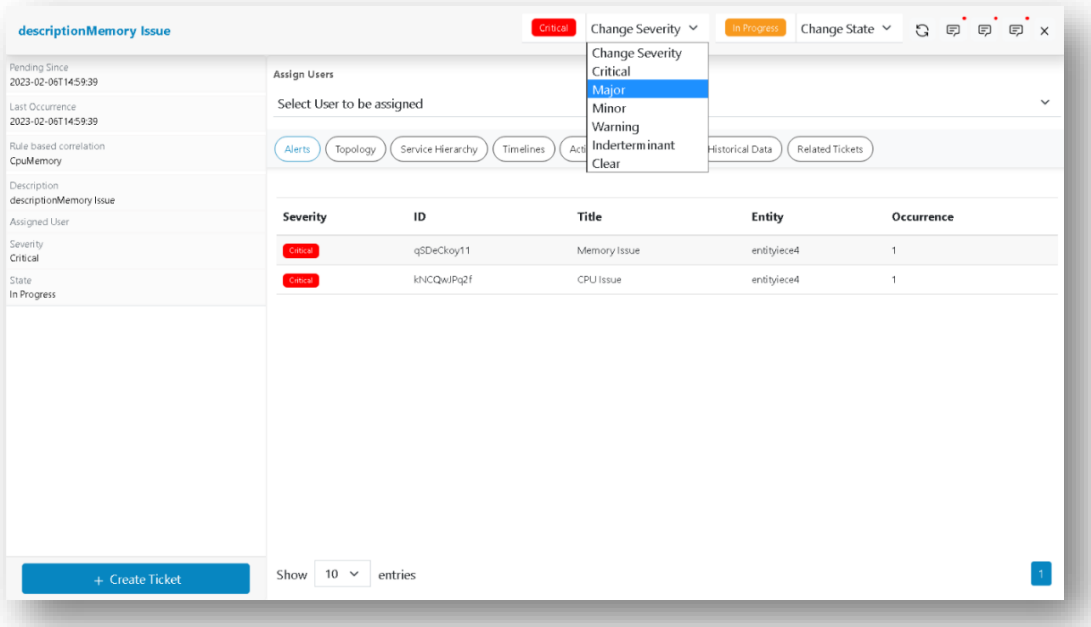

Figure 435 – To Change Severity of Actionable

3. A dialog box would appear for confirmation.

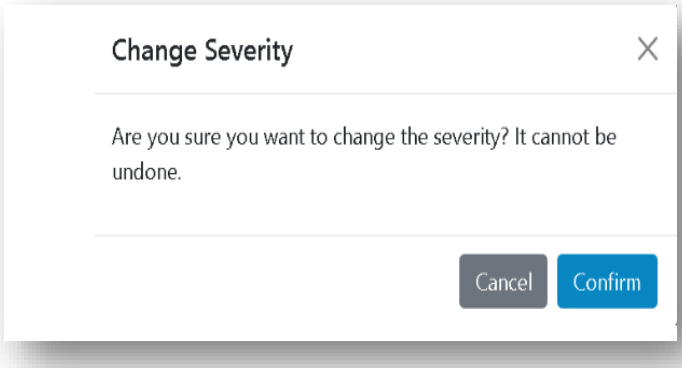

Figure 436 – Confirmation Pop- up

4. Click **Confirm**. On success, a confirmation pop-up message will be displayed.

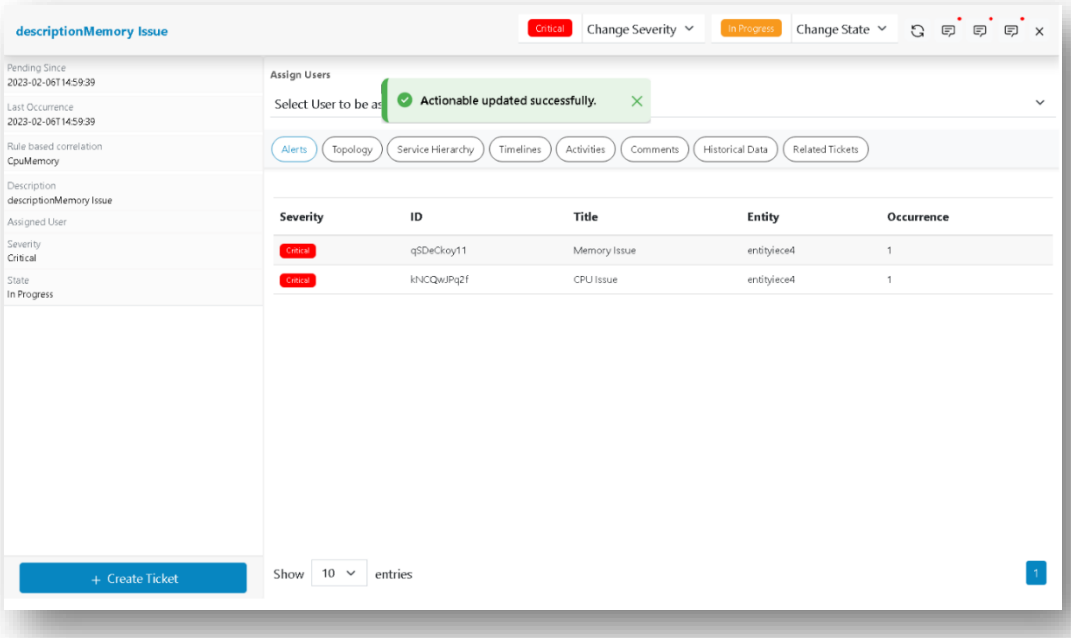

Figure 437 – Alert Message

7.2.3.12 To Change Status

The steps involve the explanation on how to change status for actionable data.

1. Click on a particular actionable on Data View-Actionable screen, then go to pop up opened for the actionable.
2. Change the status of the Actionable using the drop-down as shown in the following figure:

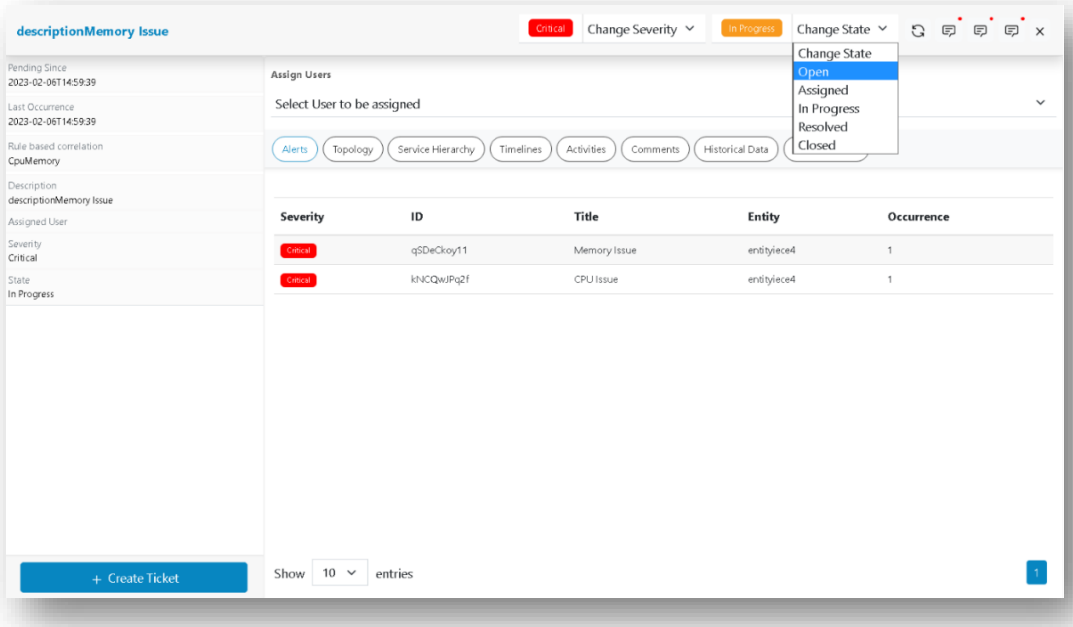

Figure 438 – To Change Status for Actionable

3. A dialog box would appear for confirmation.

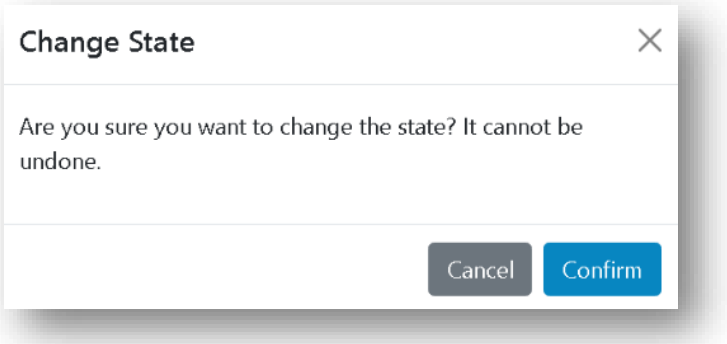

Figure 439 – Confirmation Pop- up

4. Click **Confirm**. On success, a confirmation pop-up message will be displayed.

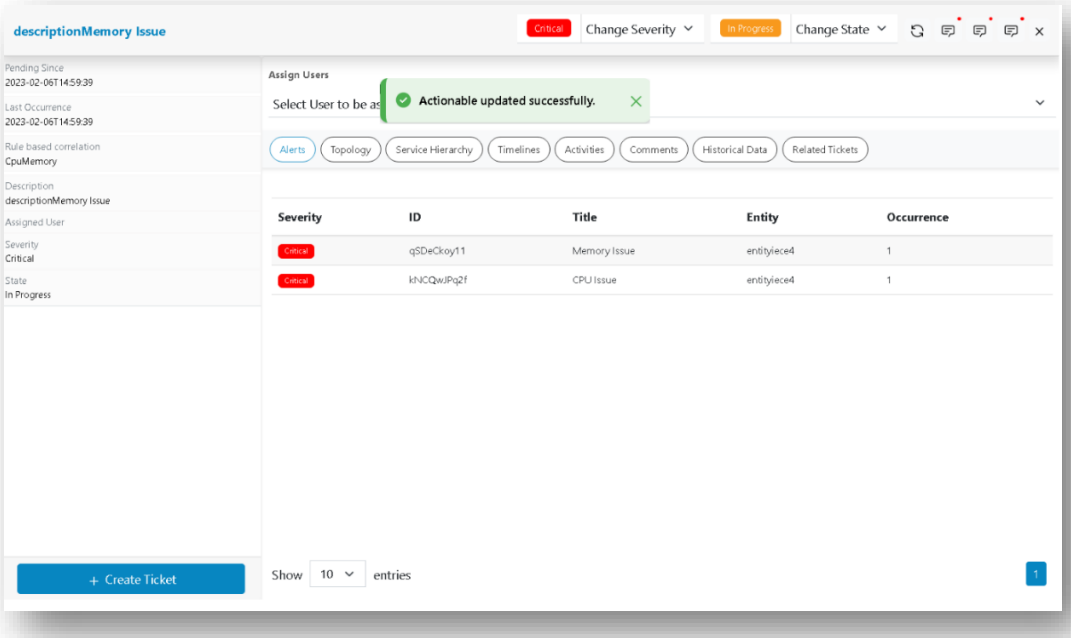

Figure 440 – Alert Message

7.2.3.13 Assign Actionable to another User

These steps enable user to assign actionable to a specific user for actionable data.

1. Click on an actionable on Data View-Actionable screen, then go to pop up opened for the actionable.
2. Click on **Assigned** header present in the actionable popup. The dropdown list of users configured in the environment will be displayed.
3. Select the user to be assigned for that actionable as shown in the following figure:

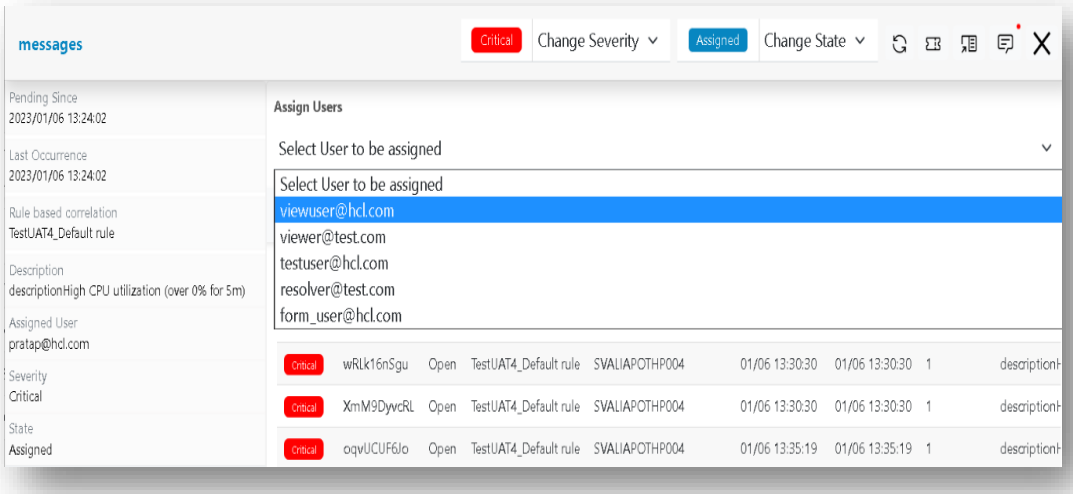

Figure 441 – Assign Actionable to Another User

4. A notification is sent to the user after the actionable is assigned.
5. A notification is also sent to the user when the actionable assigned is released by the user.

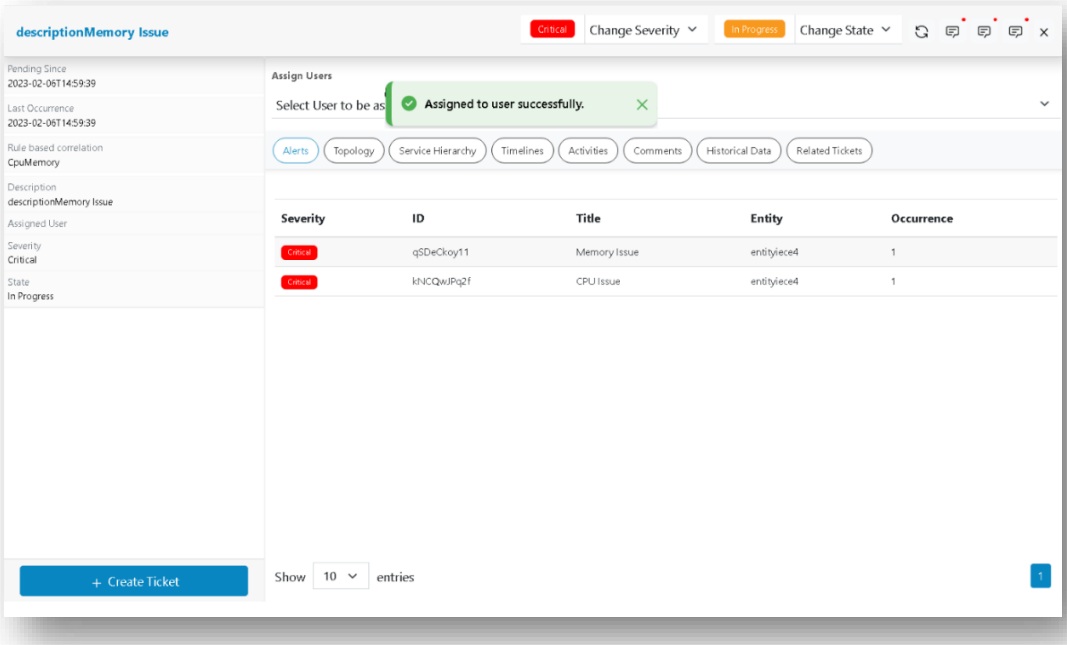

Figure 442 – Alert Message

7.2.3.14 Save Actionable

The steps explain how to save actionable data.

1. In the top navigation bar, click on Data View and click on Actionable.
2. Click on Save icon to save Actionable.

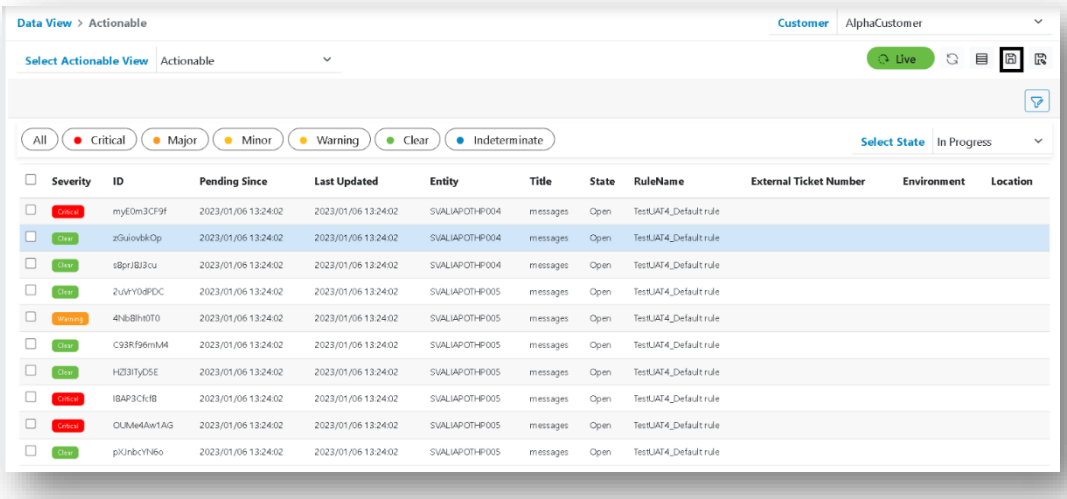

Figure 443 – Save Actionable

3. The following confirmation popup appears:

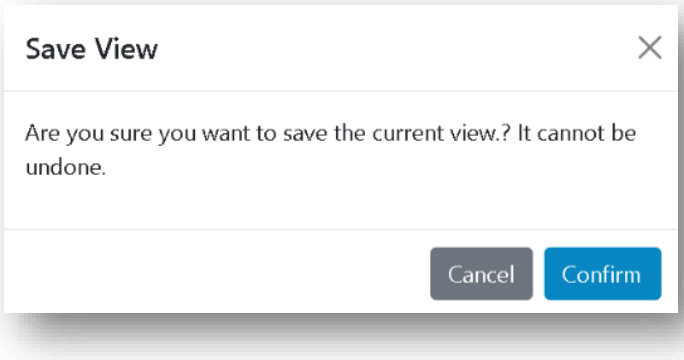

Figure 444 – Save Actionable

4. Click **Confirm.** A success pop will appear, and the grid will be updated accordingly, and the saved Actionable data starts appearing in the grid.

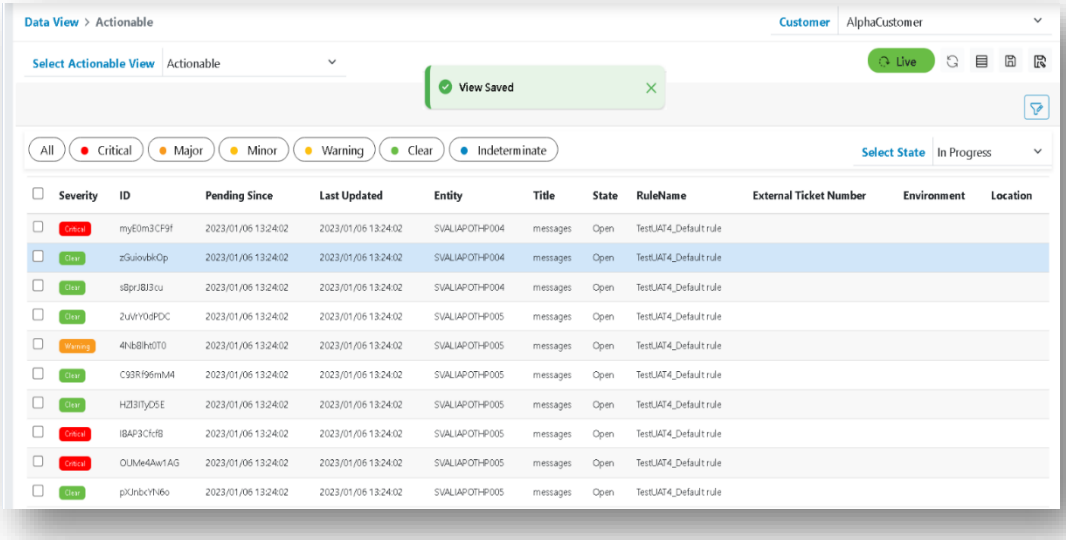

Figure 445 – Alert Message

7.2.3.15 Save As Actionable

The section explains the steps to Save a personalized view of Actionable data as per the requirement.

1. In the top navigation bar, click on Data View and click on Events.
2. Click the **Save as Actionable** icon.

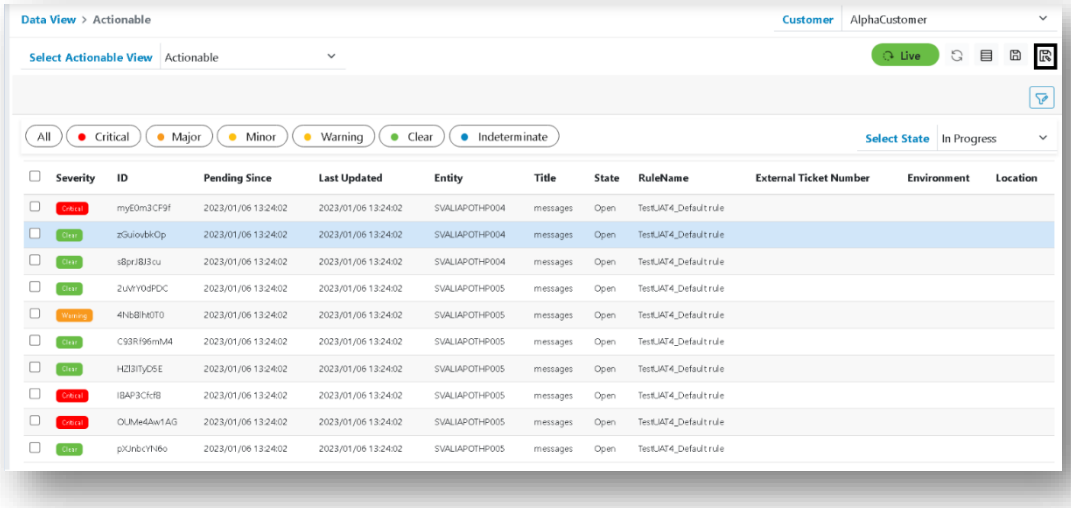

Figure 446 – Save As Actionable

3. The Save as pop-up appears:

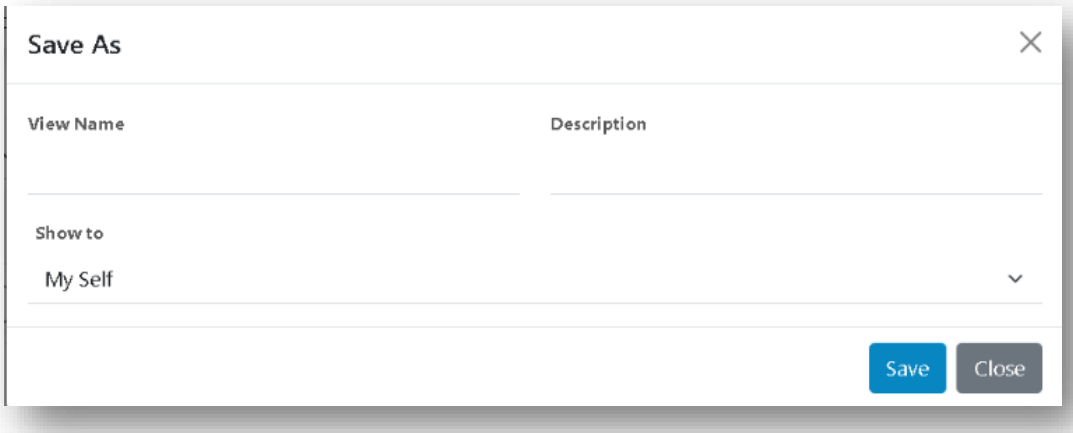

Figure 447 – Save As Actionable

4. Populate all the fields and click on **Save** button. A success message pops up.

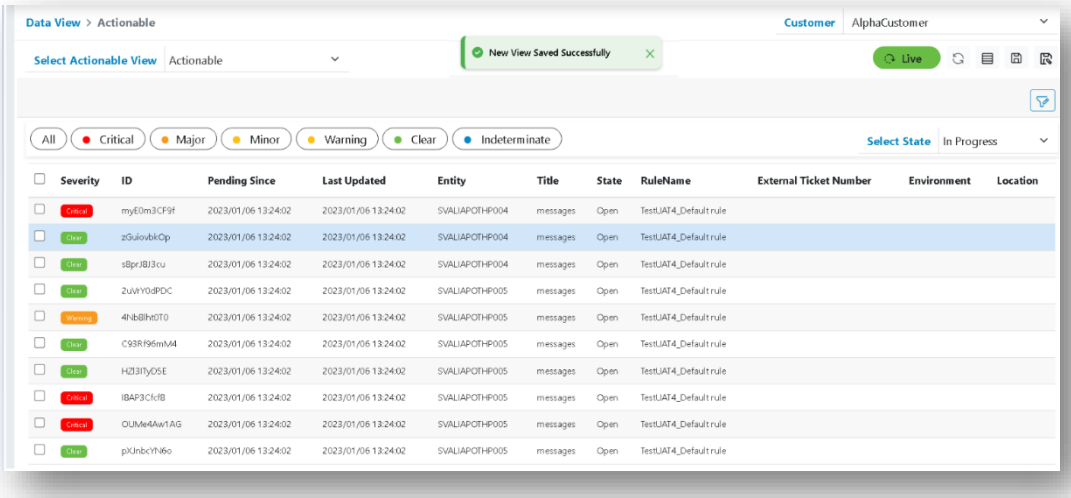

Figure 448 – Alert Message

7.2.3.16 Actionable Data

The steps explain how to view Live Actionable data.

1. In the top navigation bar, click on Data View and click on Actionable.
2. User can see the Live Actionable Data in Grid view. The data gets automatically refreshed every 4 seconds.

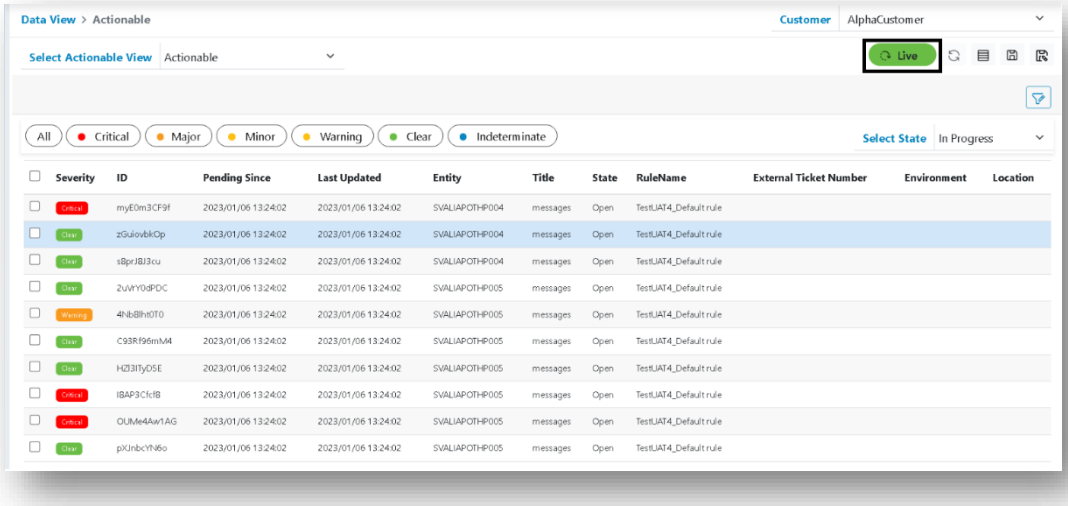

Figure 449 – Live Actionable Data

3. Click the Live Alert Data button to disable the auto refreshing the live alert data. A confirmation pop up message will appear.

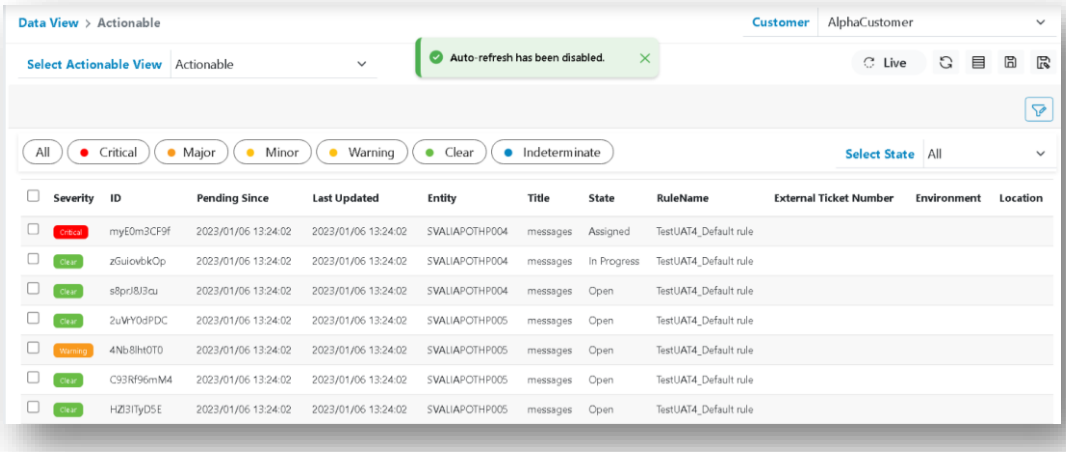

Figure 450 – Live Actionable Data Disabled

7.2.3.17 Refresh

The steps explain how to refresh the actionable data.

1. In the top navigation bar, click on Data View and click on Actionable.
2. Click the Refresh icon if the Live Actionable Data is disabled.

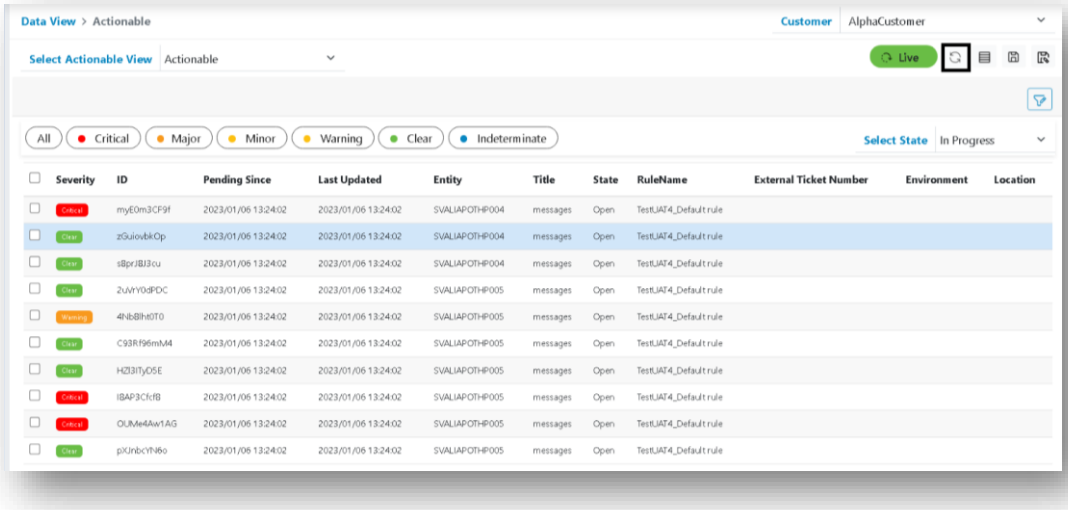

Figure 451 – Refresh time for Actionable

3. A confirmation pop up message will appear.

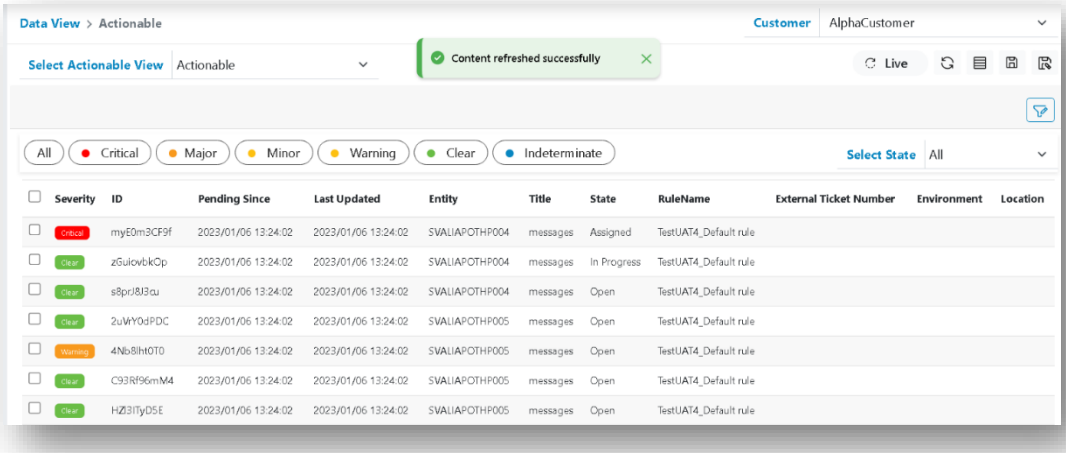

Figure 452 – Refresh time for Actionable

7.2.3.18 To see Alerts

The steps explain how to view alerts in Actionable data.

1. In the top navigation bar, click on Data View and click on Actionable.
2. Click on an actionable on Data View-actionable screen, then go to pop up opened for the actionable.
3. Click on **Alerts** header to see the alert for that actionable.

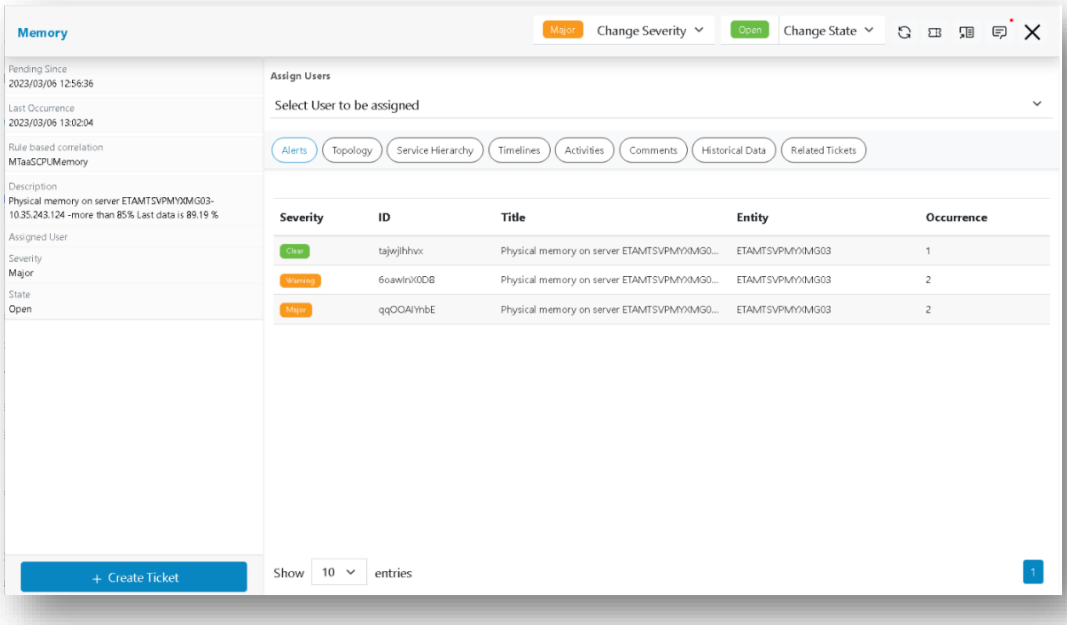

Figure 453 – Actionable Related Alerts

7.2.3.19 Topology

The steps explain how to view topology for actionable data.

1. Click on an actionable on Data View-Actionable screen, then go to pop up opened for the actionable.
2. Click on the **Topology** header present in the actionable popup.
3. Topology would be visualizing the relationship between the various services and their downstream / upstream impact due to any issue for a specific entity.
4. Impacted services can be highlighted as per custom logic (based on color-coding).

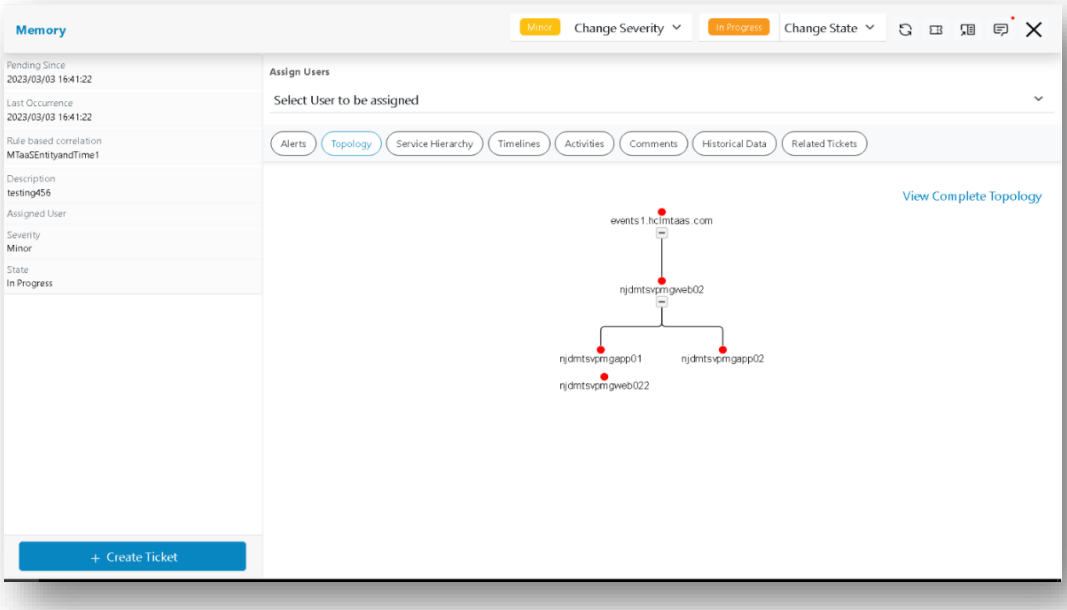

Figure 454 – Topology

7.2.3.20 Update Ticket

The steps explain how to update tickets for actionable data.

1. Click on an actionable on Data View-Actionable screen, then go to pop up opened for the actionable.
2. Click on the **Update Ticket** icon present in the actionable popup.

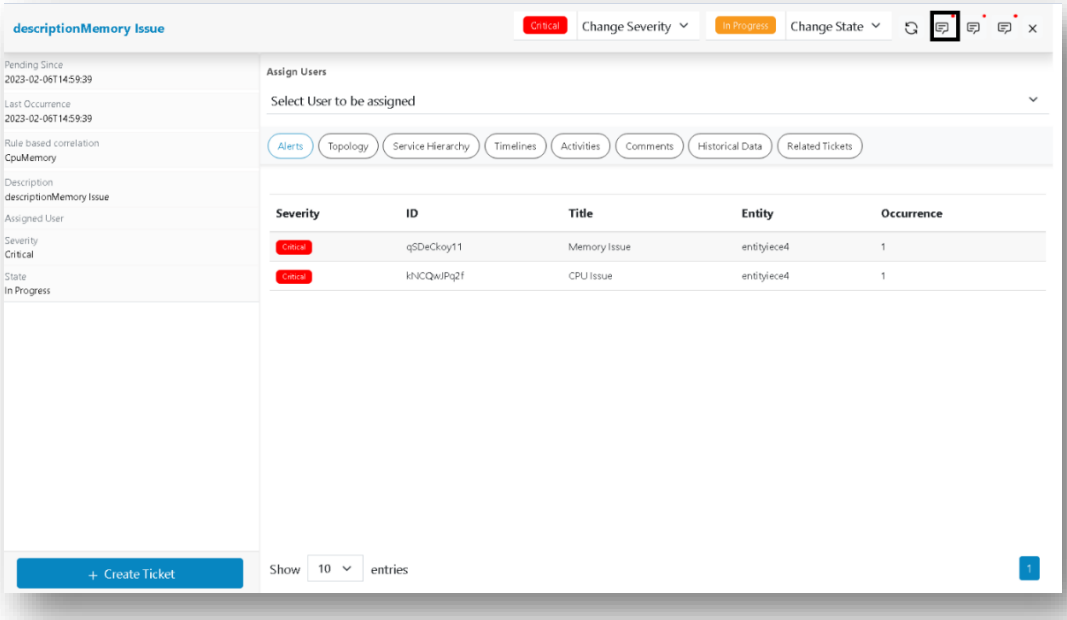

Figure 455 – Update Ticket for Actionable

3. On clicking the update ticket icon, a confirmation message pops-up:

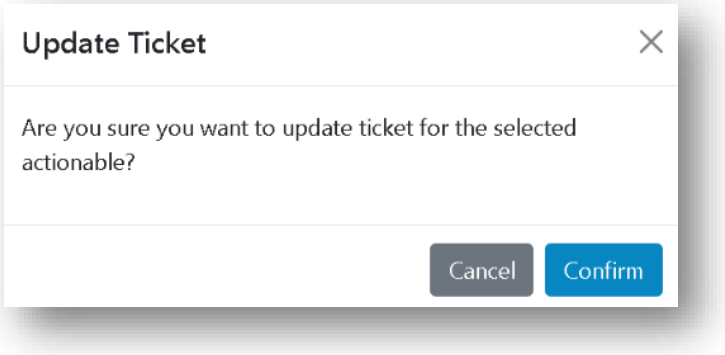

Figure 456 – Update Ticket for Actionable

4. Click on the **Confirm** button. A success message pops up as shown in the following figure:

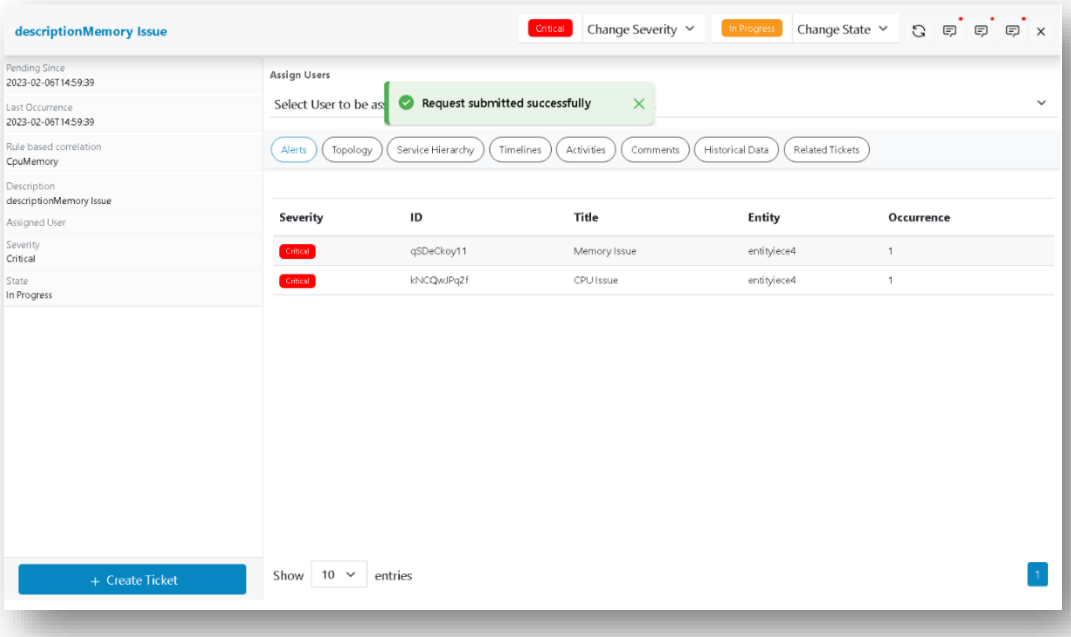

Figure 457 – Success Message for Update Ticket

7.2.3.21 Update work Notes

The steps Explain how to view Update Work Notes for actionable data.

1. Click on an actionable on Data View-Actionable screen, then go to pop up opened for the actionable.
2. Click on the **Update Work Notes** icon present in the actionable popup.

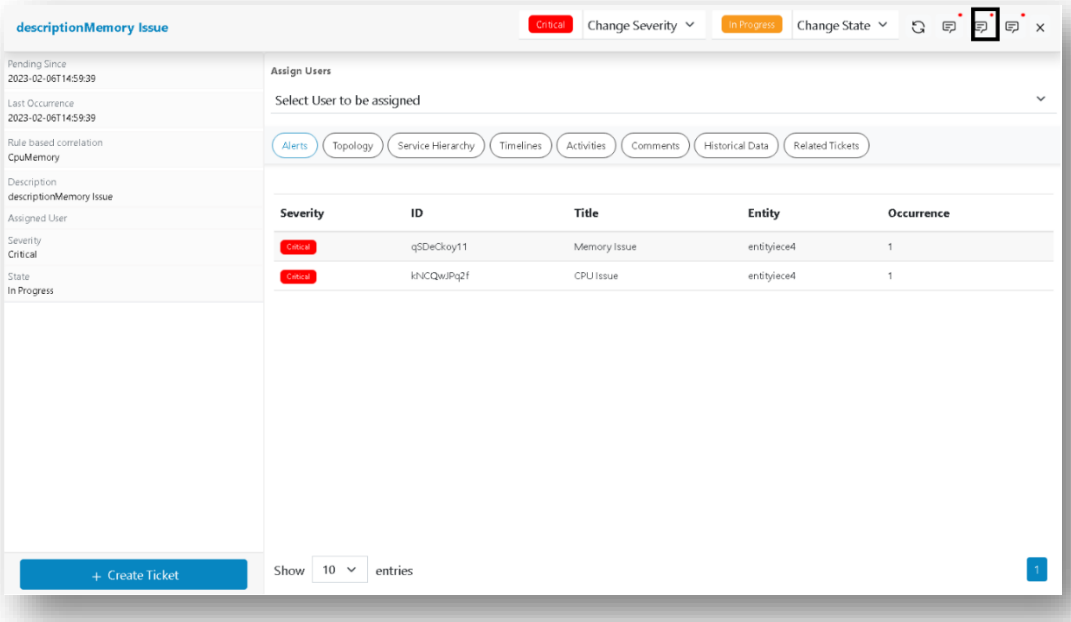

Figure 458 – Update Work Notes for Actionable

3. Click the **Update Work Notes** icon, a confirmation pop-up message will appear.

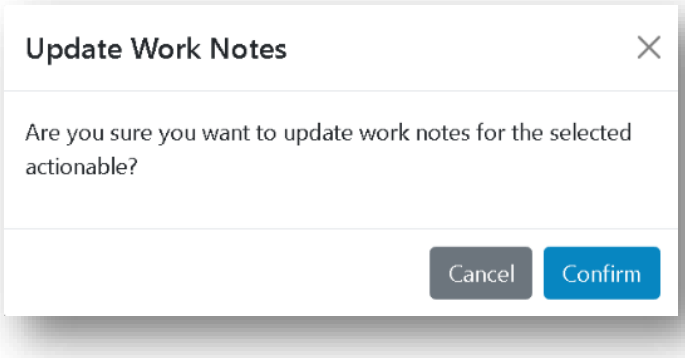

Figure 459 – Update Work Notes for Actionable

4. Click on the **Confirm** button. A success message will appear.

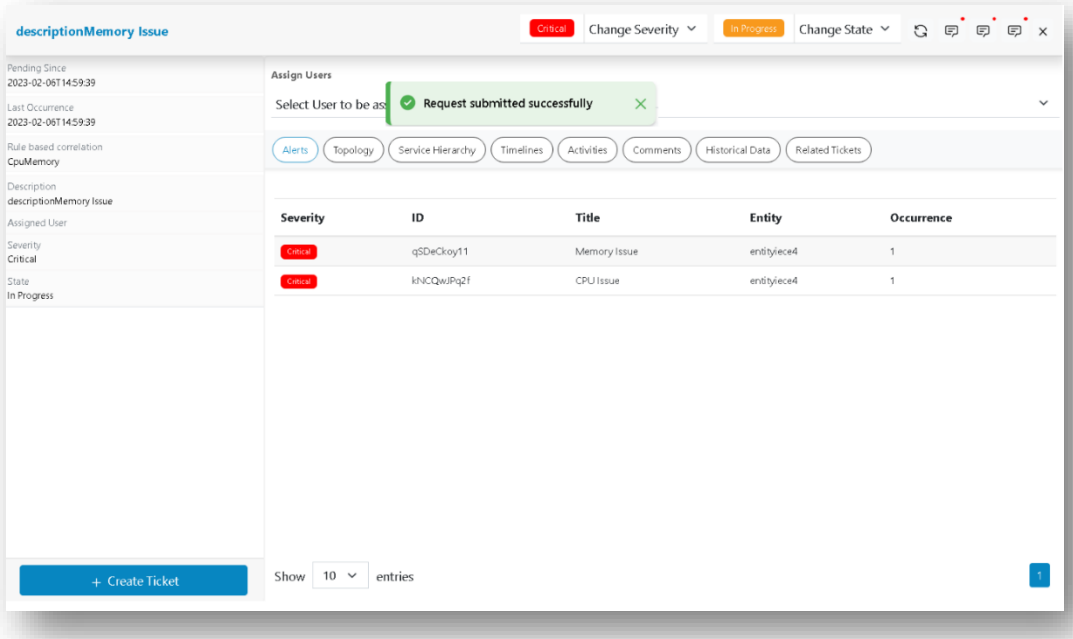

Figure 460 – Alert Message

7.2.3.22 Apply Filters

The steps explain how to apply filter to the actionable data.

1. In the top navigation bar, click on Data View and click on Actionable.
2. Click on the **Apply filter** action button present at the below header of the console.

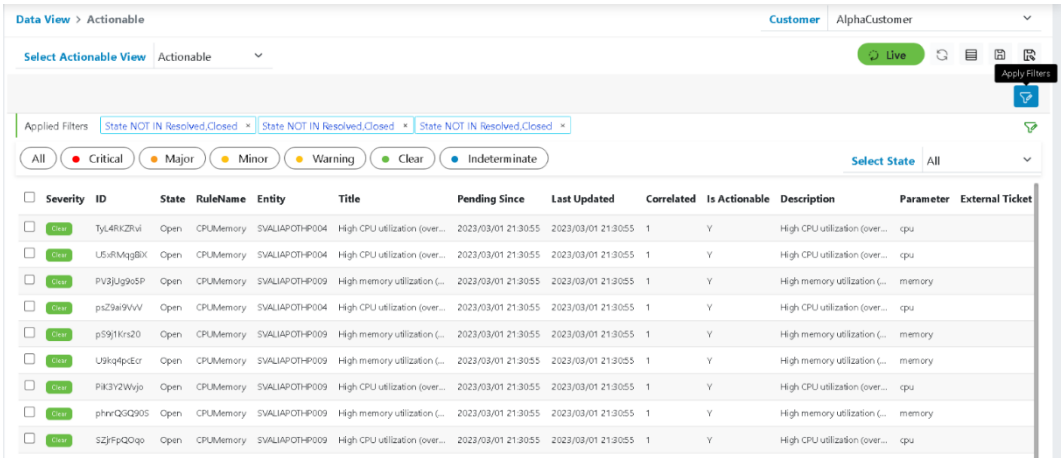

Figure 461 - More Filter Operation

3. A form opens to apply filter. Select **Field** and **Operator** from drop down list and provide **Value**. Then click on the **Apply** button.

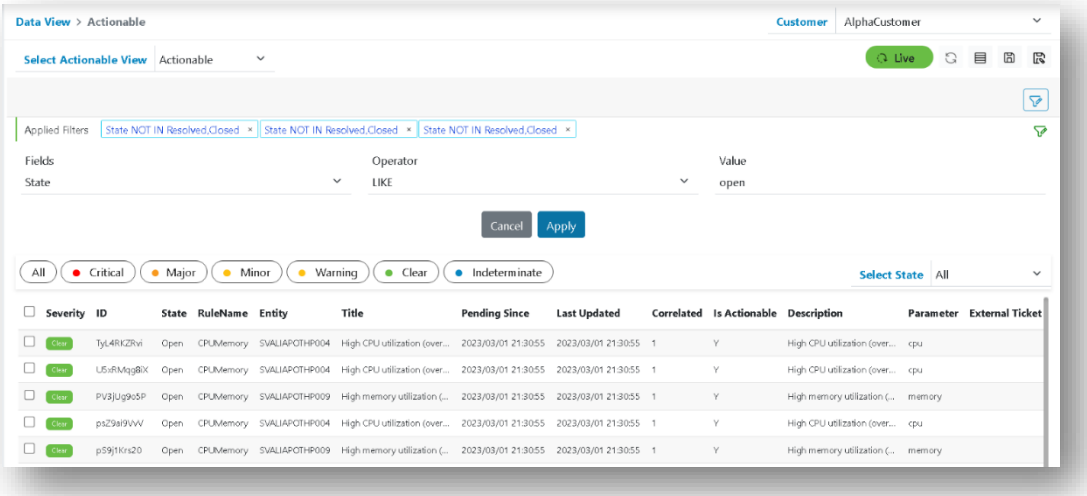

Figure 462 - More Filter Operation

4. User can see the result of applied filter as shown in the following figure:

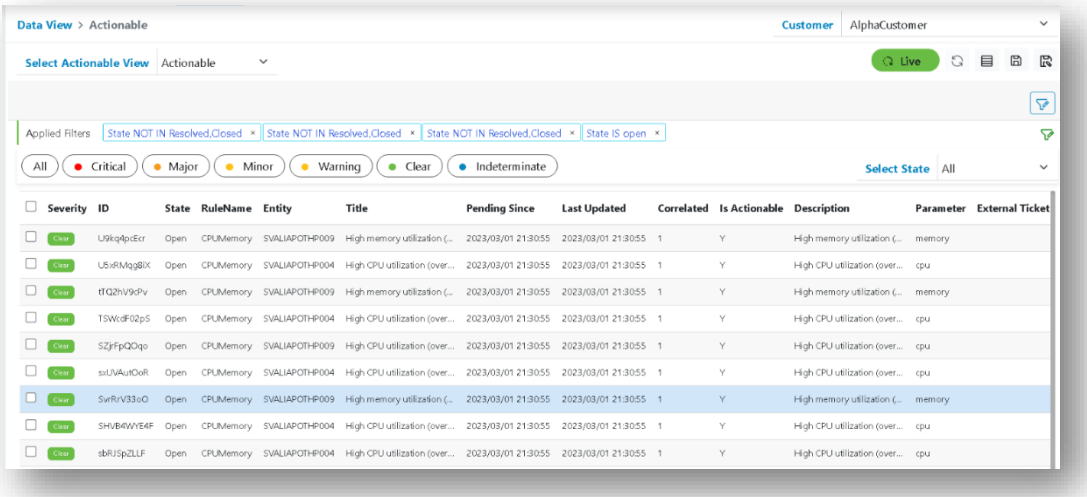

Figure 463 - More Filter Operation

5. Click on the **Select State** dropdown available action button present at the below header of the console.
6. Select state from drop down list. Then click on the state button and user can see the Applied filter based up on the state.

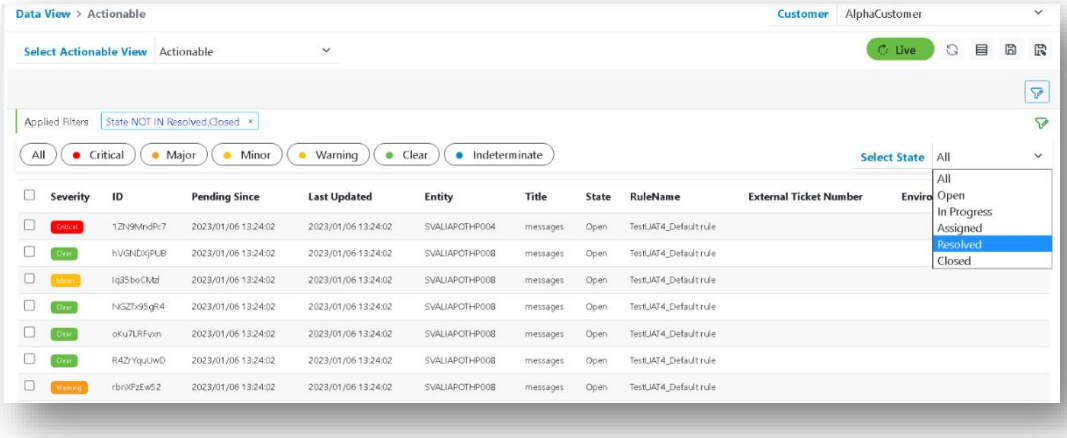

Figure 464– Select State Operation

7.2.3.23 Create Ticket

The steps explain how to Create Ticket for actionable data.

1. Click on an actionable on Data View-Actionable screen, then go to pop up opened for the actionable.
2. Click on the **+ Create Ticket** icon present in the actionable popup.

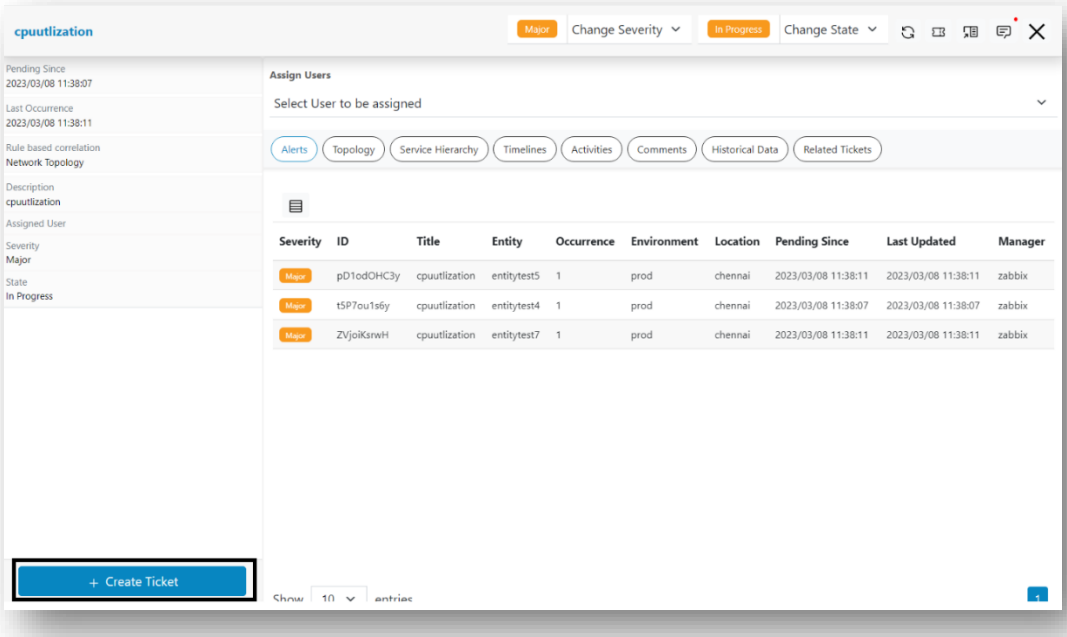

Figure 465 – Update Work Notes for Actionable

3. A confirmation pop-up message will appear.

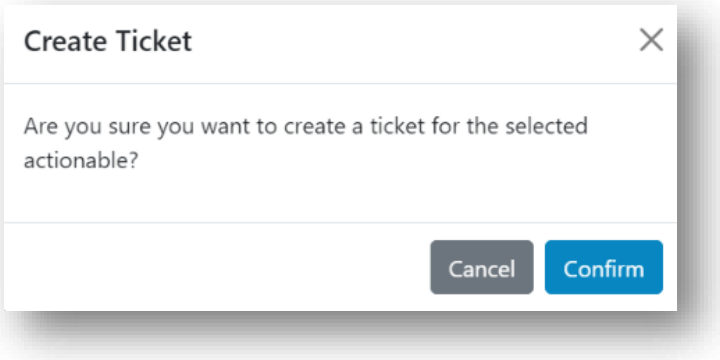

Figure 466 – Update Work Notes for Actionable

4. Click on the **Confirm** button. A success message will appear.

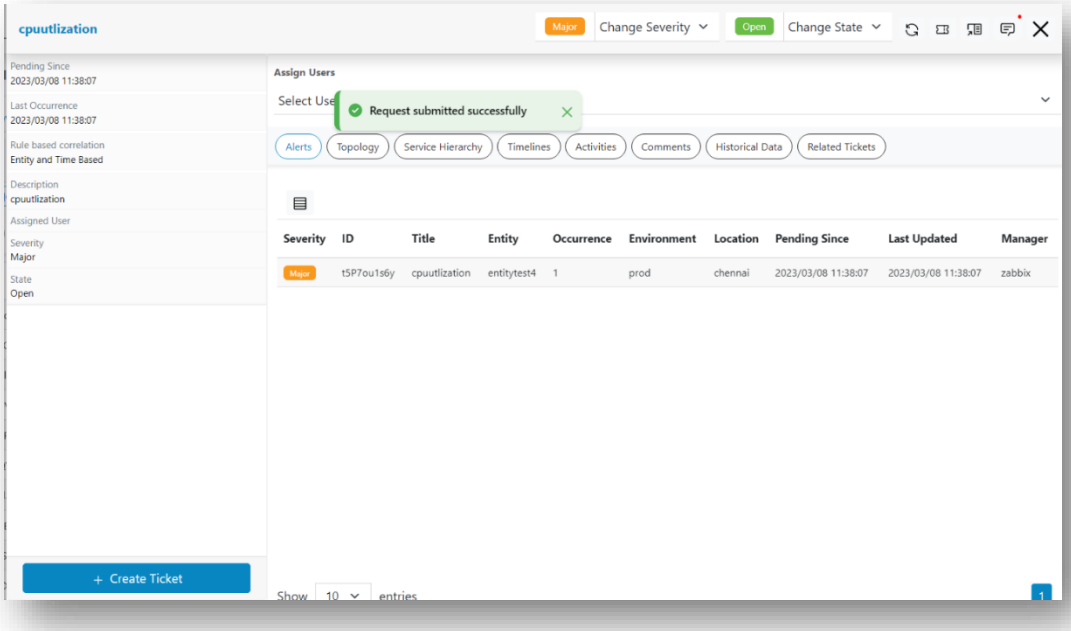

Figure 467 – Alert Message

7.2.4 All Events View

All Events View includes a grid which contains all events data that is coming to the system. It includes noise events as well as non-noise events.

Please follow below steps to view All Events data:

1. In the top navigation bar, click on **Data View** and click on **All Events**.
2. All Events data will be displayed for the customer to which user is part of.

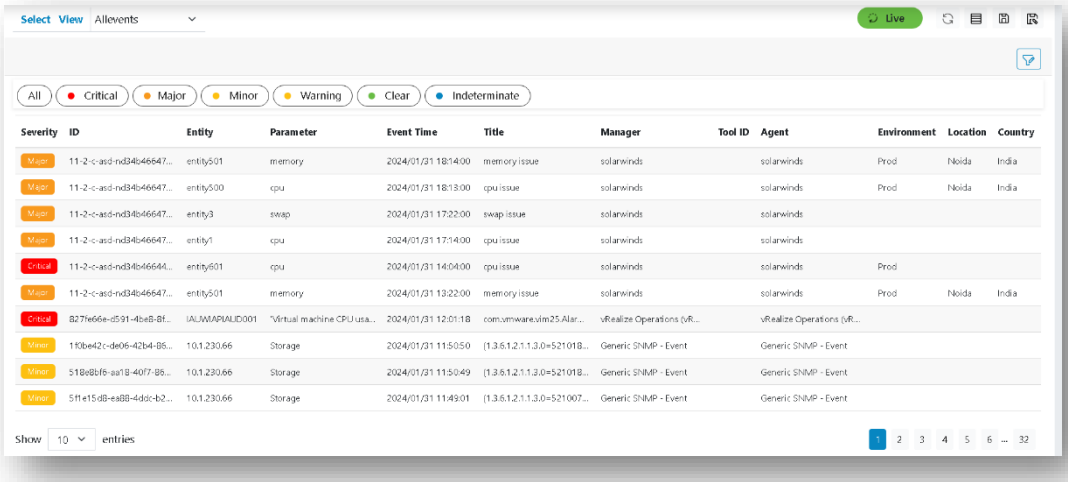

Figure 468 – All Events View

7.2.4.1 Add Column

This option will enable user to add more columns in data grid to analyze it deeply. Please follow below steps to add columns to data view.

1. In the top navigation bar, click on Data View and click on All Events.
2. Click on the Add Column action button present at right side of Live button.
3. A pop-up will open which enables user to select from list of available columns to add it in the grid as shown in figure. Then, click on save button to add selected columns in view.

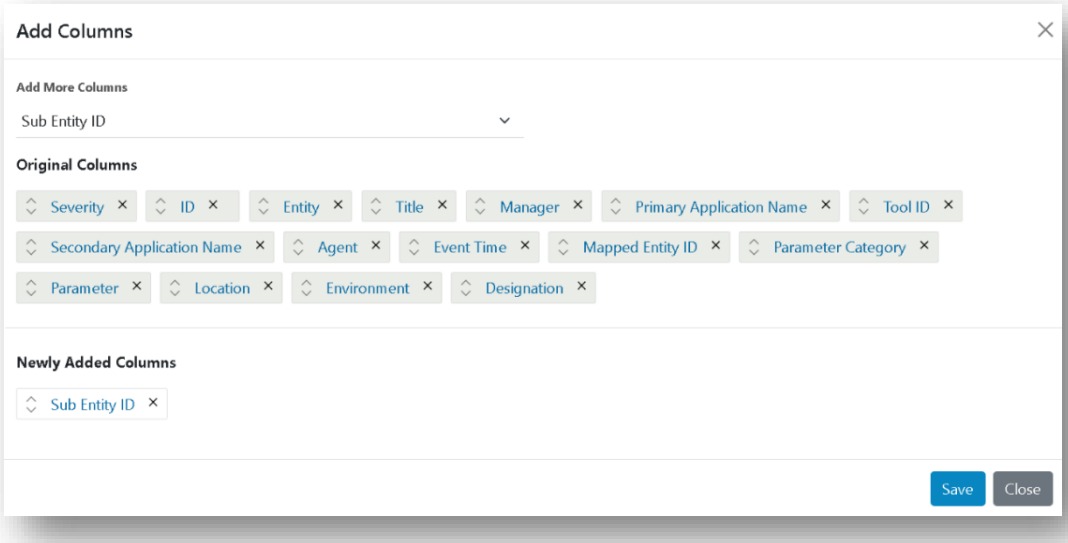

Figure 469 – Add Column

7.2.4.2 Save As All Events

This option will enable user to save currently opened view with columns populated in data grid so that same view can be shown to any other user in an organization. It is very helpful for admins to configure this kind of view for other users in an organization by creating a different view other than current view. For e.g., view to list out all events with critical severity only. Please follow below steps to save as events:

1. In the top navigation bar, click on **Data View** and click on **All Events**.

2. Once the user can click the save as button, a pop-up will open to provide following information:
    - **View Name**: name of view like critical events
    - **Description**: description of view like list all critical events
    - **Show to**: Either it will be visible to user who is saving it or to other users.

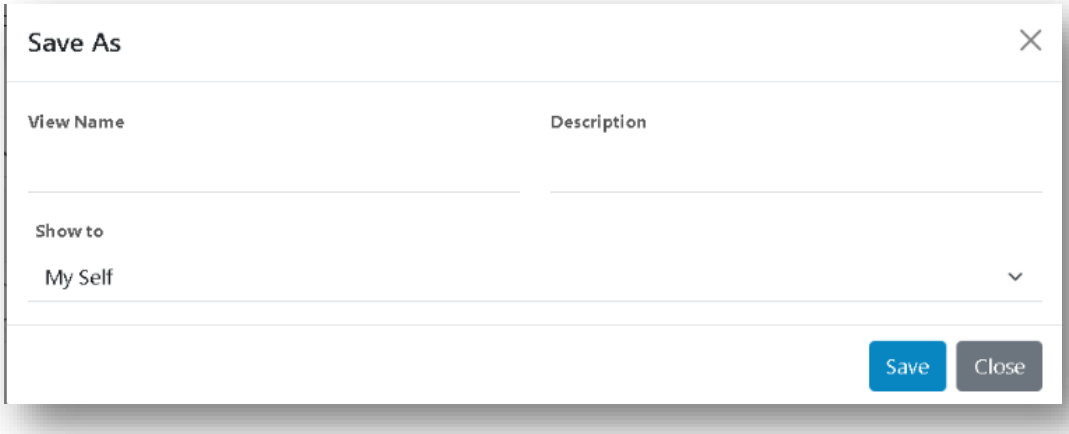

Figure 470 – Save as Events

3. Next, click on save button to save view and this view will be available in list for users.

7.2.4.3 Refresh All Events

This option will enable user to refresh data grid to populate latest data over screen.

Please follow below steps to refresh events grid:

4. In the top navigation bar, click on Data View and click on All Events.
5. Once the user can click the Refresh button, confirmation pop up message will appear.

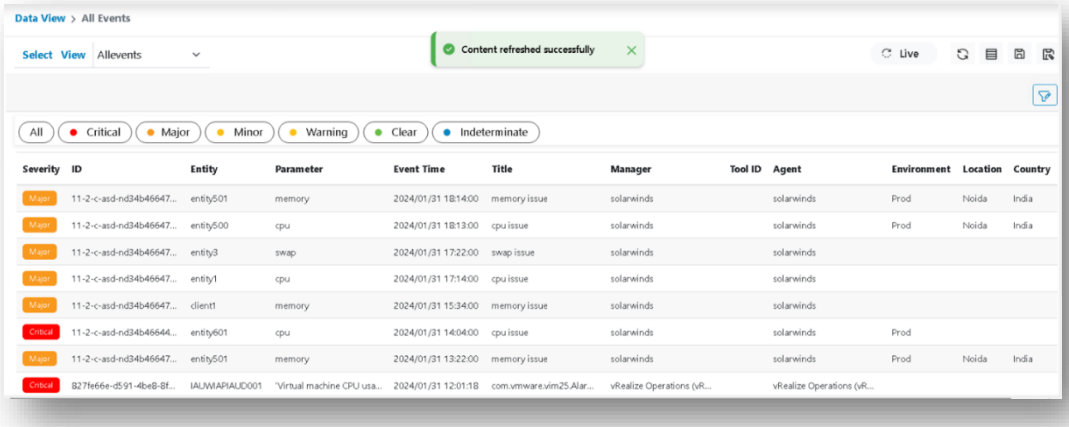

Figure 471 – Refresh All Events

7.2.4.4 Live All Events Data

This option will enable user to stop/start live update of data being shown in grid. Please follow below steps to enable/disable live events.

1. In the top navigation bar, click on Data View and click on All Events.
2. Users can see the Live All Events Data, and this will be updated regularly, and automatically refresh the grid.

7.2.4.5 Apply Filters

This option will enable user to apply filters over currently opened view to see data of specific values. For e.g., to see list of critical events, user can set filters over severity columns of all events 'data. Please follow below steps to apply filters:

1. In the top navigation bar, click on Data View and click on All Events.
2. Click on the filter option present at right side of Live button as shown in figure.

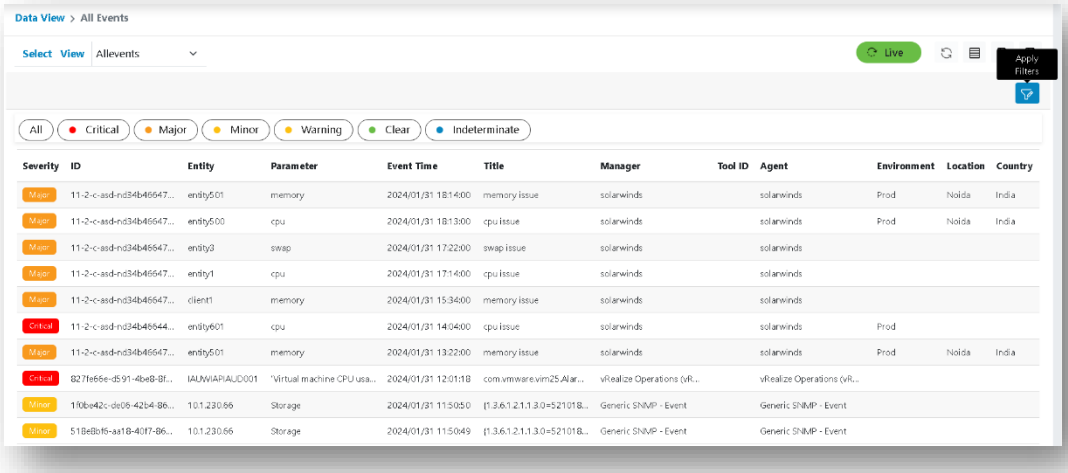

Figure 472 - Filter Operation

3. A filter screen will come up which enables user to select field and corresponding operator along with value to filter data.

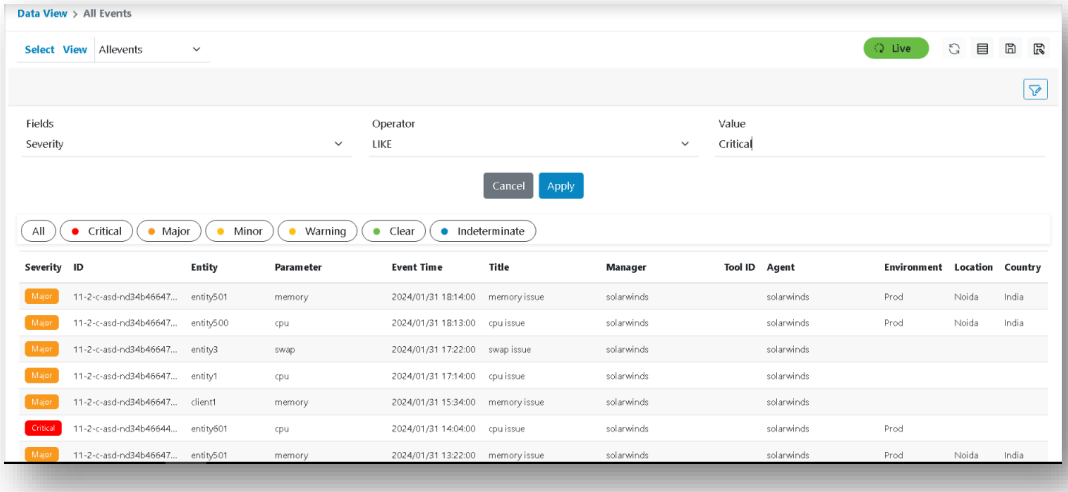

Figure 473 - Filter Operation

4. Users can see the result of applied filter.

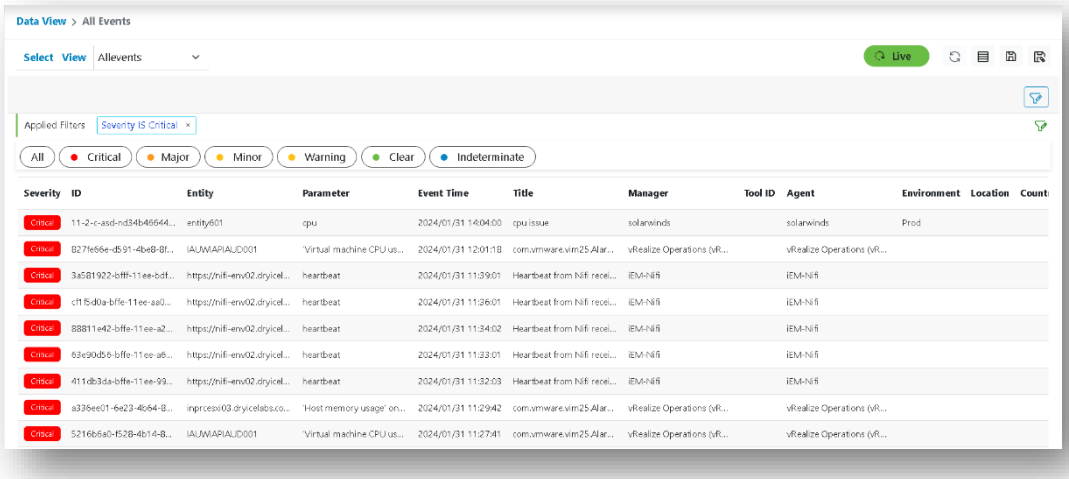

Figure 474 - Filter Operation

7.2.5 Noise Events View

Noise Events View includes a grid which contains all the noise events in a single grid.

Please follow below steps to view Noise Events data:

1. In the top navigation bar, click on Data View and click on Noise Events.
2. Noise Events data will be displayed for the customer to which user is part of.

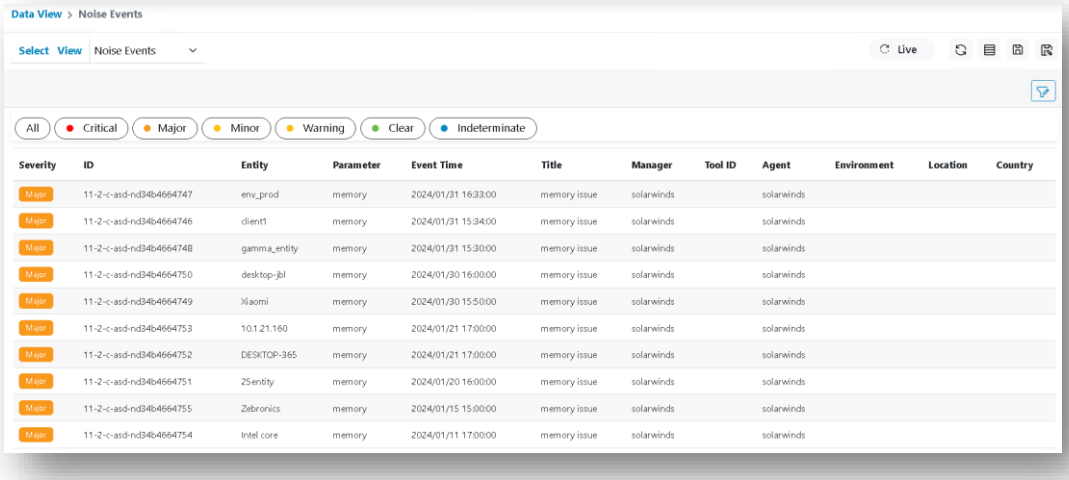

Figure 475 - Noise Events View

7.2.5.1 Add Column

This option will enable user to add more columns in data grid to analyze it deeply. Please follow below steps to add columns to data view.

1. In the top navigation bar, click on Data View and click on Noise Events.
2. Click on the Add Column action button present at right side of Live button.
3. A pop-up will open which enables user to select from list of available columns to add it in the grid as shown in figure. Then, click on save button to add selected columns in view.

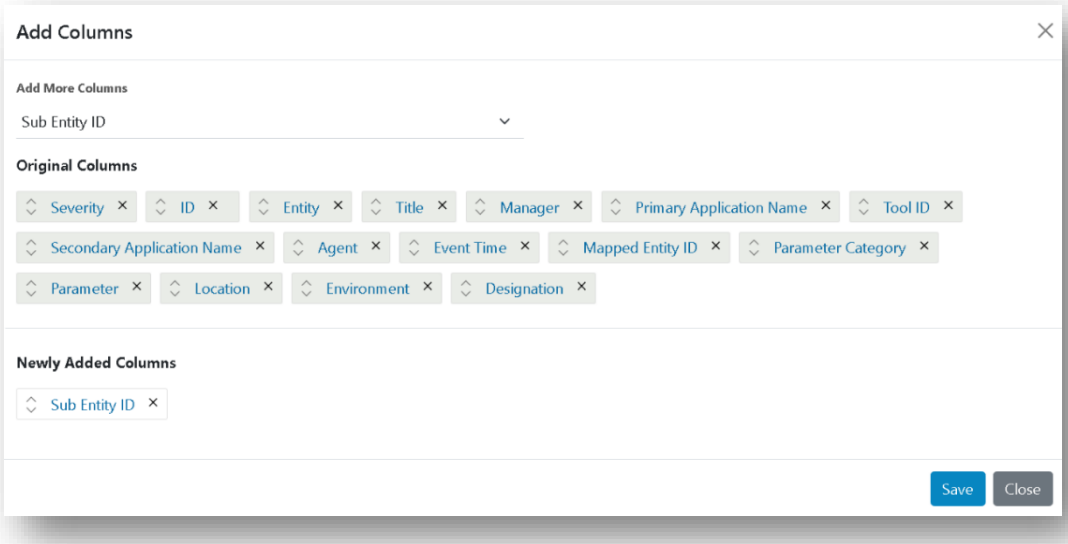

Figure 476 - Add Column

7.2.5.2 Save As Noise Events

This option will enable user to save currently opened view with columns populated in data grid so that same view can be shown to any other user in an organization. It is very helpful for admins to configure this kind of view for other users in an organization by creating a different view other than current view. For e.g., view to list out noise events with critical severity only. Please follow below steps to save as events:

1. In the top navigation bar, click on **Data View** and click on **Noise Events**.
2. Once the user can click the save as button, a pop-up will open to provide following information:
   - View Name: name of view like critical noise events
   - Description: description of view like list all critical noise events
   - Show to: Either it will be visible to user who is saving it or to other users.

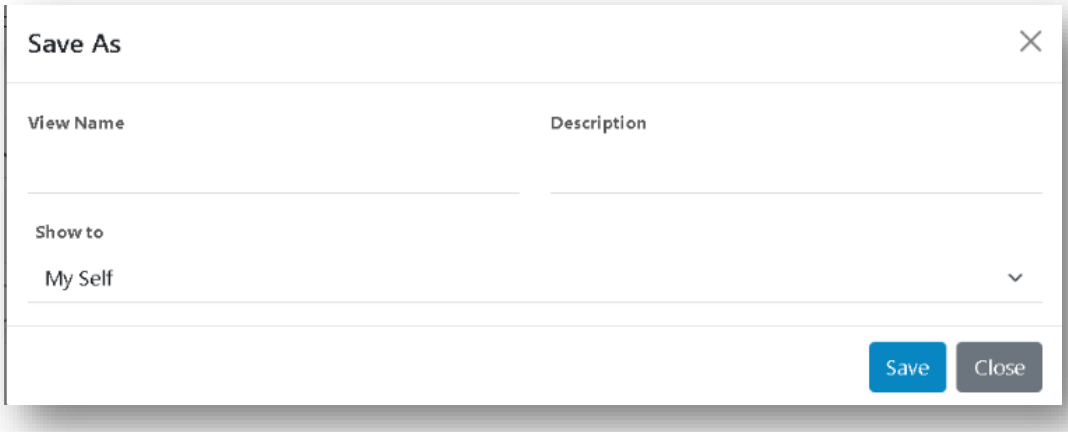

Figure 477 - Save as Events

3. Next, click on save button to save view and this view will be available in list for users.

7.2.5.3 Refresh Noise Events

This option will enable user to refresh data grid to populate latest data over screen.

Please follow below steps to refresh noise events grid:

1. In the top navigation bar, click on Data View and click on Noise Events.
2. Once the user can click the Refresh button, confirmation pop up message will appear.

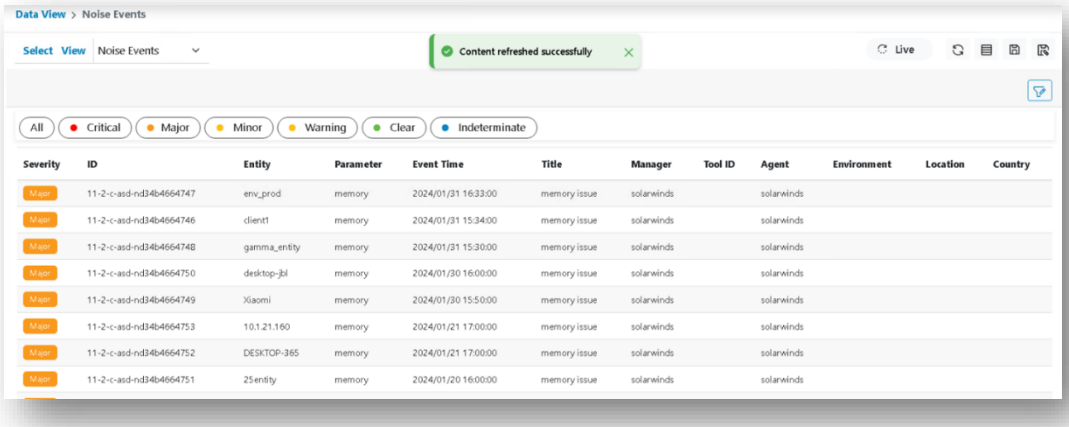

Figure 478 - Refresh Noise Events

7.2.5.4 Live Noise Events Data

This option will enable user to stop/start live update of data being shown in grid. Please follow below steps to enable/disable live noise events.

1. In the top navigation bar, click on **Data View** and click on **Noise Events**.
2. Users can see the Live Noise Events Data, and this will be updated regularly, and automatically refresh the grid.

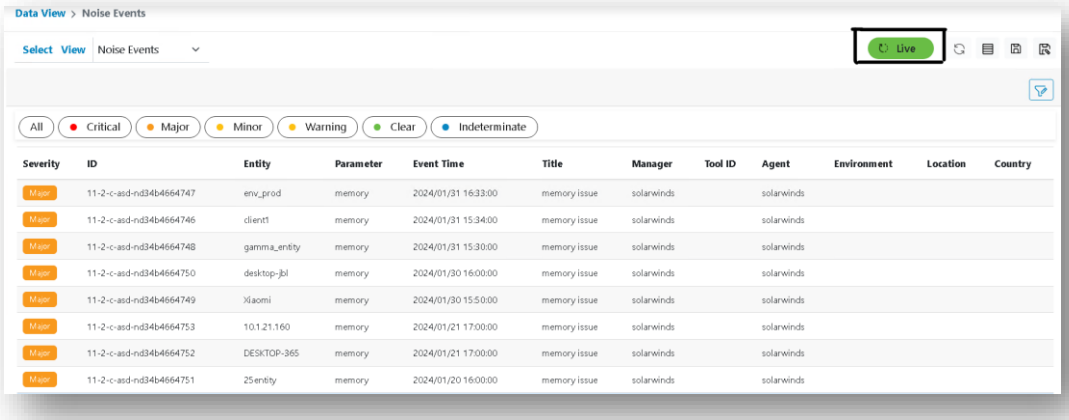

Figure 479 - Live Events Data

3. To stop live data update, please click on Live button, it stops updating the live noise event data, a confirmation message will appear, stating that “Auto – refresh has been disabled.”

7.2.5.5 Apply Filters

This option will enable user to apply filters over currently opened view to see data of specific values. For e.g., to see list of critical noise events, user can set filters over severity columns of noise events data. Please follow below steps to apply filters:

1. In the top navigation bar, click on Data View and click on Noise Events.
2. Click on the filter option present at right side of Live button as shown in figure.

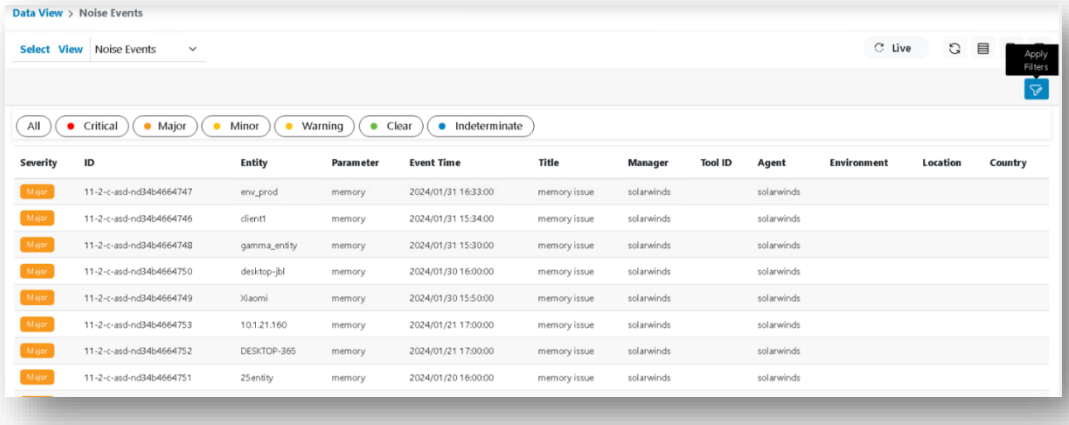

Figure 480 - Filter Operation

3. A filter screen will come up which enables user to select field and corresponding operator along with value to filter data.

8 Integration

8.1 Out Of Box NiFi Connectors Integrations

IMM (Integration Management Module) offers a list of out of box adapters for onboarding in NiFi. Below is the list of adapters with respective required fields.

In case a connector is required to be deleted then it needs to be first deleted from Nifi and then from iMM.

8.1.1 iEM Accumulator (iEA)

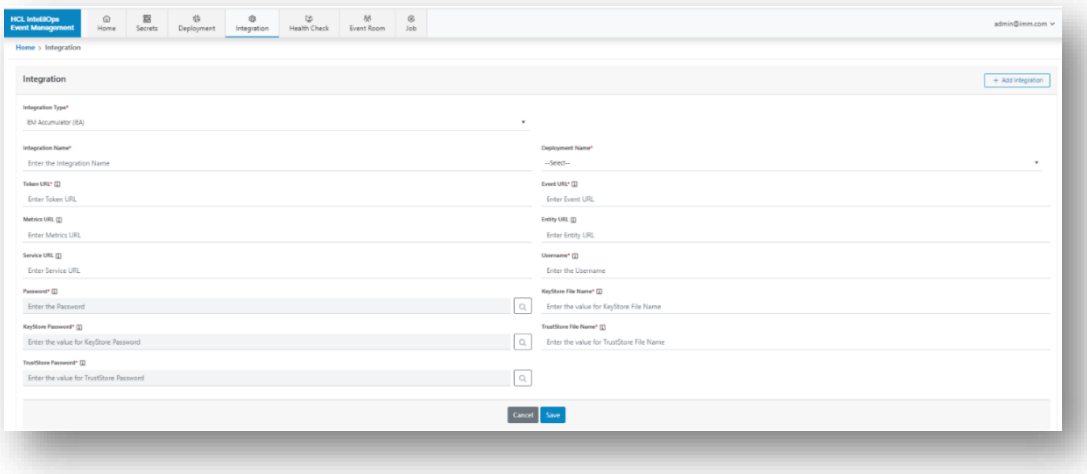

Figure 481 – iEM Accumulator (iEA)

Refer the below table to understand the fields mentioned in the above figure.

Table 4 - iEM Accumulator (iEA) - Integrations Fields

Fields	Description
Integration Name	This fields contains the Integration Name for Integration.
Deployment Name	This fields contains the Deployment name; we can select deployment from all Deployments.
Service URL	iEM Service URL
KeyStore File Name	KeyStore File Name <Path>/keystore.jks
Event URL	iEM Event URL
KeyStore Password	KeyStore Password
Password	iEM API Password
Username	iEM API Username
TrustStore File Name	TrustStore File Name <Path>/truststore.jks
Token URL	iEM Token URL
Metrics URL	iEM Metrics URL
Entity URL	iEM Entity URL
TrustStore Password	TrustStore Password

8.1.2 AppDynamics - Entity

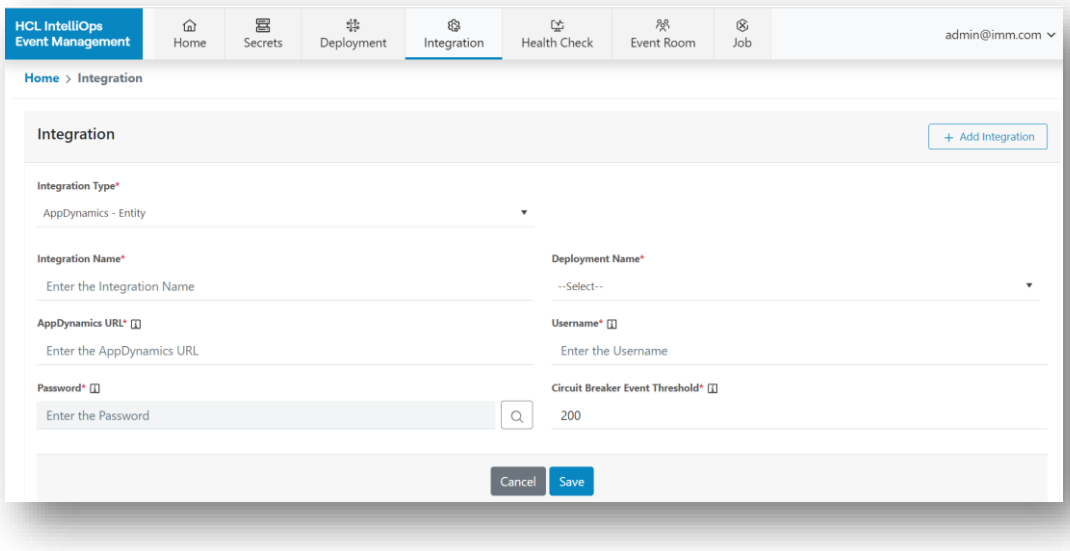

Figure 482 – AppDynamics - Entity

Refer the below table to understand the fields mentioned in the above figure.

Table 5 - AppDynamics - Entity - Integrations Fields

Fields	Description
Integration Name	This fields contains the Integration Name for Integration.
Deployment Name	This fields contains the Deployment name; we can select deployment from all Deployments.
AppDynamics Entity URL	AppDynamics API URL. Eg. https://www.exampledomain.com
Username	Username of the Client API
Password	User Password of the Client API
Circuit Breaker Event Threshold	Circuit breaker Event Threshold Value: Min value: 100, Max value: 90000

8.1.3 AppDynamics – Event

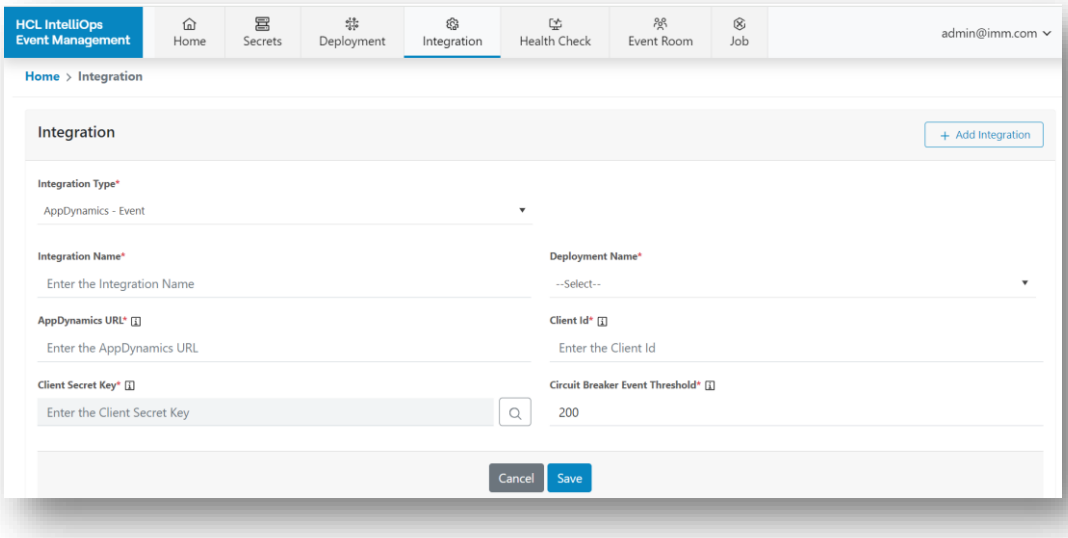

Figure 483 – AppDynamics - Event

Refer the below table to understand the fields mentioned in the above figure.

Table 6 - AppDynamics - Event - Integrations Fields

Fields	Description
Integration Name	This fields contains the Integration Name for Integration.
Deployment Name	This fields contains the Deployment name; we can select deployment from all Deployments.
Client Id	Name of the API Client
Circuit Breaker Event Threshold	Circuit breaker Event Threshold Value: Min value: 100, Max value: 90000
AppDynamics URL	AppDynamics API URL. http://<controller_host>:<controller_port>/controller/rest/<REST_URI>
Client Secret Key	UUID as the Secret of API Client (Password)

8.1.4 AppDynamics - Metrics

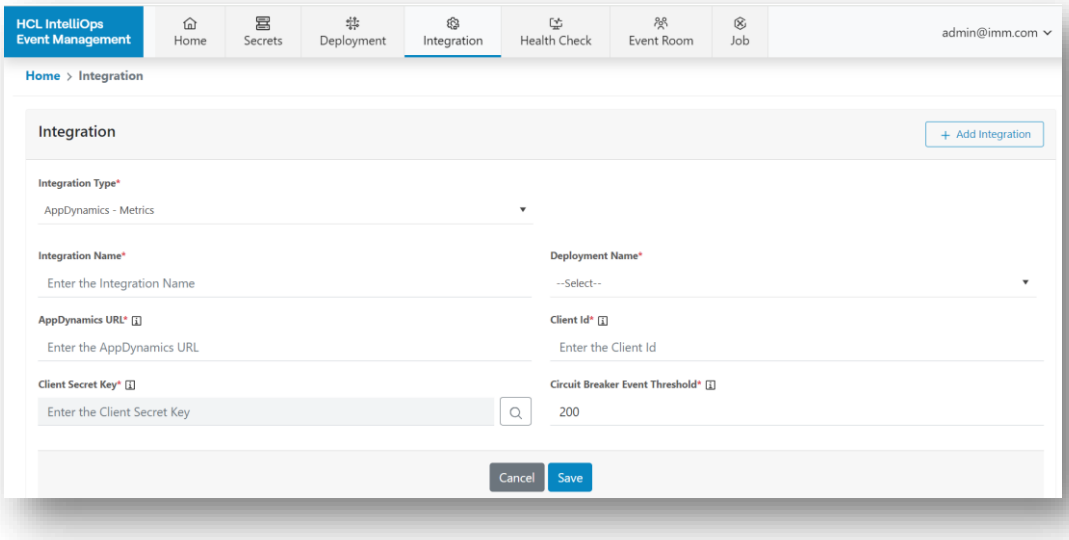

Figure 484 – AppDynamics - Metrics

Refer the below table to understand the fields mentioned in the above figure.

Table 7 - AppDynamics – Metrics - Integrations Fields

Fields	Description
Integration Name	This fields contains the Integration Name for Integration.
Deployment Name	This fields contains the Deployment name; we can select deployment from all Deployments.
Client Id	Name of the API Client
AppDynamics Metrics URL	Syntax of Metrics API http://<App Dynamics Server>/controller/rest/applications/<Application name>/metrics
Circuit Breaker Event Threshold	Circuit breaker Event Threshold Value: Min value: 100, Max value: 90000
Client Secret Key	UUID as the Secret of API Client (Password)

8.1.5 Datadog – Event

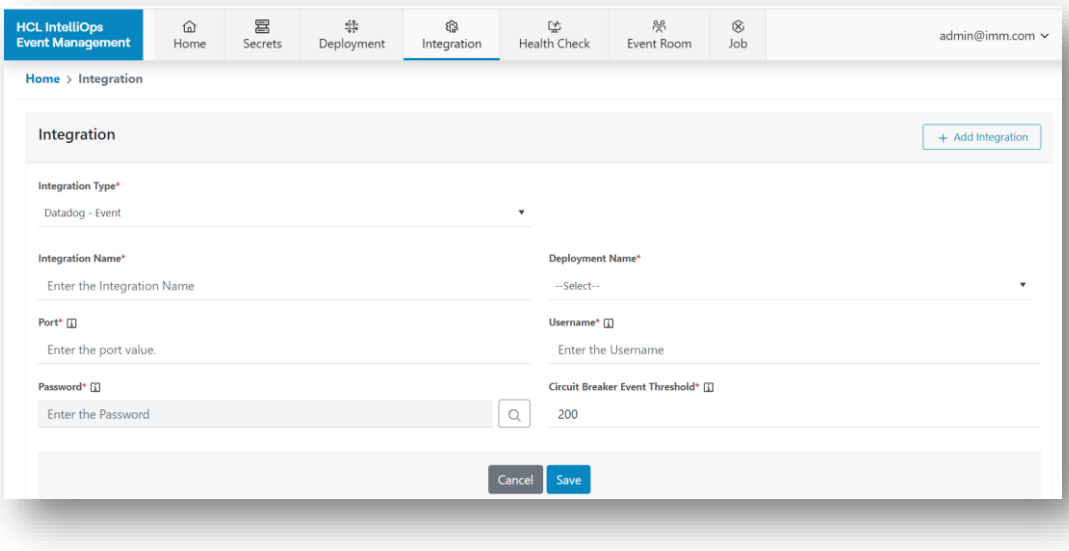

Figure 485 – Datadog - Event

Refer the below table to understand the fields mentioned in the above figure.

Table 8 – Datadog – Event - Integrations Fields

Fields	Description
Integration Name	This fields contains the Integration Name for Integration.
Deployment Name	This fields contains the Deployment name; we can select deployment from all Deployments.
Port	Webhook Port for Events Ingestion
Circuit Breaker Event Threshold	Circuit breaker Event Threshold Value: Min value: 100, Max value: 90000
Username	User Credentials with Webhook Access
Password	User Credentials with Webhook Access

8.1.6 Dynatrace – Event

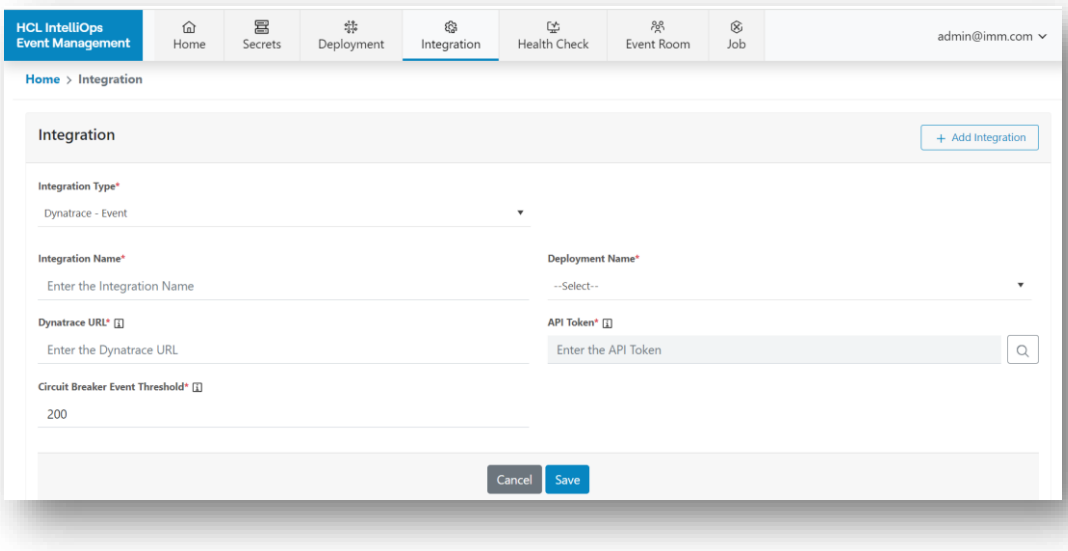

Figure 486 – Dynatrace - Event

Refer the below table to understand the fields mentioned in the above figure.

Table 9 – Dynatrace – Event - Integrations Fields

Fields	Description
Integration Name	This fields contains the Integration Name for Integration.
Deployment Name	This fields contains the Deployment name; we can select deployment from all Deployments.
Circuit Breaker Event Threshold	Circuit breaker Event Threshold Value: Min value: 100, Max value: 90000
Dynatrace URL	Dynatrace API URL. Eg. https://www.exampledomain.com:8080
API Token	Dynatrace uses a unique token format consisting of three components separated by dots (.).

8.1.7 Generic Rest – Event

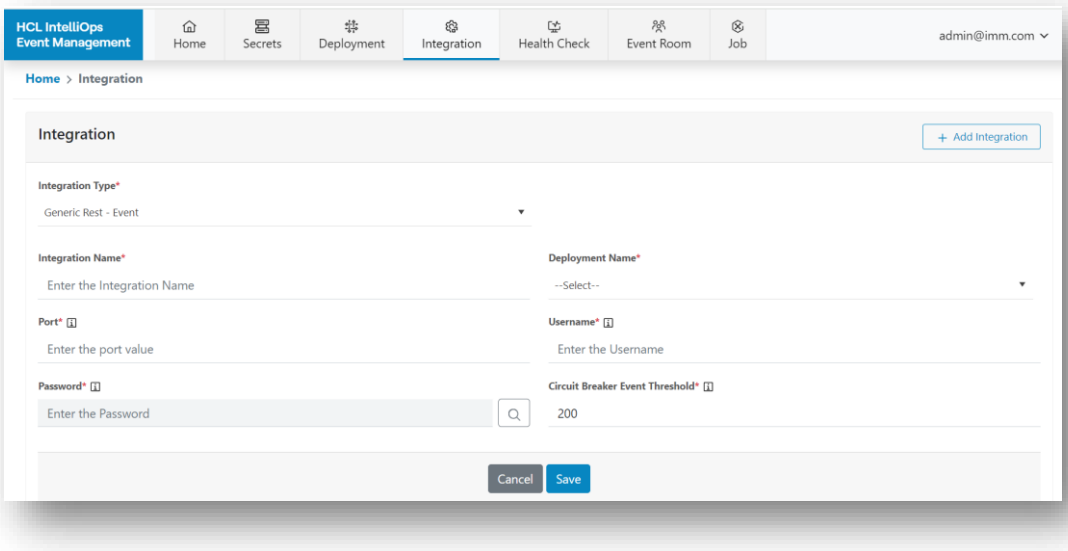

Figure 487 – Generic Rest - Event

Refer the below table to understand the fields mentioned in the above figure.

Table 10 – Generic Rest - Event - Integrations Fields

Fields	Description
Integration Name	This fields contains the Integration Name for Integration.
Deployment Name	This fields contains the Deployment name; we can select deployment from all Deployments.
Circuit Breaker Event Threshold	Circuit breaker Event Threshold Value: Min value: 100, Max value: 90000
Port	Port for Generic REST API
Username	REST Username
Password	REST Password

8.1.8 LogicMonitor – Event

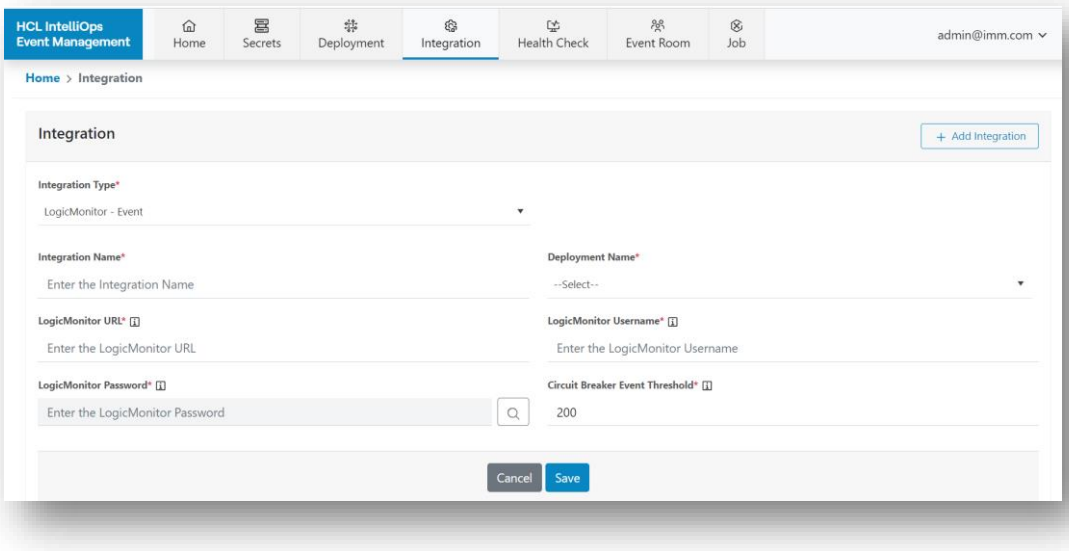

Figure 488 –LogicMonitor – Event

Refer the below table to understand the fields mentioned in the above figure.

Table 11 –LogicMonitor – Event - Integrations Fields

Fields	Description
Integration Name	This fields contains the Integration Name for Integration.
Deployment Name	This fields contains the Deployment name; we can select deployment from all Deployments.
LogicMonitor Username	Events API Username
Circuit Breaker Event Threshold	Circuit breaker Event Threshold Value: Min value: 100, Max value: 90000
LogicMonitor URL	LogicMonitor API URL Syntax https://<ACCOUNTNAME>.logicmonitor.com/santaba/rest
LogicMonitor Password	Events API Password

8.1.9 New Relic – Event

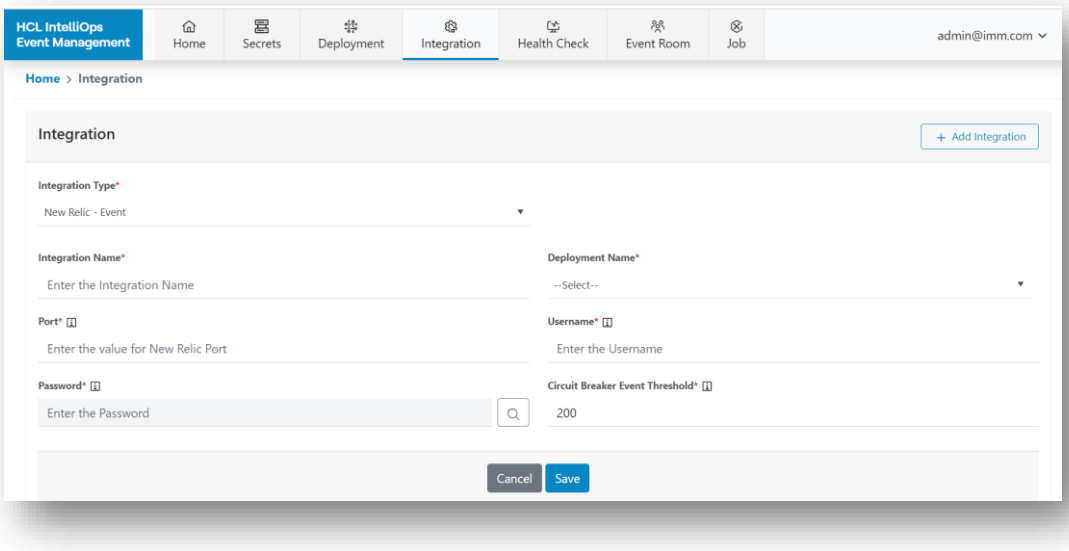

Figure 489 – New Relic - Event

Refer the below table to understand the fields mentioned in the above figure.

Table 12 – New Relic – Event - Integrations Fields

Fields	Description
Integration Name	This fields contains the Integration Name for Integration.
Deployment Name	This fields contains the Deployment name; we can select deployment from all Deployments.
Username	User Credentials with Webhook Access
Circuit Breaker Event Threshold	Circuit breaker Event Threshold Value: Min value: 100, Max value: 90000
Port	Webhook Port for Events Ingestion
Password	User Credentials with Webhook Access

8.1.10 NiFi-iEM HeartBeat

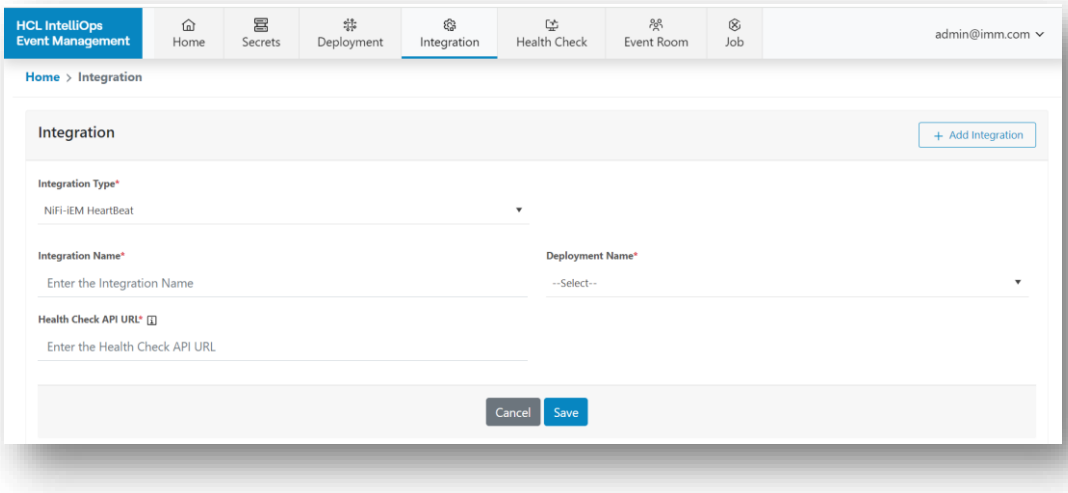

Figure 490 – NiFi-iEM HeartBeat

Refer the below table to understand the fields mentioned in the above figure.

Table 13 NiFi-iEM HeartBeat - Integrations Fields

Fields	Description
Integration Name	This fields contains the Integration Name for Integration.
Deployment Name	This fields contains the Deployment name; we can select deployment from all Deployments.
Health Check API URL	iEM Health Check API URL

8.1.11 ServiceNow – Service

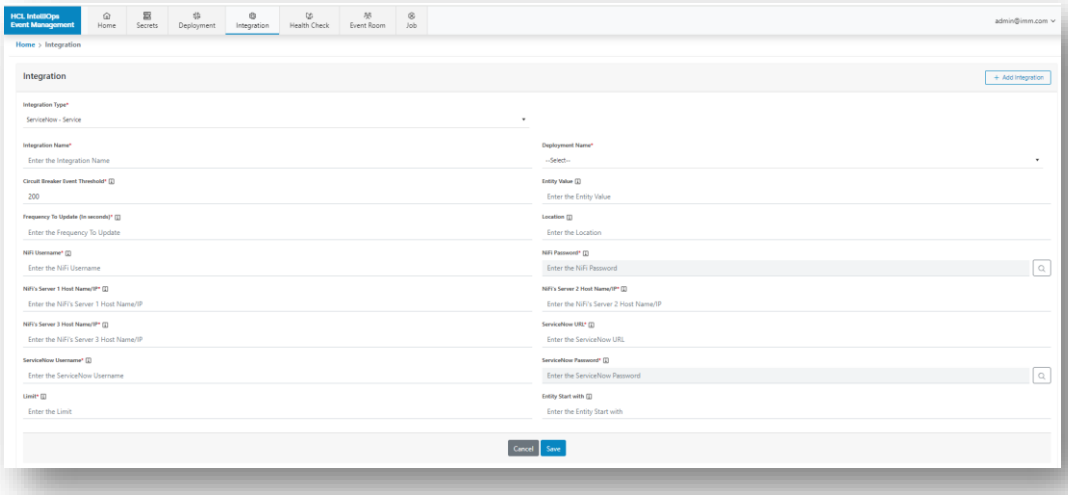

Figure 491 – ServiceNow - Service

Refer the below table to understand the fields mentioned in the above figure.

Table 14 – ServiceNow – Service - Integrations Fields

Fields	Description
Integration Name	This fields contains the Integration Name for Integration.

Deployment Name	This fields contains the Deployment name; we can select deployment from all Deployments.
Location	Location of the Source Integration
Limit	Max value should not be more than 150.
NiFi Username	NiFi Username
Circuit Breaker Event Threshold	Circuit breaker Event Threshold Value: Min value: 100, Max value: 90000
Frequency To Update	Frequency To Execute the API again (In seconds)
Entity Value	Entity Value
NiFi's Server 2 Host Name/IP	NiFi's Server 2 Host Name/IP
NiFi's Server 1 Host Name/IP	NiFi's Server 1 Host Name/IP
NiFi Password	NiFi Password
Entity Start with	To apply filter on Entity Name
ServiceNow Password	ServiceNow CMDB Password
ServiceNow Username	ServiceNow CMDB Username
NiFi's Server 3 Host Name/IP	NiFi's Server 3 Host Name/IP
ServiceNow URL	ServiceNow CMDB API URL. Eg. https://www.exampledomain.com

8.1.12 SolarWinds Hybrid Cloud Observability – Event

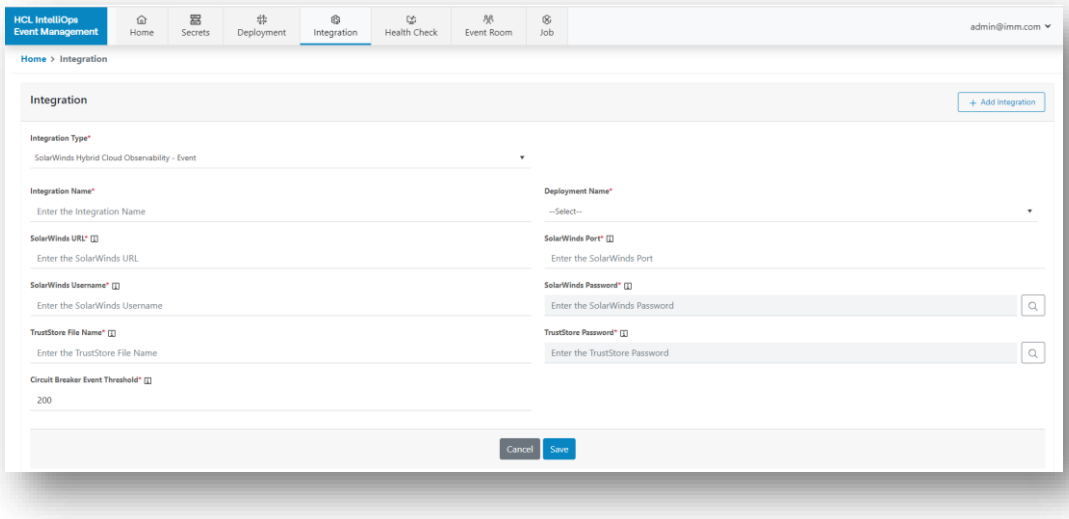

Figure 492 – SolarWinds Hybrid Cloud Observability - Event

Refer the below table to understand the fields mentioned in the above figure.

Table 15 – SolarWinds Hybrid Cloud Observability – Event - Integrations Fields

Fields	Description
Integration Name	This fields contains the Integration Name for Integration.

Deployment Name	This fields contains the Deployment name; we can select deployment from all Deployments.
SolarWinds Username	Events API Username
SolarWinds URL	SolarWinds API URL. https://<subdomain>.loggly.com/apiv2/events/iterate
SolarWinds Port	SolarWinds Port
Trust Store Password	Trust Store Password
SolarWinds Password	Events API Password
Circuit Breaker Event Threshold	Circuit breaker Event Threshold Value: Min value: 100, Max value: 90000
Trust Store File Name	TrustStore File Name (provided by HCL PS Team) <Path>/truststore.jks

8.1.13 SolarWinds Hybrid Cloud Observability – Metrics

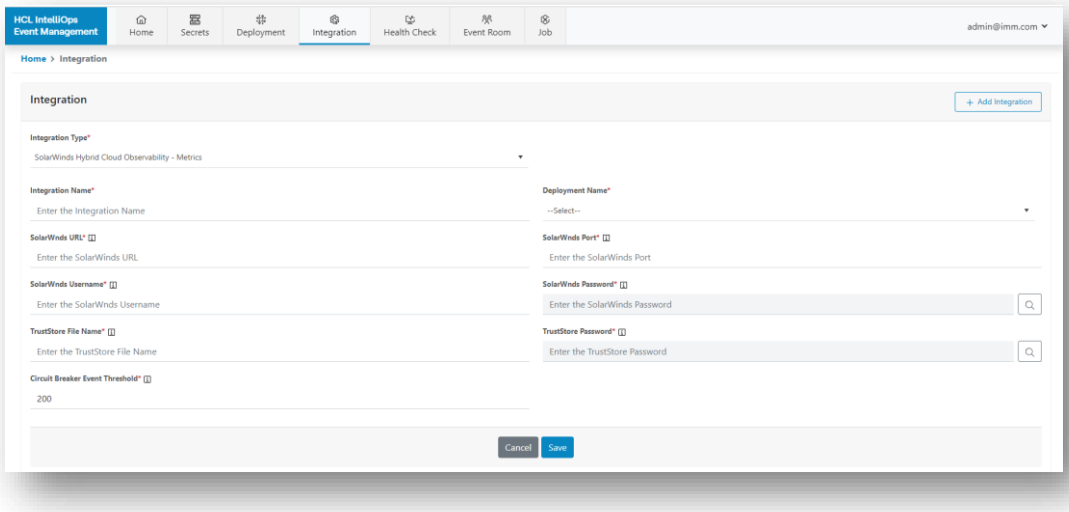

Figure 493 –SolarWinds Hybrid Cloud Observability - Metrics

Refer the below table to understand the fields mentioned in the above figure.

Table 16 –SolarWinds Hybrid Cloud Observability – Metrics - Integrations Fields

Fields	**Description**
Integration Name	This fields contains the Integration Name for Integration.
Deployment Name	This fields contains the Deployment name; we can select deployment from all Deployments.
Solarwind Username	Metrics API Username
Solarwind URL	Solarwinds API URL. Syntax: https://<SUBDOMAIN>.loggly.com/apiv2/volume-metrics
Solarwind Port	Metrics API Port
Solarwind Password	Metrics API Password

Circuit Breaker Event Threshold	Circuit breaker Event Threshold Value: Min value: 100, Max value: 90000
TrustStore File Name	TrustStore File Name <Path>/truststore.jks
TrustStore Password	<Path>/truststore.jks

8.1.14 Zabbix – Event

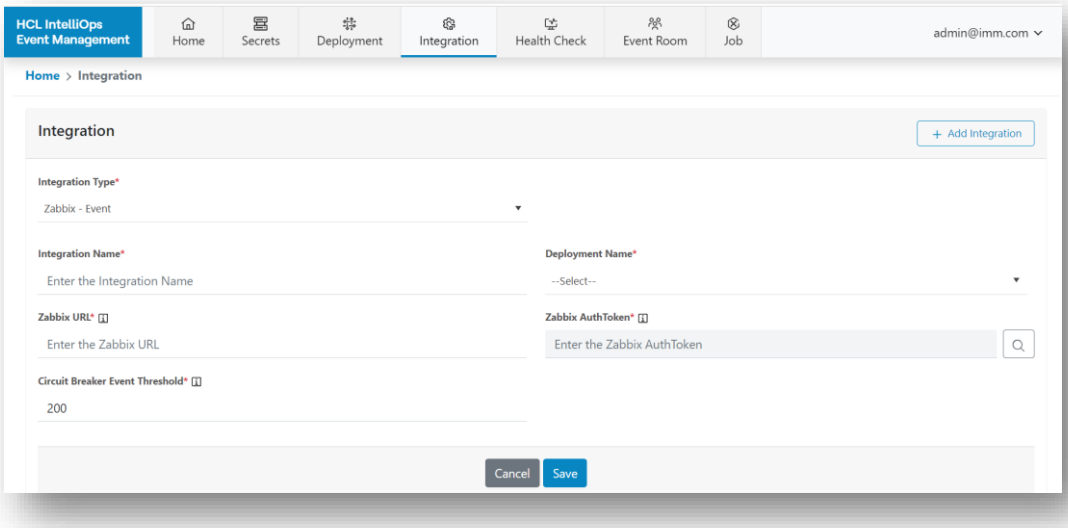

Figure 494 – Zabbix - Event

Refer the below table to understand the fields mentioned in the above figure.

Table 17 – Zabbix – Event - Integrations Fields

Fields	Description
Integration Name	This fields contains the Integration Name for Integration.
Deployment Name	This fields contains the Deployment name; we can select deployment from all Deployments.
Circuit Breaker Event Threshold	Circuit breaker Event Threshold Value: Min value: 100, Max value: 90000
Zabbix AuthToken	Authentication Token for API call
Zabbix URL	Zabbix API URL. Eg. https://www.exampledomain.com

8.1.15 vRealize Operations (vROps) - Event

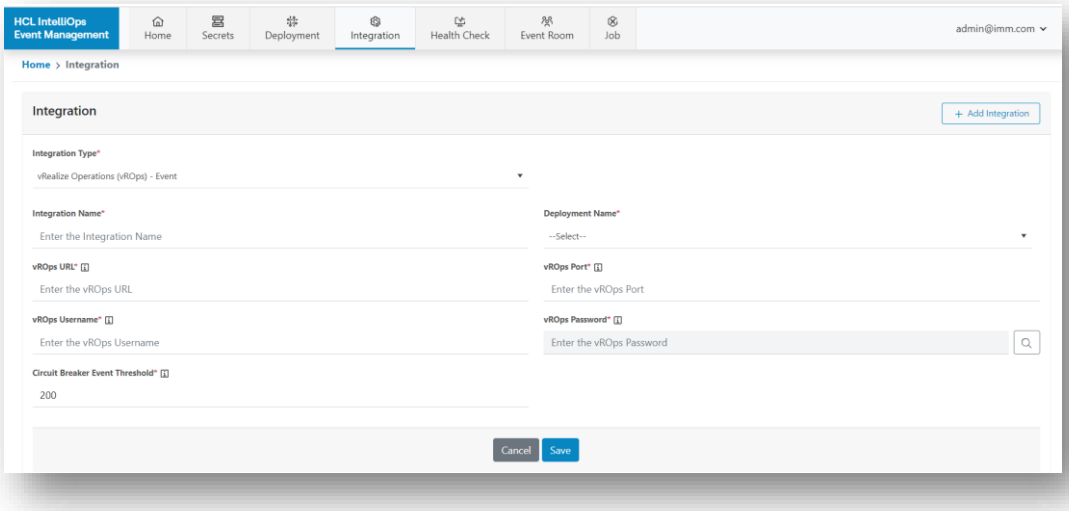

Figure 495 – vRealize Operations (vROps) - Event

Refer the below table to understand the fields mentioned in the above figure.

Table 18 – vRealize Operations (vROps) – Event - Integrations Fields

Fields	Description
Integration Name	This fields contains the Integration Name for Integration.
Deployment Name	This fields contains the Deployment name; we can select deployment from all Deployments.
Circuit Breaker Event Threshold	Circuit breaker Event Threshold Value: Min value: 100, Max value: 90000
Vrops Password	vROps API Password
Vrops Port	vROps API Port
Vrops Username	vROps API Username
Vrops URL	vROps API URL. Syntax https://<VROPS>/suite-api/

9 Glossary of Terms

9.1 Key Terminology Used in IEM

Table 19 – Key Terminology Used in IEM

IEM	IntelliOps Event Management
IMM	Integration Management Module
IEA	IntelliOps Events Accumulator
ETL	Extract, Transform, Load
AI	Artificial Intelligence
OOB	Out of the Box
NiFi	Apache NiFi (short for Niagara Files)
JVM	Java Virtual Machine
API	Application Programming Interface
UI	User Interface
NIC	Network Interface Card
SSD	Solid State Drive
CPU	Central Processing Unit
SNMP	Simple Network Management Protocol
FQDN	Fully Qualified Domain Name
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
CI	Configuration Item
CMDB	Configuration Management Database
PoC	Proof of Concept
IT	Information Technology
ITSM	IT Service Management
AIML	Artificial Intelligence and Machine Learning
SSO	Single Sign-On
SAML	Security Assertion Markup Language

HCLSoftware

hcltechsw.com