

**Oracle® Communications
EAGLE Element Management System**

Interface User's Guide

Release 46.0

E54393 Revision 2

January 2015

Oracle® Communications Interface User's Guide, Release 46.0

Copyright © 2013, 2015, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Table of Contents

Chapter 1: Introduction.....	17
Overview.....	18
Scope and Audience.....	18
Documentation Admonishments.....	18
Manual Organization.....	19
My Oracle Support (MOS).....	19
Emergency Response.....	20
Related Publications.....	20
Customer Training.....	21
Locate Product Documentation on the Oracle Technology Network Site.....	21
Chapter 2: E5-MS Administration.....	22
E5-MS Administration.....	23
E5-MS Initialization and First Configuration.....	23
Chapter 3: E5-MS Functional Description.....	24
E5-MS Overview.....	25
E5-MS Architecture.....	26
E5-MS Applications.....	26
E5-MS Security Tools.....	29
E5-MS Ports Usage and Firewall Configuration.....	30
Workstation Requirements.....	31
EAGLE Baseline Hardware	32
Chapter 4: E5-MS Graphical User Interface.....	33
Overview	34
E5-MS Login.....	34
Logging In to E5-MS.....	34
Login Page Elements.....	36
E5-MS Applications Main View	36
Menu Bar.....	36
Toolbar Icons.....	38

Alarm Summary View.....	41
Alarm Severity Representation	42
Chapter 5: EAGLE Discovery Application.....	43
Overview.....	44
Functional Description	44
EAGLE Discovery.....	44
User Access Control.....	44
Validation.....	45
Discovery GUI.....	45
Existing EAGLE(s).....	47
Add an EAGLE System	48
Active and Standby OAMs Switch.....	49
IP Address	49
Protocol.....	50
Country and City.....	50
Fault Interfaces.....	51
TL1.....	51
Active and Standby OAMs Switch.....	51
SNMP.....	51
Schedule Management Screen	52
Map Views	52
Adding a new country map to E5-MS.....	60
Map View Features.....	61
Inventory Management.....	62
Existing EAGLE(s).....	63
Inventory Commands	64
Chapter 6: E5-MS Support of EPAP Alarms via SNMP Feed.....	66
Overview.....	67
EPAP Nodes.....	67
EPAP Discovery Menu.....	68
Map Views.....	72
Cut Through Interface from Maps to EPAP.....	73
Fault Management.....	74
Chapter 7: E5-MS Support of LSMS Alarms via SNMP Feed.....	80
Overview.....	81
LSMS Nodes.....	81

LSMS Discovery Menu.....	82
Map Views.....	84
Cut Through Interface from Maps to LSMS.....	86
Fault Management.....	86
Chapter 8: Fault Management.....	90
Overview.....	91
External E5-MS Applications.....	91
Functional Description.....	91
Events and Alarms Viewer	93
Event and Notification Details.....	93
Alarm Correlations Rules.....	95
Alarm Correlation and Aggregation.....	97
Southbound Resynchronization.....	98
Buffer Incoming UAM Details.....	98
Alarm Acknowledgement and Clear.....	99
Alarm Acknowledgement.....	99
Alarm Unacknowledged	100
Alarm Clear Event	100
Alarm Maintenance Mode.....	101
Setup Alarm in Maintenance Mode.....	101
Setup Alarm in Active Mode from Maintenance Mode.....	101
IPSM Switching.....	102
IPSM Switching Algorithm.....	102
Alarm Raising Rule.....	103
Limitation.....	104
SNMP Active/Standby OAM Switching.....	104
Fault Management GUI.....	105
Network Events and Alarms Screens.....	105
Alarms.....	106
SNMP Traps.....	107
Alarm Reports.....	109
Security Operations.....	110
Chapter 9: Measurements Module.....	111
Overview.....	112
Functional Description.....	112
DataBase Overview.....	114
Log Message List.....	115
DataBase Tables.....	116

Table 'tekelec_meas_headers'.....	117
Table 'tekelec_meas_reports'.....	117
Table 'tek_nbi_ftp_config'.....	118
Measurement Northbound FTP Module.....	118
NBI FTP Configuration.....	118
File Transfer.....	120
Report Types Supported by Measurement Platform Module.....	121
Chapter 10: Reporting Studio.....	126
Overview.....	127
Measurement Reporting Studio.....	127
Functional Description.....	128
i-net Clear Reports Remote Interfaces.....	129
Remote Interface.....	129
Ad Hoc Reporting Interface.....	130
Configuration Manager.....	130
Data Source Configuration Interface.....	131
Repository Browser Interface.....	132
Scheduler Interface.....	133
Report Designer Interface.....	133
Chapter 11: Configuration Management Interface.....	135
Overview.....	136
Functional Description.....	137
Send Command.....	137
Select EAGLE(s) Pane.....	138
Create Command Pane.....	139
Category Management.....	143
Script Management.....	144
Create Script	147
Modify Script	148
View Script	148
Execute Script	149
Schedule Management.....	150
CMI Informational/Error Message List.....	152
Chapter 12: Link Utilization Interface.....	155
Overview.....	156
Functional Limitations.....	156

User Access Control.....	156
Link Utilization GUI.....	156
Link Data.....	157
Modifying Link Capacity	158
Polling Scripts Creation.....	160
Thresholding Configuration.....	164
Schedule Management.....	166
LUI Measurements Error and Informational Messages.....	166

Chapter 13: Northbound Interface (NBI).....168

Overview.....	169
Functional Description.....	169
Autonomous Events Trap Forwarding.....	170
Heartbeat Trap.....	170
Resynchronization.....	170
E5-MS SNMP Agent Configuration.....	171
Functional Limitations.....	172
Northbound Interface GUI.....	172
NMS Configuration Data.....	173
Match/Filter Criteria Data.....	175
NBI Agent Configuration GUI.....	177

Appendix A: E5-MS System Administration.....178

Security Administration.....	179
Setting Up an E5-MS Workstation.....	179
Screen Resolution.....	179
Compatible Browsers.....	179
Setting the Time Zone.....	179
Creating the E5-MS SSL Certificate.....	180
Security Administration Screen.....	181
Management of Usergroups and Users.....	182
Usergroup Management.....	183
Create New Usergroup.....	183
User Management.....	190
Add a User.....	191
Assign Attributes to a User.....	192
Modify User Profile.....	192
Password Management.....	193
User Status Icons.....	195
Login Restrictions Management.....	196

Password GUI.....	197
Account Recovery.....	199
E5-MS Administrator Password Recovery Mechanism.....	200
Appendix B: E5-MS Backup and Restore.....	201
Overview.....	202
System Requirement.....	202
Backup in E5-MS.....	202
Backup Contents.....	202
Automatic Backup.....	203
Manual Backup.....	204
Configuring Backup Schedule.....	205
Backup to an External Location.....	206
Normal Operations during Backup.....	206
Time taken in Backup.....	206
Status of Backup.....	206
Restore in E5-MS.....	210
How to Restore from Existing Backup.....	210
Default Restore Contents.....	211
Time taken in Restore.....	211
Status of Restore.....	211
File and their Locations.....	211
Appendix C: E5-MS Failover.....	213
Overview.....	214
Requirements.....	214
Primary Server.....	214
Standby Server.....	214
Client.....	215
Failover Process.....	215
Manual Failover.....	215
Files and Location in FAILOVER.....	216
Failover Setup.....	217
How to Set Up Failover.....	218
Befailover Table.....	225
Tables Replicated.....	226
E5-MS Custom Replicated Tables.....	231
Licensing.....	232
Limitations.....	232

Appendix D: E5-MS Database Password Change.....	234
E5-MS Database Password Change for Standalone Server.....	235
E5-MS Database Password Change for Failover Setup.....	236
Appendix E: EPAP Support Messages.....	238
Error/Informational Messages for EPAP Support.....	239
Appendix F: ►Fault Management GUI Custom Views◄.....	242
►Working with Custom Views◄.....	243
►Adding a New Custom View◄.....	243
►Modifying a Custom View◄.....	248
►Saving a Custom View◄.....	250
►Deleting a Custom View◄.....	253
►Renaming a Custom View◄.....	254
►Controlling the Fields Displayed In a Custom View◄.....	257
►Filter Field Descriptions for Network Events Custom View◄.....	260
►Filter Field Descriptions for Alarms Custom View◄.....	261
►Tips and Tricks for Using Custom Views◄.....	264
Glossary.....	266

List of Figures

Figure 1: E5-MS Architecture.....26

Figure 2: E5-MS Launch Screen.....34

Figure 3: E5-MS Authentication Screen.....35

Figure 4: System Tray for Notifications.....35

Figure 5: E5-MS Applications Main Screen.....36

Figure 6: E5-MS Menu Bar.....37

Figure 7: Network Map Toolbar.....38

Figure 8: Detached Network Map Toolbar.....39

Figure 9: Network Event Toolbar.....40

Figure 10: Alarm Summary View Icons.....41

Figure 11: Alarm Summary Views.....41

Figure 12: EAGLE Discovery.....45

Figure 13: EAGLE Discovery Screen.....46

Figure 14: EAGLE Discovery Screen for Existing EAGLE(s).....47

Figure 15: Country and City.....48

Figure 16: Fault Interface.....49

Figure 17: EMSALM Port.....49

Figure 18: SNMP as Fault Interface.....49

Figure 19: IP Address.....50

Figure 20: Protocol.....50

Figure 21: Country and City.....50

Figure 22: Fault Interface.....51

Figure 23: EMSALM Ports.....	51
Figure 24: SNMP Interface.....	51
Figure 25: World Level Map.....	53
Figure 26: Continent Level Map.....	54
Figure 27: Country Level Map.....	55
Figure 28: Eagle Frame Map.....	56
Figure 29: Chassis View.....	57
Figure 30: Shelf View.....	58
Figure 31: EAGLE Inventory GUI.....	63
Figure 32: PDB Only EPAP Configuration.....	69
Figure 33: PROV/Non PROV EPAP Configuration.....	71
Figure 34: Country Level Map with EPAP servers.....	73
Figure 35: LSMS Discovery Screen.....	83
Figure 36: Country Level Map with LSMS servers.....	85
Figure 37: Network Events and Alarm Tree Node.....	93
Figure 38: Fault Management Tree Node.....	105
Figure 39: Historical Network Events	105
Figure 40: Alarms Pane.....	106
Figure 41: NBI FTP Configuration Tree Node.....	119
Figure 42: NBI FTP Configuration Screen.....	120
Figure 43: Add User.....	128
Figure 44: System Permissions.....	129
Figure 45: i-net Clear Report.....	130
Figure 46: Ad Hoc Reporting.....	130
Figure 47: Configuration Manager Interface.....	131

Figure 48: Data Source Configuration Interface.....	132
Figure 49: Repository Browser Interface.....	132
Figure 50: Scheduler.....	133
Figure 51: Report Designer.....	134
Figure 52: CMI Tree Node.....	137
Figure 53: Send Command Screen.....	137
Figure 54: Select EAGLE(s) Pane.....	138
Figure 55: Create Command.....	139
Figure 56: Build Command Tab.....	139
Figure 57: Command Class Menu.....	139
Figure 58: Command Menu.....	140
Figure 59: Get Parameters.....	140
Figure 60: Type Command Pane.....	141
Figure 61: Command Execution Results Pane.....	142
Figure 62: Category Management Screen.....	143
Figure 63: Script Management Screen.....	145
Figure 64: Script Execution Result screen.....	146
Figure 65: Script Deletion Confirmation.....	146
Figure 66: Create Script Screen.....	147
Figure 67: Edit Script Screen.....	147
Figure 68: Execute Script Screen.....	149
Figure 69: CMI Scheduler Screen.....	150
Figure 70: CMI Scheduler Confirmation.....	151
Figure 71: Link Utilization Tree Node.....	156
Figure 72: Link Data Screen.....	157

Figure 73: Link data for EAGLE: eagle11.....	157
Figure 74: Modify User Defined Capacity.....	158
Figure 75: RTRV-SLK Command Output.....	160
Figure 76: REPT-STAT-CARD Command Output.....	161
Figure 77: REPT-STAT-IPTPS Command Output.....	162
Figure 78: On Demand Polling.....	163
Figure 79: Polling Script Execution Results.....	164
Figure 80: Thresholding Configuration Screen.....	165
Figure 81: Schedule Management.....	166
Figure 82: NBI Tree Node.....	171
Figure 83: NBI Agent Configuration.....	172
Figure 84: NBI Agent Configuration Plain Text.....	172
Figure 85: E5-MS SNMP NBI GUI.....	173
Figure 86: System Administration Tree Node.....	181
Figure 87: Security Administration Screen.....	182
Figure 88: Security Administration Screen with Groups and Users.....	183
Figure 89: Groups Wizard screen.....	184
Figure 90: Usergroup Attributes.....	185
Figure 91: Select Users.....	186
Figure 92: Permitted Operations for Group.....	187
Figure 93: Assign Permissions Screen.....	188
Figure 94: Select EAGLE(s).....	189
Figure 95: Select Command Classes.....	190
Figure 96: User Administration Screen.....	191
Figure 97: Permitted Operations for User.....	192

Figure 98: Modify User Profile.....	193
Figure 99: Lock Screen.....	197
Figure 100: Password Composition.....	198
Figure 101: Password Restrictions.....	198
Figure 102: Add Custom View By Using Menu Bar.....	243
Figure 103: Add Custom View By Using Left Navigation Pane.....	244
Figure 104: Specify Event Filter Criteria.....	245
Figure 105: Specify Alarm Filter Criteria.....	246
Figure 106: Custom View for Network Events.....	247
Figure 107: Custom View for Alarms.....	248
Figure 108: Modify Custom View By Using Menu Bar.....	249
Figure 109: Modify Custom View By Using Left Navigation Pane.....	250
Figure 110: Saving Custom View By Using Menu Bar.....	251
Figure 111: Saving Custom View By Using Left Navigation Pane.....	252
Figure 112: Custom View Saved Successfully.....	252
Figure 113: Deleting a Custom View By Using Menu Bar.....	253
Figure 114: Deleting a Custom View By Using Left Navigation Pane.....	254
Figure 115: Rename a Custom View By Using Menu Bar.....	255
Figure 116: Rename a Custom View By Using Left Navigation Pane.....	256
Figure 117: Entering a New Name for a Custom View.....	257
Figure 118: Selecting Table Columns for Network Events.....	258
Figure 119: Selecting Table Columns for Alarms.....	258
Figure 120: Specifying Additional Table Columns for Network Events.....	259
Figure 121: Specifying Additional Table Columns for Alarms.....	259

List of Tables

Table 1: Admonishments.....	18
Table 2: Ports Used by E5-MS.....	30
Table 3: Network Map Toolbar Icons.....	39
Table 4: Detached Network Map Toolbar Icons.....	39
Table 5: Network Event Toolbar Icons.....	40
Table 6: E5-MS Maps List.....	58
Table 7: Inventory Commands.....	64
Table 8: Automatic Resynchronization Scenarios.....	74
Table 9: Event Details - Automatic Resynchronization Initiated.....	75
Table 10: Event Details - Automatic Resynchronization Successful.....	75
Table 11: Event Details - Automatic Resynchronization Failure.....	75
Table 12: Event Details - Resynchronization Initiated by User.....	76
Table 13: Event Details - Resynchronization Initiated by User Is Successful.....	76
Table 14: Event Details - Resynchronization Initiated by User Has Failed.....	77
Table 15: Event Details - Buffer Overflow During Southbound Resynchronization.....	77
Table 16: Event Details - Traps Buffer Overflow.....	78
Table 17: Event Details - Heartbeat Trap Not Received at Configured Interval.....	78
Table 18: Event Details - Traps Buffer Overflow.....	87
Table 19: Event Details - Unable to Fetch LSMS Status.....	87
Table 20: E5-MS Action When Status Cannot be Obtained.....	87
Table 21: Alarm Correlations Rules.....	96
Table 22: LUI Measurements Error and Informational Messages.....	167

Table 23: Backup and Restore related Files and Directories.....212

Table 24: Error/Informational Messages for EPAP Support.....239

Chapter 1

Introduction

Topics:

- *Overview.....18*
- *Scope and Audience.....18*
- *Documentation Admonishments.....18*
- *Manual Organization.....19*
- *My Oracle Support (MOS).....19*
- *Emergency Response.....20*
- *Related Publications.....20*
- *Customer Training.....21*
- *Locate Product Documentation on the Oracle Technology Network Site.....21*

This chapter contains general information, such as an overview of the guide, how the guide is organized, and how to get technical assistance.

Overview

This guide includes administrative and interface information for the Oracle Communications EAGLE Element Management System (E5-MS).

Scope and Audience





This guide is intended for anyone responsible for the following activities:

- E5-MS configuration and administration, and use of the E5-MS Graphical User Interface (GUI).
- Use of the E5-MS to configure and monitor an Oracle Communications EAGLE Signal Transfer Point (STP) in a network.
- Use of the E5-MS to receive and manage alarms for Oracle Communications LSMS and Oracle Communications EAGLE Application Processor (EPAP).

Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

Table 1: Admonishments

Icon	Description
 DANGER	Danger: (This icon and text indicate the possibility of <i>personal injury</i> .)
 WARNING	Warning: (This icon and text indicate the possibility of <i>equipment damage</i> .)
 CAUTION	Caution: (This icon and text indicate the possibility of <i>service interruption</i> .)
 TOPPLE	Topple: (This icon and text indicate the possibility of <i>personal injury and equipment damage</i> .)

Manual Organization

This document is organized into these sections:

- *Introduction* contains general information, such as an overview of the guide, how the guide is organized, and how to get technical assistance.

E5-MS Administration

- *E5-MS Administration* introduces administration, initialization, and first configuration of E5-MS.
- *E5-MS Functional Description* provides an overview of the E5-MS.
- *E5-MS Graphical User Interface* provides an overview of the functions provided by the E5-MS GUI.

E5-MS Core Applications

- *EAGLE Discovery Application* describes how the EAGLE nodes are discovered in the network.
- *E5-MS Support of EPAP Alarms via SNMP Feed* describes support for EPAP fault management.
- *E5-MS Support of LSMS Alarms via SNMP Feed* describes support for LSMS fault management.
- *Fault Management* provides descriptions of the functions provided by E5-MS Fault Management Interface.
- *Measurements Module* provides information about the E5-MS Measurements Module.

Optional Applications

- *Reporting Studio* provides information about the I-net Clear Reports remote interfaces.
- *Configuration Management Interface* provides an overview of the functions provided by the E5-MS Configuration Management Interface (CMI).
- *Link Utilization Interface* provides information about the E5-MS Link Utilization Interface (LUI).
- *Northbound Interface (NBI)* provides information about the E5-MS Northbound Interface.

Appendixes

- *E5-MS System Administration* provides an overview of the embedded security management tool and interface available in the E5-MS.
- *E5-MS Backup and Restore* describes the configuration and execution of the backup and restore procedure for the E5-MS.
- *E5-MS Failover* describes the failover procedure for the E5-MS.
- *E5-MS Database Password Change* describes the process to change the E5-MS database password.
- *EPAP Support Messages* lists the error and informational messages for E5-MS support of EPAP fault management.
- *Fault Management GUI Custom Views* describes the use of custom views for events/alarms in the Fault Management GUI.

My Oracle Support (MOS)

MOS (<https://support.oracle.com>) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at **1-800-223-1711** (toll-free in the US), or call the Oracle Support hotline for your local country from the list at <http://www.oracle.com/us/support/contact/index.html>. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select **2** for New Service Request
2. Select **3** for Hardware, Networking and Solaris Operating System Support
3. Select one of the following options:
 - For Technical issues such as creating a new Service Request (SR), Select **1**
 - For Non-technical issues such as registration or assistance with MOS, Select **2**

You will be connected to a live agent who can assist you with MOS registration and opening a support ticket.

MOS is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at **1-800-223-1711** (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at <http://www.oracle.com/us/support/contact/index.html>. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Related Publications

For information about additional publications that are related to this document, refer to the *Related Publications Reference* document, which is published as a separate document on the Oracle Technology Network (OTN) site. See [Locate Product Documentation on the Oracle Technology Network Site](#) for more information.

Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training:

<http://education.oracle.com/communication>

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site:

www.oracle.com/education/contacts

Locate Product Documentation on the Oracle Technology Network Site

Oracle customer documentation is available on the web at the Oracle Technology Network (OTN) site, <http://docs.oracle.com>. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at www.adobe.com.

1. Log into the Oracle Technology Network site at <http://docs.oracle.com>.
2. Select the **Applications** tile.
The **Applications Documentation** page appears.
3. Select **Apps A-Z**.
4. After the page refreshes, select the **Communications** link to advance to the **Oracle Communications Documentation** page.
5. Navigate to your Product and then the Release Number, and click the **View** link (note that the Download link will retrieve the entire documentation set).
6. To download a file to your location, right-click the **PDF** link and select **Save Target As**.

Chapter 2

E5-MS Administration

Topics:

- [E5-MS Administration.....23](#)
- [E5-MS Initialization and First Configuration...23](#)

The first part of this manual describes E5-MS administration, initialization, and first configuration.

E5-MS Administration

This E5-MS Administration part describes how to administer the E5-MS after the initialization and first configuration are complete.

E5-MS Functional Description describes E5-MS platform, inventory, fault management, alarms, and measurement functions.

E5-MS Graphical User Interface describes the E5-MS GUI menus and how to use them to perform configuration, discovery of inventory, fault management, alarms, and measurement operations.

E5-MS Initialization and First Configuration

Before the E5-MS GUI can be used, the activities described in *E5-MS System Administration* must be performed:

- E5-MS setup - install to a client's workstation.
- Initialization and first configuration of the E5-MS software for a new installation or an upgrade - log in as the "root" user, allow the automatic discovery of the EAGLE systems.

Note: When the initialization and first configuration are complete, the E5-MS GUI will be available for use.

Chapter 3

E5-MS Functional Description

Topics:

- *E5-MS Overview.....25*
- *E5-MS Architecture.....26*
- *E5-MS Applications.....26*
- *E5-MS Security Tools.....29*
- *E5-MS Ports Usage and Firewall Configuration.....30*
- *Workstation Requirements.....31*
- *EAGLE Baseline Hardware32*

This chapter provides an overview of the E5-MS.

E5-MS Overview

The E5-MS consolidates real-time management at a centralized point within the signaling network to provide a consistent approach for configuring and monitoring the client's network. The E5-MS is an optional product in the EAGLE product family.

It is based on Zoho WebNMS Framework that provides a single or multi-user visual graphical view of the EAGLE Network Elements. Using this framework, E5-MS reports the discovery, physical and logical topology maps, centralized event management, graphs and statistical information of the EAGLE system.

The E5-MS DataBase (DB) uses an embedded MySQL Enterprise Edition DB. This DB Data Model is documented including the details on the tables, data formats, and the number of entries supported. The rules are incorporated to evaluate DB size based on the number of managed objects, and measurements are documented in this guide.

The user-configurable windows, based on the customer's choice of filtering and viewing criteria, provide a flexible, efficient way to view and monitor alarms. The E5-MS enables management of alarms from EAGLE, EPAP, and LSMS. Features include:

- Easy-to-use GUI point-and-click operation
- Scene drill-down capability
- Geographical or logical network views
- Color-coded alert severity

There are multiple integrated GUIs that enable users to monitor, control, and predict the overall operation of their signaling network more accurately and cost effectively, while controlling initial and ongoing costs. The core applications of the E5-MS are the:

- EAGLE Discovery
- EPAP Discovery
- LSMS Discovery
- Fault Management
- Measurements Module

The optional applications are the:

- Inventory Management
- Configuration Management Interface
- Link Utilization Interface
- Northbound Interface
- Reporting Studio

The E5-MS captures real-time events from a network of EAGLE systems to provide a full presentation of the EAGLE health, performance, configuration, and inventory.

The System Administrator is provided a Security Interface to enable user access at different levels of the E5-MS and EAGLE systems. Once the System Administrator has set up the individual EAGLE commands, the user will have access to complex command scripts that can be created, managed, executed, and scheduled for execution on one or more remote EAGLE systems.

The E5-MS provides a mechanism for forwarding alarms from EAGLE, EPAP, and LSMS systems, and from the E5-MS (including E5-MS agents and interfaces) to a Northbound Interface. Alarms are

synchronized between the E5-MS and the monitored systems, upon request from the Northbound Interface.

E5-MS Architecture

A general E5-MS setup is shown in *Figure 1: E5-MS Architecture*:

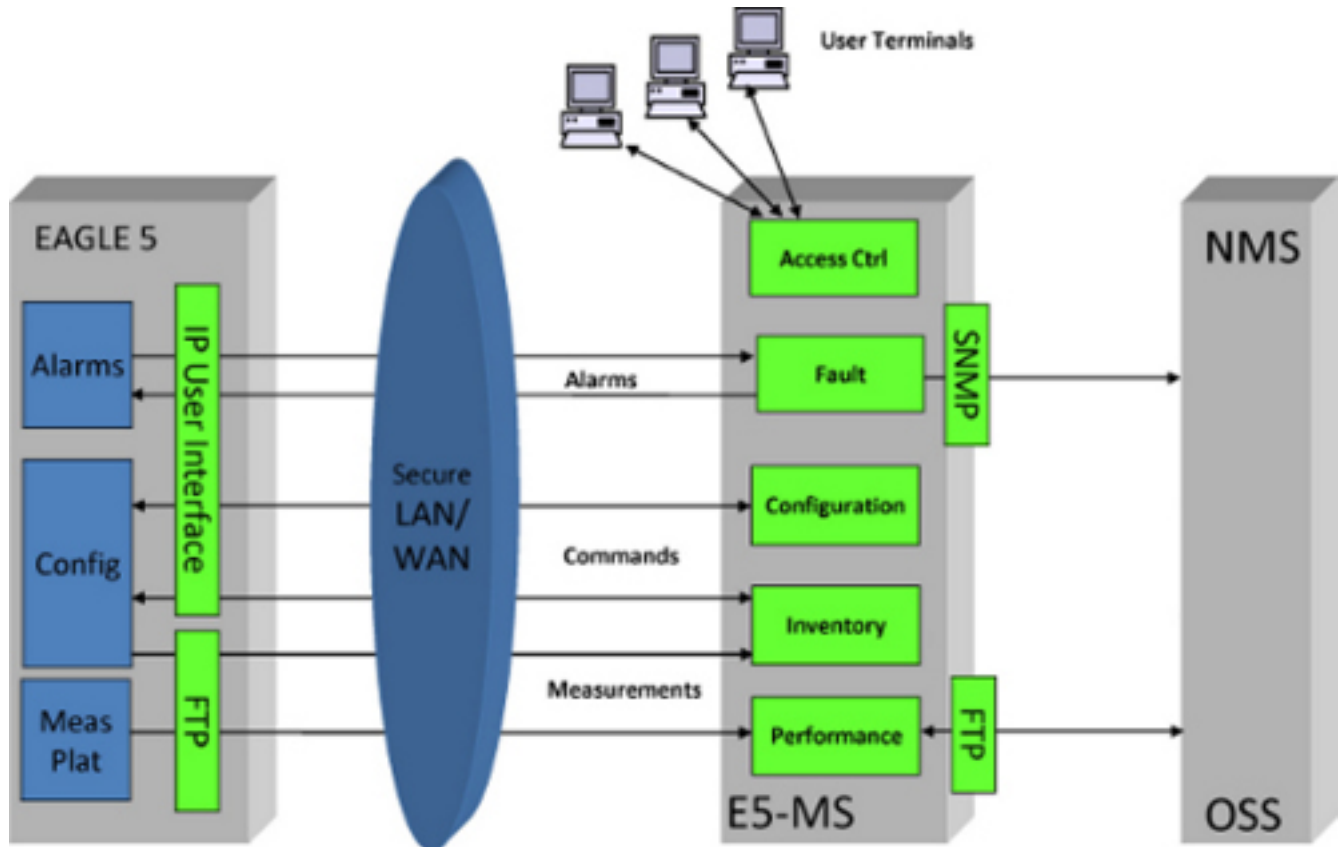


Figure 1: E5-MS Architecture

E5-MS Applications

The E5-MS GUI displays a view of the global network down to the card level with event-filtering capabilities. When outages occur, E5-MS provides fault isolation tools to quickly isolate the problem and enable service restoration. Direct access to the EAGLE Send Command application is provided and operators have the flexibility to remotely manage EAGLE systems based on customer defined rules for common and repetitive actions.

The E5-MS applications available include:

- **EAGLE Discovery Application**

The EAGLE Discovery tool discovers the EAGLE systems within the client network. This tool allows the System Administrator or user with administration access to add a new EAGLE, modify the details of an existing EAGLE, rediscover an existing EAGLE, and delete an existing EAGLE. The EAGLE Inventory tool is an optional application that fetches the inventory information to build the EAGLE system chassis view and create a geographical view for the EAGLE, starting from World level to Continent level to Country level to EAGLE Frame level. The Schedule Management screen allows the user to schedule updates to inventory and graphics.

- **EPAP Discovery Application**

The EPAP Discovery tool enables the discovery of EPAP nodes within the client network for EPAP alarm management. EPAP nodes are then visible in the Fault Management menus and maps. EPAP alarms received from the southbound SNMP interface can be forwarded on the E5-MS northbound interface.

- **LSMS Discovery Application**

The LSMS Discovery tool enables the discovery of LSMS nodes within the client network for LSMS alarm management. LSMS nodes are then visible in the Fault Management menus and maps. LSMS alarms received from the southbound SNMP interface can be forwarded on the E5-MS northbound interface. LSMS supports SNMPv1.

- **Fault Management**

The E5-MS Fault Management application stores all event history in a database (DB). In normal conditions the historical information can be accessed for a minimum of 30 days. The Fault Management application and DB support a minimum of 200 entries per second: 200 TPS.

- **Measurements Module**

The E5-MS Measurement Module parses measurement files received from the EAGLE Measurements Platform Agent, and then transfers the data to the E5-MS database as .csv files. The Measurement Reporting Studio can convert the .csv files into a comprehensive report. There are a set of pre-defined reports integrated in the Measurement Studio, such as:

- STP System Total Measurements
- Component Measurements
- Network Management Measurements
- Daily Availability Measurements
- Availability Measurements
- Daily Maintenance Measurements
- Hourly Maintenance Measurements
- Gateway Measurements

The files are sent via FTP to the E5-MS Database. The data is used to create reports.

- **Security Administration**

The E5-MS customer is in charge of the system administration and the OS administration. The System Administrator is the owner of the Root Account and setting all privileges for the Group Users.

- **Reporting Studio**

The E5-MS Reporting Studio is a reporting tool. The E5-MS uses the OEM Software (I-net Clear Reports Plus®) to create pre-defined measurement reports. It produces an array of output data formats, such as PDF, JPG. The Reporting Designer generation reports using a remote interface

provided by I-net Clear Report[®]. E5-MS Users can create/update a report template as per their requirement.

- **Configuration Management Interface (CMI)**

The E5-MS Configuration Management Interface is the application used to access EAGLE commands, parameters, and historical data. The following functions are provided by the Configuration Management Interface:

- Administrator access rights for E5-MS users according to User group
- Create and send commands to one or more EAGLE systems
- Create, manage, and schedule for execution EAGLE command scripts
- Manage and review logs containing information about E5-MS activities, including EAGLE command script execution, all E5-MS User activities, and all accesses to EAGLE systems

The CMI application requires accounts and users to be created on the EAGLE STP. The requirements are documented. Once the user is assigned an EAGLE, they can perform the needed configuration on EAGLE. All E5-MS and EAGLE activity performed by the users, successful or not, are logged and documented.

- **Link Utilization Interface**

The E5-MS Link Utilization Interface (LUI) collects and stores link capacity information about EAGLE signaling links in the E5-MS database. There is a default capacity selection defined by the card configuration or Oracle defined values, however the user can override link capacity thresholds to allow fine tuning to utilization. The Threshold Alarm feature allows the user to set measurement thresholds to generate alarms for the LUI. The Measurement Reports Studio and CMI are required for the Link, Linkset and card utilization reports.

- **Northbound Interface**

The E5-MS Northbound Interface selectively forwards SNMP alert traps to a maximum 10 client-registered Network Management Systems (NMS). Alerts can be synchronized between the E5-MS and a Network Management System. The Northbound Interface is an optional application that converts all E5-MS alarms into northbound SNMP v2c standard traps (LSMS supports SNMPv1). The FTP Northbound Interface allows E5-MS raw measurement reports to be forwarded to a database.

- **Backup and Restore**

E5-MS is used to manage and monitor EAGLE, EPAP, and LSMS nodes in the network. E5-MS has database tables, configuration files and other data, that must be backed up to take care of any data loss due to any reason. The E5-MS provides both manual and daily automatic back up functionality and scheduled backup intervals can be configured as per user requirement. Backed up content can be restored by user manually.

- **Failover**

In E5-MS, failover support is provided with two redundant servers configured as primary and standby servers. In the failover setup, the primary and standby servers has access to the replicated database. Mysql data files are kept at /Tekelec/Webnms/mysql/data directory.

E5-MS Security Tools

The Security Administration application GUI is used to provide security for the client's network management environment.

The E5-MS provides secured access control mechanisms including:

- Password management
 - Password complexity management
 - Password expiration rules management
 - Password are stored in a secured and encrypted file (or database).
- Robust authentication methods including SSL and secure RMI server access control (J2EE security model). LDAP authentication server use is an optional feature.

The E5-MS log files are protected from E5-MS user modifications. The System Administrator will configure each user with the following:

- Authorization for users and groups views
- Roles views
- Operations views
- Managed Object views

Each user will generate user activity logs. The details of those logs are available in each feature FRS. Overall and all logs are documented. The E5-MS users cannot modify the log files. For more information about log files, see *Purpose of E5-MS Log Files* in *Upgrade/Install Guide*.

The E5-MS System Administrator assigned by the client will update their OS with the latest security patches without impacting the software behavior. Oracle will document the system and OS details of the platforms used during development or testing phases.

Since the clients provide the Hardware and Operating system, they own the Root account or any privileged accounts (super users). Oracle requires a privileged account to perform installation, configuration, maintenance, support and upgrades. It is assumed that the customer provides privileges to Oracle personnel according to their needs/requirements but it also assumes the client is the system administrator of the platform.

The E5-MS software and all OEM components are free of critical/major security fault or vulnerability. The default settings (including password) of the software components delivered by Oracle will follow strong security rules (i.e complex passwords).

The E5-MS OEM components are configured or set in a way to ensure the maximum security possible. For instance, if several levels of security are possible, the most secured parameters or options (for instance, logging levels, permissions granularity) are used.

For more information about E5-MS security, see [Security Administration Screen](#).

E5-MS Ports Usage and Firewall Configuration

Primary and secondary servers need to be behind a single firewall and should not have their individual firewalls turned ON. Client machine used to access E5-MS client and managed EAGLE(s) could be on the other side of the firewall.

In case a firewall is enabled between E5-MS servers and client or E5-MS servers and managed EAGLE(s), the ports used by E5-MS need to be opened on the firewall for proper functioning of E5-MS with the firewall.

The ports used by E5-MS, their type, and their purpose are provided in [Table 2: Ports Used by E5-MS](#). All of these ports must be opened up on the firewall. None of the ports are encrypted.

Note: Ports for SSH (22), Telnet (23), and SNMP (161) must be opened bidirectionally.

Table 2: Ports Used by E5-MS

S#	Port (Type)	Description
1	20 (TCP)	Data port for FTP
2	21 (TCP)	Command port for FTP
3	22 (TCP)	Port used for SSH connection
4	23 (TCP)	Port used for Telnet connection to support outbound connections to STPs configured without the SSH option; E5-MS does not provide Telnet as a login service
5	69 (UDP)	TFTP service port used by WebNMS
6	161 (UDP)	SNMP port
7	162 (UDP)	SNMP trap port used for receiving traps
8	1099 (TCP)	RMI Registry port used in Client-Server communication
9	2000 (TCP)	NMS BE port used for communication between BE and FE servers
10	2300 (TCP)	Config Server port
11	3306 (TCP)	MySQL
12	4500 (TCP)	SAS (SNMP Applet server) port In BE - FE combination, all SAS-related information is passed through a socket.
13	4567 (TCP)	Web NMS Client-Server communication port

S#	Port (Type)	Description
14	8001 (UDP)	Web NMS Agent port
15	8002 (UDP)	Port to receive SNMP set request from NMS
16	8443 (TCP)	SSL connection port
17	9000 (TCP)	I-net Clear Reports server port
18	9999 (TCP)	SUM port
19	36001 (TCP)	NMS FE secondary port
20	36002 (TCP)	Web NMS Client-Server communication port
21	36003 (TCP)	RMI Server Socket port
22	<i>Port Range</i> (TCP)	For the NBI FTP module to transfer measurement files from E5-MS to NMS using FTP (passive mode), the port range (ports used for ftp) for the FTP server needs to be configured at NMS. The ports specified in the port range on NMS need to be opened on the E5-MS server firewall as well.

Workstation Requirements

The workstation hardware requirements provided by the customer are as follows:

- **Small System**
 - CPU at 2MHz minimum - 1 CPU system supported
 - Memory 2GB or higher - 8 GB recommended
 - Disk space, a minimum of 400MB for software installation + 200MB for swap, however 500GB SAS disks are recommended. (for database and history requirements)
- **Medium System**
 - CPU at 2MHz minimum - 1 CPU system supported
 - Memory 4GB or higher - 8 GB recommended
 - Disk space, a minimum of 400MB for software installation + 200MB for swap, however 500GB SAS disks are recommended. (for database and history requirements)
- **Large System**
 - CPU at 2MHz minimum - 1 CPU system supported

- Memory 8GB or higher - 16GB recommended
- Disk space, a minimum of 400MB for software installation + 200MB for swap, however 500GB SAS disks are recommended. (for database and history requirements)

The E5-MS end user interface is based on a Java 7 client interface. The E5-MS can be viewed using either of the following web browsers provided by the customer:

- Microsoft® Internet Explorer version 8.0 or later
- Mozilla Firefox® version 16 or later.

Note: Your browser of choice should have pop-ups enabled.

The E5-MS requires a Linux 64-bit operating system, such as Oracle Enterprise Linux 6.4. E5-MS was tested on Oracle Enterprise Linux 6.4.

For more information, see *Upgrade/Install Guide*.

EAGLE Baseline Hardware

To prepare for the installation of the E5-MS, the customer will be in charge of the hardware of the EAGLE systems in their network. The E5-MS product is available in a tiered architecture using the following configurations:

- **Small Network:**
 - up to 4 Network Elements (2 STP pairs)
 - up to 5 concurrent Users
- **Medium Network:**
 - up to 20 Network Elements (10 STP pairs)
 - up to 15 concurrent Users
- **Large Network:**
 - up to 50 Network Elements (25 STP pairs)
 - up to 25 concurrent Users

The EAGLE must be equipped with the following:

- At least one IPSM card (supports up to 3 cards)
- Measurement Platform activation
 - Either Integrated Measurement Platform on E5-MASP cards
 - Or Measurement Platform on CPM cards
- User and for Command Interface and Topology collection
- Terminal settings for Alarm Management
 - Two terminals per IPSM are required.

¹ Microsoft is a registered trademark of the Microsoft Corporation.

² Firefox is a registered trademark of the Mozilla Foundation.

Chapter 4

E5-MS Graphical User Interface

Topics:

- [Overview34](#)
- [E5-MS Login.....34](#)
- [E5-MS Applications Main View36](#)
- [Alarm Summary View.....41](#)

This chapter describes the E5-MS Graphical User Interface (GUI), how to log into E5-MS, and how to use the E5-MS user interface menus.

Overview

The E5-MS Graphical User Interface (GUI) provides a comprehensive geographical view for users to monitor and control their EAGLE system network. The user receives real-time performance data from the EAGLE system that assists in maintenance operations. The System Administrator and Users launch the E5-MS and log in from a client workstation as shown in [Figure 2: E5-MS Launch Screen](#).

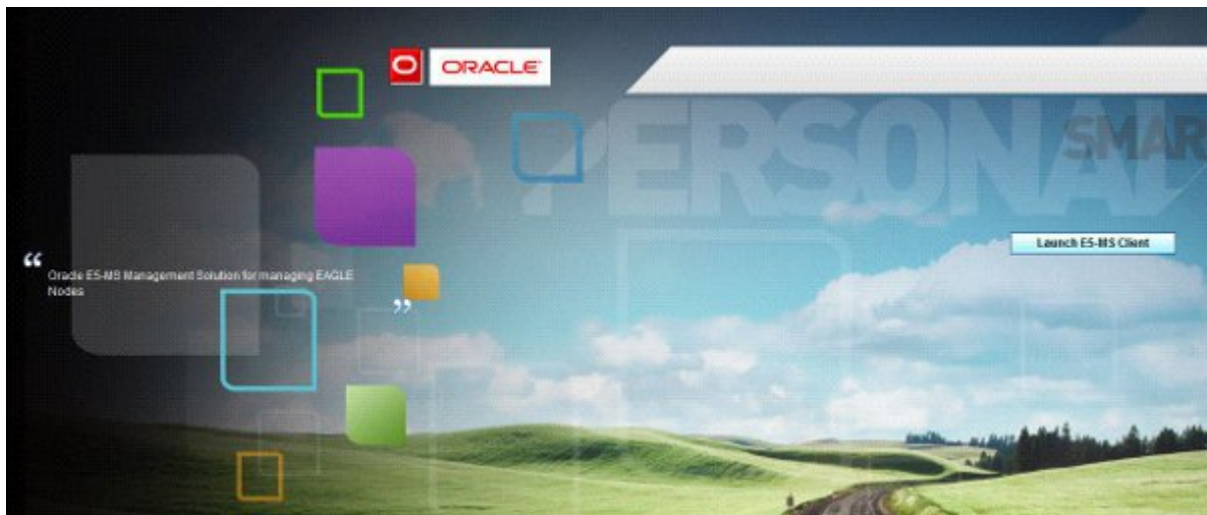


Figure 2: E5-MS Launch Screen

Please contact your System Administrator to assign **E5-MS Authentication** security operation.

E5-MS Login

The E5-MS login page is used to authenticate users of the E5-MS.

Logging In to E5-MS

Please contact your System Administrator to assign **E5-MS** security operation.

This procedure describes how to log in to the E5-MS.

1. Click **Launch E5-MS Client** on the **E5-MS Launch** screen (see [Figure 2: E5-MS Launch Screen](#)).
2. Enter the **User ID** and **Password** on the **E5-MS Authentication** screen (see [Figure 3: E5-MS Authentication Screen](#)).



Figure 3: E5-MS Authentication Screen

Please contact your System Administrator for your User ID and Password.

3. Click the **Connect** button or press the **Enter** key on the keyboard.

If the user name and password entered in [Step 2](#) are correct, the E5-MS User is authenticated and notification is received on the lower right of the screen as shown in [Figure 4: System Tray for Notifications](#).

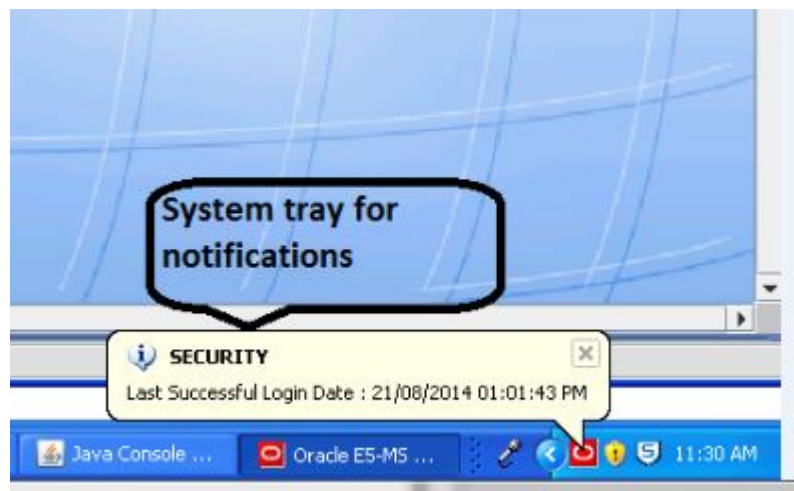


Figure 4: System Tray for Notifications

If there is a problem with the user name or password, an error message appears:

- If your password has expired, the **Change Password** page is displayed.
- If an authentication failure message appears, check to make sure the user name and password are correct and repeat the login.

If login was not successful after repeating the login attempt, contact a System Administrator.

Login Page Elements

Element	Description
UserID Field	Enter your E5-MS User name in this field.
Password Field	Enter your password in this field. If your password is not known, contact a System Administrator to reset the password.
Connect Button	Click on this button to sign in to the E5-MS.

E5-MS Applications Main View

After the user has access to the E5-MS GUI, the E5-MS Applications Main Screen is displayed:

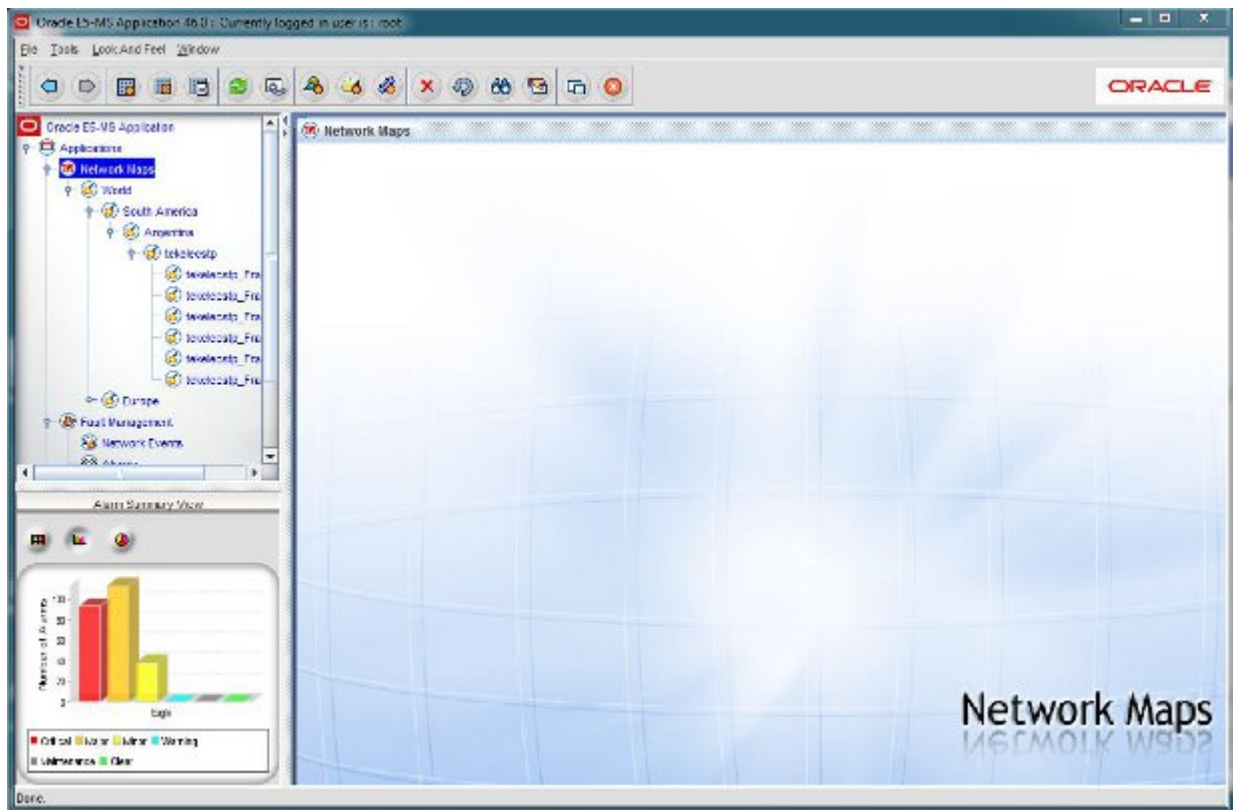


Figure 5: E5-MS Applications Main Screen

Menu Bar

The E5-MS Menu Bar is the horizontal strip at the top of the E5-MS GUI that contains available drop down menus. It includes links to the specific E5-MS applications. Many items located within the menu

bar have keyboard shortcuts that enable the user to choose menu options by just pressing a key combination.

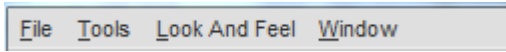


Figure 6: E5-MS Menu Bar

Menu Bar Submenus

Main Menu Selection	Submenu
File	<ul style="list-style-type: none"> <u>B</u>ack <u>F</u>orward <u>D</u>etach <u>C</u>lose C<u>l</u>ose All E<u>x</u>it
Tools (only Security Administration has a keyboard shortcut available)	<ul style="list-style-type: none"> <u>S</u>ecurity Administration C<u>h</u>ange Password T<u>h</u>emes E<u>a</u>gle Discovery E<u>a</u>gle Inventory L<u>S</u>MS D<u>I</u>scovery E<u>P</u>AP Discovery R<u>e</u>port Designer R<u>e</u>porting Studio N<u>B</u>I N<u>B</u>I Agent Configuration N<u>B</u>I F<u>T</u>P Configuration L<u>i</u>cence Details E5-MS N<u>o</u>tifications E5-MS N<u>o</u>tifications Settings
Look and Feel	<ul style="list-style-type: none"> <u>M</u>etal <u>C</u>DE Motif <u>W</u>indows <u>W</u>indows Classic
Window	<ul style="list-style-type: none"> C<u>a</u>scade







Main Menu Selection	Submenu
	Tile Horizontal Tile Vertical Save Location and Size Show Toolbar

Toolbar Icons

The toolbars are a set of icons that are part of the E5-MS Application. The common toolbar is easy-to-use and always available for performing common functions. Then there are several other Toolbars associated with the application such as the:

- Map toolbar, which is viewed at the top of the E5-MS GUI when the maps are viewed in the display screen
- Detached network map toolbar, which is specific to the maps view when the display screen is detached
- Network event and Network Database toolbar, which is specific to the network events view

Common Toolbar Icons

ICON	ICON Name	Description
	Go Back to Previous	Navigating through active windows
	Go Forward to Next	
	Find	Searching elements in a map, searching events, searching alarms
	Properties	Viewing properties, viewing row details
	Detach Current Window	Detaching a window from the display window
	Stop	Stops the current process that is being executed














Network Map Toolbar Icons

There are additional options within the Network Map display as shown in [Figure 7: Network Map Toolbar](#) and [Table 3: Network Map Toolbar Icons](#).



Figure 7: Network Map Toolbar

Table 3: Network Map Toolbar Icons

ICON	ICON Name	Description
	Select Mode	Zooming In and Out
	Zoom Window	
	Zoom Mode	
	Zoom In	
	Zoom Out	
	Cut	
	Copy	
	Paste	
	Undo	To undo the last operation performed in the map
	Group View	Grouping Map Symbols - The user must have permission to use these icons from the System Administrator
	Expand Selected (or All) Groups	
	Group Selected Symbols	
	Filter Symbols	



Detached Network Map Toolbar Icons









The toolbar and icons for detached network maps are shown in [Figure 8: Detached Network Map Toolbar](#) and [Table 4: Detached Network Map Toolbar Icons](#).



Figure 8: Detached Network Map Toolbar

Table 4: Detached Network Map Toolbar Icons

ICON	ICON Name	Description
	Add Map	Adding Custom Maps
	Delete Map	Deleting Map Layout

ICON	ICON Name	Description
	Save Map	Saving Map Layout
	Refresh	Refreshing Map Layout
	Relayout	Resetting Map Layout
	Add Symbol	Adding a Symbol
	Add Container	Adding a Container
	Add Link	Adding a Link
	Delete	Deleting a selected Symbol
	Undo Add/Delete	To undo the last operation performed of adding or deleting a Symbol







Network Events Toolbar Icons

The Network Events toolbar has the additional options of Save and Print as shown in [Figure 9: Network Event Toolbar](#) and [Table 5: Network Event Toolbar Icons](#).



Figure 9: Network Event Toolbar

Table 5: Network Event Toolbar Icons

ICON	ICON Name	Description
	Save	Saving Events available only in Network Events and Alarms view
	Print	Printing Events available only in Network Events and Alarms view
	Refresh	Refreshing the Page View
	Add Custom View	A tailored view for viewing a subset of data that satisfies specific criteria.
	Modify Custom View	
	Remove Custom View	

Alarm Summary View

The Alarm Summary View panel in the lower left of the E5-MS GUI provides the user with an immediate view of the alarms.

The three icons at the top of the Alarm Summary View are shown in *Figure 10: Alarm Summary View Icons*.

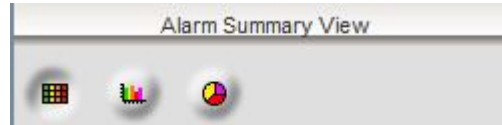


Figure 10: Alarm Summary View Icons

Use the Alarm Summary View icons to display the summary by severity and category in tabular form, by severity and category in graphical form, or by severity alone, as shown in *Figure 11: Alarm Summary Views*.

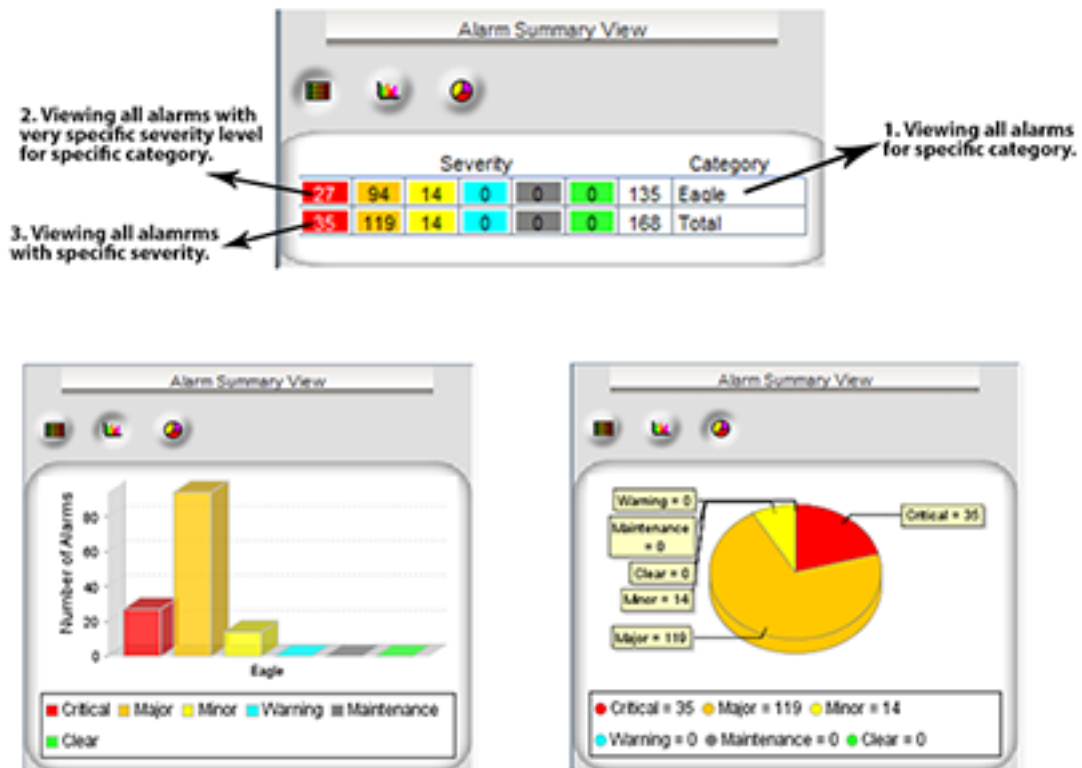








Figure 11: Alarm Summary Views

Alarm Severity Representation

Color	ICON Name
	Critical
	Major
	Minor
	Warning
	Maintenance
	Clear

Chapter 5

EAGLE Discovery Application

Topics:

- *Overview.....44*
- *Functional Description44*
- *EAGLE Discovery.....44*
- *Discovery GUI.....45*
- *Schedule Management Screen52*
- *Map Views52*
- *Inventory Management.....62*

This chapter provides information about the EAGLE Discovery application.

Overview

The E5-MS has three elements of the inventory process are the

- EAGLE Discovery GUI, which runs various commands on EAGLE to populate inventory data in E5-MS database.
- EAGLE Inventory GUI, which is used for building various map views and provide input to other E5-MS interfaces such as the CMI, Security and Fault Management, etc.
- Schedule Management GUI, which automatically schedules updates for the Update Inventory and Update Graphics for each EAGLE added the E5-MS.

Functional Description

EAGLE Discovery

The E5-MS System Administrator will initiate the first discovery of inventory in the existing EAGLE network using the **EAGLE Discovery** tool.

The EAGLE Discovery tool in the E5-MS retrieves the EAGLE inventory data as a topology collection of frames, shelves, cards and card type. The map data populates the Network Maps screen and inventory data provides a fresh inventory in the inventory database. As data is collected it is logged as topology collection in Logs and topology action in Audit trails.

The **EAGLE Discovery** process populates EAGLE inventory data in E5-MS with the following data:

- Inventory data
- Map data

The E5-MS logs all topology collection into logs and action to Audit trails. This discovery supports TL1, SNMP, Telnet and SSH enabled EAGLE systems.

As the EAGLE systems are added or deleted, the E5-MS provides a clean up process. The Update Inventory and Update Graphics are scheduled daily to ensure the Inventory and Map data are correct. By default, the **Update Graphics** operation is scheduled to run on 00:00 AM per day and **Update Inventory** are scheduled to run on 01:00 AM per day.

Note: Users have the ability to update the frequency and timing of the **Update Inventory** and **Update Graphics** operations as desired.

User Access Control

Before performing this procedure, you must be granted access by a System Administrator.

This procedure describes how to discover the EAGLE systems in your network.

1. Click **Tools** at the top of the E5-MS GUI menu bar.

2. Select EAGLE Discovery from the dropdown menu. As shown the EAGLE Discovery

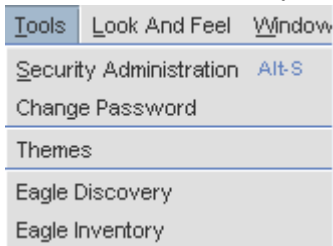


Figure 12: EAGLE Discovery

Validation

The communication path used for the discovery process is an IP ping. This is required to validate the user configured the EAGLE system.

E5-MS selects any of the available EAGLE IPSM IP addresses and corresponding terminals except **EMSALM** terminal for performing EAGLE discovery, in case the EAGLE communication is a **TL1**. During the discovery process, the first ping is sent to the first able **IPSM IP**. If the first able **IPSM IP** does not respond to EAGLE commands, the next configured **IPSM IP** is pinged.

Once there is a successful EAGLE discovery with one of the configured IPSM IP, then other configured IPs (if any) are maintained in E5-MS database without performing any ping test. The user can perform discovery for a single EAGLE at a time.

Note: No verification is performed to validate that the user configured EAGLE is an EAGLE or not. Only IP ping based mechanism is used for kicking off discovery process.

Discovery GUI

The main functions of the **EAGLE Discovery** screen as shown in [Figure 13: EAGLE Discovery Screen](#) are the:

- **Existing EAGLES(s)**, which display the list of existing EAGLE systems.
- **New EAGLE**, which shows the required fields needed for EAGLE Discovery. In case, of an existing EAGLE, the fields are filled in with the EAGLE values.
- **Add, Modify and Delete** operations buttons.

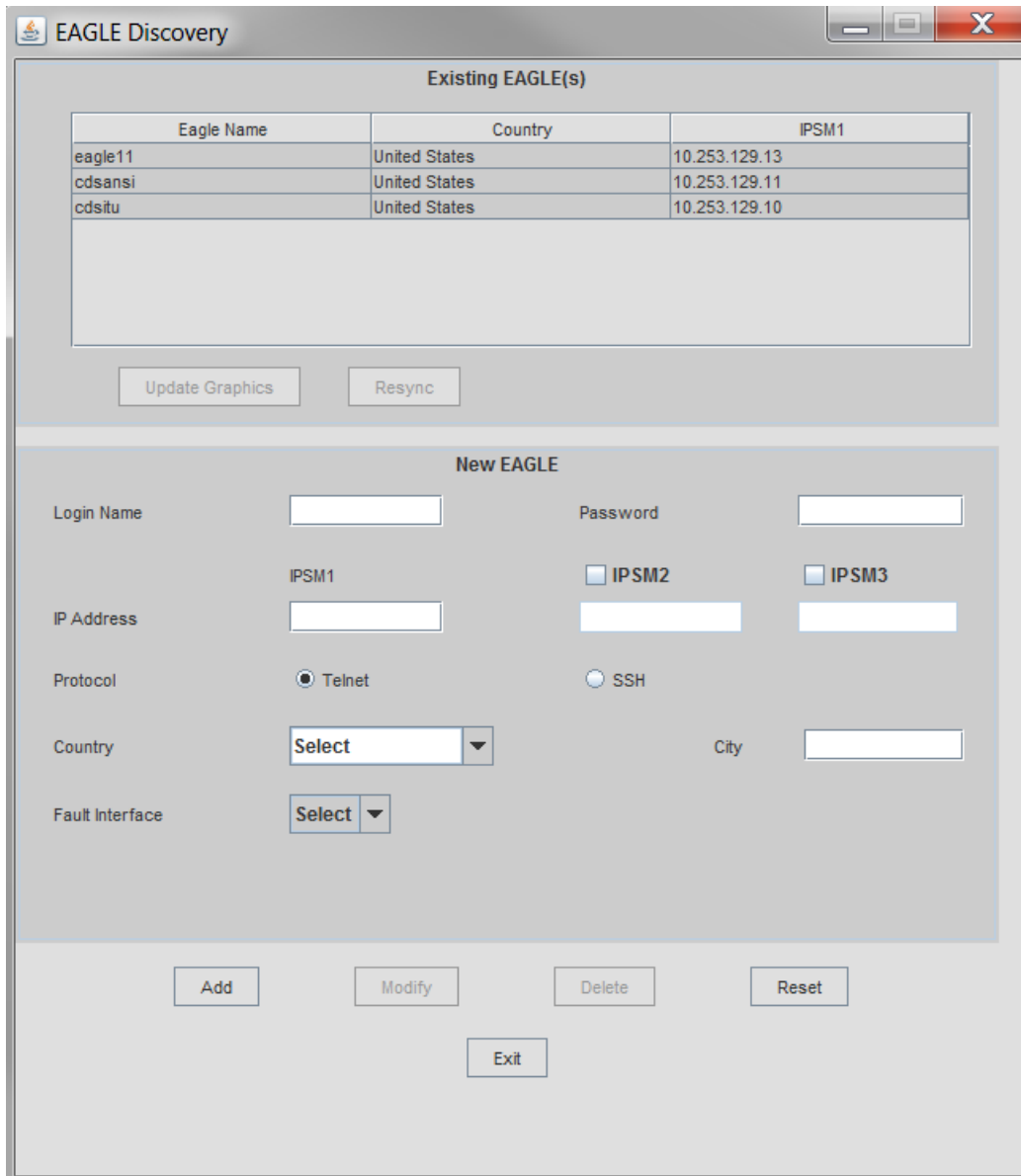


Figure 13: EAGLE Discovery Screen

For the **Existing EAGLE(s)** listed in **EAGLE Discovery** screen, users can trigger a **Resynchronization** of alarms as shown in *Figure 14: EAGLE Discovery Screen for Existing EAGLE(s)*.

Note: If the **Update Graphics**, **Update Inventory** and **Stop Inventory** are grayed out the user is not assigned to the Inventory GUI. Please contact your System Administrator. The Inventory GUI applications is an optional, to the Core features. Please check the Licenses.

Existing EAGLE(s)

Eagle Name	Country	IPSM1
eagle11	United States	10.253.129.13
cdsansi	United States	10.253.129.11
cdsitu	United States	10.253.129.10

Update Graphics Resync

eagle11

Login Name: eagle Password: ●●●●

IPSM1: 10.253.129.13 IP SM2 IP SM3

IP Address: 10.253.129.13

Protocol: Telnet SSH

Country: United States City: Morrisville

Fault Interface: TL1

EMSALM Port: 23 17 17

Add Modify Delete Reset

Exit

Figure 14: EAGLE Discovery Screen for Existing EAGLE(s)

Existing EAGLE(s)

Update Inventory operation is the interface to manually update either single or multiple EAGLE(s) complete inventory. Update Inventory operation triggered from EAGLE Discovery GUI stores data fetched from EAGLE systems in flat files. There is only one file per command per EAGLE maintained in E5-MS system. This inventory update shall overwrite existing files(if any exists).

Update Graphics operation is the interface to update inventory data (i.e. frame, shelf, slot and card) on single or multiple EAGLE systems that are required to update the graphics available in Chassis View. Update Graphics shall run subset of Update Inventory commands. This update is pertaining to the specific EAGLE the user is fetching updates.

EAGLE Discovery GUI shall support minimum of one hundred (i.e. 100) EAGLEs that can be configured in E5-MS.

When the user clicks on existing EAGLE, configuration section of the EAGLE Discovery GUI should display all details of EAGLE.

If EAGLE Update graphics operation is successful, an E5-MS Information dialog box will appear stating Graphics updated for EAGLE <EAGLE NAME> by user <USER NAME>.

If EAGLE Update graphics operation fails, an E5-MS Error message will appear stating EAGLE <EAGLE NAME> graphics update failed! Reason: <REASON> Please resolve the issue and retry

If EAGLE Update Inventory operation is successful, an E5-MS Information dialog box will appear stating Inventory updated for EAGLE <EAGLE NAME> by user <USER NAME>.

If EAGLE Update Inventory operation fails, an E5-MS Error message will appear stating EAGLE <EAGLE NAME> inventory update failed! Reason: <REASON> Please resolve the issue and retry

Note: The Inventory module notifies other E5-MS management modules (like Fault, Configuration and Security etc.) of EAGLE add, modify and delete events.

Add an EAGLE System

Before performing this procedure, you must be granted the right to **EAGLE Discovery** by a System Administrator.

This procedure describes how to add each EAGLE system to which the E5-MS is connected.

1. Click Tools icon on the Menu Bar.
2. Select **EAGLE Discovery**
EAGLE Discovery screen pops up as shown in [Figure 13: EAGLE Discovery Screen](#)
3. Type the name and password of the EAGLE in their respective fields.
The System Administrator will provide the name and password of the EAGLE system being discovered.
4. Enter the IP address of the EAGLE in IPSPM 1. There must be at least one IP address for each EAGLE system.
It is possible to configure a total of three (3) IPSPM interfaces for each EAGLE in IPSPM 2 and IPSPM 3 fields.
5. Enable the Protocol by selecting either Telnet or SSH.
6. Select the country the EAGLE system is located. Click the drop down arrow to select the country. A county must be selected. If the country is not listed, select **Others**. As shown in figure

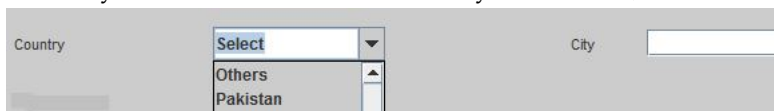


Figure 15: Country and City

There is no validation when selecting the country.

7. Type in the City the EAGLE system is located as shown in figure Country and City.
There is not validation when the city is entered.

8. Select the Fault Interface as a TL1 or SNMP.

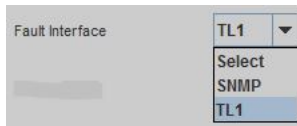


Figure 16: Fault Interface

If TL1 is selected, the EMSALM Port must be selected for each IPSM interface as shown in

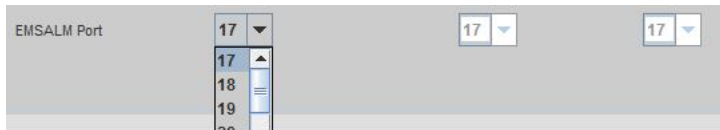


Figure 17: EMSALM Port

If SNMP is selected the following fields:

- Read Community
- Write Community
- Active OAM IP
- Standby OAM IP

As shown in



Figure 18: SNMP as Fault Interface

9. Click the **Add** button at the bottom of the EAGLE Discovery screen.
An E5-MS Information dialog box will appear stating EAGLE addition request has been sent to server. Please wait for status.

Active and Standby OAMs Switch

If the active and standby OAMs switch on the EAGLE, the Active OAM IP and Standby OAM IP fields will updated after a user triggers resync with the EAGLE and after completion of resync, selects the EAGLE in the existing EAGLE(s) list.

IP Address

The validation on the authenticity of the IPSM terminals is provided by E5-MS user in the IP Address fields.

1. Ensure all terminals exist on the EAGLE IPSM card IP by contacting the System Administrator for the IP addresses.
2. Enter the IP address of the EAGLE in IPSM 1. There must be at least one IP address for each EAGLE system.

It is possible to configure a total of three (3) IPSM interfaces for each EAGLE in IPSM 2 and IPSM 3 fields. As shown in figure IP Address

Figure 19: IP Address

If IPSM 1 is not entered before IPSM 2 / 3, an E5-MS Error dialog box will appear stating Please enter IP address for IPSM1!

If the IPSM IP address is invalid, an E5-MS error message dialog box will appear IP address <IP Entered> entered for <IPSM> is not valid! Please provide a valid IP Address

If the IP address is used on another EAGLE IPSM, an E5-MS error message dialog box will appear IP addresses provided for one or more IPSM cards are same!

EAGLE Discovery validates which of the IPs specified as Active OAM IP is valid with a message Please provide a valid IP address for Active OAM IP! and the Standby validation with Please provide a valid IP address for Standby OAM IP!.

Protocol

The two options to enabled the protocol on the EAGLE are Telnet and SSH as shown in figure

Figure 20: Protocol

Telnet is the protocol used for the Cut Through interface.

Country and City

To populate the maps automatically, a Country must be selected.

1. Click the drop down arrow to select the country the EAGLE system is located as shown in figure Country and City

Country is a required field. If the country is not listed, select **Others**

There is not validation when the country is entered.

Figure 21: Country and City

2. Type in the City the EAGLE system is located as shown in figure Country and City. City must be less than 30 characters else, an error message. If more than 30 characters are put in, an error message City name cannot exceed 30 characters!. City can not contain any special characters or numbers, an error message Please enter a valid city name! There is not validation when the city is entered.

Fault Interfaces

TL1

Select the Fault Interface as a TL1 or SNMP. As shown in Fault Interface

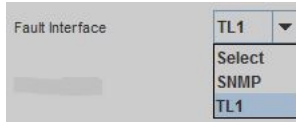


Figure 22: Fault Interface

TL1 / EMSALM ports

Select the range for the EMSALM ports.

All three EMSALM ports for different IPSM interfaces (IPSM1, IPSM2 and IPSM3) configured on EAGLE Discovery GUI should be in different ranges. Valid terminal ranges can be [17-24], [25-32] and [33-40] EMSALM Ports of two or more IPSM cards lie in the same terminal range. Valid ranges are [17-24], [25-32] and [33-40].

As shown in EMSALM Ports



Figure 23: EMSALM Ports

Active and Standby OAMs Switch

If the active and standby OAMs switch on the EAGLE, the Active OAM IP and Standby OAM IP fields will updated after a user triggers resync with the EAGLE and after completion of resync, selects the EAGLE in the existing EAGLE(s) list.

SNMP

Select the Fault Interface as a SNMP. As shown in SNMP Interface



Figure 24: SNMP Interface

The following fields must be filled:

- Read Community
- Write Community

- Active OAM IP
 - Standby OAM IP
1. Read Community must have less than 30 characters. The field will blot out once the characters are entered.
If more than 30 characters, this message will appear Read community cannot be longer than 30 characters!.
 2. Write Community must have less than 30 characters. The field will blot out once the characters are entered.
If more than 30 characters, this message will appear Write community cannot be longer than 30 characters!.
 3. Active OAM IP a validation on whether the IPs specified is the Active OAM IP.
If an invalid IP address is entered, this message will appear Please provide a valid IP address for Active OAM IP!
 4. Standby OAM IP a validation on whether the IPs specified is the Standby OAM IP.
If an invalid IP address is entered, this message will appear Please provide a valid IP address for Standby OAM IP!

Schedule Management Screen

EAGLE Discovery is executed when a new EAGLE is added to the network or modification are performed on an existing EAGLE.

The Schedule Management screen provides the user to setup an automatic schedule to Update Inventory and Update Graphics. The inventory data is used to populate and build various map views and provide input to other E5-MS modules such as CMI, Security and Fault Management.

For each EAGLE added to E5-MS, two operations are automatically scheduled on Schedule Management screen - **Update Inventory** and **Update Graphics**. By default, **Update Graphics** operation are scheduled to run on 00:00 AM per day and Update Inventory are scheduled to run on 01:00 AM per day. A user has the ability to stop the scheduled execution of either of these operations by disabling the corresponding scheduled tasks. Also, users have the ability to update the frequency and timing of the operations as desired

Map Views

The EAGLE Discovery data provides the E5-MS the geographic locations of the EAGLE systems. This data is used to populate maps for all discovered EAGLE(s) automatically. During the EAGLE Discovery the user inputs the Country of the EAGLE system. The Country will provide enough data to construct the graphical map drill down view.

The graphical map drill down levels are the following:

- [Figure 25: World Level Map](#)
- [Figure 26: Continent Level Map](#)
- [Figure 27: Country Level Map](#)
- [Figure 28: Eagle Frame Map](#)

- *Figure 29: Chassis View*
- *Figure 30: Shelf View*

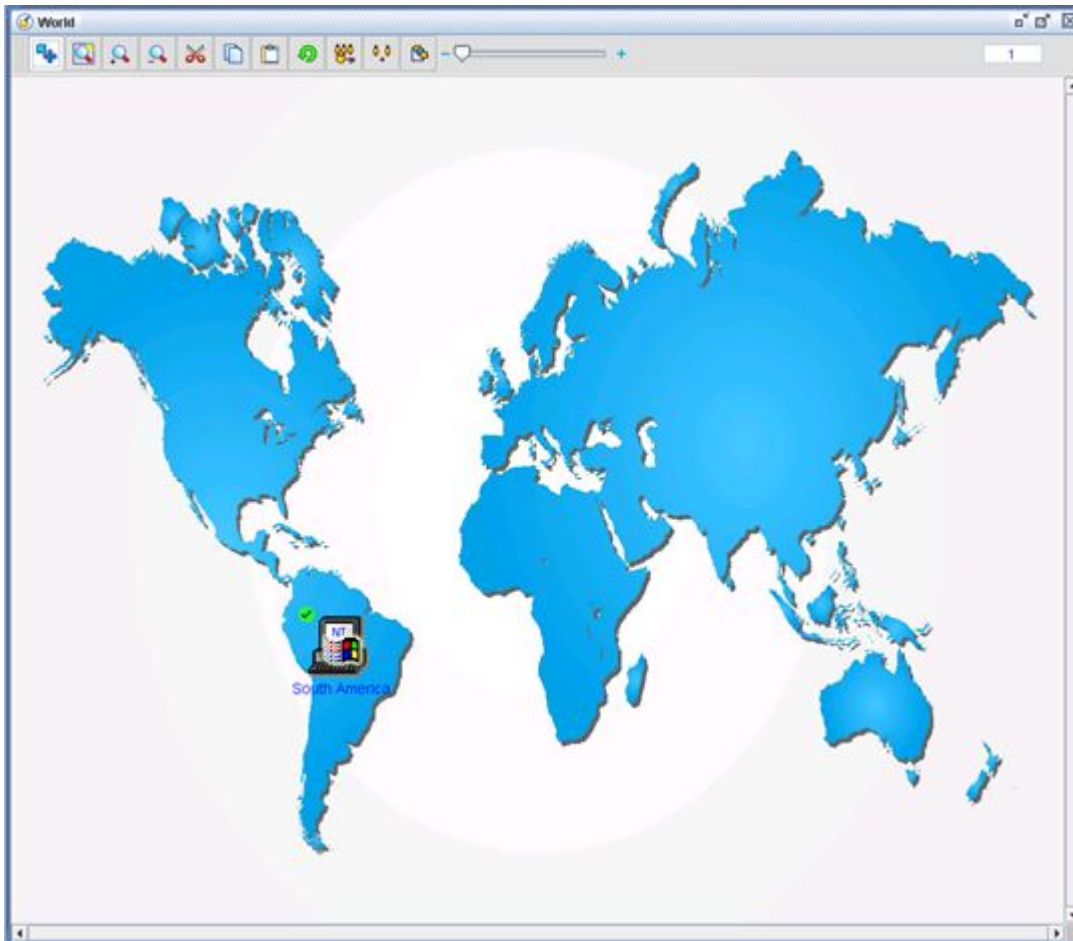


Figure 25: World Level Map



Figure 26: Continent Level Map



Figure 27: Country Level Map

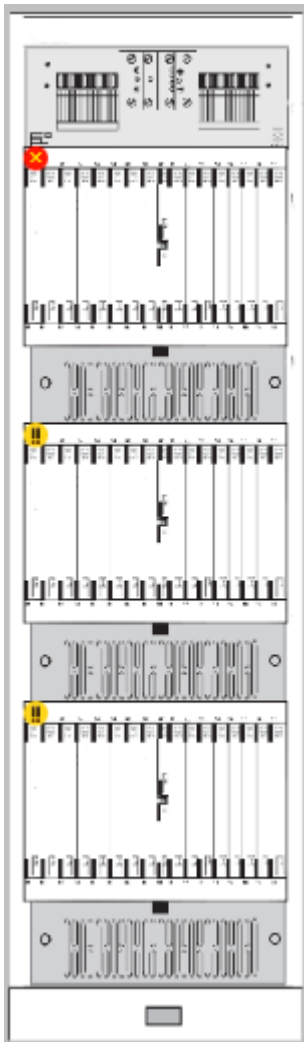


Figure 29: Chassis View



Figure 30: Shelf View

In case, the country is not available in the list of countries presented in **EAGLE Discovery** screen as the EAGLE is deployed, as shown in Table E5-MS Maps List, there is an **Others** option in the Country drop down list the user selects.

Table 6: E5-MS Maps List

Continent Map	Country Map
Africa	Algeria Cameroon Egypt Ghana Ivory Coast Kenya Mali Morocco Senegal Tunisia
Asia	China India Indonesia Japan

Continent Map	Country Map
	Kuwait Malaysia Pakistan Russia Singapore Sri Lanka Taiwan Turkey UAE Vietnam
Europe	Albania Austria Belgium Bosnia Bulgaria Croatia Czech Republic Finland France Germany Greece Hungary Iceland Ireland Italy Macedonia Moldova Norway Poland Portugal Serbia Slovakia Slovenia

Continent Map	Country Map
	Sweden Netherlands Romania Spain Switzerland UK
North America	Canada Costarica Elsalvador Guatemala Honduras Jamaica Mexico Nicaragua United States
Oceania	Australia New Zealand
South America	Argentina Brazil Chile Columbia Ecuador Peru Uruguay
Others	All countries not covered in above list are shown in this map.

Adding a new country map to E5-MS

This procedure describes how to add a country map for a country that is not supplied in the base E5-MS system.

Perform the following steps on the E5-MS server:

1. Copy the required country map image to the `/Tekelec/WebNMS/images` directory.
Supported image file types are `gif` and `png`.

For example, copy the India map image (say `mapindia.gif`) to the `/Tekelec/WebNMS/images` directory.

2. In the `/Tekelec/WebNMS/conf/tekelec/ContinentZonalMap.xml` file, add the following entry under the appropriate continent:

```
<Zone>
  <ZNAME>CountryName</ZNAME>
  <ZIMAGE>CountryMapFileName</ZIMAGE>
  <ZTREEICON>redDot.png</ZTREEICON>
</Zone>
```

For example, for India, search for the `<CNAME>Asia</CNAME>` tag in the `/Tekelec/WebNMS/conf/tekelec/ContinentZonalMap.xml` file and add the following entry beneath it:

```
<Zone>
  <ZNAME>India</ZNAME>
  <ZIMAGE>mapIndia.gif</ZIMAGE>
  <ZTREEICON>redDot.png</ZTREEICON>
</Zone>
```

3. In the `/Tekelec/WebNMS/conf/mapIcon.data` file, add an icon for the new country by searching for the entry for Algeria and adding an entry for the new country beneath it.

```
<DATA TYPE="Algeria" iconName="workstation.png" menuName="DrillDownMenu"/>
<DATA TYPE="CountryName" iconName="workstation.png" menuName="DrillDownMenu"/>
```

For example:

```
<DATA TYPE="Algeria" iconName="workstation.png" menuName="DrillDownMenu"/>
<DATA TYPE="India" iconName="workstation.png" menuName="DrillDownMenu"/>
```

4. Restart the E5-MS server for the changes to take effect.

To verify that the country has been added successfully, log in to the E5-MS client and select **Tools > EAGLE Discovery** to search for the newly added country in the **Country** drop down menu.

Map View Features

E5-MS automatically plots EAGLE symbols on various maps; however, user needs to drag symbol to appropriate coordinates in map and save map from Custom Views on the toolbar at the top of E5-MS, then select Save Map. The symbol remains associated with the coordinates on map where it was saved.

If the System Administrator assigns a users to **Map Editing Operations**, they can save the edits.

The double clicking functionality allows the user to move from upper level map to a lower level map except for the movement from EAGLE frame view to chassis view, which is through a menu item on the EAGLE frame symbol.

Note: Chassis menu item limitation is as per the framework.

To navigate upwards (i.e. from lower to higher map view) user need to use the tree view. For example, while navigating from EAGLE frame map to Country map, E5-MS user uses the tree view provided in the left side of E5-MS main screen.

Note: Feasibility of providing single click option for navigating upwards is checked.

In World map, symbol(s) is corresponding to continent(s) and other.

In Continent map, symbol(s) is corresponding to country(s).

In Country map, symbol(s) is corresponding to EAGLE(s).

In Country map, EAGLE symbol displays city information in tool tip as configured in EAGLE Discovery GUI. (If the Inventory application is available to the user, when an EAGLE added to E5-MS operations the Update Inventory and Update Graphics is automatically scheduled as separate tasks on Schedule Management GUI. By default, Update Graphics operation is scheduled to run on 00:00 AM per day and Update Inventory are scheduled to run on 02:00 AM per day. The scheduled time can be changed by the user.)

In EAGLE frame map, symbol(s) correspond to frame(s) available for that particular EAGLE.

In Chassis View, single frame view of an EAGLE display all cards are at their appropriate location.

Inventory updates (if any) is reflected in Chassis View on re launch of Chassis View from EAGLE Frame view.

User is provided with menu items on chassis view to view alerts, events of a card, by right-clicking the card.

User is provided with menu item on chassis view to write certain editorial comments via journal menu item.

User is provided with a menu item on chassis view to view card details.

Chassis view displays last inventory update time in format DD:MM:YYYY HH:MM:SS. Inventory update time refers to following operations:

1. Update Inventory triggered from EAGLE Discovery GUI.
2. Update Graphics triggered from EAGLE Discovery GUI.
3. Modify operation performed from EAGLE Discovery GUI.
4. Scheduled EAGLE rediscovery operation performed from scheduler interface

All maps are created dynamically during the discovery process itself.

Maps is available in the tree view in the left pane for navigation purpose.

Note: *- Only maps for which EAGLE discovery has been performed are available in tree and map View.

All maps and map symbols are supplied with E5-MS itself and contain static images. However, user have the option to change the map images via `ContinentZonalMap.xml` file available at `<E5-MS_HOME>/conf/tekelec`. Any modifications to specified XML file requires server restart for changes to take effect. Such changes will not apply to existing maps, all existing will have to be re-added(deleted then added)for changes to take effect.

All cards, map symbols and map images are reused from the classic EMS after converting the images to the desired format. New images if any are procured from Oracle.

Inventory Management

E5-MS support a GUI interface `Eagle Inventory` to view inventory files generated on Update Inventory operation. As shown in EAGLE Inventory GUI

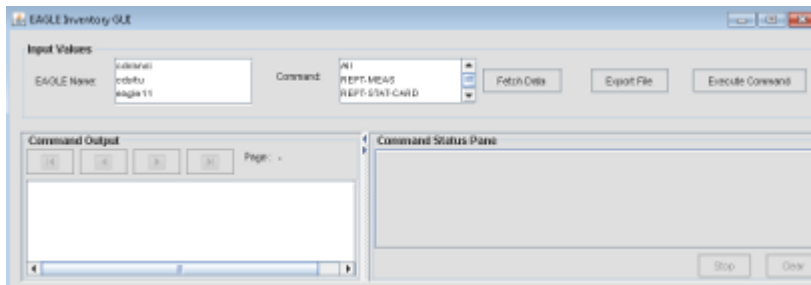


Figure 31: EAGLE Inventory GUI

Authorized E5-MS user assigned Eagle Inventory operation from security GUI launches the Eagle Inventory GUI from Tools > Eagle Inventory menu item.

The Eagle Inventory GUI has two panes:

- Input Values pane
- Output pane

Input Values pane shall allow user to select EAGLE Name, Command and Fetch Data button for which data needs to be read from flat files available on server.

Output pane displays the data fetched from flat files available on server for the command selected for an EAGLE.

EAGLE Inventory GUI shall refresh list of available EAGLE(s) on selecting Eagle Name drop down.

EAGLE Inventory GUI shall contain a drop down for EAGLE(s) and a drop down for command name.

Selection of both the EAGLE and the command is mandatory for fetching inventory data.

EAGLE Inventory GUI fills the fetched inventory data in the Output Pane provided.

EAGLE Inventory data is exportable to a text file.

Existing EAGLE(s)

Update Inventory operation is the interface to manually update either single or multiple EAGLE(s) complete inventory. Update Inventory operation triggered from EAGLE Discovery GUI stores data fetched from EAGLE systems in flat files. There is only one file per command per EAGLE maintained in E5-MS system. This inventory update shall overwrite existing files (if any exist).

Update Graphics operation is the interface to update inventory data (i.e. frame, shelf, slot and card) on single or multiple EAGLE systems that are required to update the graphics available in Chassis View. Update Graphics shall run subset of Update Inventory commands. This update is pertaining to the specific EAGLE the user is fetching updates.

EAGLE Discovery GUI shall support minimum of one hundred (i.e. 100) EAGLEs that can be configured in E5-MS.

When the user clicks on existing EAGLE, configuration section of the EAGLE Discovery GUI should display all details of EAGLE.

If EAGLE Update graphics operation is successful, an E5-MS Information dialog box will appear stating Graphics updated for EAGLE <EAGLE NAME> by user <USER NAME>.

If EAGLE Update graphics operation fails, an E5-MS Error message will appear stating EAGLE <EAGLE NAME> graphics update failed! Reason: <REASON> Please resolve the issue and retry

If EAGLE Update Inventory operation is successful, an E5-MS Information dialog box will appear stating Inventory updated for EAGLE <EAGLE NAME> by user <USER NAME>.

If EAGLE Update Inventory operation fails, an E5-MS Error message will appear stating EAGLE <EAGLE NAME> inventory update failed! Reason: <REASON> Please resolve the issue and retry

Note: The Inventory module notifies other E5-MS management modules (like Fault, Configuration and Security etc.) of EAGLE add, modify and delete events.

Inventory Commands

The table for Inventory Commands lists the commands that are run in the Nightly scheduled inventory for each EAGLE system.

Table 7: Inventory Commands

No.	For Each EAGLE System
1.	rtrv-shlf
2.	rept-stat-card
3.	rtrv-card
4.	rtrv-map
5.	rtrv-scr-aftpc
6.	rtrv-scr-blkdpc
7.	rtrv-scr-blkopc
8.	rtrv-scr-cdpa
9.	rtrv-scr-cgpa
10.	rtrv-scr-destfld
11.	rtrv-scr-dpc
12.	rtrv-scr-isup
13.	rtrv-scr-opc
14.	rtrv-scr-tt
15.	rtrv-scr-sio
16.	rtrv-scr-scrset
17.	rept-stat-db
18.	rtrv-gpl
19.	rept-stat-gpl

No.	For Each EAGLE System
20.	rept-stat-rte
21.	rept-stat-ls
22.	rtrv-ls
23.	rept-stat-slk
24.	rtrv-slk
25.	rtrv-tbl-capacity
26.	rept-meas
27.	rtrv-log
	For Each EAGLE System
28.	rtrv-bip
29.	rtrv-card

Chapter 6

E5-MS Support of EPAP Alarms via SNMP Feed

Topics:

- [Overview.....67](#)
- [EPAP Nodes.....67](#)
- [EPAP Discovery Menu.....68](#)
- [Map Views.....72](#)
- [Cut Through Interface from Maps to EPAP.....73](#)
- [Fault Management.....74](#)

This chapter provides information about E5-MS support for EPAP. EPAP nodes can be discovered in the network so that they are visible in the E5-MS fault management menus and maps, enabling receipt and management of EPAP alarms through the E5-MS.

Overview

E5-MS Support of EPAP Alarms via SNMP Feed enables the use of the E5-MS to manage EPAP alarms through the following interfaces:

- **Discovery**
The EPAP Discovery interface enables discovery and configuration of EPAP servers in the E5-MS.
- **Map**
The map interface displays discovered EPAP servers in the E5-MS map views.
- **Fault Management**
The fault management interface displays the EPAP alarms in both tabular views and map views.
- **Security**
The security interface restricts access to the EPAP Discovery and Fault Management operations.

Configuration of an EPAP node in the E5-MS is through an EPAP Discovery menu. EPAP nodes are then visible in the fault management menus and maps. The E5-MS receives alarms from managed EPAP servers over the southbound SNMP interface. This alarm feed is processed by E5-MS and presented to the user in the form of events and alarms. EPAP alarms can be forwarded on the E5-MS northbound interface to one or more client Network Management Systems. E5-MS users can monitor the EPAP alarm state and take relevant actions to maintain the EPAP servers in a healthy state.

Notes:

- E5-MS 46.0 supports EPAP 16.0.
- EPAP supports SNMPv2c.

EPAP Nodes

EPAP can be configured in the following ways:

PROV EPAP	An EPAP system that includes both a provisioning database (PDB) and a real time database (RTDB)
Non PROV EPAP	An EPAP system that includes only an RTDB (no PDB)
PDB only EPAP	An EPAP system that includes only a PDB (no RTDB)

E5-MS supports both PDB single and segmented EPAPs.

The E5-MS defines EPAP nodes as follows:

- One EPAP server for PDB only EPAP (1 server = 1 node)
- Two EPAP servers for PROV EPAP and Non PROV EPAP; the two servers are mated and located on the same site (2 servers = 2 nodes)

EPAP Discovery Menu

From the E5-MS menu bar, select **Tools > EPAP Discovery** to access the EPAP Discovery application and discover EPAP servers within your network. A user must have permission to the **EPAP Discovery** administrative operation to perform EPAP Discovery.

The specific EPAP Discovery screen that is displayed depends upon the type of EPAP configuration selected, but each screen contains the following general sections:

- Existing EPAP(s)

The top section displays a list of previously added EPAP nodes. In addition, the **Resync** button is used to resynchronize E5-MS with the alarm state for the selected (check boxes) EPAP nodes (for example, due to connection failure between E5-MS and EPAP).

- EPAP Configuration

This section shows the required and optional fields used for EPAP discovery. By default, the fields are blank. When an existing EPAP is selected in the top section, the fields are populated with the values provided by the user when discovering that EPAP.

- Action Buttons

The buttons at the bottom are used to perform the **Add, Modify, Delete, Reset,** and **Exit** operations.

If the value selected for the **Select EPAP Type** field is **PDB Only**, the **PDB Only EPAP Configuration** fields are displayed as shown in [Figure 32: PDB Only EPAP Configuration](#).

The screenshot shows a web-based interface for EPAP Discovery. At the top, there is a table titled "Existing EPAP(s)" with columns: Resync EPAP A, Resync EPAP B, EPAP Type, EPAP A IP Address, EPAP A Name, EPAP B IP Address, EPAP B Name, and Country. Below the table is a "Resync" button. The main section is titled "New EPAP Configuration" and includes a dropdown menu for "Select EPAP Type:" set to "PDB Only". A sub-dialog box titled "PDB Only EPAP Configuration" contains the following fields:

- EPAP PDB**
 - Name:* (text input)
 - SNMP/SSH IP Address:* (text input)
 - PROV IP Address:* (text input)
 - Web IP Address:* (text input)
 - Country:* (dropdown menu, currently showing "Select")
 - Description: (text area)
 - Login Name:* (text input)
 - Login Password:* (text input)
 - SNMP Read Community:* (text input)
 - SNMP Write Community:* (text input)
 - SNMP GET/SET Port:* (text input)
 - Status:* (dropdown menu, currently showing "PDBONLY_NONE")

At the bottom of the dialog box are buttons for "Add", "Modify", "Delete", "Reset", and "Exit".

Figure 32: PDB Only EPAP Configuration

The PDB Only EPAP Configuration fields are as follows:

- | | |
|----------------------------|---|
| Name | Required Common Language Location Identifier (CLLI) configured on the EPAP server. Valid names are 5 - 20 characters, including alphanumeric characters, hyphen, and underscore. The first character must be an alphabetic character. |
| SNMP/SSH IP Address | Required IP address used by EPAP for the SNMP interface. |
| PROV IP Address | Required IP address used to provision EPAP. |
| Web IP Address | Required IP address used by EPAP to access the web-based GUI. |

Note: The SNMP/SSH IP address, the PROV IP address, and the Web IP address can all be the same or they can all be different.

Country	Required field that indicates the country where the EPAP servers are installed, to allow presenting the EPAP nodes on a graphical map. If the country in which EPAP is deployed is not available in the drop-down list, select Others . You can also add a new country map to E5-MS; for information, see Adding a new country map to E5-MS .
Description	Optional field used to add text/comments to describe a node, its location, and other useful information. Maximum length is 200 characters.
Login Name / Login Password	Required login name and login password to access EPAP.
SNMP Read Community / SNMP Write Community	Required SNMP authentication strings for querying and writing. Valid strings contain 1 - 20 characters.
SNMP Get/Set Port	Required SNMP Agent Get/Set request port. Valid numeric values are 0 - 65535.
Status	Required current state of the EPAP server. E5-MS does not validate the EPAP status configured by the user.

If the value selected for the **Select EPAP Type** field is **PROV** or **Non PROV**, the **PROV/Non PROV EPAP Configuration** fields are displayed as shown in [Figure 33: PROV/Non PROV EPAP Configuration](#).

Figure 33: PROV/Non PROV EPAP Configuration

The PROV/Non PROV EPAP Configuration fields are as follows:

Name	Required CLI configured on EPAP A and EPAP B. Valid names are 5 - 20 characters, including alphanumeric characters, hyphen, and underscore. The first character must be an alphabetic character.
IP Address	Required IP address for EPAP A and EPAP B.
Login Name / Login Password	Required login name and login password to access EPAP A and EPAP B.
Description	Optional field used to add text/comments to describe a node, its location, and other useful information. Maximum length is 200 characters.

SNMP Read Community / SNMP Write Community	Required SNMP authentication strings for querying and writing. Valid strings contain 1 - 20 characters.
SNMP Get/Set Port	Required SNMP Agent Get/Set request port for EPAP A and EPAP B. Valid numeric values are 0 - 65535.
Status	Required current state of the EPAP servers. E5-MS does not validate the EPAP status configured by the user.
Country	Required field that indicates the country where the EPAP servers are installed, to allow presenting the EPAP nodes on a graphical map. If the country in which EPAP is deployed is not available in the drop-down list, select Others . You can also add a new country map to E5-MS; for information, see Adding a new country map to E5-MS .

Action Buttons

The following action buttons are available at the bottom of the **EPAP Discovery** screen:

Add	The Add operation initiates the discovery process. The EPAP version must be greater than 15 for the EPAP node to be successfully added. After successful discovery, EPAP nodes are displayed in the Existing EPAPs section. EPAP nodes are added without pinging the configured IP address.
Modify	The Modify operation updates an EPAP node in the E5-MS database. Upon successful modification, EPAP nodes are updated as needed in the Existing EPAPs section.
Delete	The Delete operation deletes an EPAP node from the E5-MS database. Upon successful deletion, EPAP nodes are removed from the Existing EPAPs section.
Reset	The Reset operation resets all EPAP Discovery configuration components to their default state.
Exit	The Exit operation exits the EPAP Discovery GUI.

Map Views

E5-MS automatically populates maps for all discovered EPAPs by using the **Country** field entered by the user on the **EPAP Discovery** screen. The graphical map drill down view includes the following levels:

- World level map
- Continent level map
- Country level map

The EPAP map views are similar to the EAGLE map views described in [Map Views](#). For example, see [Figure 34: Country Level Map with EPAP servers](#).



Figure 34: Country Level Map with EPAP servers

If the country in which EPAP is deployed was not available in the **Country** drop down list provided by EPAP Discovery and **Others** was specified, the EPAP will be displayed in the Others map under the World map. Thus, all EPAP nodes are visible on either a Country map or the Others map.

Note: New country maps can be added to E5-MS. For information, see [Adding a new country map to E5-MS](#).

For more information about map views, see [Map View Features](#).

Cut Through Interface from Maps to EPAP

E5-MS provides a Cut Through interface to connect from the map views to discovered EPAP servers through the Web and SSH interfaces. To access the Cut Through interface, right click on the desired EPAP node in the map view and select either **Launch SSH terminal** or **Launch Web interface**.

Note: The E5-MS user must provide login credentials on the launched interface.

Fault Management

The E5-MS fault management support for EPAP includes the following:

- [Events and Alarms Viewer](#)
- [Event and Notification Details](#)
- [Southbound Resynchronization](#)
- [Alarm Acknowledgement and Clear](#)
- [Alarm Maintenance/Active Mode](#)
- [Northbound Interface](#)
- [Status Management](#)

For general information about E5-MS fault management, see [Fault Management](#).

Events and Alarms Viewer

The Network Events and Alarms interface displays events and alarms in a tabular format. The network events and alarms can be viewed via **Fault Management > Network Events** and **Fault Management > Alarms** on the left panel of the E5-MS.

EPAP SNMP traps are processed into events and added to the **Network Events** GUI, and then processed into alarms and displayed in the **Alarms** GUI and drill down view. Alarms represented on the drill down view depict the alarms state at the following levels:

- EPAP nodal view
 - Displays the alarm state of an EPAP.
- Zonal view
 - Displays the alarm state of all the EPAP, LSMS, and EAGLE systems in a zone.

Event and Notification Details

This section includes details for automatic resynchronization, manual resynchronization, buffer overflow during resynchronization, traps buffer overflow, and heartbeat trap not received. Other events will generate additional notifications. For a complete list of messages, see [EPAP Support Messages](#).

E5-MS automatically triggers southbound resynchronization under the scenarios listed in [Table 8: Automatic Resynchronization Scenarios](#).

Table 8: Automatic Resynchronization Scenarios

Scenarios	Message
On EPAP addition	EPAP added to E5-MS.
On receipt of resyncRequiredTrap for resynchronization	Received 'resyncRequiredTrap' from EPAP for alarm resynchronization.
On receipt of heartbeat after fault interface for an EPAP is down	Regaining connection.
On warm start of server	Warm start of E5-MS server.

Corresponding resynchronization events are raised along with client notifications:

- Automatic resynchronization initiated

Table 9: Event Details - Automatic Resynchronization Initiated

Element	Description
Source	E5-MS
Sub Resource	<EPAP NAME>
Severity	Info
Category	Fault
Message	Initiating alarm resynchronization with EPAP.
Reason	See Table 8: Automatic Resynchronization Scenarios .

The following notification is sent:

```
Initiating alarm resynchronization with EPAP <EPAP NAME>.
```

- Automatic resynchronization successful

Table 10: Event Details - Automatic Resynchronization Successful

Element	Description
Source	E5-MS
Sub Resource	<EPAP NAME>
Severity	Info
Category	Fault
Message	Automatic alarm resynchronization completed for EPAP.

The following notification is sent:

```
Automatic alarm resynchronization completed for EPAP <EPAP NAME>.
```

- Automatic resynchronization failure

Table 11: Event Details - Automatic Resynchronization Failure

Element	Description
Source	E5-MS
Sub Resource	<EPAP NAME>
Severity	Info
Category	Fault

Element	Description
Message	Automatic alarm resynchronization failed for EPAP! Reason: <REASON> Please resolve the issue and try again.

The following notification is sent:

```
Automatic alarm resynchronization failed for EPAP: <EPAP NAME>!
Reason: <REASON>
Please resolve the issue and try again.
```

Resynchronization can also be initiated by the user, and corresponding resynchronization events are raised along with client notifications:

- Resynchronization initiated by user

Table 12: Event Details - Resynchronization Initiated by User

Element	Description
Source	E5-MS
Sub Resource	<EPAP NAME>
Severity	Info
Category	Fault
Message	Initiating alarm resynchronization with EPAP.

The following notification is sent:

```
Alarm resynchronization initiated for EPAP: <EPAP name> by user: <USER NAME>!
```

- Resynchronization initiated by user is successful

Table 13: Event Details - Resynchronization Initiated by User Is Successful

Element	Description
Source	E5-MS
Sub Resource	<EPAP NAME>
Severity	Info
Category	Fault
Message	Alarm resynchronization completed for EPAP.

The following notification is sent:

```
Alarm resynchronization completed for EPAP: <EPAP NAME> initiated by user: <USER NAME>!
```

- Resynchronization initiated by user has failed

Table 14: Event Details - Resynchronization Initiated by User Has Failed

Element	Description
Source	E5-MS
Sub Resource	<EPAP NAME>
Severity	Info
Category	Fault
Message	Alarm resynchronization failed for EPAP. Reason: <REASON> Please resolve the issue and try again.

The following notification is sent:

```
Alarm resynchronization failed for EPAP: <EPAP NAME> initiated by user: <USER NAME>!
```

Events are also raised along with client notifications for buffer overflows and when the heartbeat trap is not received at the configured interval:

- Buffer overflow during southbound resynchronization
A maximum of 130 alarms can be present in the EPAP database during resynchronization.

Table 15: Event Details - Buffer Overflow During Southbound Resynchronization

Element	Description
Source	E5-MS
Sub Resource	AlarmMemory_<EPAP NAME>
Severity	Warning
Category	Fault
Message	Buffer overflows during southbound resynchronization for EPAP: <EPAP NAME>! This could result in loss of alarms.

The buffer size (EPAP_RESYNC_QUEUE_MAX_SIZE) can be configured in the `fault.properties` file in the `/Tekelec/WebNMS/conf/tekelec` directory.

- Traps buffer overflow

To prevent loss of traps, E5-MS buffers EPAP SNMP traps per EPAP before processing them into events. The buffer size is configurable and defaults to 6000 alarms/EPAP (20 alarms/sec for 5 minutes).

Table 16: Event Details - Traps Buffer Overflow

Element	Description
Source	E5-MS
Sub Resource	AlarmMemory_<EPAP NAME>
Severity	Warning
Category	Fault
Message	Buffer overflows during traps processing for EPAP: <EPAP NAME>! This could result in loss of alarms.

The buffer size (EPAP_QUEUE_MAX_SIZE) can be configured in the `fault.properties` file in the `/Tekelec/WebNMS/conf/tekelec` directory.

- Heartbeat trap not received at configured interval

The E5-MS fault management module listens for a heartbeat trap at a configured interval (default is 15 minutes) to verify connectivity with EPAP servers.

Table 17: Event Details - Heartbeat Trap Not Received at Configured Interval

Element	Description
Source	E5-MS
Sub Resource	AlarmMemory_<EPAP NAME>
Severity	Warning/Critical depending upon the alarm raised
Message	Cannot connect to EPAP for receiving alarms

E5-MS notifies all active E5-MS client sessions with the following message:

```
E5-MS cannot connect to EPAP: <EPAP NAME> for receiving alarms! Please check the connection.
```

For a complete list of messages, see [EPAP Support Messages](#).

Southbound Resynchronization

There can be scenarios where the E5-MS becomes out of sync with the EPAP alarm state, such as in the case of connection failure between E5-MS and EPAP. To resynchronize the E5-MS and EPAP in such scenarios, E5-MS provides a southbound resynchronization feature. Southbound resynchronization can be performed for a single EPAP node or for multiple EPAP nodes simultaneously via the **Resync** button available on the **EPAP Discovery** GUI.

E5-MS users must be authorized to use the **EPAP Resync** operation and the **EPAP Discovery** operation to perform southbound resynchronization from the **EPAP Discovery** GUI. An E5-MS user authorized

for the **EPAP Resync** operation, but not the **EPAP Discovery** operation, can perform resynchronization via the **Resync** menu item available by right clicking an EPAP node in the map view.

Alarm Acknowledgement and Clear

E5-MS extends its alarm acknowledgement and clear functionality to EPAP alarms. Alarm acknowledgement allows a user to be associated with alarms to track and resolve them. The alarm clear operation raises a clear event for an alarm and clears the alarm from E5-MS (but does not make any changes on EPAP).

Alarm Acknowledgement and Clear are secured operations. The Alarm Acknowledgement operation requires the **Alert Pickup** permission and the Alarm Clear operation requires the **Clear Alerts** permission.

Alarm Maintenance/Active Mode

E5-MS extends its alarm maintenance/active mode operation to EPAP alarms. Maintenance mode is useful when an alarm is being generated on EPAP at a rapid rate due to a particular failure, leading to a flood of events at the E5-MS that continually increases the alarm count of a particular alarm.

In such cases, you can place an EPAP alarm in maintenance mode, which will drop the particular alarm as soon as it is received on E5-MS, without processing. After the failure scenario is resolved on EPAP, you can take the alarm out of maintenance mode and place it back in active mode. After an alarm is placed in active mode on E5-MS, it is cleared from the alarms view and processed in a normal fashion.

Maintenance and Active mode are secured operations requiring the user to have the **Maintenance** and **Active** permissions.

Northbound Interface

E5-MS extends the northbound interface feature to forward alarms from EPAP to one or more client Network Management Systems. Incoming SNMP events and the outgoing events are mapped as follows:

- Outgoing alertTime = As received in incoming event
- Outgoing alertResourceName = Node name (CLLI)
- Outgoing alertSubResourceName = As received in incoming event
- Outgoing alertSeverity = As interpreted by E5-MS for incoming event
- Outgoing alertAcknowledgeMode = Acknowledge value as available in E5-MS
- Outgoing alertTextMessage = As received in incoming event
- Outgoing alertSequenceNumber = Set by E5-MS northbound interface module

Status Management

E5-MS manages EPAP status as follows:

- E5-MS allows configuration of the EPAP status via the EPAP Discovery GUI, and no verification of the status is performed during configuration.
- Upon receiving an alarm or resync trap from EPAP, the fault management module analyzes the received EPAP status and determines whether the configured status value is up to date in E5-MS. In the case of a mismatch, the status is updated with the latest value.
- On the map view, hovering the mouse over the EPAP node displays the current EPAP status.

E5-MS Support of LSMS Alarms via SNMP Feed

Topics:

- [Overview.....81](#)
- [LSMS Nodes.....81](#)
- [LSMS Discovery Menu.....82](#)
- [Map Views.....84](#)
- [Cut Through Interface from Maps to LSMS.....86](#)
- [Fault Management.....86](#)

This chapter provides information about E5-MS support for LSMS. LSMS nodes can be discovered in the network so that they are visible in the E5-MS fault management menus and maps, enabling receipt and management of LSMS alarms through the E5-MS.

Overview

E5-MS Support of LSMS Alarms via SNMP Feed enables the use of the E5-MS to manage LSMS alarms through the following interfaces:

- Discovery
The LSMS Discovery interface enables discovery and configuration of LSMS servers in the E5-MS.
- Map
The map interface displays discovered LSMS servers in the E5-MS map views.
- Fault Management
The fault management interface displays the LSMS alarms in both tabular views and map views.

Configuration of an LSMS node in the E5-MS is through an LSMS Discovery menu. LSMS nodes are then visible in the fault management menus and maps. The E5-MS receives alarms from managed LSMS servers over the southbound SNMP interface. Configuration is required on the LSMS end so that the server sends the asynchronous alarm feed to E5-MS. This alarm feed is processed by E5-MS and presented to the user in the form of events and alarms.

LSMS alarms can be forwarded over the E5-MS northbound interface to one or more client Network Management Systems. E5-MS also allows users to access the web and command line interfaces of the LSMS servers. E5-MS users can monitor the LSMS alarm state and take relevant actions to maintain the LSMS servers in a healthy state.

Notes:

- E5-MS supports LSMS 12.0 and 13.0.
- LSMS supports SNMPv1.

LSMS Nodes

Each LSMS consists of a mated pair of LSMS servers, where one server is the active primary server and the other server is the backup secondary server. The primary and secondary LSMS servers are identified by the host names **lsmspri** and **lsmssec**. LSMS uses Network Attached Storage (NAS) for backup of the system logs, application logs, and databases.

The E5-MS defines an LSMS node as follows:

- Each LSMS server is considered a node (2 servers = 2 nodes).
- The NAS is not visible to E5-MS and is not considered to be a node, but rather a sub-resource of one of the LSMS servers.

The LSMS Discovery menu requires information for both LSMS servers and generates two nodes. The E5-MS can receive SNMP traps from three different resources (two LSMS servers and one NAS), but from only two IP addresses; the NAS alarms are sent to the LSMS servers and then from the LSMS servers to E5-MS.

LSMS Discovery Menu

From the E5-MS menu bar, select **Tools > LSMS Discovery** to access the LSMS Discovery application and discover LSMS servers within your network.

Note: **Tools > LSMS Discovery** is an available choice only for users that have permission to the **LSMS Discovery** administrative operation.

As shown in [Figure 35: LSMS Discovery Screen](#), the **LSMS Discovery** screen contains the following sections:

- Existing LSMS(s)

This section displays a list of previously added LSMS nodes.

- LSMS Configuration

This section shows the required and optional fields used for LSMS discovery. By default, the fields are blank. When an existing LSMS is selected in the top section, the fields are populated with the values provided by the user when discovering that LSMS.

- Action Buttons

The buttons at the bottom are used to perform the **Add**, **Modify**, **Delete**, **Reset**, and **Exit** operations.

Figure 35: LSMS Discovery Screen

As shown in [Figure 35: LSMS Discovery Screen](#), the **LSMS Discovery** screen contains the following fields:

- Name** Required CLI for both the primary and secondary LSMS servers. Valid names are 5 - 20 characters, including alphanumeric characters, hyphen, and underscore. The first character must be an alphabetic character.
- IP Address** Required IP address for both the primary and secondary LSMS servers.
Note: The NAS server IP address is not required, but can be added for informational purposes in the **Description** field.
- Login Name / Login Password** Required login name and login password to access the LSMS servers. Valid login names are 5 - 20 characters, including alphanumeric characters, hyphen, and underscore. The first character must be an alphabetic character. The password string cannot exceed 20 characters, and a blank string is not allowed.

System Number	Optional LSMS system number defined by the E5-MS user. Maximum length is 20 characters.
Description	Optional field used to add text/comments to describe a node, its location, and other useful information. Maximum length is 200 characters.
Country	Required field that indicates the country where the LSMS servers are installed, to allow presenting the LSMS nodes on a graphical map. If the country in which LSMS is deployed is not available in the drop-down list, select Others . You can also add a new country map to E5-MS; for information, see Adding a new country map to E5-MS .

Action Buttons

The following action buttons are available at the bottom of the **LSMS Discovery** screen:

Add	The Add operation initiates the discovery process. When adding an LSMS, the user must provide details for both the primary and secondary LSMS servers. After successful discovery, two LSMS nodes are displayed in the Existing LSMS(s) section. LSMS nodes are added without pinging the configured IP address.
Modify	The Modify operation updates an LSMS node in the E5-MS database. Upon successful modification, LSMS nodes are updated as needed in the Existing LSMS(s) section.
Delete	The Delete operation deletes an LSMS node from the E5-MS database. Upon successful deletion, LSMS nodes are removed from the Existing LSMS(s) section.
Reset	The Reset operation resets all LSMS Discovery configuration components to their default state.
Exit	The Exit operation exits the LSMS Discovery GUI.

Map Views

E5-MS automatically populates maps with all discovered LSMS servers by using the **Country** field entered by the user on the **LSMS Discovery** screen. The graphical map drill down view includes the following levels:

- World level map
- Continent level map
- Country level map

The LSMS map views are similar to the EAGLE map views described in [Map Views](#) . For example, see [Figure 36: Country Level Map with LSMS servers](#).



Figure 36: Country Level Map with LSMS servers

If the country in which LSMS is deployed was not available in the **Country** drop down list provided by LSMS Discovery and **Others** was specified, the LSMS will be displayed in the Others map under the World map. Thus, all LSMS nodes are visible on either a Country map or the Others map.

Note: New country maps can be added to E5-MS. For information, see [Adding a new country map to E5-MS](#).

For information about map view features, see [Map View Features](#).

Cut Through Interface from Maps to LSMS

E5-MS provides a Cut Through interface to connect from the map views to discovered LSMS servers through the Web and SSH interfaces. To access the Cut Through interface, right click on the desired LSMS node in the map view and select either **Launch SSH terminal** or **Launch Web interface**.

Note: The E5-MS user must provide login credentials on the launched interface.

Fault Management

The E5-MS fault management support for LSMS includes the following:

- [Events and Alarms Viewer](#)
- [Event and Notification Details](#)
- [Alarm Correlation and Aggregation](#)
- [Alarm Acknowledgement and Clear](#)
- [Alarm Maintenance/Active Mode](#)
- [Northbound Interface](#)
- [Status Management](#)

For general information about E5-MS fault management, see [Fault Management](#).

Events and Alarms Viewer

The Network Events and Alarms interface displays events and alarms in a tabular format. The SNMP traps received from LSMS are processed into events and displayed in the Network Events GUI (**Fault Management > Network Events**). Events that are associated with a defined pair event number are further processed into alarms and displayed in the Alarms GUI (**Fault Management > Alarms**) and map drill down view. Alarms represented on the drill down view depict the alarms state at the following levels:

- LSMS nodal view
Displays the alarm state of an LSMS server.
- Zonal view
Displays the alarm state of all the LSMS, EPAP, and EAGLE systems in a zone.

Event and Notification Details

- The E5-MS fault management module applies correlation to only those LSMS events that have corresponding pair events of "clear" severity.
- E5-MS buffers LSMS SNMP traps per LSMS before processing them into events to prevent loss of traps. The buffer size is configurable and the default is 6000 alarms/LSMS server (10 traps/sec for 10 minutes). If the buffer size is exceeded, a warning alarm is raised as follows:

Table 18: Event Details - Traps Buffer Overflow

Element	Description
Source	E5-MS
Sub Resource	AlarmMemory_<LSMS NAME>
Severity	Warning
Category	Fault
Message	Buffer overflows during traps processing for LSMS: <LSMS NAME>. This could result in loss of alarms.

The buffer size (LSMS_QUEUE_MAX_SIZE) can be configured in the `fault.properties` file in the `/Tekelec/WebNMS/conf/tekelec` directory.

- E5-MS fetches and stores the status (active/standby/inhibited) of both the primary and secondary LSMS servers during LSMS Discovery (Add/Modify) and during warm start of the E5-MS server. If E5-MS cannot fetch the status of an LSMS node, the following critical alarm is raised:

Table 19: Event Details - Unable to Fetch LSMS Status

Element	Description
Source	E5-MS
Sub Resource	LSMS_<node name>_ Status
Severity	Critical
Category	Fault
Entity	E5MS_LSMS_<node_name>_ Status
Message	Unable to fetch device status from <node_name>.

The following table shows the action performed in various scenarios when the LSMS status cannot be obtained.

Table 20: E5-MS Action When Status Cannot be Obtained

Scenario	E5-MS Action
A new LSMS is being added by the user	The LSMS is not added to E5-MS. The user receives the failure message with the reason "Status command failed on LSMS. Unable to fetch correct status".
An existing LSMS is being modified by the user	LSMS is modified successfully and a critical alarm is raised by E5-MS. This alarm must be manually cleared by the user.
During a warm start of the E5-MS server	A critical alarm is raised. This alarm must be manually cleared by the user.

Scenario	E5-MS Action
No "SwitchOverStarted" trap received, but "SwitchOverCompleted" trap received	A critical alarm is raised by the E5-MS. This alarm must be manually cleared by the user.

Alarm Correlation and Aggregation

The E5-MS fault management module applies correlation to only those LSMS events that have corresponding pair events of "clear" severity.

E5-MS aggregates alarms of child managed objects to reflect the status of the parent managed object as follows:

```
Parent MO alarm status = max [max(Child MO alarm(s)), parent MO alarms(if any)]
```

For example, the country server status in the continent map will be the total of all servers available in the country map (that is, EAGLE, LSMS, and EPAP).

Alarm Acknowledgement and Clear

E5-MS extends its alarm acknowledgement and clear functionality to LSMS alarms. Alarm acknowledgement allows a user to be associated with alarms to track and resolve them. The alarm clear operation raises a clear event for an alarm and clears the alarm from E5-MS (but does not make any changes on LSMS).

Alarm Acknowledgement and Clear are secured operations. The Alarm Acknowledgement operation requires the **Alert Pickup** permission and the Alarm Clear operation requires the **Clear Alerts** permission.

Alarm Maintenance/Active Mode

E5-MS extends its alarm maintenance/active mode operation to LSMS alarms. Maintenance mode is useful when an alarm is being generated on LSMS at a rapid rate due to a particular failure, leading to a flood of events at the E5-MS that continually increases the alarm count of a particular alarm.

In such cases, you can place an LSMS alarm in maintenance mode, which will drop the particular alarm as soon as it is received on E5-MS, without processing. After the failure scenario is resolved on LSMS, you can take the alarm out of maintenance mode and place it back in active mode. After an alarm is placed in active mode on E5-MS, it is cleared from the alarms view and processed in a normal fashion.

Maintenance and Active mode are secured operations requiring the user to have the **Maintenance** and **Active** permissions.

Northbound Interface

E5-MS extends the northbound interface feature to LSMS alarms. The northbound interface forwards alarms from LSMS to one or more client Network Management Systems. Incoming SNMP events and the outgoing events are mapped as follows:

- Outgoing alertTime = As received in the incoming trap
- Outgoing alertResourceName = LSMS node name defined in E5-MS
- Outgoing alertSubResourceName = As set by E5-MS
- Outgoing alertSeverity = As set by E5-MS

- Outgoing alertAcknowledgeMode = To be taken from E5-MS Fault Management status
- Outgoing alertTextMessage = As set by E5-MS
- Outgoing alertSequenceNumber = As set by E5-MS

Status Management

E5-MS manages LSMS status as follows:

- E5-MS fetches and stores the status (active/standby/inhibited) of both the primary and secondary LSMS servers during LSMS Discovery (Add/Modify) and during warm start of the E5-MS server.

For information about cases where E5-MS might fail to fetch the status of LSMS see [Table 20: E5-MS Action When Status Cannot be Obtained](#).

- Receipt of the 'SwitchOverCompleted' trap without receipt of a "SwitchOverStarted" trap from the LSMS server indicates that the active LSMS server has completed the automatic switchover of services to the standby LSMS server. In this case, the status of both LSMS servers is fetched and updated in E5-MS.
- Receipt of the 'SwitchOverFailed' trap from the LSMS server indicates that the automatic switchover of services from the active LSMS server to the standby LSMS server has failed. In this case, the status of both LSMS servers remains unchanged in E5-MS.
- On the map view, hovering the mouse over the LSMS node displays the current status of the LSMS server.

Chapter 8

Fault Management

Topics:

- *Overview.....91*
- *External E5-MS Applications.....91*
- *Functional Description.....91*
- *Events and Alarms Viewer93*
- *Alarm Correlations Rules.....95*
- *Southbound Resynchronization.....98*
- *Alarm Acknowledgement and Clear.....99*
- *Alarm Maintenance Mode.....101*
- *IPSM Switching.....102*
- *SNMP Active/Standby OAM Switching.....104*
- *Fault Management GUI.....105*
- *SNMP Traps.....107*
- *Alarm Reports.....109*
- *Security Operations.....110*

This chapter provides descriptions of the functions provided by the E5-MS Fault Management Interface.

Overview

The Fault Management Interface enables users to monitor multiple EAGLE system alarm streams managed by E5-MS. The Fault Management Interface gathers the EAGLE southbound information from the EAGLE Inventory application database, if the customer has the Inventory application available. The E5-MS supports EAGLE alarms using both SNMP and TL1 southbound protocols, and processes them into events. Each alarm depicts the alarm state of the EAGLE and all its sub components (i.e. frame, shelf, and card). The Fault Management Interface also enables users to receive EPAP and LSMS alarm streams using an SNMP southbound interface.

External E5-MS Applications

EAGLE inventory the base for fault management module. Fault management module associates all events and alarms to managed object (i.e. eagle and its sub components) populated by inventory module, also, it displays alarms on the drill down view generated by inventory module.

A System Administrator will assign the users single or multiple operations of the Fault Management application, such as maintenance, active, resynchronization, alarm acknowledgement, unacknowledgement and clear.

Functional Description

Fault management module can be divided into following features:

- **Alarm/Event Viewer**
 - E5-MS provides a tabular interface for displaying all events and alarms. EAGLE UAMs/SNMP traps are processed into events and added to the **Network Events** GUI then processed into alarms and displayed in the **Alarms** GUI and drill down view. Alarms represented a drill down view as follows:
 - Chassis view displays an alarm state of each card in an EAGLE frame.
 - Frame view displays an alarm state of each EAGLE frame.
 - EAGLE nodal view displays an alarm state of an EAGLE.
 - Zonal view displays an alarm state of multiple EAGLE(s) in a zone.
- **Alarm Correlation and Aggregation**
 - E5-MS fault management module applies correlation and aggregation rules ([Table 21: Alarm Correlations Rules](#)) on events to generate alarms. This ensures that all events generated shall get logically grouped to represent actual alarm state of EAGLE and its sub components.
- **Southbound Resynchronization**
 - E5-MS constructs an alarm state of managed EAGLE and its sub components (i.e. frame, shelf, card) by processing UAMs/SNMP traps, however, there are scenarios where the E5-MS is out

of sync with EAGLE alarm state (for e.g. due to connection failure between E5-MS and EAGLE etc.). To resolve the out of sync scenarios, the E5-MS has a southbound resynchronization feature which synchronizes the E5-MS with the EAGLE alarm state.

- **Alarm Acknowledgement and Clear**

- E5-MS provides the user an acknowledge or clear an alarm functionally. Both acknowledgement and clear are secured operations and only user(s) assigned with these security operations are able to perform these operations.
- Alarm acknowledgement allows a user associated with alarm for tracking and resolving of alarms. An optional email feature will send the user a notification for the alarm.
- Alarm clear operation clears an event for alarm in E5-MS; however, this does not make any changes on EAGLE.

- **Alarm Maintenance mode**

- E5-MS provides a user to put an alarm in maintenance mode. This functionality is useful when an alarm is getting generated on EAGLE at a rapid rate due to a particular failure. The flood of events at the E5-MS keep increasing the alarm count of a particular alarm till the same alarm is resolved. In such cases the user can put an alarm in maintenance mode, which drops the particular EAGLE alarm as soon as it is received on E5-MS without processing. Once the failure is resolved on the EAGLE then the user is able to get the alarm out of maintenance mode by using active mode. Alarm once the alarm is active on E5-MS it is cleared from alarms view and processed in a normal fashion.
- Maintenance and Active mode are a secured operation and only authorized users are able to perform these operations.

- **IPSM Switching**

- E5-MS provides an automatic recovery from fault interface failure when EAGLE is TL1 enabled. If the E5-MS loses connectivity to EAGLE via one of IPSM interface; the other configured IPSM on the EAGLE is used for listen for the UAM/UIM data. In this case E5-MS automatically switches between the available IPSM interfaces to maintain connectivity with EAGLE as per the algorithm stated in **IPSM Switching Algorithm**.

- **SNMP Active/Standby OAM Switching**

- E5-MS has an automatic switchover between Active and Standby OAM in case the EAGLE is SNMP enabled. If there is a switchover, the EAGLE does not have a mechanism to notify E5-MS, however, the southbound resynchronization at the E5-MS fails as the resync request is sent to current active OAM IP. In this case a southbound resync fails at E5-MS then resync request is sent to standby OAM IP. If resync is successful then the E5-MS is switched between active and standby OAM in the database, unless there is a resync failure message sent to the client.

- **Custom View**

- E5-MS shall provide provision for creating custom views which is tailored for viewing a subset of data that satisfies specific criteria. Custom views are persistent in nature and can be created by each user for both Alarms and Network Events View. E5-MS provides a right click menu option to create, modify and delete custom view as shown in Network Events and Alarm Tree Node available on left panel under Fault Management.

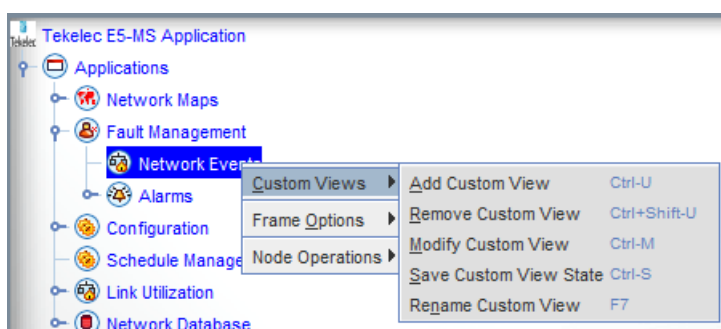


Figure 37: Network Events and Alarm Tree Node

Events and Alarms Viewer

The Network Events and Alarms interface displays events and alarms. The EAGLE UAMs/SNMP traps, also known as events are added to **Network Events** GUI then processed into alarms and get displayed in **Alarms** GUI. Alarms represented on drill down view depicts the alarms state at each level as follows:

- Chassis view displays alarm state of each card in an EAGLE frame.
- Frame view displays alarm state of each EAGLE frame.
- EAGLE nodal view displays alarm state of an EAGLE.
- Zonal view displays alarm state of multiple EAGLE systems in a zone.

The Fault Management Interface gathers EAGLE southbound protocol information from inventory module.

Event and Notification Details

E5-MS shall automatically trigger southbound resynchronization under scenarios listed below and corresponding resynchronization initiation events are raised along with client notifications.

Event Details

Element	Description
Source Field	E5-MS
Sub Resource Field	<EAGLENAME>
Severity Pane	Info.
Category	Fault
Message	Initiating alarm resynchronization with EAGLE
Reason	Specified below along with each use case

Notification Details

Initiating alarm resynchronization with EAGLE <EAGLENAME>.

Reason: Specified below along with each use case.

Automatic resynchronization Scenarios:

Scenarios	Message
On EAGLE addition	EAGLE added to E5-MS
On receipt of 'UIM 1340' for resynchronization, in case southbound protocol is TL1	Received UIM 1340 from EAGLE for alarm resynchronization
On receipt of 'resyncRequiredTrap' for resynchronization, in case southbound protocol is SNMP	Received resyncRequiredTrap from EAGLE for alarm resynchronization.
Change of EAGLE southbound protocol or protocol specific configurations	EAGLE configuration details modified by user.
On switching to next configured EMSALM terminal (if configured on other IPSM interface) in case existing EMSALM connection breaks	Connection established on EMSALM port <EMSALMPORT> on IPSM IP <IP ADDRESS>.
On receipt of heartbeat once fault interface for an eagle is down, in case southbound protocol is SNMP	Regaining connection.
On warm start of server	Warm start of server.
E5-MS shall send automatic resynchronization operation status notifications to all active E5-MS clients	Automatic Alarm resynchronization completed for EAGLE <EAGLENAME>.

Failure of Automatic Resynchronization

In case of failure of automatic resynchronization for an EAGLE an event will occur and notifications are sent to all active E5-MS clients. Event details are as follows:

Fields	Description
Source	E5-MS
Sub resource	<EAGLENAME>
Category	Fault

Fields	Description
Severity	INFO
Message	Automatic resynchronization failed for EAGLE.

If a notification is sent to client the message would be Alarm resynchronization failed for EAGLE: <EAGLENAME>.

Automatic Resynchronization

E5-MS shall trigger resynchronization on active OAM in case SNMP FAK is enabled on EAGLE. If resynchronization fails on active OAM then E5-MS shall automatically trigger resynchronization on standby OAM as configured during EAGLE Add operation on EAGLE Discovery GUI. If resynchronization gets successful then active and standby OAM are switched at E5-MS, else an error message Alarm resynchronization failed for EAGLE: <EAGLENAME> are displayed to user. Event details are as follows:

Fields	Description
Source	E5-MS
Sub resource	<EAGLENAME>
Category	Fault
Severity	INFO
Scenario and message	<ul style="list-style-type: none"> Switching completed successfully: - Switched to standby OAM IP <New Active OAM IP> from <NEW Standby OAM IP> for EAGLE. Switching detected but OAM not updated at E5-MS: - Switching of Active/Standby OAMs detected but data not updated. Reason: DB operation failed

Note: This functionality are applicable in case EAGLE supports SNMP at southbound for fault management.

Alarm Correlations Rules

To ensure all events are generated in a logical group to represent the alarm state of the EAGLE and its sub components, the FMI applies correlation and aggregation rules on events to generate alarms. As shown in the table Alarm Correlations Rules below

Table 21: Alarm Correlations Rules

Step #	Step	Severity	Resource	SubResource	Behavior on Alarms	Behavior on Network Events	Alarm Entry in database
1	Send Minor Alarm with Resource as A and SubResource as B	Minor	A	B	New Minor alarm is displayed in Alarms (count is 1, severity is Minor, previous severity is Blank).	New Minor event is displayed in Network Events (count is 1, severity is Minor).	New entry in database for this minor alarm (count = 1, Severity is minor, Previous severity is Blank).
2	Send Major Alarm with Resource as A and SubResource as B	Major	A	B	Minor alarm (step1) is replaced by Major alarm (count is reset to 1, severity is major, previous severity is Minor).	New Major event displayed in Network events (count is 1, severity is Major), while the old Minor event is still visible.	Update existing alarm entry in database for resource, sub resource combination. Updated alarm is(count = 1, Severity = major, Previous severity = minor).
3	Send <u>SAME</u> Major Alarm with Resource as A and SubResource as B	Major	A	B	Old Major alarm (step2) is replaced by new Major alarm (count is incremented to 2, severity is major, previous severity is Minor).	New major event displayed in Network events with count = 1 and severity = Major.	Update existing alarm entry in database for this major alarm (count = 2, Severity = Major, Previous severity = Minor).
4	Send Minor Alarm with Resource as A and	Minor	A	B	Major alarm (step3) is replaced by new Minor alarm	New Minor alarm is displayed	Update existing alarm entry in database

Step #	Step	Severity	Resource	SubResource	Behavior on Alarms	Behavior on Network Events	Alarm Entry in database
	SubResource as B				(count is set to 1, severity is Minor, previous severity is Major).	in Network Events (count is 1; severity is Minor while the old Minor (step1) and major event (step2, step 3) are still visible.	for this minor alarm (count = 1, Severity = Minor, Previous severity = Major).
5	Send <u>Same</u> Minor Alarm with Resource as A and SubResource as B	Minor	A	B	Minor alarm (step4) is replaced by new Minor alarm (count is incremented to 2, severity is Minor, previous severity is Major).	New minor event displayed in Network events with count = 1 and severity = Minor.	Update existing entry in database for this minor alarm (count = 2, Severity = Minor, Previous severity = Major).

Alarm Correlation and Aggregation

An EAGLE aggregated alarms are child managed object(s) to reflect the status of parent managed object as follows:

```
Parent MO alarm status = max [max(Child MO alarm(s)), parent MO alarms(if any) ]
```

Aggregation Details

The aggregation details work as follows:

- Zonal alarm is the max of all EAGLE alarms that exist in that zone.
- EAGLE alarm is the max of all frame alarms that are configured for that EAGLE and EAGLE alarms.
- EAGLE frame alarm is the max of all card alarms for that frame and EAGLE Frame alarms.

The EAGLE events in the Network Events screen are linked to the alarms referenced in [link to Alarm Correlation Rules](#)

Southbound Resynchronization

E5-MS manages the alarms status of the EAGLE and its sub components (i.e. frame, shelf, card) by processing UAMs/SNMP traps. There are cases when the E5-MS gets out of sync with EAGLE alarm state (for e.g. due to connection failure between E5-MS and EAGLE etc.). To handle such cases, E5-MS has a southbound resynchronization feature which gets E5-MS in sync with EAGLE alarm state.

The southbound resynchronization functionality is performed on multiple EAGLE systems simultaneously regardless of the southbound protocol (i.e. SNMP or TL1). The E5-MS user resynchronizes the southbound resynchronization both manually and automatically facility clicking the **RESYNC** button from the EAGLE Discovery tool, as mentioned in Inventory Chapter....

Buffer Incoming UAM Details

E5-MS buffers incoming UAMs for an EAGLE for which southbound resynchronization has been initiated in case southbound protocol is TL1.

Note: In case of SNMP, buffering happens at EAGLE end itself.

Location of Buffered Southbound Resynchronization

E5-MS buffers configurable number be named as `QUEUE_MAX_SIZE` at file location `/Tekelec/WebNMS/conf/tekelec/fault.properties` (4 Alarms/sec for 20 minutes per EAGLE = 5000 alarms) of EAGLE alarms during southbound resynchronization. If number of alarms cross the buffer size then buffer is overwritten and a 'Warning' alarm is raised with following properties:

Fields	Description
Source	E5-MS
Sub resource	AlarmMemory<EAGLENAME>
Category	Fault
Severity	Warning
Scenario and message	Buffer overflows during southbound resynchronization for EAGLE: <EAGLE NAME>.This could result in loss of alarms.

Note: If SNMP, buffering happens at EAGLE end itself. The buffer value is further fine tuned during performance testing.

E5-MS shall randomly select any available IPSM terminal as RESYNC terminal for fetching EAGLE alarm(s) snapshot using TL1 protocol. If no terminals are available on EAGLE for RESYNC then a failure message Southbound resynchronization failed for EAGLE: <EAGLE NAME>!Reason: Terminal not available on EAGLE to perform 'RESYNC'. Please resolve the issue and try again.

Alarm Acknowledgement and Clear

Alarm acknowledgement and clear alarm functions are secured functions that a System Administrator assigns the users the **Alert Pickup** security operation.

Alarm acknowledgement is an interface a user associates an alarm for tracking and resolving. An email notification is sent to the assigned user.

Alarm clear operation clears the alarm in E5-MS; however it does not make any changes on EAGLE.

Alarm Acknowledgement

On alarm acknowledgement operation, alarm are updated with the user name (i.e. alarm owner field is updated with user name that is assigned) and acknowledged timestamp (i.e. AckDate) in database. The following event is generated on acknowledging an alarm:

Fields	Description
Source	<Alarm Source>
Sub resource	<Alarm Subresource>
Category	Fault
Severity	INFO
Scenario and message	<p>Success Scenario:</p> <p>Alarm acknowledged for user <User to whom alarm is assigned> by < User who assign alarm ></p> <p>Failure scenarios :</p> <ul style="list-style-type: none"> Invalid User: Alarm acknowledgement operation failed for user <User to whom alarm is assigned > by <User who assigned alarm>. Reason: <User to which alarm is assigned> is invalid user. Disabled user: Alarm acknowledgement operation failed for user <User to whom alarm is assigned > by <User who assigned alarm>. Reason: <User to which alarm is assigned> is disabled user.

Email Alarm Acknowledgement

An optional feature of the Fault Management Interface is an Alarm Acknowledgement email sent to the user assigned to the alarm. The mail configuration GUI allows email ID configuration for all E5-MS users.

Alarm Unacknowledged

If the user does not acknowledge the alarm associated with the username, the alarm will be removed from the data base (i.e. alarm owner field and AckDate is reset). The following event is generated:

Fields	Description
Source	<Alarm Source>
Sub resource	<Alarm Subresource>
Category	Fault
Severity	INFO
Scenario and message	Success Scenario: Alarm unacknowledged by user <Username>. Failure scenario: Alarm unacknowledged operation failed for user <User who unassign alarm>

Email Alarm Unacknowledged

An optional feature of the Fault Management Interface is an Alarm Unacknowledged email sent to the user assigned to the alarm. The mail configuration GUI allows email ID configuration for all E5-MS users.

Alarm Clear Event

Clear Alert operation is available to only authorized E5-MS users having **Clear Alerts** security operation assigned.

The Alarm Clear event function provides the following event is generated:

Fields	Description
Source	<Alarm Source>
Sub resource	<Alarm Subresource>
Category	Alarm Category
Severity	Clear
Scenario and message	<ul style="list-style-type: none"> Manual Clear: - Alarm cleared by E5-MS user <USERNAME>. Automatic Clear: - Alarm cleared by E5-MS. Maintenance Alarm changed to Active mode message - Maintenance alarm cleared by E5-MS user <USERNAME>. Buffer overflow alarm clear message - Buffer overflow alarm cleared by E5-MS.

Note: Alarm clear operation triggered from E5-MS does not send any notification to corresponding EAGLE.

To clear the alarm (Edit > Clear Alerts). If there is a failure, an error message stating Alarm acknowledgement operation failed for Resource: <RESOURCE> and Sub resource: <SUBRESOURCE>! Reason: <REASON> Please resolve the issue and try again. will pop up on the screen.

Alarm Maintenance Mode

The **Maintenance** mode function is available to authorized E5-MS users assigned by a System Administrator.

An alarm can be put in a **Maintenance** mode by the user when an alarm is generated by the EAGLE at a rapid rate due to a particular failure. To prevent the events from flooding the E5-MS, the user would put the alarm in **Maintenance** mode. This function is for a particular alarm to drop as soon as it is received on E5-MS without processing. Once the failure scenario gets resolved on EAGLE then user can put the alarm out of **Maintenance** mode by using **Active** mode functionality. Once the alarm is active on E5-MS it is cleared from alarms view and processed as normal.

The alarms in **Maintenance** mode alarm severity is highlighted in grey color.

Setup Alarm in Maintenance Mode

The alarm severity is set in the maintenance mode then all events received at the E5-MS corresponding the set alarm are dropped without processing. The following event is generated to put the alarm in maintenance mode:

Fields	Description
Source	<Alarm SOURCE>
Sub resource	<Alarm SUBRESOURCE>
Severity	Maintenance
Message	Error message: Alarm set to maintenance by user <USER NAME>

Notification such as Alarm maintenance operation failed for all/some alarms! Please try again. is sent to user in case of a failure of the Maintenance operation.

Note: This is only available to authorized E5-MS user assigned security operations Maintenance and Active mode.

Setup Alarm in Active Mode from Maintenance Mode

This is only available to authorized E5-MS user assigned security operations **Maintenance** and **Active** mode.

Once the alarm is set to active mode from maintenance mode all events are processed as normal. The following event is generated to put the alarm in active mode:

Fields	Description
Source	<Alarm SOURCE>
Sub resource	<Alarm SUBRESOURCE>
Severity	Clear
Message	Error message: Maintenance alarm cleared by E5-MS user <USER NAME>

To set the alarm to **Active** mode click (View > Maintenance and View > Active)

Notification such as Alarm maintenance operation failed for all/some alarms! Please try again. is sent to user in case of a failure of the Active operation.

IPSM Switching

E5-MS provides an automated mechanism to recover from fault interface failure in case EAGLE is TL1 enabled. If E5-MS loses connectivity to EAGLE via one of IPSM interface another IPSM can be configured on EAGLE that is used for listening UAM/UIM data.

IPSM Switching Algorithm

IPSM switching is required in Fault module to ensure automated recovery once the existing Fault interface breaks between E5-MS and EAGLE.

1. On EAGLE addition via inventory module, Fault module automatically connects to EAGLE IPSM interface on EMSALM port to receive UAM's/UIM's.
 - a. Order of connection to IPSM interface is IPSM1, IPSM2 and then IPSM3 as configured on EAGLE Discovery GUI.
2. As soon as first EAGLE gets added to E5-MS a fault scheduler gets started. This scheduler runs at one second interval to check E5-MS Fault interface connectivity to all EAGLE(s).
3. Fault interface between E5-MS and EAGLE is assumed connected; if UIM 1083 gets received at every 15 minutes interval, it is assumed to be down. Specified interval is configurable.
4. In case fault interface gets down then IPSM switching is done as per the below mentioned procedure:
 - a. Case 1:- E5-MS is able to make session to IPSM card on EMSALM terminal
 - a. If UIM 1083 is not received in 15 minutes, raise an alarm. Refer '**Alarm raising rule**'.
 - b. Break the existing connection.
 - c. Recreate session with EAGLE.
 - a. If only one IPSM is available it is tried again.
 - b. If more IPSM are available then next configured IPSM is tried. Next IPSM is chosen from the set of available IPSM before the current one is retried. If set has two IPSM (i.e. if 3 IPSM are configured) then they are chosen in increasing order. For e.g. if connection was

braked with IPSM3 then IPSM1 is tried before IPSM2. If the connection can't be established with IPSM1 and IPSM2 then IPSM3 is tried again.

- c. Automatic Resync gets performed with EAGLE.
- d. Wait for UIM 1083 for 15 minutes again and go to step a.
- b. Case 2: E5-MS is not able to make session to any IPSM card on EMSALM terminal
 - a. E5-MS can't connect to IPSM
 - b. Wait for 15 minutes (i.e. inactive for that time).
 - c. Raise an alarm, refer 'Alarm raising rule'.
 - d. Retry connection with configured IPSMs.
 - a. If only one IPSM is configured then it is tried again.
 - e. If 2 or more IPSM are available then the next configured IPSM is tried before the current one which is IPSM1.
 - f. If connection gets established then wait for UIM 1083 for 15 minutes or if connection can't be established with any configured IPSM go to step a.
5. If UIM 1083 gets received in configured interval (i.e. 15 minutes) then following steps are performed:
 - a. Clear alarm gets raised. Alarm Details is as shown in

Source	E5-MS
Sub Resource	<EAGLENAME>
Severity	Clear
Message	Fault interface is up

Alarm Raising Rule

For EAGLE, the number of warning alarms are equal to number of IPSMs configured for that Eagle. Critical alarm is generated thereafter (i.e. count of alarm shall keep incrementing).

- Warning Alarm Details:

Source	E5-MS
Sub Resource	<EAGLENAME>
Severity	Warning
Message	Connection failure detected on EMSALM <EMSALM> on IPSM IP <IPSM IP>

Note: In case E5-MS is unable to make connection to any configured IPSM IP on EMSALM terminal then in the above message IPSM IP and EMSALM port is of the IPSM1 IP for the first time on eagle addition to initiate switching.

- Critical Alarm Details:

Source	E5-MS
--------	-------

Sub Resource	<EAGLENAME>
Severity	Critical
Message	Cannot connect to EAGLE for receiving alarms

Note: In case of critical alarm notification to user shall also be sent every time critical alarm gets raised with following message E5-MS cannot connect to EAGLE: <EAGLENAME> for receiving alarms! Please check the connection.

For EPAP, if a heartbeat trap is not received at the configured interval (default is 15 minutes), a warning alarm is raised first followed by a critical alarm after each successive interval.

- Warning Alarm Details:

Source	E5-MS
Sub Resource	AlarmMemory_<EPAP NAME>
Severity	Warning
Message	Cannot connect to EPAP for receiving alarms

- Critical Alarm Details:

Source	E5-MS
Sub Resource	AlarmMemory_<EPAP NAME>
Severity	Critical
Message	Cannot connect to EPAP for receiving alarms

E5-MS notifies all active E5-MS client sessions with the following message:

```
E5-MS cannot connect to EPAP: <EPAP NAME> for receiving alarms! Please check the connection.
```

Limitation

As specified in algorithm step 2, Fault scheduler kicks off as soon as first EAGLE gets added, however, session creation to EAGLE at EMSALM may take some time. In this case there can be a scenario when though heartbeat is sent by EAGLE but not received at E5-MS during configured time interval due to which an alarm may get raised even though the connectivity is working fine. This scenario has an impact only for first time and not afterwards as the E5-MS shall then get sync up with EAGLE heartbeat received time and shall check at appropriate time afterwards.

SNMP Active/Standby OAM Switching

E5-MS provides an automated mechanism to switch over between Active and Standby OAM in case EAGLE is SNMP enabled. If there is a switch over between active and standby OAM, the EAGLE does

not have a mechanism to notify E5-MS about the switch over. The E5-MS fails the resynchronization request sent to current active OAM IP. After the southbound resynchronization fails, a resync is sent to the new active OAM IP. At the successful resynchronization the E5-MS switches between active and standby OAM in database then resync failure message is sent to client.

Fault Management GUI

E5-MS provides two GUIs for displaying **Network Events** and **Alarms** available on left panel as tree node under **Fault Management**.

Network Events and Alarms Screens

The **Network Events** and **Alarms**, screens are accessed from the **Fault Management** tree node on the left panel of the E5-MS.



Figure 38: Fault Management Tree Node

Network Events

Network Events GUI displays the historical events pertaining to EAGLE system.

Resource	Sub-Resource	UAM/UIM/MRN Number	Severity	Message	Protocol	Device Time Stamp	E5-MS Timestamp
eagle11_Frame1	-		Critical	Status Update	-		Aug 28,2013 02:08:44 AM
eagle11_Frame1	-		Minor	Status Update	-		Aug 28,2013 04:18:32 AM
eagle11_Frame1	-		Major	Status Update	-		Aug 28,2013 12:00:12 AM
eagle11_Frame1	-		Clear	Status Update	-		Aug 28,2013 02:08:44 AM

Figure 39: Historical Network Events

The Network Events display the following fields:

- Resource
- Sub-Resource
- UAM/UIM/MRN Number
- Severity
- Message
- Protocol
- Device Timestamp
- E5-MS Timestamp

Alarms

Alarms GUI displays alarms from EAGLE system after applying correlation rules. This view displays active alarms pertaining to EAGLE system managed by E5-MS as shown in Figure

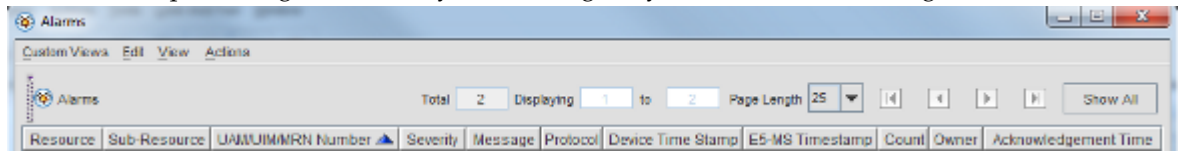


Figure 40: Alarms Pane

The Alarms display the following fields:

- Resource
- Sub-Resource
- UAM/UIM/MRN Number
- Severity
- Message
- Protocol
- Device Timestamp
- E5-MS Timestamp
- Count
- Owner
- Acknowledgement Time

Network Events and **Alarms** GUIs support paging, sorting and searching functionality to help a user quickly browse through the records. Following search criteria is supported in Network Events/Alarms GUI:

- Severity
- Resource
- Sub-Resource
- Message
- Event/Alarm ID
- Device Timestamp
- E5-MS Timestamp

The users functionality of **Add/Remove/Modify** custom views. **Custom Views** are used to filter the views of **Alarms** and **Network Events** GUI based of following criteria:

- Severity
- Resource
- Sub-Resource
- Message
- Event/Alarm ID

The user creates a custom view by right clicking **Network Events** or **Alarms** tree node available on left panel under **Fault Management**.

Fault management provides an interface to query events database. It allows querying database based on date, time, event type, severity, resource, sub-resource, text and UAM number.

 **Notes:**

- To filter based on event/alarm ID, do not include the leading zero for event/alarm ID values that start with zero. For example, for filtering alarms having alarm ID 0387, the filter must be created with value 387. A filter created using value 0387 will not work.
- To create a filter for a sub-resource or entity value that includes a comma (,), create the filter using an asterisk in place of the comma. For example, to filter for alarms having sub-resource value "ENET 1101,A", specify "ENET 1101*A". A filter created with the comma will not work.
- For detailed information about custom views, see [Fault Management GUI Custom Views](#).



SNMP Traps

The Fault Management monitors EAGLE alarms at a rate (4 Alarms/sec/EAGLE) at which each EAGLE in a network sends alarms. E5-MS fault management module supports both TL1 and SNMP southbound interfaces simultaneously.

Note: Through this requirement, E5-MS is able to support a network where some EAGLEs are SNMP enabled and some are not.

E5-MS fault management module gathers EAGLE southbound protocol information from inventory module. E5-MS listens to SNMP traps and process them into events in case southbound protocol is SNMP.

E5-MS listens to UAMs and UIMs: resynchronization required) and process them into events in case southbound protocol is TL1.

E5-MS buffers EAGLE UAMs/SNMP traps per EAGLE before processing them into event to prevent loss of UAM/trap. Buffer size is configurable; however, it defaults to 5000 alarms/EAGLE (i.e. 4 Alarms/sec for 20 minutes). In case number of alarms cross the buffer size then buffer is overwritten and a 'Warning' alarm is raised with the following properties:

- Source = E5-MS
- SubResource = AlarmMemory_<EAGLENAME>
- Category = Fault
- Severity - Warning
- Message :
 - During Resync: - Buffer overflows during southbound resynchronization for EAGLE: <EAGLENAME>.This could result in loss of alarms
 - During UAM Processing: - Buffer overflows during UAMs/traps processing for EAGLE: <EAGLENAME>.This could result in loss of alarms.

Note: Buffer value is further fine tuned during performance testing

E5-MS listens for traps from multiple EAGLE(s) at configured trap port. E5-MS listens to UAMs and UIMs received on EMSALM terminal configured by user in case southbound protocol is TL1. E5-MS makes connection to EAGLE EMSALM terminal on successful EAGLE discovery and connection is terminated on deletion of EAGLE from E5-MS inventory. E5-MS fault management module receives EAGLE modification event from inventory module will validate if EMSALM terminal it's listening

for UAMs exists or not. In case it doesn't exist then existing connection with the EMSALM terminal is destroyed and new connection is constructed.

Note: This functionality is applicable in case EAGLE supports TL1 at southbound for fault management and not SNMP.

E5-MS fault management module listens for 'UIM 1083: System alive' at configured interval (default being 15 minutes) to verify EMSALM connection for a TL1 EAGLE. In case specified UIM is not received for configured interval then E5-MS performs following steps:-

1. Case 1:- E5-MS is able to make session to IPSM card on EMSALM terminal
 - a. If UIM 1083 is not received in 15 minutes, raise an alarm. Refer 'Alarm raising rule' in [IPSM Switching Algorithm](#).
 - b. Destroy the existing connection.
 - c. Recreate session with the EAGLE.
 - a. If only one IPSM is available, is tried again.
 - b. If more IPSM are available then the next configured IPSM is tried. Next IPSM is chosen from the set of available IPSM before the current one is retried. If set has two IPSM (i.e. if 3 IPSM are configured) then they are chosen in increment order. For e.g. if connection was destroyed with the IPSM3 then IPSM1 is tried before the IPSM2. If the connection can't be established with the IPSM1 and IPSM2 then IPSM3 is retried.
 - c. Automatic resynchronization gets performed with the EAGLE.
 - d. Wait for UIM 1083 for 15 minutes again and continue as mentioned in Step a.
2. Case 2: E5-MS is not able to make session to any IPSM card on EMSALM terminal
 - a. E5-MS cannot connect to IPSM.
 - b. Wait for 15 minutes (i.e. inactive for that time).
 - c. Raise an alarm, refer 'Alarm raising rule' in [IPSM Switching Algorithm](#).
 - d. Retry connection with configured IPSMs.
 - a. If only one IPSM is configured then same is retried.
 - e. If 2 or more IPSM are available then the next configured IPSM is tried before the current one which in this case is IPSM1.
 - f. If connection get established then wait for UIM 1083 for 15 minutes else if connection cannot be established with any configured IPSM continue from to step a.

If UIM 1083 is received in configured interval (i.e. 15 minutes) then Clear alarm is raised to clear any IPSM switching alarm, if one exists in E5-MS for that EAGLE.

Following alarms are raised during IPSM switching as per 'Alarm Raising rule' mentioned in [IPSM Switching Algorithm](#):

- Source = E5-MS
- SubResource = <EAGLENAME>
- Category = Fault

Messages and severity:

- Warning Alarm:- Connection failure detected on EMSALM <EMSLAM PORT> on IPSM IP <IP ADDRESS>.
- Critical Event: - Cannot connect to EAGLE for receiving alarms.

- Info event message to try on IPSM for new connection: - Trying to connect to EMSALM <EMSALM PORT> on IPSM IP <IP Address>
- Connection establishment INFO message: - Connection established on EMSALM <EMSALM PORT> on IPSM IP <IP Address>.

E5-MS notifies all active E5-MS client sessions about fault interface failure the message
E5-MS cannot connect to EAGLE: <EAGLE NAME> for receiving alarms! Please check the connection.
to the EAGLE in case a Critical alarm is raised.

Clear alarm details is as follows:

- Source = E5-MS
- Sub resource = <EAGLENAME>
- Severity = Clear
- Message = Fault interface is up.

Note: This functionality is applicable in case EAGLE supports TL1 at southbound for fault management and not SNMP.

E5-MS fault management module listens for 'heartbeat Trap' at configured interval (default being 15 minutes) to verify SNMP EAGLE fault management interface.

If a specified trap is not received for configured interval, then a warning alarm is raised first followed by Critical alarm after each time configured interval lapses. E5-MS shall notify all active E5-MS client sessions about fault interface failure the message

E5-MS cannot connect to EAGLE: <EAGLE NAME> for receiving alarms! Please check the connection.
to EAGLE in case a Critical alarm is raised.

If heartbeat gets received in configured interval (i.e. 15 minutes) then Clear alarm gets raised to clear any IPSM switching alarm, if one exists in E5-MS for that EAGLE.

E5-MS stores events and alarms in database and allows access to historical information (i.e. events). At maximum E5-MS database provides access to 30 million network event records. E5-MS Network Event GUI provides access to latest 10000 event records only. Complete database events is accessible via reporting tool.

E5-MS automatically cleans up events older than 31 days or if number of events in database crosses the limit of 30 million.

E5-MS provides an interface an option to archive historical events into dump files and clean up database. User can schedule archival and clean up via E5-MS scheduler interface as per his convenience.

E5-MS logs all fault management logs in a separate log file. E5-MS fault management application and database supports a minimum of 200 entries per second (i.e. 200 TPS).

Alarm Reports

E5-MS shall provide a reporter interface for generating fault management reports.

E5-MS fault management module shall support following reports:

- Daily-Alarm-Totals - contains an aggregate number of alarms for any day within a selected date/time range.
- Audit-Trail-Report - report for auditing alarms

- Maintenance-Mode-History - contains the resources that were placed in maintenance mode within a selected date/time range, and the amount of time each resource remained in this mode.
- Most-Active-Alarmed-Resources - contains the top ten alarms occurring in the network within a selected date/time range for selected resources.
- Alarms-Durations - contains the time (in seconds) that a resource(s) was in an alarm state within a selected date/time range.
- Alarm-History - contains alarms that occurred for selected resources in the network.
- Alarm-Severities - contains percentages of each severity level that occurred within a selected date/time range for selected resources.

Security Operations

Fault management module shall introduce following new operations in E5-MS:

1. Alarm Acknowledgement operation > **Alert Pickup**.
2. Alarm Clear operation > **Clear Alerts**.
3. Maintenance and Active operation > **Maintenance and Active**.
4. EAGLE Alarm Resynchronization operation > **Eagle Resync**.

Chapter 9

Measurements Module

Topics:

- *Overview.....112*
- *Functional Description.....112*
- *DataBase Overview.....114*
- *DataBase Tables.....116*
- *Measurement Northbound FTP Module.....118*
- *File Transfer.....120*
- *Report Types Supported by Measurement Platform Module.....121*

The chapter provides descriptions of the feature and functions of the E5-MS Measurements Module. As an interface with the EAGLE Measurement Platform, it processes the measurement files then loads them into a Data Base (DB). This data is compiled to build reports and/or measurement thresholds based alarms.

Overview

E5-MS Measurements Platform module is used for parsing and management of EAGLE's performance data. The E5-MS Measurements FTP module parses the measurement files to northbound servers using FTP protocol. Measurement platform module is a core part of the license issued for E5-MS. No separate key is needed for it. However, E5-MS Measurements FTP module is licensed and a license must be purchase to use this feature.

Functional Description



Measurement module manages the measurement CSV files received from all managed EAGLE(s). Support of OAM measurements is not be provided.

All the log messages generated by Measurement platform module are captured in a log file `measurement.txt`. The Measurement module log file is present under `/var/E5-MS/measurement/logs` directory.

Input and output directories used by the Measurement platform module exist on the system before the module starts. The E5-MS creates them during installation. The default path for the input directory is `/root/E5-MS/measurement/csvinput`, and the path for the output directory is `/var/E5-MS/measurement/csvoutput`.

The default input directory `/root/E5-MS/measurement/csvinput` is owned by root. For any user other than root to be able to upload FTP measurement files to the input directory, use the `inputDirectory` parameter in the `/Tekelec/WebNMS/conf/tekelec/common.config` file to set the location that E5-MS scans for incoming measurement CSV files. If the `inputDirectory` parameter is modified while the E5-MS server is active, restart the server to activate the change.

- The Measurement platform module during startup will first verify the existence of `tekelec_meas_headers` table in E5-MS database and a the log message (refer to message 1 in the [Log Message List](#)) is written in the log file `measurement.txt`.
- After verification of `tekelec_meas_headers` table, Measurement platform module verifies the existence of `tekelec_meas_reports` table in the E5-MS database a the log message (refer to message 2 in the [Log Message List](#)) is written in the log file `measurement.txt`.
- After verification of `tekelec_meas_headers` table and `tekelec_meas_reports` tables, the Measurement platform module verifies whether the data (measurement report types and corresponding database tables) required in `tekelec_meas_reports` table is available. If the data is filled, it logs the messages of all the measurement report types supported and their corresponding database tables (refer to message 3 in the [Log Message List](#)). If the data is not available, then it logs the message (refer to message 4 in the [Log Message List](#)).
- The Measurement platform module scans the input directory for measurement report files received from Eagle(s). While scanning, log message (refer to message 5 in the [Log Message List](#)) is written in the log file `measurement.txt`. If no measurement report files are found in the input directory or the module finished the parsing of all the previous measurement report files, it sleeps for a fixed time interval and an log message (refer to message 6 in the [Log Message List](#)) is written in the log file `measurement.txt`.

-  When the Maintenance Module fails to process a measurement file (for example, xxxxxx_mtch-path_0820_1300.csv), it is moved to the `/var/E5-MS/measurement/csvoutput/notParsed` directory, and processing continues with the next measurement file. The `ignoreMeasFiles` parameter can be configured in the configuration file `/Tekelec/WebNMS/conf/tekelec/common.config` to ignore particular reports during processing and move them to the `notParsed` directory. For example, to ignore file `tklc1170501_mtcd-path_0728_2400.csv`, `ignoreMeasFiles = mtcd-path`. To ignore multiple files, `ignoreMeasFiles` has more than one entry separated by a comma (for example, `ignoreMeasFiles = mtcd-path, comp-link`). To start parsing of an ignored measurement report again, remove its entry and restart E5-MS. 
- The sleep interval (in seconds) used by Measurement platform module is configured using a configuration file `/Tekelec/WebNMS/conf/tekelec/common.config` by System Administrator. The parameter for it shall be `measSleepInterval` and by default, the interval is 30 seconds. Any change in the sleep interval by administrator is effective after the E5-MS server restarts.
- Any non CSV file found in input directory is moved to directory `others` in output directory (`/var/E5-MS/measurement/csvoutput`) without processing. The log message (refer to message 7 and 8 in the [Log Message List](#)) are written in the log file `measurement.txt`.
- Any empty measurement report file found in input directory is moved to directory `others` in output directory (`/var/E5-MS/measurement/csvoutput`) and a log message (refer to message 8 and 10 in the [Log Message List](#)) are written in the log file `measurement.txt`.
- If the measurement report file found in input directory is not supported (refer to supported report types in **Table Report Types Supported** by Measurement Platform Module by the module, it is moved to directory `others` in output directory (`/var/E5-MS/measurement/csvoutput`) without processing, and a log message (refer to message 8 and 11 in the [Log Message List](#)) are written in the log file `measurement.txt`.
- If the measurement report file found in input directory is supported by the module, a log message (refer to message 12 in the [Log Message List](#)) is written in the log file `measurement.txt`.
- The Measurement module does not support the 5-minute measurements file. If a file is found in input directory, it is deleted from the system.
- The Measurement platform module replaces the peg name in case of parsing any reports with peg names shall take care of peg name replacement in case of parsing any reports having such peg names.
- The Measurement platform module creates the database table for a report type if it does not exist. The log message (refer to message 13 in the [Log Message List](#)) is written in the log file `measurement.txt`.
- If the measurement report file found in input directory is non-empty and is supported (refer to supported report types in **Table Report Types Supported** by Measurement platform module, then the module parses it and inserts the data in database. The log message (refer to message 15 in the [Log Message List](#)) are written in the log file `measurement.txt`.
- After parsing of a valid (non-empty and supported) measurement report file, it is moved to an appropriate sub-directory under output directory (`/var/E5-MS/measurement/csvoutput`).
 - If a CLLI name is found in report file, the sub-directory is named as CLLI. The log message (refer to message 9 in the [Log Message List](#)) are written in the log file `measurement.txt`.
 - If a CLLI name is not found in report file, the sub-directory is `others` and log message (refer to message 8 in the [Log Message List](#)) is written in the log file `measurement.txt`.
- Measurement platform module expands an existing database table for creation of new columns in case new measurement pegs are added to an existing measurement report file. In such case, a log message (refer to message 14 in the [Log Message List](#)) is written in the log file `measurement.txt`.

- All the measurement files in output directory (`/var/E5-MS/measurement/csvoutput`), which are older than 'n' days, are archived in a compressed version (`tar.bz2` format) and then the original files are removed. Here 'n' is the value of the parameter 'Days, directories older than is archived' in `tekelecMeasArchiveCleanupConfig.txt` file placed in `/Tekelec/WebNMS/bin/scripts/measurement/` directory. By default, value of 'n' is 2 and the admin is able to update the value as required.
- All the archive files in output directory (`/var/E5-MS/measurement/csvoutput`), that are older than 'n' days, are removed from system. Here 'n' is the value of the parameter 'Days, archived files older are deleted' in `tekelecMeasArchiveCleanupConfig.txt` file placed in `"/Tekelec/WebNMS/bin/scripts/measurement/"` directory. The default, value of 'n' is 30 and the admin is able to update the value as required.
- The Measurement data in various database tables that is older than 'n' days are dropped, where 'n' is the number of days mentioned in `tekelecMeasDBCleanupConfig.txt` configuration file for various tables. This configuration file is present under `/Tekelec/WebNMS/bin/scripts/measurement` directory and the admin is able to update the values as required. Any change to the file is effective from the next time when database cleanup script is run.
- The E5-MS software installation is customer friendly and executable. The Measurement file collection and DB storage feature is a core function of E5-MS and is installed together with all other core applications.

Database Overview

The E5-MS Measurement platform is depend on the following two database tables:

1. Table `tekelec_meas_headers` - This table stores the reporting data related to the CLI (name of the EAGLE), software release (release on EAGLE), report date (date of the report), report time (time of the report), report type (measurement report type), time zone etc. of a measurement report.
2. Table `tekelec_meas_reports` - This table is used to store the report types of Measurement files supported, their corresponding database tables names and number of days after the table is pruned.

These database tables are created during the installation of E5-MS.

The EAGLE(s) connected to E5-MS are configured to FTP their measurement files (CSV files) into a particular location, such as the default input directory `/root/E5-MS/measurement/csvinput`, on the E5-MS server. E5-MS Measurement platform module scans the input directory for incoming measurement report files, parse the report files found, insert the measurement data into E5-MS database and move the processed report files to their appropriate place in the output directory (`/var/E5-MS/measurement/csvoutput`). In output directory, a measurement file is placed under a sub-directory named after the CLI mentioned in the file. In case, the value of CLI is not available, it is moved to `others` directory in output directory (`/var/E5-MS/measurement/csvoutput`). The different database tables required for different report types (as defined in `tekelec_meas_reports` table) are created by the module when the module finds a report type for the first time. Each measurement peg name in the report is used to create a column with the same name in the table. Once the database table for a particular report type is created, the module inserts the measurement data from all the future reports of same type in the same table.

While creating columns in a database table for a report, there can be an issue because of long measurement peg names resulting in an error while column creation because of MySQL's limit on the width of column names.

To handle this issue, a configuration file `/Tekelec/WebNMS/conf/tekelec/tekmeas.conf` is provided which has the report type, original peg name and its replacement name to be used while creating the following column: Report Type=<Report type whose counter needs to be renamed in DB> <Original measurement peg name in the report>=<Replacement peg name to used while column creation in DB>, as shown in this example:

- For report **DAILY MAINTENANCE MEASUREMENTS ON GTT ACTION PER-PATH**
 - Wide columns - `PATH-CDSN-SCDGTA-CGSN-CGGTA-OPSN-PKG-OPCODE-<A>/F` = Short columns - `PN_DS_SD_GS_SG_OS_P_O_AF`.
 - Wide columns - `PATH-CDSN-SCDGTA-ECDGTA-CGSN-SCGGTA-ECGTA-OPSN-PKG-OPCODE-<A>/F=PN_DS_SD_ED_GS_SG_EG_OS_P_O_AF`.
- For report **HOURLY MAINTENANCE MEASUREMENTS ON GTT ACTION PER-PATH**. This would be with wide columns
 - Wide columns - `-PATH-CDSN-SCDGTA-ECDGTA-CGSN-SCGGTA-ECGTA-OPSN-PKG-OPCODE-<A>/F=` Short columns - `PN_DS_SD_ED_GS_SG_EG_OS_P_O_AF`.
 - Wide columns - `-PATH-CDSN-SCDGTA-CGSN-CGGTA-OPSN-PKG-OPCODE-<A>/F` = Short columns - `PN_DS_SD_GS_SG_OS_P_O_AF`

If there are no measurement report files in the input directory, the module go into a sleep time interval for a fixed time interval (30 seconds). After completion of the sleep time interval, it scans the input directory again and processes any reports found. This sleep time interval is configured by E5-MS System Administrator through a configuration file (`/Tekelec/WebNMS/conf/tekelec/common.config`). Any changes done to the file are effective on E5-MS server restart.

If the module finds a non-CSV file or an empty measurement file in input directory, it simply moves it to the `others` directory in output directory.

The report files stored in output directory are automatically managed on regular basis. Directories older than 2 days are archived in a compressed version and then the original directories are deleted. The compressed files older than 30 days are deleted. Also, the data in various database tables that is older than 'n' days are dropped, where 'n' is the number of days mentioned in `/Tekelec/WebNMS/bin/scripts/measurement/tekelecMeasDBCleanupConfig.txt` configuration file. E5-MS System Administrator can update the value of days for cleanup of database tables in `tekelecMeasDBCleanupConfig.txt` file. Any change done to the file is effective from the next time when database cleanup script is run

There is no separate GUI for measurement platform module in E5-MS client. However, the **User Audit** screen has audit logs showing the operations performed by module. The extensive logs are provided in `/var/E5-MS/measurement/logs` directory to enable an administrator to verify that it is working fine. Any errors encountered by the module are logged so that the administrator can take corrective actions.

Log Message List

No.	Description
1.	Database table <code>tekelec_meas_headers</code> verified.

No.	Description
2.	Database table tekelec_meas_reports verified.
3.	Supporting report type <Report Type> with database table <Table name>.
4.	Please restart the server after module schema is installed.
5.	Searching location <input directory path> for new reports.
6.	Sleeping for <sleep time interval> seconds.
7.	Report <input directory path>/<report name> is not a CSV file!
8.	Report <input directory path>/<report name>: Moved to location <output directory path>/others.
9.	Report <input directory path>/<report name>: Moved to location <output directory path>/<CLLI>.
10.	Report <input directory path>/<report name> is empty!
11.	Could not parse <input directory path>/<report name>! Report type <Report Type> not supported by module.
12.	Supporting table of report type <Report Type> is <table name>.
13.	Created <table name> with columns <column name1>, <column name2>,.... <column nameN>.
14.	Modified <table name>, added column <column name>.
15.	Inserted <number of rows> rows in table <table name> with HEADERINDEX value <header index value>.

DataBase Tables

The E5-MS Measurement platform is depend on the following two database tables:

1. Table tekelec_meas_headers - This table stores the reporting data related to the CLLI (name of the EAGLE), software release (release on EAGLE), report date (date of the report), report time (time of the report), report type (measurement report type), time zone etc. of a measurement report.
2. Table tekelec_meas_reports - This table is used to store the report types of Measurement files supported, their corresponding database tables names and number of days after the table is pruned.

The Database tables are created during the installation of the E5-MS. Measurement module starts functioning when the E5-MS server starts.

The Measurement module database tables are removed when the E5-MS is uninstalled.

Table 'tekelec_meas_headers'

The table tekelec_meas_headers is used by Measurement module to store the report generation related data like CLLI (name of the EAGLE which generated the report), software release (release on EAGLE), report date (date of report generation), report time (time of report generation), report type (measurement report type), time zone etc. of a measurement report. It contains an auto-incremented key named **HEADERINDEX** used to map a report's header data to its measurement data in another table.

Field Name	Value	Description
HEADERINDEX	INTEGER, NOT NULL AUTO_INCREMENT, PRIMARY KEY	Primary Key with auto incremented
CLLI	VARCHAR(15), NOT NULL	Name of the EAGLE
SWREL	VARCHAR(50), NOT NULL	Software release name
RPTDATE	DATE, NOT NULL	Measurement report date
RPTIME	TIME, NOT NULL	Measurement report time
TZ	VARCHAR(5)	Time zone
RPTTYPE	VARCHAR(100)	Measurement report name
RPTPD	VARCHAR(50)	Measurement report period
IVALDATE	DATE, NOT NULL	Date
IVALSTART	TIME, NOT NULL	Start time
IVALEND	TIME, NOT NULL	End time
NUMEMTIDS	INT, NOT NULL	Number of records existing in report file.

Table 'tekelec_meas_reports'

The tekelec_meas_reports table contains the measurement report types supported by the module.

Field Name	Value	Description
RPTTYPE	VARCHAR(100)	Measurement report type (value of 'RPTTYPE' key in a measurement report file.)
TABLE_NAME	VARCHAR(30), NOT NULL	Database table name which are used to store data form the report file.
DB_RETENTION_DAYS	INTEGER, NOT NULL	Data retention days for database table, data older then this is dropped.

Table 'tek_nbi_ftp_config'

Field Name	Value	Description
ID	INTEGER, NOT NULL, AUTO_INCREMENT, PRIMARY KEY	ID of the record
ip	VARCHAR(20), NOT NULL	IP address of the server where measurement files are to be FTPed
port	VARCHAR(10), NOT NULL	Port number to be used for FTPing the files
username	VARCHAR(20), NOT NULL	Username to be used for connecting to the sever
password	VARCHAR(20), NOT NULL	password for the username provided
ftplocation	VARCHAR(100), NOT NULL	On the remote server, the absolute path till the directory where measurement files need to be FTPed

Measurement Northbound FTP Module

E5-MS Measurement Northbound FTP module provides the functionality of transferring measurement report files to northbound servers.

The System Administrator assigns this operation to a usergroup. For more information on assigning permissions to a Usergroup go to [Assign Attributes to a Usergroup](#) in Appendix A for the System Administration. If assigned, all the users of that usergroup have the ability to manage server(s) on which the measurement files are to be FTPed.

NBI FTP Configuration

The System Administrator and all users assigned **NBI FTP Configuration** operation, have access to the measurement files by setting up a secure FTP IP address in the **NBI FTP Configuration** screen. You can access this screen from the main toolbar under the **Tools** menu.

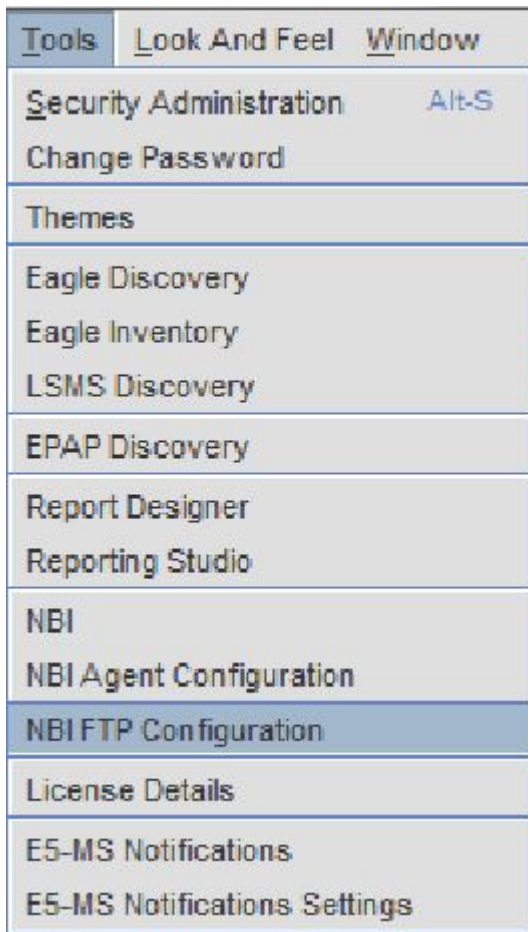


Figure 41: NBI FTP Configuration Tree Node

For every server, following details are required to be entered by the user:

- IP Address - IP address of the server where measurement files are to be FTPed.
- Username - Username to be used for connecting to the server.
- Password - Password for the above username.
- FTP Directory - On the remote server, the absolute path to the directory where measurement files need to be FTPed. Note that this directory will exist on the server.

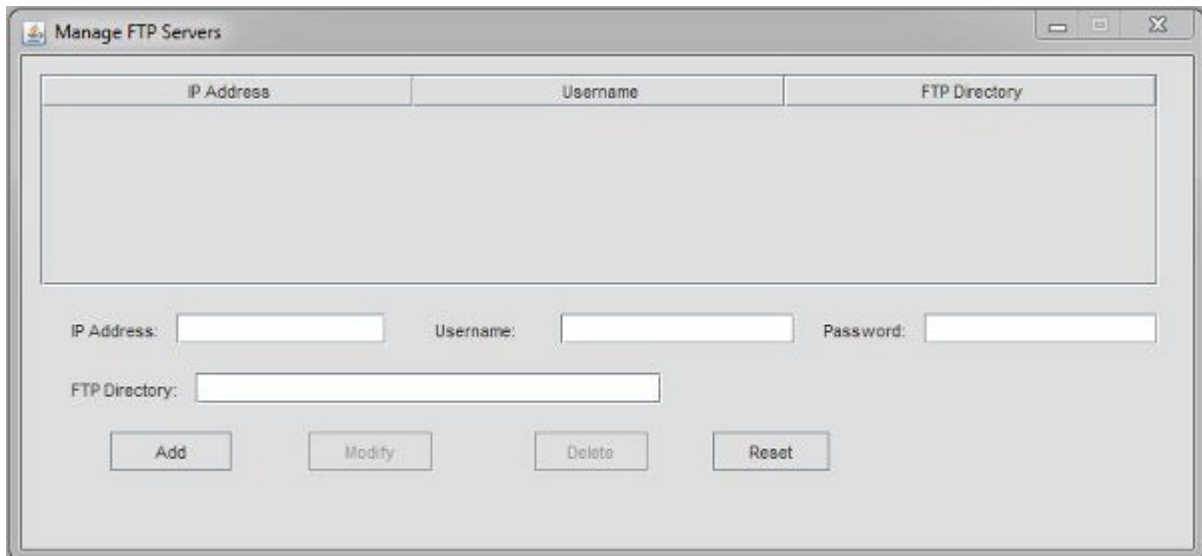


Figure 42: NBI FTP Configuration Screen

Once all the fields are completed, the user will click the Add button at the bottom of the screen. The new server will show up in the upper pane on the screen. A user can modify/delete any existing servers by selecting the corresponding server in the list and then clicking on Modify/Delete button.

The user has to modify the exiting details of a server then click **Modify** button.

The user has to select the server to delete then click the **Delete** button. A confirmation dialog box will pop up to confirm the deletion of the server.

The **Reset** button clears all the previously populated fields in the NBI FTP GUI.

File Transfer

The following points must be taken care of for file transfer to work properly:

- The FTP server details must be correctly configured by the user. There are basic validation checks done by the GUI, however the user must ensure the correctness of details like server IP address, port, username, password and FTP directory.
- The server(s) configured in **Manage FTP Servers** screen are running FTP in order to receive measurement files from E5-MS through FTP.
- The user in the **Username field** must have permission to create directory in the FTP directory so the E5-MS can create directories in the FTP directory.

The output directory (`/var/E5-MS/measurement/csvoutput`) of E5-MS Measurement platform module serves as the input directory for E5-MS Measurement FTP module. It scans the output directory for measurement reports and FTP the reports found to the server(s) configured on **Manage FTP Servers** window, every minute. After FTP, the files are moved from

`/var/E5-MS/measurement/csvoutput/<EAGLE_NAME>` directory to
`/var/E5-MS/measurement/csvoutput/ftp/< EAGLE_NAME>` directory or from
`/var/E5-MS/measurement/csvoutput/others` directory to
`/var/E5-MS/measurement/csvoutput/ftp/others` directory. This ensures that once a file has

been found in output directory scan and has been attempted for FTP, it should not found in the scan next time.

To place the FTPed files on the remote server, the E5-MS creates directories with eagle names in the FTP directory. Inside each eagle named directory, folders with date names are created. The date is the one that is currently on the E5-MS server. So, the directory structure for measurement files is similar to following:

- FTP Directory
 - EAGLE1
 - Date1
 - Date2

The logs of E5-MS Measurement FTP module are available in `/var/E5-MS/measurement/logs/ftp.txt` file. Apart from the successful file transfers, any errors encountered by the module are also logged so that the administrator can take corrective actions.

Report Types Supported by Measurement Platform Module

RPTTYPE	TABLE_NAME	DB_RETENTION DAYS
AVAILABILITY MEASUREMENTS ON LINK	TEK_MEAS_AVL_LINK	14
AVAILABILITY MEASUREMENTS ON STPLAN	TEK_MEAS_AVL_STPLAN	14
COMPONENT MEASUREMENTS ON LINK	TEK_MEAS_COMP_LINK	14
COMPONENT MEASUREMENTS ON LNKSET	TEK_MEAS_COMP_LNKSET	14
COMPONENT MEASUREMENTS ON SCTPASOC	TEK_MEAS_COMP_SCTPASOC	14
COMPONENT MEASUREMENTS ON SCTPCARD	TEK_MEAS_COMP_SCTPCARD	14
COMPONENT MEASUREMENTS ON UA	TEK_MEAS_COMP_UA	14
DAILY AVAILABILITY MEASUREMENTS ON LINK	TEK_MEAS_AVLD_LINK	30
DAILY MAINTENANCE MEASUREMENTS ON EIR SYSTEM	TEK_MEAS_MTCD_EIR	30
DAILY MAINTENANCE MEASUREMENTS ON GTT ACTION PER-PATH	TEK_MEAS_MTCD_GTTACTPATH	30

RPTTYPE	TABLE_NAME	DB_RETENTION DAYS
DAILY MAINTENANCE MEASUREMENTS ON GTT ACTION SYSTEM	TEK_MEAS_MTCD_GTTACTSYS	30
DAILY MAINTENANCE MEASUREMENTS ON LINK	TEK_MEAS_MTCD_LINK	30
DAILY MAINTENANCE MEASUREMENTS ON LNKSET	TEK_MEAS_MTCD_LNKSET	30
DAILY MAINTENANCE MEASUREMENTS ON LNP LRN	TEK_MEAS_MTCD_LNPLRN	30
DAILY MAINTENANCE MEASUREMENTS ON LNP NPANXX	TEK_MEAS_MTCD_LNPNPANX	30
DAILY MAINTENANCE MEASUREMENTS ON LNP SSP	TEK_MEAS_MTCD_LNPSSP	30
DAILY MAINTENANCE MEASUREMENTS ON LNP SYSTEM	TEK_MEAS_MTCD_LNPSTPM	30
DAILY MAINTENANCE MEASUREMENTS ON MAP SCREENING PATH	TEK_MEAS_MTCD_MAPPATH	30
DAILY MAINTENANCE MEASUREMENTS ON MAP SCREENING SYSTEM	TEK_MEAS_MTCD_MAPSYS	30
DAILY MAINTENANCE MEASUREMENTS ON MAPSCRN PER-SERVER	TEK_MEAS_MTCD_MAPSRV	30
DAILY MAINTENANCE MEASUREMENTS ON MAPSCRN SYSTEM	TEK_MEAS_MTCD_MAPSYS	30
DAILY MAINTENANCE MEASUREMENTS ON NP SSP	TEK_MEAS_MTCD_NPSSP	30
DAILY MAINTENANCE MEASUREMENTS ON NP SYSTEM	TEK_MEAS_MTCD_NPSTPM	30
DAILY MAINTENANCE MEASUREMENTS ON SCTPASOC	TEK_MEAS_MTCD_SCTPASOC	30
DAILY MAINTENANCE MEASUREMENTS ON SCTPCARD	TEK_MEAS_MTCD_SCTPCARD	30
DAILY MAINTENANCE MEASUREMENTS ON STP	TEK_MEAS_MTCD_STP	30
DAILY MAINTENANCE MEASUREMENTS ON STPLAN	TEK_MEAS_MTCD_STPLAN	30

RPTTYPE	TABLE_NAME	DB_RETENTION DAYS
DAILY MAINTENANCE MEASUREMENTS ON UA	TEK_MEAS_MTCD_UA	30
DAY-TO-HOUR AVAILABILITY MEASUREMENTS ON LINK	TEK_MEAS_DTTHA_LINK	14
DAY-TO-HOUR MAINTENANCE MEASUREMENTS ON LINK	TEK_MEAS_DTHM_LINK	14
DAY-TO-HOUR MAINTENANCE MEASUREMENTS ON LINKSET	TEK_MEAS_DTHM_LNKSET	14
DAY-TO-HOUR MAINTENANCE MEASUREMENTS ON STP	TEK_MEAS_DTHM_STP	14
DAY-TO-HOUR MAINTENANCE MEASUREMENTS ON STPLAN	TEK_MEAS_DTHM_STPLAN	14
GATEWAY MEASUREMENTS ON LNKSET	TEK_MEAS_GTWY_LNKSET	14
GATEWAY MEASUREMENTS ON LSDESTNI	TEK_MEAS_GTWY_LSDESTNI	14
GATEWAY MEASUREMENTS ON LSONISMT	TEK_MEAS_GTWY_LSONISMT	14
GATEWAY MEASUREMENTS ON LSORIGNI	TEK_MEAS_GTWY_LSORIGNI	14
GATEWAY MEASUREMENTS ON ORIGNI	TEK_MEAS_GTWY_ORIGNI	14
GATEWAY MEASUREMENTS ON ORIGNINC	TEK_MEAS_GTWY_ORIGNINC	14
GATEWAY MEASUREMENTS ON STP	TEK_MEAS_GTWY_STP	14
HOURLY MAINTENANCE MEASUREMENTS ON EIR SYSTEM	TEK_MEAS_MTCH_EIR	14
HOURLY MAINTENANCE MEASUREMENTS ON GTTACTION PER-PATH	TEK_MEAS_MTCH_GTTACTPATH	14
HOURLY MAINTENANCE MEASUREMENTS ON GTTACTION SYSTEM	TEK_MEAS_MTCH_GTTACTSYS	14
HOURLY MAINTENANCE MEASUREMENTS ON LNP LRN	TEK_MEAS_MTCH_LNPLRN	14
HOURLY MAINTENANCE MEASUREMENTS ON LNP NPANXX	TEK_MEAS_MTCH_LNPNPANX	14

RPTTYPE	TABLE_NAME	DB_RETENTION DAYS
HOURLY MAINTENANCE MEASUREMENTS ON LNP SSP	TEK_MEAS_MTCH_LNPSSP	14
HOURLY MAINTENANCE MEASUREMENTS ON LNP SYSTEM	TEK_MEAS_MTCH_LNPSTYSM	14
HOURLY MAINTENANCE MEASUREMENTS ON MAP SCREENING PATH	TEK_MEAS_MTCH_MAPPATH	14
HOURLY MAINTENANCE MEASUREMENTS ON MAP SCREENING SYSTEM	TEK_MEAS_MTCH_MAPSYS	14
HOURLY MAINTENANCE MEASUREMENTS ON MAPSCRN PER-SERVER	TEK_MEAS_MTCH_MAPSRV	14
HOURLY MAINTENANCE MEASUREMENTS ON MAPSCRN SYSTEM	TEK_MEAS_MTCH_MAPSYS	14
HOURLY MAINTENANCE MEASUREMENTS ON NP SSP	TEK_MEAS_MTCH_NPSSP	14
HOURLY MAINTENANCE MEASUREMENTS ON NP SYSTEM	TEK_MEAS_MTCH_NPSTYSM	14
MAINTENANCE STATUS INDICATORS ON LINK	TEK_MEAS_MSI_LINK	14
MAINTENANCE STATUS INDICATORS ON LINKSET	TEK_MEAS_MSI_LNKSET	14
NETWORK MANAGEMENT MEASUREMENTS ON LINK	TEK_MEAS_NM_LINK	14
NETWORK MANAGEMENT MEASUREMENTS ON LNKSET	TEK_MEAS_NM_LNKSET	14
NETWORK MANAGEMENT MEASUREMENTS ON STP	TEK_MEAS_NM_STP	14
RECORD BASE MEASUREMENTS ON LINK	TEK_MEAS_RBASE_LINK	14
RECORD BASE MEASUREMENTS ON LINKSET	TEK_MEAS_RBASE_LNKSET	14
RECORD BASE MEASUREMENTS ON STP	TEK_MEAS_RBASE_STP	14
STP SYSTEM TOTAL MEASUREMENTS ON CGTT	TEK_MEAS_SYSTOT_CGTT	14

RPTTYPE	TABLE_NAME	DB_RETENTION DAYS
STP SYSTEM TOTAL MEASUREMENTS ON IDPR	TEK_MEAS_SYSTOT_IDPR	14
STP SYSTEM TOTAL MEASUREMENTS ON STP	TEK_MEAS_SYSTOT_STP	14
STP SYSTEM TOTAL MEASUREMENTS ON STPLAN	TEK_MEAS_SYSTOT_STPLAN	14
STP SYSTEM TOTAL MEASUREMENTS ON TT	TEK_MEAS_SYSTOT_TT	14

Chapter 10

Reporting Studio

Topics:

- *Overview.....127*
- *Measurement Reporting Studio.....127*
- *Functional Description.....128*
- *i-net Clear Reports Remote Interfaces.....129*

This chapter provides an overview of the E5-MS Reporting Studio.

Overview

The default i-net Clear Reports remote interfaces is utilized for catering to the requirements of E5-MS Reporting Studio. i-net Clear Reports remote interfaces are web based interfaces that open in the default browser of the client machine and allow users perform various reporting functions.

Measurement Reporting Studio

The Reporting Studio feature is a Reporting tool to manage EAGLE Measurements. The feature is based on the use of an OEM Software (i-Net Clear Reports Plus). with a few pre-defined reports and will allow the users to create customized reports.

The Measurement Reporting Studio offers a set of standard reports for our customers:

- Alarm/Event summary:
 - Possibility to extract alarm and event history with selective date, time, severity, alarm reference (UAM number) and resource/sub-resource and generate reports.
 - Statistics per node, date, time, severity
 - Top 10 alarms and top 10 resources per day (possibly week and month)
- EAGLE STP Measurements
 - STP - Systot
 - Daily Systot reports concatenating key counters (granularity will be either 30 minutes or 15 minutes depending on STP settings)
 - ORIGMSUS
 - TRMDMSUS
 - THRSWMSU
 - GTTPERFD
 - NMSCCPMH
- Link Utilization Interface Reports
 - If LUI feature is ON, Link, Linkset and Card reports are made available (as the current LUI feature does on Classic EMS)

The E5-MS Measurement Reporting Studio have the following output formats:

- HTML, PDF, Text, RTF, XML, JPG
- Optional formats: emails, JAR, XLS, ZIP

The user can schedule automatic report execution using the Reporting Studio. There is a Drill Down Report which provides several layers of data, such as linkset based report navigating the user to the link level alarms.

The Reporting Studio supports multiple languages.

Functional Description

The E5-MS Reporting Studio shall provide its users below mentioned features:

- Creating reports on ad hoc basis
- Creating reports using a defined template
- Providing a designer interface to users to create/update templates as required
- Exporting reports in various report formats to choose from (pdf, html, xls, jpeg, png, gif, xml, csv, rtf, txt)
- Report template management
- Providing a Repository browser to users, for managing existing report templates and view created reports
- Providing a scheduler interface to user, for scheduling report generation

By default, both **Reporting Studio** and **Report Designer** menu items are visible for the System Administrator with **root** access. There are two menu items under to the Tools icon on the main toolbar of the E5-MS, the **Reporting Studio** and **Report Designer**. The System Administrator provides permission to other user by assigning them **Reporting Studio** permission. The user must have the same username in i-net Clear Reports tool.

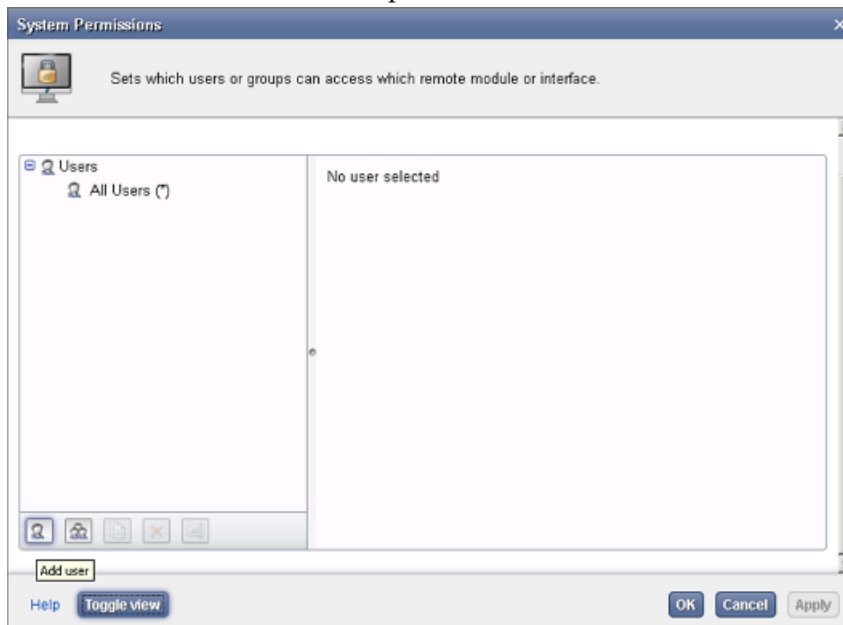


Figure 43: Add User

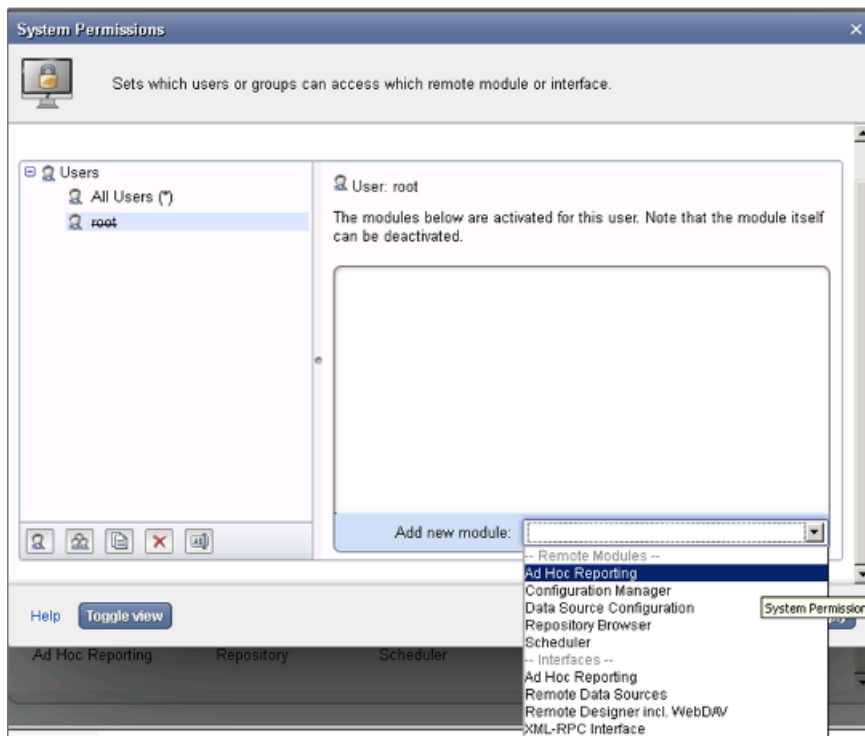


Figure 44: System Permissions

i-net Clear Reports Remote Interfaces

i-net Clear Reports provides following remote interfaces:

- **Ad Hoc Reporting** - Allows creating reports on the fly without any predefined template.
- **Configuration** - Allows a user management of i-net Clear Reports configurations. A configuration contains all options to configure i-net Clear Reports.
- **Data Source Configuration** - Allows configuring the data sources to be used for report generation.
- **Repository Browser** - Shows listing of existing reporting templates and allowing management of them.
- **Scheduler** - Allows a user schedule report templates to generate reports at desired time.
- **Report Designer**

- Apart from the above web based remote interfaces, there is another webstart application named 'Report Designer' that is used by users to design report templates. User can create/update a report template as per their requirement.

Remote Interface

The remote interface allows a user access to various remote interfaces as shown in i-net Clear Reports.

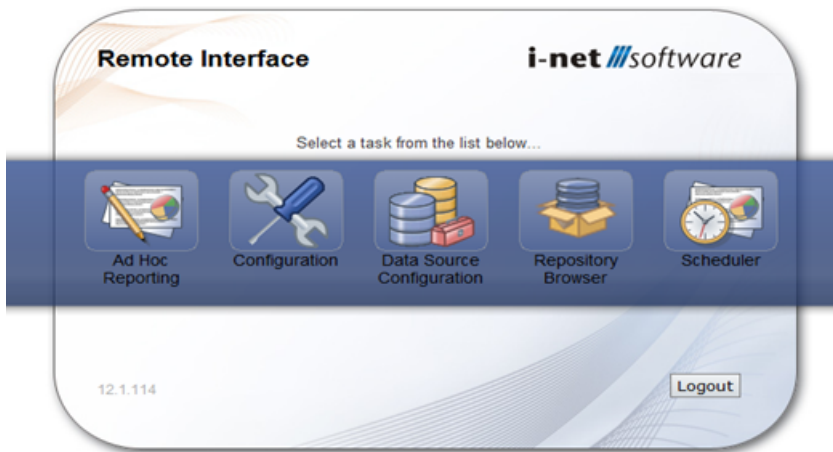


Figure 45: i-net Clear Report

Ad Hoc Reporting Interface

This chapter provides an overview of the EAGLE 5-Management System.

The Ad Hoc Reporting interface is simple and intuitive web based interface, to generate a report on the fly without using any template. To assign a user access to Ad Hoc Reporting, refer to System Permissions.

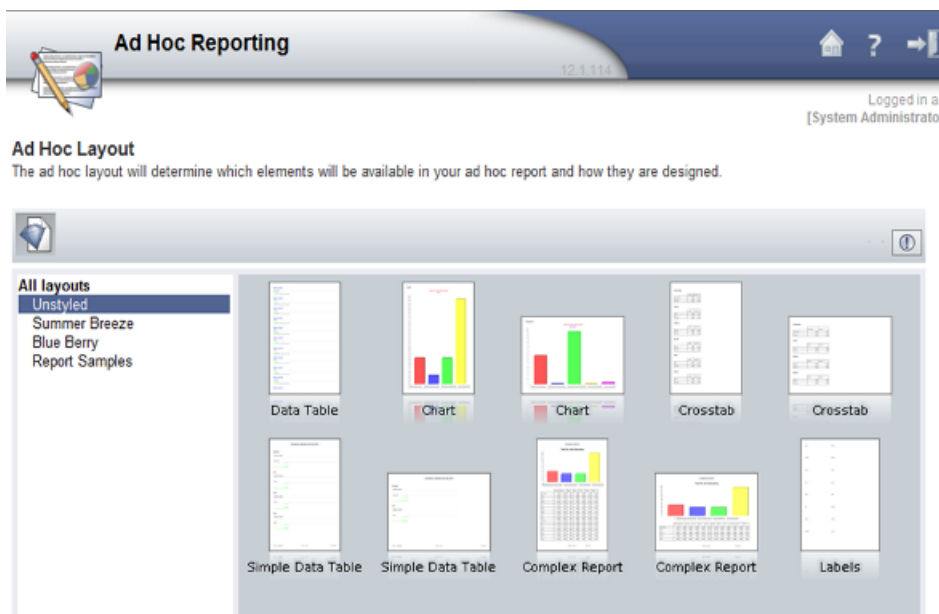


Figure 46: Ad Hoc Reporting

Configuration Manager

The Configuration Manager interface allows a user to manage all the reporting, security and performance related settings.

To assign a user access to the Configuration Manager, refer to System Permissions.



Figure 47: Configuration Manager Interface

Post installation of i-net Clear Reports, it needs to be configured for use with E5-MS. This configuration involves steps such as creating 'root' user and assigning him permissions, activating scheduler, creating and activating remote repository, adding data source etc. These actions are performed in Configuration Manager Interface.

Data Source Configuration Interface

The Data Source Configuration interface allows a user to manage data sources. To assign a user access to the Data Source Configuration, refer to System Permissions.

Post installation of i-net Clear Reports, E5-MS database needs to be added as a data source to i-net Clear Reports for report generation using Data Source Configuration.

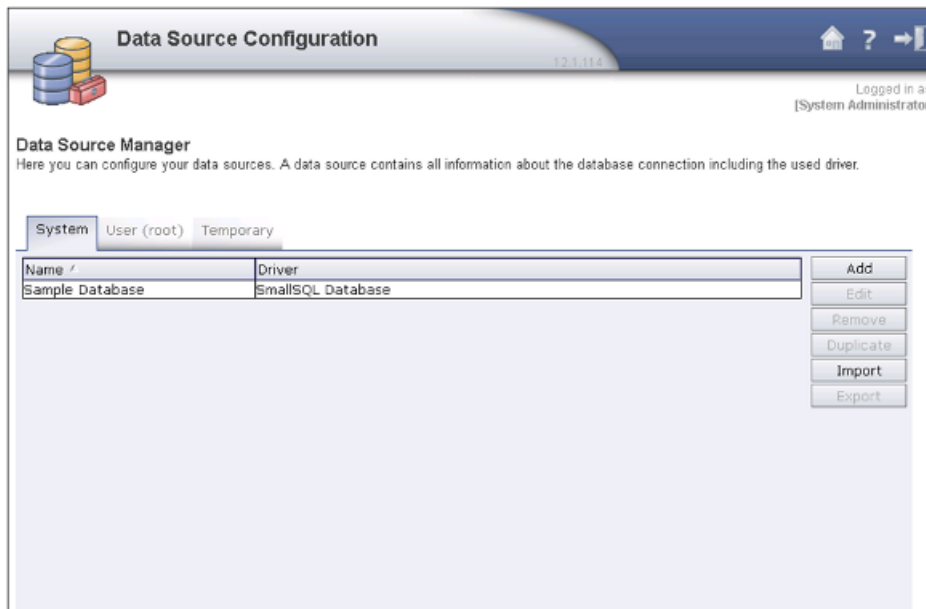


Figure 48: Data Source Configuration Interface

Repository Browser Interface

The Repository Browser interface allows users to manage report templates. Users can see the list of stored templates, edit them, download and upload them. The user can also generate reports in various formats by executing an existing template.

The repository browser is not just restricted to report templates. It can also be used to create a report repository, where reports published by scheduled or manual execution can be kept.

To assign a user access to the Repository Browser Interface, refer to System Permissions.

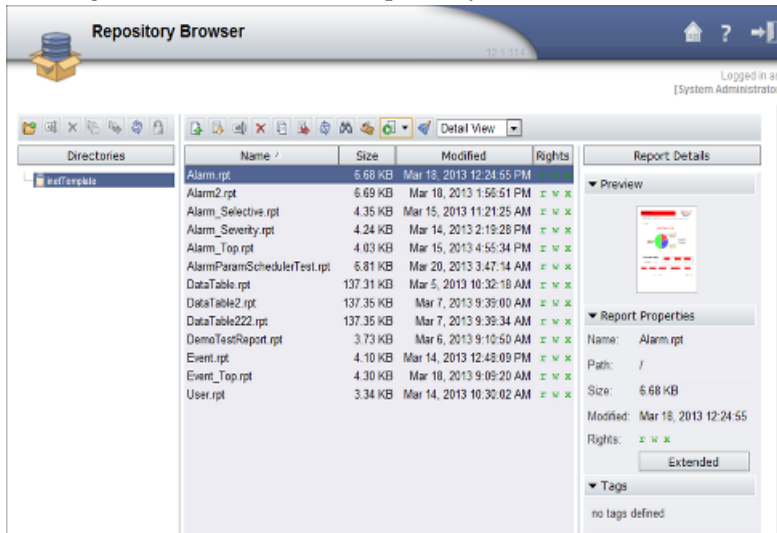


Figure 49: Repository Browser Interface

Scheduler Interface

The Scheduler interface allows scheduling of report generation by creating named scheduled tasks.

A task can be scheduled for a particular or repeated number of times. Post execution the status of the scheduled task is known and the resulted report can be downloaded, FTPed or mailed to users. It also has provision of instant execution of a scheduled task.

To assign a user access to the Scheduler Interface, refer to System Permissions.

By default, Scheduler feature is not activated in i-net Clear Reports. Scheduler needs to be activated using Configuration Manager.

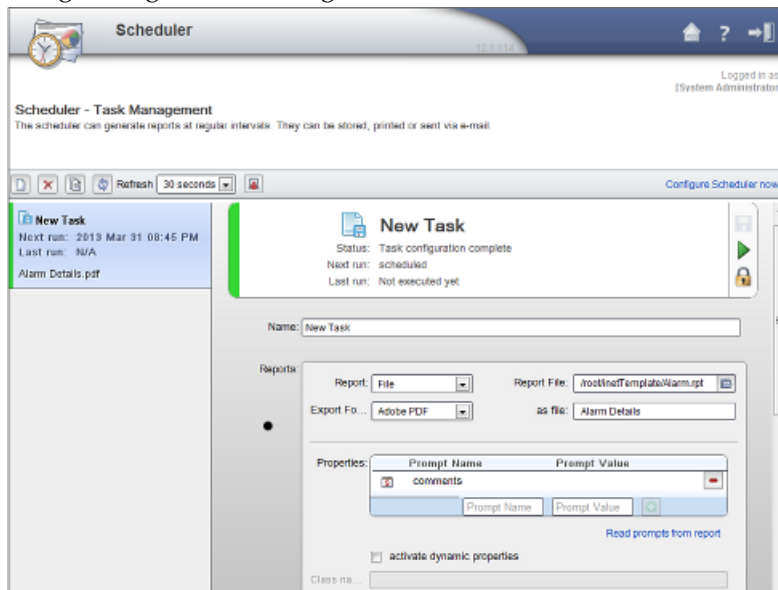


Figure 50: Scheduler

Report Designer Interface

The Report Designer interface allows creating or editing a report template.

The remote interface of Report Designer allows saving a report template at local as well as configured remote report repository location.

To assign a user access to the Report Designer, interface 'Remote Designer incl. WebDAV' refer to System Permissions. as shown in **Report Designer Interface** needs to be assigned to the user.

If a user is assigned access to Report Designer, then it is mandatory to assign 'Remote Data Sources' interface also so that the user can access E5-MS database while creating/updating report templates.

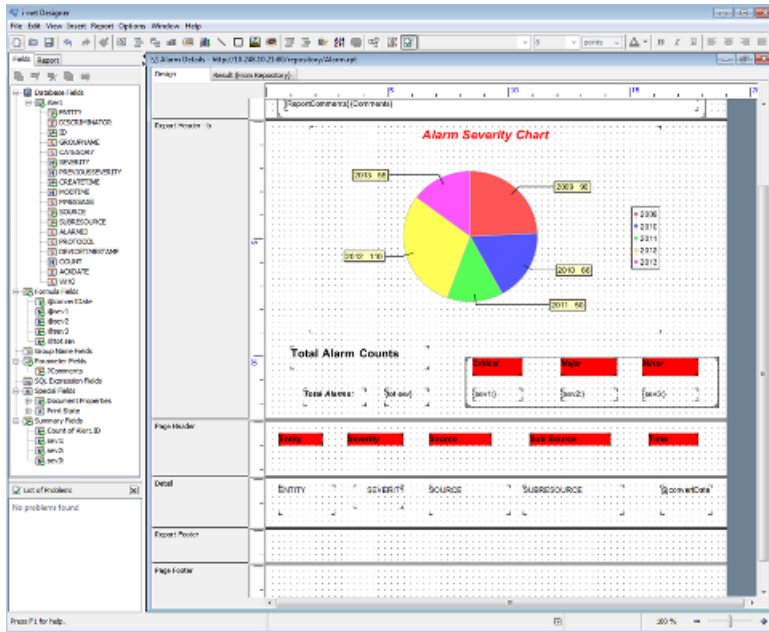


Figure 51: Report Designer

Chapter 11

Configuration Management Interface

Topics:

- *Overview.....136*
- *Functional Description.....137*
- *Send Command.....137*
- *Category Management.....143*
- *Script Management.....144*
- *Schedule Management.....150*
- *CMI Informational/Error Message List.....152*

This chapter provides descriptions of the features and functions provided by the E5-MS Configuration Management Interface (CMI).

Overview

The Configuration Management Interface provides access to EAGLE commands, parameters, and historical data.

CMI module provides two functions:

- Command execution on EAGLE(s) - The **Send Command** screen enables the users execute single commands on desired EAGLE(s).
- Command script creation, management and execution on EAGLE(s) - The following screens are provided to E5-MS users for this functionality:
 - Category Management - To view and manage (create/rename/delete) script categories
 - Script Management - To view the listing of existing scripts, manage (create/modify/delete) them and see execution results
 - Create Script - To create scripts
 - Modify Script - To modify a script
 - View Script - To view the contents of a script
 - Execute Script - To manually execute a script
 - Schedule Management - To schedule a script for execution on EAGLE(s)

Note: The CMI module is pre-populated with the command set from the EAGLE release with which the E5-MS is associated. The following commands are not supported:

- Commands in the DEBUG command class
- Commands requiring passwords:
 - act-user
 - chg-ftp-serv
 - chg-pid
 - chg-user
 - ent-ftp-serv
 - ent-user
 - login
 - unlock
 - ent-gtwyls
 - chg-gtwyls
 - dlt-gtwyls
 - rtrv-gtwyls
 - chg-serial-num
 - help
 - rtrv-data-gtt
 - rtrv-pe
- Logout command

Functional Description

The assigned users can send commands and scripts to the EAGLE and get results. The CMI has an auto-completion of command and command history maintenance to help the users. If the CMI is grayed out the application is not available to the client or the user.

CMI module connects to EAGLE using the IPSM card(s) configured on EAGLE. Please reference the EAGLE Discovery Application chapter for the setup of the IP address from the E5-MS to the EAGLE.

The Configuration Management Interface is accessed from the left pane of the E5-MS GUI tree node. As shown in CMI Tree Node.



Figure 52: CMI Tree Node

Send Command

If the Send Command is grayed out, contact your System Administrator. The administrator assigns the **Send Command** operation to the user groups. The System Administrator should refer to [E5-MS System Administration](#) to assign Usergroups and User.

The **Send Command** is located under **Configuration** node in the left pane. The Configuration node is enabled/disabled based on permission of the usergroup. The **Send Command** is shown in [Figure 53: Send Command Screen](#).

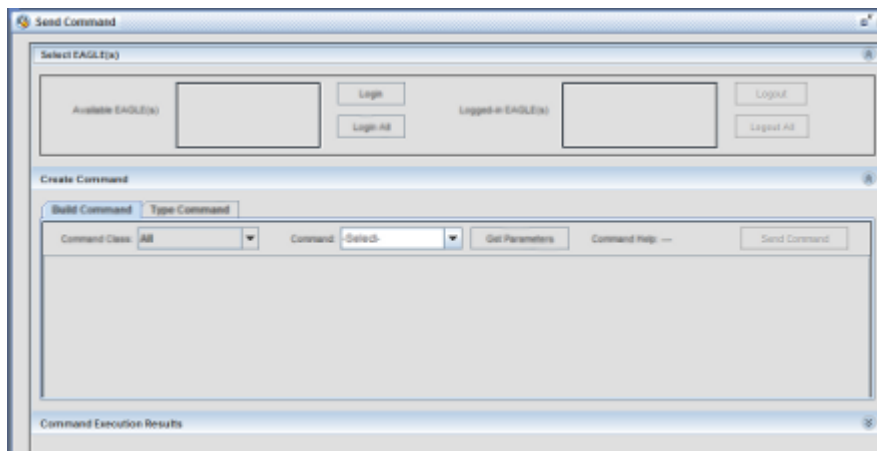


Figure 53: Send Command Screen

The operations that can be performed using the CMI **Send Command** include:

- **Select EAGLE(s)** pane - enables user to choose EAGLE(s) for login/logout.
- **Create Command** pane - shall enable user to create a command to be sent to EAGLE(s).

- **Command Execution Results** pane - shall display the login, logout and other command execution results from EAGLE(s).

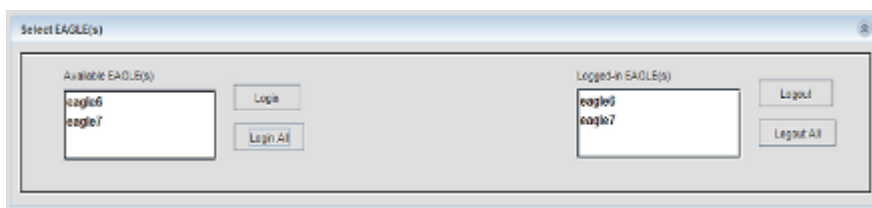
Select EAGLE(s) Pane

There are two lists available in this pane.

- **Available EAGLE(s)** list the names of all the EAGLE(s) assigned to usergroup and users.
- **Logged-in EAGLE(s)** list the names of EAGLE(s) on which user has successfully logged in.

As shown in [Select EAGLE\(s\) Pane](#)

Figure 54: Select EAGLE(s) Pane



Select EAGLE(s)

If the Send Command is grayed out, please contact your System Administrator. This procedure describes how to login EAGLE systems. These are the EAGLE systems the E5-MS User has permission to login that appear in the **Available EAGLE(s)** list.

- Select the EAGLE system name(s) from the **Available EAGLE(s)** list. Click the **Login** link on the right side of the list.
 - If all of the EAGLE systems are to receive the command, click the **Login All** button.
 - If a subset of the **Available EAGLE(s)** systems are to receive the command, select those systems from the **Available EAGLE(s)** list and click the **Login** button. Multiple EAGLE systems can be selected by sequentially clicking on each of their names while holding down the <Ctrl> key on your keyboard.

At the bottom of the **Send Command** screen is the **Command Execution Results** pane. It is clear until you send a command or script to the EAGLE. Once a command is executed, the most recent 5,000 lines of the EAGLE's responses to the commands issued while the User is using the Send Command page are displayed in the **Command Execution Results** pane.

- To log out from an EAGLE system, select the name of the EAGLE from the **Logged-In EAGLE(s)** list and click the **Logout** button. To log out from all of the EAGLE systems, click the **Logout All** button.

Note: The E5-MS User remains logged in to these EAGLE system(s) until the E5-MS User logs out.

Login will not be attempted on EAGLE(s) that the E5-MS is already logged in, reference message 3 in the [CMI Informational/Error Message List](#).

Create Command Pane

There are two tabs available in this pane.

- **Build Command** tab provides a user a drop-down list of a Command Class and Commands to build a valid command to be sent to EAGLE systems.
 - The **Command Class** drop-down list enables a user build a valid command to be sent to EAGLE.
 - The **Command** drop-down list contains the commands associated with the command class selected in the **Command Class** drop-down.
- **Type Command** tab provides a proficient user to type commands sent to EAGLE systems.

As shown in Create Command

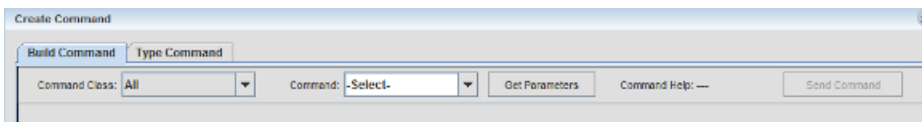


Figure 55: Create Command

Build Command

The **Build Command** pane has two drop-down lists named **Command Class** and **Command**, a button named **Get Parameters** and another named **Send Command**.



Figure 56: Build Command Tab

Command Class

- The **Command Class** drop-down list has all the EAGLE command classes assigned to the user's user group. The **All** corresponds to all the commands. By default, the **All** option is pre-selected in the **Command Class** drop-down. As shown in Command Class Menu

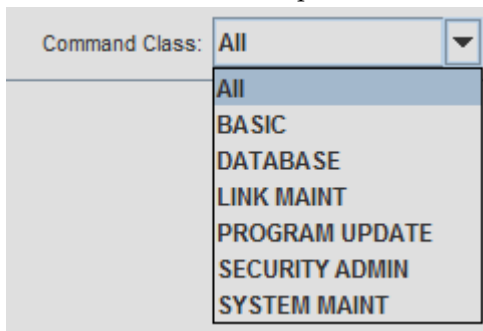


Figure 57: Command Class Menu

- The user will select the command class in the drop-down.

Command

The **Command** drop-down list has all the commands on which the user has access. The **All** corresponds to all the commands.

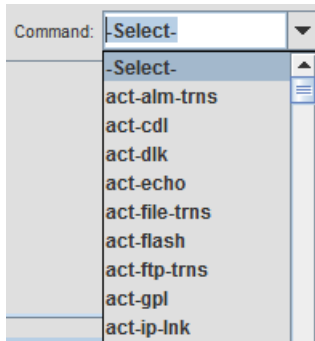


Figure 58: Command Menu

- When selecting a command class in the **Command Class** drop-down list, the **Command** drop-down list is populated with all the commands belonging to that command class. To the commands associated with the command class selected in the **Command Class** drop-down, the **Command** drop-down has an option **-Select-**, that is selected by default in the **Command** drop-down.
- The **Command** drop-down provides the auto-complete ability to the user. As a user shall start typing in characters in the **Command** box, the commands available in the **Command** box are searched and the command most matching to the characters typed in shall be auto completed in the box. The commands that follow the auto-completed command alphabetically are displayed below the box in a popup list and the user can select any of the commands displayed in the popup list into the **Command** box.
- If a user types in characters in **Command** box that do not match any of the command in the **Command** box, then the selection in **Command** box shall not change.
- The user can manually select the desired command in the **Command** drop-down list.
- After selection of the desired command in the **Command** drop-down list and clicking on the **Get Parameters** button, all parameters of the command and the corresponding HTML help file link are displayed in the pane.

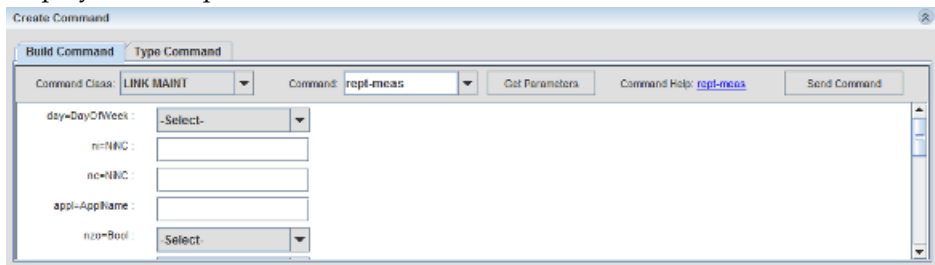


Figure 59: Get Parameters

- If the command is one of the last n commands used in the current user session, then the previously used values for various parameters is automatically get populated.
- Reference message 9 in the [CMI Informational/Error Message List](#) that displays if the user clicks on **Get Parameters** button while default option **-Select-** is selected in the **Command** drop-down list.
- When clicking on the help file link of the command, HTML help file for the command will opened in the default browser configured on the system.
- The labels of mandatory parameters are followed by asterisks * to highlight that they are required.

- When clicking the **Send Command** button after building the command, the command parameters are checked for various validations applicable as per the command. The validations are as provided by EAGLE:
 - Whether a parameter is mandatory
 - Validation on the type of permitted value for a parameter (number, alphanumeric string, letter followed by alphanumeric string etc.)
 - Validation on the range of permitted value for a parameter
- If all the applicable validations on the command parameters successfully pass, the command is sent for execution to the EAGLE(s) selected by the user in the **Logged-in EAGLE(s)** list.
- If any of the applicable validations on the command parameters does not pass, the command is not sent for execution to the EAGLE(s) selected by the user in the **Logged-in EAGLE(s)** list and an error message is displayed to the user.

Type Command

The **Type Command** pane has a text field for the users to type in a complete command string (command and its parameters).

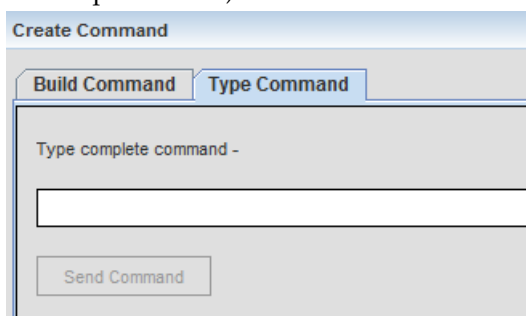


Figure 60: Type Command Pane

A **Send Command** button is below the text field. This button is disabled when text field is empty, until the user starts typing in the text field. Once the **Send Command** button is click, the command is checked for following cases:

- That the command is a valid command
- That the user has permission to use the command

If the command string passes both the validations, the command is sent for execution to the EAGLE(s) selected by the user in the **Logged-in EAGLE(s)** list.

In case the command string does not pass any of the validations the command is not sent for execution to the EAGLE(s) selected by user in the **Logged-in EAGLE(s)** list reference message 7 in the [CMI Informational/Error Message List](#).

Command Execution Results Pane

This pane is used to display results of login, logout and other commands as shown in [Figure 61: Command Execution Results Pane](#). For each EAGLE a user attempts to login, a new tab is created in this pane. The name of the tab is the same as the name of the EAGLE. All the command execution results from an EAGLE is displayed in its own tab. There is a close (x) button associated with each tab and user has the ability to close the tab using this button. On clicking the close (x) button, a confirmation

box is shown to user to confirm whether the user really wants to close the tab. If the EAGLE is not logged in, the tab will close. In case EAGLE is logged in, an error message is shown to the user and the tab is not closed.

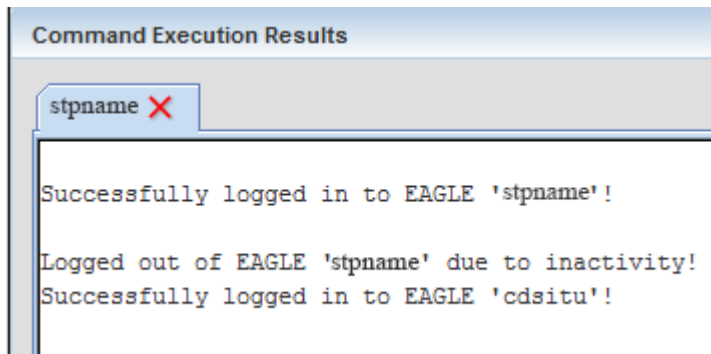


Figure 61: Command Execution Results Pane

Command Execution Results Pane

This procedure describes how to view the login, logout and other commands sent to the EAGLE systems.

1. See the **Results:** pane to view command output.

The **Results:** pane will continue to store output (including results from multiple consecutive **Send Command** submissions made while on the **Send Command** page) up to 5000 lines. Beyond this limit, the information in the **Results:** pane will roll-over with new lines appending at the bottom of the pane and old lines will be deleted from the top.

2. To view the most recent send-command execution results from the current User login session, click the tab of the corresponding EAGLE system (see **View complete result**).

This link is displayed as soon as script results start to appear in the **Results:** pane. Click on the link to open a browser window to view the complete result file.

The browser window displays up to the most recent 500,000 lines of **Send Command** results from the current User login session (see **Complete Results Browser Window**

The complete results file will continue to grow up to the most recent 500,00 lines. Beyond this limit, the information in the complete results file will roll-over. When the user leaves the **Send Command** page and comes back to this page without logging out, the **Results:** pane is cleared but the complete results data is retained and is accessible by clicking the **To view complete result, click here** link. However, if the user logs out and returns to the **Send Command** page after logging in again, both the **Results:** pane and the complete results data will be cleared.

3. Click the **Clear Results** button to clear the complete results file and the **Results:** pane (see **Send Command** pane).

The link **To view complete result, click here** file will not be visible after the **Clear Results** button is clicked.

Note: A user can not clear the result data while command execution is in progress. The button will be disabled while command execution is in progress.

Category Management

The **Category Management** page is accessed by clicking on the link labeled **Category Mgmt** in the main menu on the left side of the E5-MS under Configuration Management Interface. An example of this screen is shown in *Figure 62: Category Management Screen*.

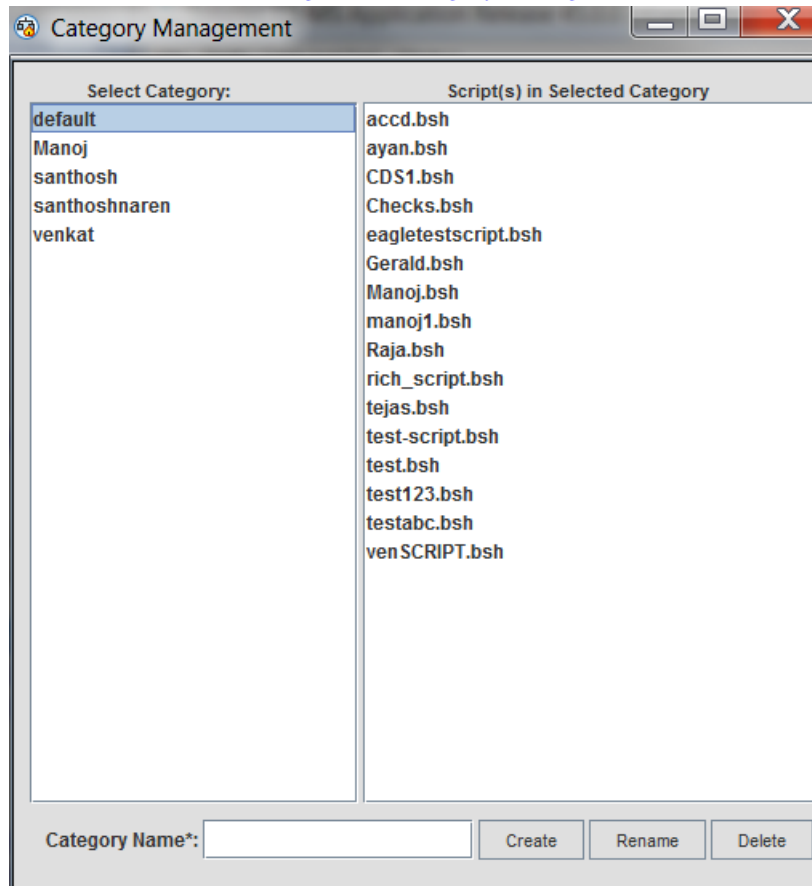


Figure 62: Category Management Screen

Category Management screen has two columns namely **Select Category** and **Script(s) in Selected Category**:

- **Select Category** column - It lists all the existing categories. A user will select a category by clicking on that category name. A category named `Default` exists by default for every E5-MS user.
- **Script(s) in Selected Category** column - It lists all the scripts belonging to the category selected in **Select Category** column.

A text box labeled **Category Name*** and three buttons at the bottom of the pane are **Create**, **Rename** and **Delete**. A user has the ability to:

- Create a new category by providing a valid category name in **Category Name*** field and clicking on the **Create** button.
- Rename an existing category by selecting that category in **Select Category** column, providing a new and valid category name in **Category Name*** field and clicking on the **Rename** button.

- Delete an existing category by selecting that category in **Select Category** column and clicking on the **Delete** button. If there are scripts in the category being deleted, they are moved to category **Default**. In case, one or more scripts in the category being deleted have identical names as those in category **Default**, then category deletion will fail (reference message 17 and 18 in the [CMI Informational/Error Message List](#)).

The user can view the scripts associated to a category.

To create a category, the user has rules regarding category names, failing which, the category is not created:

- Cannot be blank (reference message 19 in the [CMI Informational/Error Message List](#))
- Must have a minimum of 3 characters (reference message 20 in the [CMI Informational/Error Message List](#))
- Must have maximum 255 characters (reference message 21 in the [CMI Informational/Error Message List](#))
- Must not be 'All' (reference message 22 in the [CMI Informational/Error Message List](#))
- Must only have alphanumeric characters (0-9, a-z, A-Z) (reference message 23 in the [CMI Informational/Error Message List](#))
- Must be unique for the user (reference message 24 in the [CMI Informational/Error Message List](#))

In case a category creation fails reference message 25 in the [CMI Informational/Error Message List](#).

In case a category renaming fails reference message 26 and 27 in the [CMI Informational/Error Message List](#)

A user can delete a category, other than the **default** category. While deleting a category, the user is shown a confirmation dialogue box. On confirmation from user, it is checked if there are any scripts in this category having identical names as those in category 'default'. If yes, then the category is not deleted, reference message 30 in the [CMI Informational/Error Message List](#).

After confirmation of category deletion by user, if there are no scripts in this category having identical names as those in category '**default**', then all the associated scripts are moved to 'default' category and thereafter the category is deleted.

In case a category deletion fails reference message 28 and 29 in the [CMI Informational/Error Message List](#).

In case a user is deleted from E5-MS system, his/her categories shall also be deleted from system if no script exists in any of the categories. In case one or more scripts exist for the user, his/her categories shall not be deleted.

Script Management

The Script Management screen is accessed by clicking on the **Script Management** link in the main menu on the left side of the E5-MS GUI under Configuration. An example of this page is shown in .

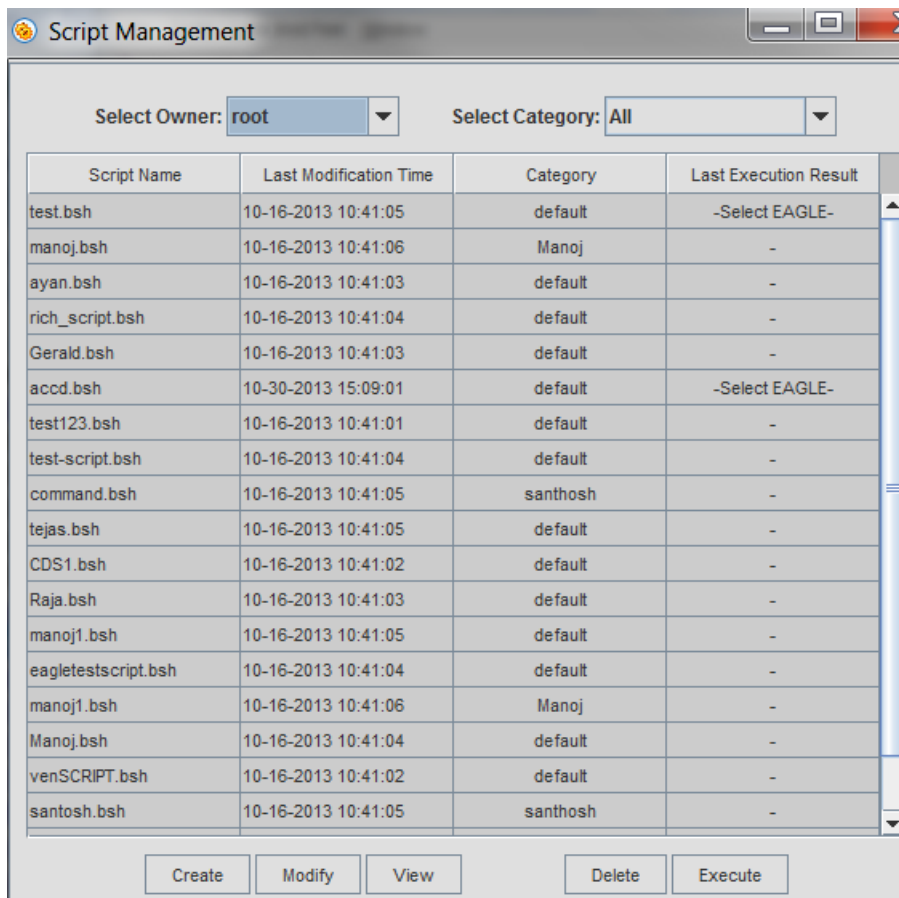


Figure 63: Script Management Screen

On top of the **Script Management**' screen, the **Select Owner** and **Select Category** drop-downs menus are provided. The **Select Owner** drop down allow the System Administrator to enabled and disabled a non-admin user. It list all the E5-MS users and the currently logged in user's name. The **Select Category** drop down has the listing of all the categories for the user selected in **Select Owner** drop down. The **All** option is set by default. Below these drop downs, the listing of scripts are provided based on the user and category selected above. Following four columns shall be provided:

- Script Name - Name of the script
- Last Modification Time - Time when the script was last modified
- Category - Name of the category the script belongs to
- Last Execution Result - Name of the EAGLE(s) on which the script has been executed

Selecting an EAGLE name in the `Last Execution Result` column shall launch a new **Script Execution Result** window showing the script execution result for that EAGLE as shown in Script Execution Result Screen. Note that only 2000 lines of script execution output is visible on the screen at a time. In case, the execution output is more than 2000 lines, then the user can view the desired output by using the navigational buttons provided on the window.

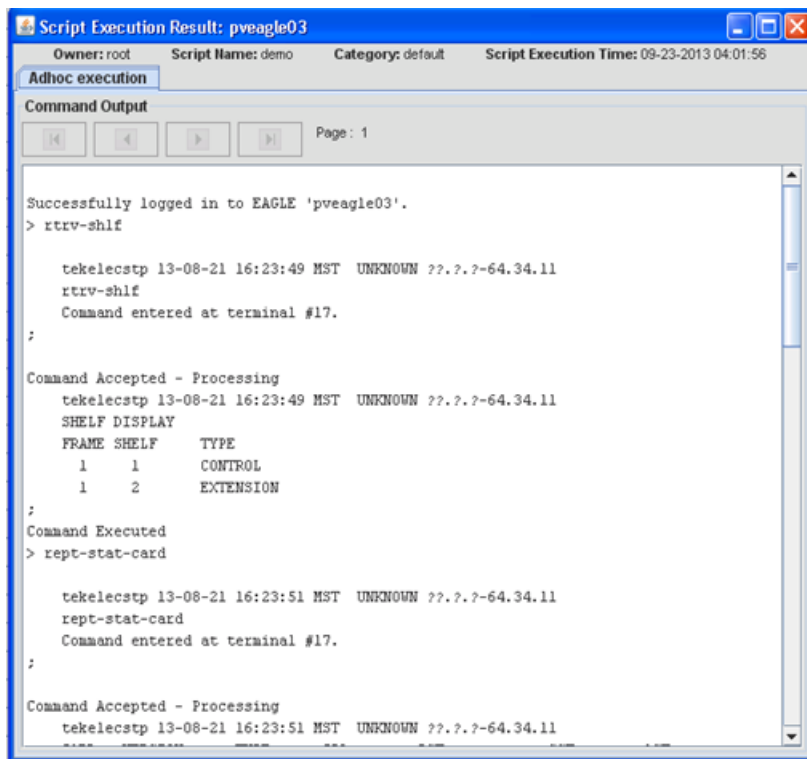


Figure 64: Script Execution Result screen

This section presents procedures available for CMI **Script Management**. Operations that can be performed for CMI **Script Management** include:

- **Create** - Clicking it launches the **Create Script** screen. This button is enabled only if the user's user group has been provided the **Create Script** operation by E5-MS admin.
- **Modify** - Selecting a script on the page and clicking **Modify** button shall launch the **Modify Script** screen. This button shall be enabled only if the user's user group has been provided the **Create Script** operation by E5-MS admin.
- **View** - Selecting a script on the page and clicking it shall launch the **View Script** screen.
- **Delete** - Selecting a script on the page and clicking **Delete** button shall launch a confirmation box asking for deletion of the selected script as shown in Script Deletion Confirmation
- **Execute** - Selecting a script on the page and clicking **Execute** button shall launch the **Execute Script** screen. This button is enabled only if the user's user group has been provided the **Execute Script** operation by E5-MS admin.

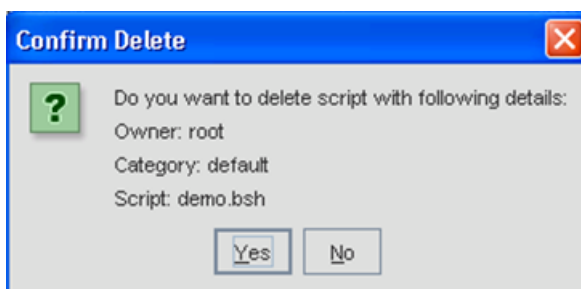


Figure 65: Script Deletion Confirmation

Create Script

Create Script screen has three panes, as follows:

- **Build Command** pane - It shall enable user to build a command to be included in the script.
- **Edit Script** pane - It shall enable user to manually edit the script.
- **Save Script Results** pane - It shall display the results of saving the script.

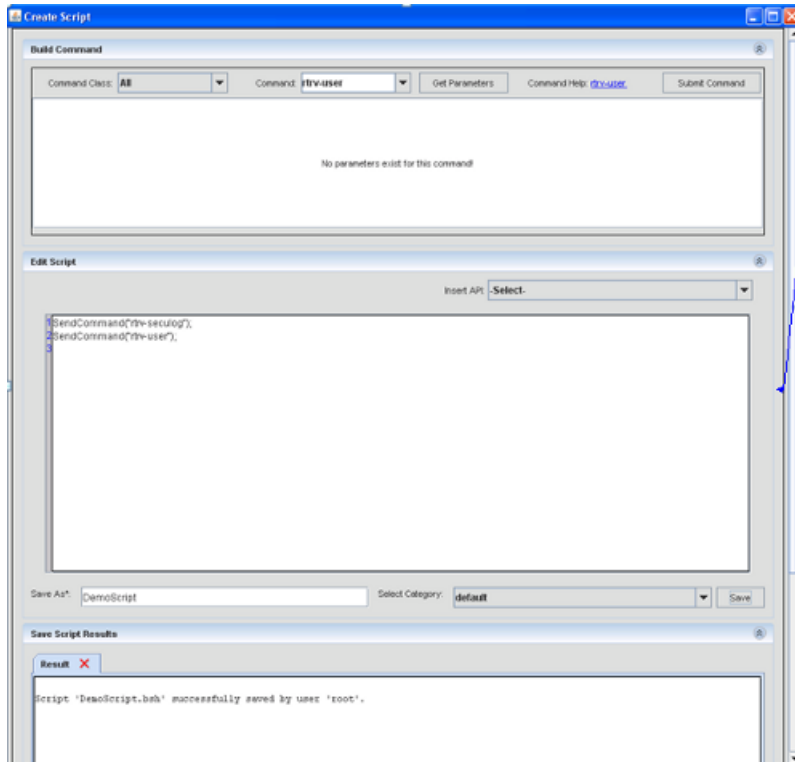


Figure 66: Create Script Screen

Edit Scripts

This pane allows a user to edit a script manually. The drop down menu "Insert API" is provided above the free edit text area which has all the APIs defined in CMI Scripting Functions

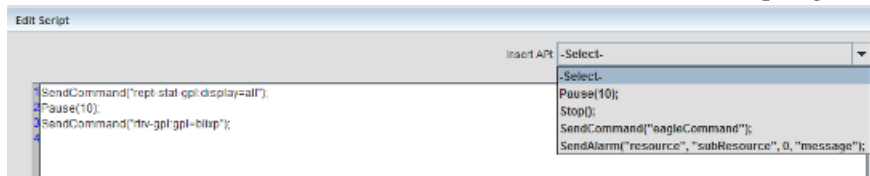


Figure 67: Edit Script Screen

Selecting an API in the drop down shall add it to the edit area at the location of the cursor.

A text box namely 'Save As*' shall be provided below the edit area. A drop down namely 'Select Category' shall also be provided adjacent to it. Providing a valid script name and selecting a desired category and then clicking the 'Save' button shall save the script in the category. In case user has used

one or more commands in the script on which he/she does not have access, then script shall not be saved and an appropriate error message is shown to the user.

These functions are described below:

1. **Pause(10)**: This function shall introduce a pause of '10' seconds during script execution. A user can use a desired value instead of 10. This function can be used in a scenario when a command fails and user wants to retry that command once again. In such a case, the script can be paused for a given seconds of time. Another example of its usage can be where a user wants the script to deliberately wait for some time.
2. **Stop()**: This function shall stop the execution of a script. This function can be used in case a user wants to stop the script execution altogether in case of a mandatory command failure. Every command executed from within a script returns a status showing whether it completed successfully or not. In case it was not successful and the rest of the commands in the script are dependent on it, then a user can stop the script.
3. **SendCommand("eagleCommand")**: This function shall send a command to EAGLE for execution. It returns the status of command execution in Boolean (true=success, false=failure). Note that when a user manually writes the complete command in SendCommand API instead of building the command, then while saving the script, only command name is validated for user's access. In case a user writes invalid parameters/values for the command, then those shall not be validated while saving the script.
4. **SendAlarm("resource", "subResource", 0, "message")**: This function shall generate an alarm on a Resource "resource" and Sub-Resource 'subResource' with severity (denoted by 0) and alarm message as provided in "message" field. The user is required to update the default values as per his/her requirement. This function can be used to generate a custom alarm to indicate a success or failure in script execution. For example, if a command fails in the script, an alarm can be generated so that the user can take corrective action later.
 - a. **resource** = Script execution
 - b. **subResource** = <Script name>
 - c. **0 (severity)** = <Desired severity>, e.g. 1 (Critical), 2 (Major), 3 (Minor), 4 (Warning) and 7 (Info)
 - d. **message** = <Desired message>, e.g. "Command 'Rept-stat-card' failed", "Script Failed", "Script completed successfully" etc.

Modify Script

This screen is similar to 'Create Script screen. When launched, it has the details of script (script contents, name and category) pre-populated on the page. The user can modify the script contents, name and category and save.

If a user modifies the script content on **Modify Script** screen and tries to close the window without saving the changes, a warning message is shown to the user, if they want to save the script.

View Script

View Script screen details and contents of a script in a non-editable edit area.

Execute Script

Execute Script screen has two panes, in the following order, top to bottom:

- **Select Script** pane - It enables user to select desired script and EAGLE(s) for execution.
- **Script Execution Results** pane - It displays the script execution results

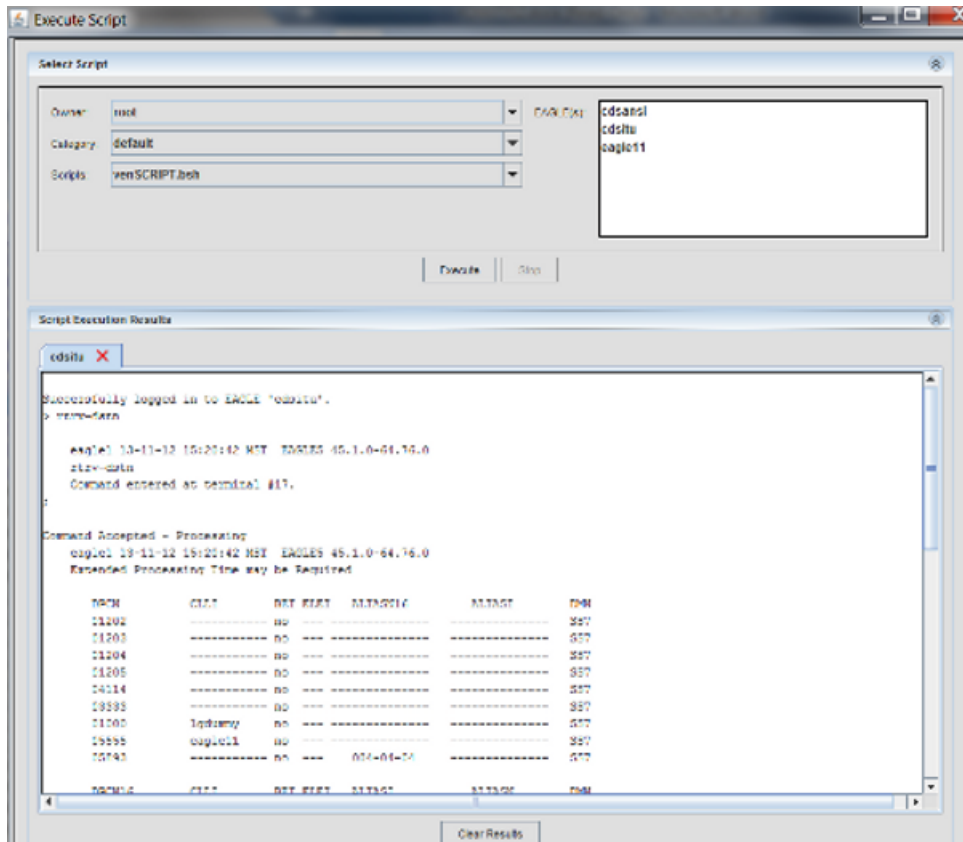


Figure 68: Execute Script Screen

Select Script pane

The **Select Script** pane allows a user to select a desired script and EAGLE(s). The **Owner** drop down lists all the E5-MS users and it is enabled for an admin and disabled for a non-admin user. So, an admin has the ability to select a user in Owner drop down, then a category belonging to that user in **Category** drop down and then select the desired script to execute. A non-admin user select their own scripts and execute them.

Below the **Select Script** pane, two buttons namely **Execute** and **Stop** is provided. Selecting a desired script and EAGLE(s) and clicking on the **Execute** button executes the script if the user has access to all the commands used in the script. In case there are one or more commands in the script on the user does not have access, then script execution fails and an appropriate error message is shown to the user. The **Stop** button is disabled by default and is enabled when script execution is in progress. Clicking on it, a user is able to stop a script execution. On clicking the **Stop** button, script execution stops on all the EAGLE(s) which were selected by the user while sending the script for execution. While a script execution is in progress, **Select Script** pane is disabled so that a user cannot change the

previously made selections. The pane is enabled again for the user to select desired script and EAGLE(s) when script execution has been completed/stopped.

Script Execution Results pane

The **Script Execution Results** pane displays the script execution results for various EAGLE(s). Each EAGLE's execution results are in a separate tab, which is created when the first script is sent to that EAGLE for execution. Once an EAGLE's tab has been created, execution results of all the scripts executed on that EAGLE is displayed in that tab only till the time the tab is open. Note that only the latest 5000 lines of results are shown in an EAGLE's tab. In case the lines are more than 5000, then older lines are removed to display the latest results.

A user has the ability to close an EAGLE's tab. However, when a script is being executed on an EAGLE, the corresponding tab is not allowed to be closed.

A **Clear Results** button is provided at the bottom of the screen, which is used to clear the results from the currently selected EAGLE tab.

Schedule Management

Schedule Management Screen enables users to schedule CMI scripts. There is an **Add Task** button at the bottom of the screen the user can schedule scripts. This button is enabled only if the user's user group is provided the **Schedule CMI Script** operation by the E5-MS System Administrator.

Selecting **CMI** in the drop down adjacent to **Add Task** button and clicking on the button opens a the **CMI Scheduler**. As shown in CMI Scheduler Screen.

Figure 69: CMI Scheduler Screen

The CMI Scheduler window has two panes:

- **Select CMI Task** pane - enables a user selecting the desired script for execution and the EAGLE(s) which the script is executed.
- **Time** pane - enables a user select the frequency of script execution.

Select CMI Task pane

This pane enables a user select the desired script and EAGLE(s). Three drop downs is available to aid a user in selecting a desired script for scheduling:

- **Owner** - This drop down has the listing of all the E5-MS users. This is enabled for an admin user and disabled for a non-admin user. So, an admin is able to select a desired user in this drop down.
- **Category** - This drop down has the listing of all the categories for the user selected in **Owner** drop down.
- **Scripts** - This drop down has the listing of scripts as per the owner and category selected in **Owner** and **Category** drop downs.

The EAGLE(s) assigned to the user's user group is displayed in the **EAGLE(s)** list. Selection of a script and at least one EAGLE is mandatory for the script to be scheduled.

Time pane

This pane provides the user various means of selecting a desired frequency of scheduled script execution. A user can select following timing options:

- Date of execution - All the dates/Particular dates OR All the days of week/Specific day(s) of week.
- Time of execution - All the hours of day/Specific hour and All the minutes/Specific minute.

After selecting a script, EAGLE(s) and the frequency of execution and submitting the values using **Submit** button on the window, a confirmation box is shown to the user with the values filled up by the user. On clicking **Yes** on the confirmation box the script is scheduled.

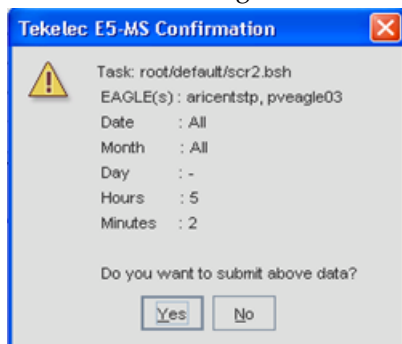


Figure 70: CMI Scheduler Confirmation

Note: By default, the scheduled script is **enabled** i.e. it runs at the given frequency. However, the user has the ability to disable the scheduled execution of a script by un-checking the box in the **Enabled** column for that script. This will stop the scheduled execution of the script. The user has the ability to start the scheduled execution again by checking the box in **Enabled** column.

Note: While scheduling scripts, following points should be kept in mind:

- A script should not be scheduled for execution for every minute of the all the days i.e. the value in **Scheduled Time** column on **Schedule Management** page should not read "All the days, every minute of the day". A script scheduled with this frequency will try to run every minute and might make E5-MS server unstable.

- E5-MS admin ensures there is a gap of at least 2 minutes between every two scheduled CMI script executions. This is because in case two scripts try to login to the same EAGLE at (almost) the same time, then only one of them succeeds in logging into EAGLE. This is because EAGLE does not present the list of free IPSM terminals to a login session when another session has already been presented the list of free IPSM terminals and in the process of choosing a terminal and logging in. So, it is recommended to have a time gap between every two script executions.

CMI Informational/Error Message List

S. NO.	CMI Functionality	Error Message
1.	Send Command	No EAGLE(s) selected for login! Please select EAGLE(s) in the 'Available EAGLE(s)' list.
2.		Please wait...Already logging in to EAGLE '<eagle name>'
3.		Already logged in to <eagle name>.
4.		No EAGLE(s) selected for logout! Please select EAGLE(s) in the 'Logged-in EAGLE(s)' list.
5.		Command execution failed! No EAGLE(s) in the 'Logged-in EAGLE(s)' list.
6.		No EAGLE(s) selected for command execution! Please select EAGLE(s) in the 'Logged-in EAGLE(s)' list.
7.		Either command is incorrect or user does not have access on command!
8.		EAGLE '<eagle name>' is already executing a command! Please try later.
9.		Please select a command in 'Command' combo box!
10.		Cannot close the results tab while EAGLE is logged-in!
11.		Logged out of EAGLE '<eagle name>' due to your access to it being revoked by administrator
12.		Successfully logged in to EAGLE '<eagle name>'
13.		Successfully logged out to EAGLE '<eagle name>'
14.		Login to EAGLE '<eagle name>' failed!
15.		Logout of EAGLE '<eagle name>' failed!
16.		Logged out of EAGLE '<eagle name>' due to inactivity!
17.	Category Management	Category 'default' can not be renamed!
18.		Category 'default' can not be deleted!
19.		Mandatory field 'Category Name' is blank! Please provide a valid category name.

S. NO.	CMI Functionality	Error Message	
20.		Category name must have minimum 3 characters!	
21.		Category name must not have more than 255 characters!	
22.		Category name cannot be set as 'All'! This is a reserved keyword.	
23.		Only alphanumeric characters (0-9, a-z, A-Z) are allowed for category name! Please provide a valid category name.	
24.		A category by name '<category name>' already exists! Please provide a unique category name.	
25.		Category creation failed! Please contact the E5-MS administrator.	
26.		Renaming of category '<category name>' failed! Category does not exist.	
27.		Renaming of category '<category name>' failed! Please contact the E5-MS administrator	
28.		Deletion of category '<category name>' failed! Category does not exist.	
29.		Deletion of category '<category name>' failed! Please contact the E5-MS administrator.	
30.		Deletion of category '<category name>' failed! One or more scripts with identical names already exist in category 'default'.	
31.		Script Management	Script viewing failed! Script '<script name>' does not exist.
32.			Script modification failed! Script '<script name>' does not exist.
33.	Script execution failed! Script '<script name>' does not exist.		
34.	Script deletion failed! Script '<script name>' does not exist.		
35.	Create / Modify Script	User '<user name>' does not have access on command(s): <command names>.	
36.		Mandatory field 'Save As' is blank! Please provide a valid script name.	
37.		Script name must have minimum 3 characters!	
38.		Script name must not have more than 255 characters!	
39.		Only alphanumeric characters (0-9, a-z, A-Z), underscore and hyphen are allowed for script name! Please provide a valid script name.	
40.		Script '<script name>' already exists in category '<category name>'! Please provide a unique script name.	
41.		Script saving failed! Script has no content.	
42.		Script saving failed! Syntax errors found in the script.	

S. NO.	CMI Functionality	Error Message
Execute Script 43. 44. 45.		Script execution failed! Please select at least one EAGLE for script execution.
		EAGLE ' <eagle name>' is already executing a script! Please try later.
		Cannot close the results tab while script is being executed on the EAGLE!

Chapter 12

Link Utilization Interface

Topics:

- *Overview.....156*
- *Functional Limitations.....156*
- *Link Utilization GUI.....156*
- *Schedule Management.....166*
- *LUI Measurements Error and Informational Messages.....166*

This chapter provides information about the Link Utilization Interface (LUI). This interface is used for configuring capacity information in the E5-MS for links in EAGLE systems.

Overview

The Link Utilization Interface gathers configured capacity information from each EAGLE system. It creates and periodically executes polling scripts that retrieve the capacity information, ensuring the information is current. The information is stored in the E5-MS database, along with the data collected by the Measurements Module so the E5-MS Users can request ad-hoc utilization reports on links, linksets, and cards.

Functional Limitations

The LUI functionality is available upon successful installation of these modules:

- Measurements Module
- Fault Management
- Configuration Management Interface (CMI)

User Access Control

Administrators and usergroups assigned **Link Utilization** operation have access to Link Data, On Demand Polling, Threshold Configuration of LUI module and the polling script entries on **Schedule Management** screen. The LUI module automatically detect **New EAGLE(s)** added to E5-MS module and create polling scripts so it is mandatory that a user assigned **Link Utilization** operation have access to all EAGLE(s).

The usergroup assigned the **Link Utilization** operation are automatically assigned access to all **Existing EAGLE(s)** and the commands (`rtrv-slk`, `rept-stat-card`, `rept-stat-iptps`) needed in LUI module. Any EAGLE added to E5-MS are automatically be assigned to the usergroups.

Link Utilization GUI

Link Utilization is located in the E5-MS applications tree node. There are three elements under Link Utilization as shown in [Figure 71: Link Utilization Tree Node](#)



Figure 71: Link Utilization Tree Node

The elements are the:

- Link Data
- On Demand Polling
- Threshold Configuration

The user is granted access to this application by the System Administrator.

Link Data

Before performing this procedure, the user must be associated with a Usergroup that is authorized to use the **Link Utilization** application.

The procedure below will provide a user the steps to view information about each link supported by an EAGLE system.

1. Select **Link Data** under the **Link Utilization** tree node in the main menu on the left side of the E5-MS GUI page link.

Link Data

A screen will appear, as shown in Link Data Screen.

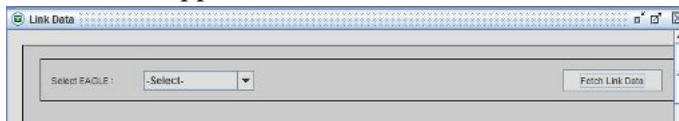


Figure 72: Link Data Screen

The Link Data screen provides the following:

- **Select EAGLE** to view the available link data: This field contains a drop-down list of the EAGLE systems to which the E5-MS is connected.
 - **Fetch Link Data** button: Clicking the **Fetch Link Data** button retrieves the link information for the selected EAGLE system.
2. **Select** the EAGLE system of the drop-down list to view the link data.
 3. Click **Fetch Link Data** button, to retrieves the link information for the selected EAGLE system. The Data Link screen populates with a table as shown in the example of Link data for EAGLE: eagle11.

LOC	LINK	LSN	TYPE	USER DEFINED CAPACITY	LINK CAPACITY
1121	A	21101400	LR11	50000	50000
1121	A1	21101400	LR11	50000	50000
1121	A2	21101400	LR11	50000	50000
1121	A3	21101400	LR11	50000	50000
1121	B	21101400	LR11	50000	50000
1121	B1	21101400	LR11	50000	50000

Figure 73: Link data for EAGLE: eagle11

Note: An error message

EAGLE not selected! Please select an EAGLE to view link data.

will display, if the user clicks on **Fetch Link Data** button without selecting an EAGLE system from the drop-down.

Link Data Screen Elements

Element	Description
LOC Field	The location of the card on which the link resides.
Link Field	Identifies the signaling link within the linkset identified in LSN
LSN	The name of the linkset that contains the link.
Type	The type of the link.
USER DEFINED CAPACITY:	A hypothetical capacity of the link BPS value for Non-IP link and SLKTPS value for IP link that can be modified by the user.
LINK CAPACITY	Link capacity value as configured on the EAGLE or calculated by LUI agent based on the available information from EAGLE polling.

Modifying Link Capacity

Before performing this procedure, the user must be associated with a Usergroup that is authorized to use the **Link Utilization** application.

This procedure describes how to manually change the hypothetical, user-defined link capacity information associated with a link in a selected EAGLE system to which the E5-MS is connected. This information is stored in the E5-MS, not in the EAGLE 5 system.

1. **Double click** on a row in table showing link data for an EAGLE. In the following example, you will see the [Figure 74: Modify User Defined Capacity](#) screen for the link data of the EAGLE11.

The screenshot shows a window titled "Modify User Defined Capacity". Inside the window, the following information is displayed:

- CLI : eagle11
- LOC : 1102
- LINK : A
- LSN : ls1102a00
- TYPE : LIMT1
- USER DEFINED CAPACITY : 56000
- LINK CAPACITY : 56000

At the bottom of the window, there are two buttons: "Update" and "Cancel".

Figure 74: Modify User Defined Capacity

This window provides:

- **CLLI:** The identity of the EAGLE containing the link for which the hypothetical capacity value is to be modified.
- **LOC:** the location of the card on which the link resides.
- **Link:** identifies the signaling link within the linkset identified in **LSN**.
- **LSN:** the name of the linkset that contains the link.
- **Type:** the type of the link.
- **USER DEFINED CAPACITY:** the hypothetical capacity value of the link (BPS value for Non-IP link and SLKTPS value for IP link) that can be modified by the user.
- **LINK CAPACITY:** link capacity value as configured on the EAGLE or calculated by LUI agent based on the available information from EAGLE polling.

The screen displays the CLLI, LOC, LINK, TYPE, LSN, USER DEFINED CAPACITY and LINK CAPACITY for the selected link. Two buttons **Update** and **Cancel** are at the bottom of the screen.

2. Enter the new hypothetical capacity value fro BPS or SLKTPS into the **USER DEFINED CAPACITY** field.
 - The textbox must not be blank.
 - Value entered in the textbox must be a positive non-zero integer.
 - Value entered in the textbox must be of maximum 14 digits.

If the user enters a valid integer value starting with zero(s) in the **User Defined Capacity** field, then the integer value following the zero(s) is updated as the new user capacity value in the table. For example, if the user enters capacity value as "0001200" then this will be updated as 1200.

If the user enters a valid integer value starting with zero(s) in the **User Defined Capacity** field, the leading zero(s) are ignored. For example, if the user enters capacity value as "0001200" then this will be updated as 1200.

3. Click on **Cancel** button to cancel the changes in the hypothetical capacity value for the link. The **Link Data** screen will be displayed.
4. Click on the **Update** button to save the new hypothetical capacity value in the EAGLE E5-MS database.

The **Link Data** screen will be displayed with updated link data table.

All links with modified hypothetical capacity values will be displayed in yellow colored rows. If the new capacity value provided does not follow the restrictions in , appropriate error messages will be displayed as follows.

- If the capacity field is blank the message displayed is USER DEFINED CAPACITY field is blank! Please provide a valid value for the field.
- If the capacity value provided by user is not a positive integer the message displayed is Capacity value provided for USER DEFINED CAPACITY field is not valid! Please provide only positive non-zero integer value (maximum 14 digits) for this field.
- If the capacity value provided by user is of more than 14 digits, not starting with 0, the message displayed is USER DEFINED CAPACITY value is more than 14 digits!

Reset User Defined Capacity button: clicking the **Reset User Defined Capacity** button causes a confirmation dialog box to be displayed. Once the user clicks the **Ok** button, the link capacity values for BPS value for Non-IP links and SLKTPS value for IP links are populated under the **USER DEFINED CAPACITY** column.

Polling Scripts Creation

Every polling script shall consist of three EAGLE commands which runs on the EAGLE to fetch link capacity data. These commands are:

- **RTRV-SLK**

This command is required to retrieve all the links and parameters. LOC, LINK, LSN, SLC, TYPE, BPS, and SLKTPS of configured links are available from this command output and defined in the column headers of the output. Some capacity values are not available from this command. Default values are used. For example, the SS7IPGW, IPGWI, IPLIM and IPLIMI do not show a SLKTPS value. In order to get SLKTPS for these link types we can use the maximum possible capacity values using the REPT-STAT-CARD command or the configured value using the REPT-STAT-IPTPS command. As shown in [Figure 75: RTRV-SLK Command Output](#).

```

cdsitu X
Command Accepted - Processing
eagle1 . EAGLE5

LOC LINK LSN      SLC TYPE      ANAME      SLKTPS/      MAXSLKTPS
      RSVDSLKTPS

1213 A   lgdummy  0   IPSTG   lgdummy    1000        1000
1213 B   m3uastp2 0   IPSTG   m3uastp2   100         100
1213 A1  stp11m2pa 0   IPSTG   stp11m2pa  1000        5000
1214 A   mgtsm3ua 0   IPSTG   mgtsm3ua   100         100
1214 A1  stp11m2paj 0   IPSTG   stp11m2paj7 1000        5000

LOC LINK LSN      SLC TYPE      L2T      PCR PCR   E1  E1
      SET BPS   ECM  N1  N2      LOC PORT TS
1203 A   ls1203mgts 0   LIME1  11  64000  BASIC ---- - 1203 1  1
1203 B   ls1203mgts 2   LIME1  11  64000  BASIC ---- - 1203 2  1
1203 A1  ls1203mgts 1   LIME1  11  64000  BASIC ---- - 1203 1  2
1204 A   ls1204stp2 1   LIME1  11  64000  BASIC ---- - 1204 1  1

SLK table is (9 of 1200) 1% full.

;
Command Executed

```

Figure 75: RTRV-SLK Command Output

- **REPT-STAT-CARD**

This command is used to further define type and capacity of different link types. If a link, fetched from the EAGLE using RTRV-SLK command, does not display capacity value, its location is searched in the output of the REPT-STAT-CARD command. Through location of the card, its hardware type and the APPL/GPL running on it can easily be found. And now with the help of link type, its card type and the GPL, the capacity is fetched from a pre-defined set of values maintained in a structure on E5-MS. As shown in [Figure 76: REPT-STAT-CARD Command Output](#)


```

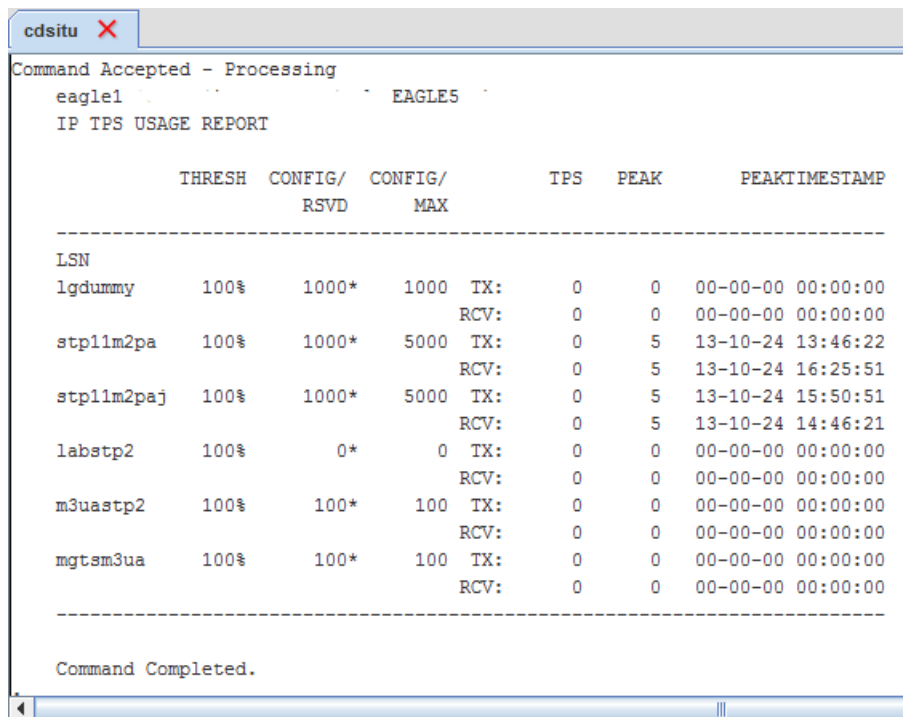
cdsitu X
Command Accepted - Processing
eagle1
CARD  VERSION  TYPE  GPL  PST  SST  AST
1103  134-076-000  DSM  SCCPHC  IS-NR  Active  -----
1105  134-076-000  DSM  DEIRHC  IS-NR  Active  -----
1108  134-076-000  IPSM  IPSHC  IS-NR  Active  -----
1109  134-069-000  HIPR2  HIPR2  IS-NR  Active  -----
1110  134-069-000  HIPR2  HIPR2  IS-NR  Active  -----
1111  134-076-000  DSM  SCCPHC  IS-NR  Active  -----
1113  134-076-000  ESMCAP  OAMHC  IS-NR  Active  -----
1114  -----  E5TDM  IS-NR  Active  -----
1115  134-076-000  ESMCAP  OAMHC  IS-NR  Standby  -----
1116  -----  E5TDM  IS-NR  Active  -----
1117  -----  E5MDAL  IS-NR  Active  -----
1203  134-076-000  LIME1  SS7HC  IS-NR  Active  -----
1204  134-076-000  LIME1  SS7HC  IS-NR  Active  -----
1209  134-069-000  HIPR2  HIPR2  IS-NR  Active  -----
1210  134-069-000  HIPR2  HIPR2  IS-NR  Active  -----
1213  134-076-000  E5ENET  IPSG  IS-NR  Active  -----
1214  134-076-000  E5ENET  IPSG  IS-NR  Active  -----
1309  134-069-000  HIPR2  HIPR2  IS-NR  Active  -----
1310  134-069-000  HIPR2  HIPR2  IS-NR  Active  -----
Command Completed

```

Figure 76: REPT-STAT-CARD Command Output

- REPT-STAT-IPTPS

This command is used to get CONFIG capacity values for IPGWx type of IP links, as `rtrv-slk` command gives SLKTPTS value for IPSG link types only. Polling scripts with the `rept-stat-iptps` command capability are generated after the first `rtrv-slk` poll defining the different links, link sets and their respective types. This polling script replaces the earlier script. The subsequent execution of these polling scripts shall run `rept-stat-iptps` command for all the IPGW link sets and shall try to fetch SLKTPTS value for IPGW linksets. As shown in [Figure 77: REPT-STAT-IPTPS Command Output](#).



```

cdsitu X
Command Accepted - Processing
eagle1 EAGLE5
IP TPS USAGE REPORT

      THRESH  CONFIG/  CONFIG/      TPS  PEAK      PEAKTIMESTAMP
          %   RSVD     MAX
-----
LSN
lgdummy    100%    1000*   1000 TX:    0    0    00-00-00 00:00:00
           RCV:    0    0    00-00-00 00:00:00
stp11m2pa  100%    1000*   5000 TX:    0    5    13-10-24 13:46:22
           RCV:    0    5    13-10-24 16:25:51
stp11m2paj 100%    1000*   5000 TX:    0    5    13-10-24 15:50:51
           RCV:    0    5    13-10-24 14:46:21
labstp2    100%      0*      0 TX:    0    0    00-00-00 00:00:00
           RCV:    0    0    00-00-00 00:00:00
m3uastp2   100%    100*    100 TX:    0    0    00-00-00 00:00:00
           RCV:    0    0    00-00-00 00:00:00
mgtsm3ua   100%    100*    100 TX:    0    0    00-00-00 00:00:00
           RCV:    0    0    00-00-00 00:00:00
-----
Command Completed.

```

Figure 77: REPT-STAT-IPTPS Command Output

The polling scripts are scheduled for regular execution. The timing and frequency of those script executions is configurable. By default, LUI polling script execution time is 01:00 AM as per current implementation. To change the schedule of polling script execution or to stop further execution of polling scripts, see *Modifying Polling Script Execution Schedule*.

On Demand Polling

Before performing this procedure, the user must be associated with a Usergroup that is authorized to use the **Link Utilization** application.

On-Demand Polling retrieves link capacity information for each EAGLE system for which polling scripts were created and saved..

Before polling the EAGLE systems, a check is made for any other instance of the same EAGLE system polling script is running for the selected EAGLE system. If another instance of the EAGLE system polling scripts is found running for the selected EAGLE system, on-demand execution of the corresponding scripts is aborted and an information message

An instance of polling script for EAGLE <CLLI> is already running. Please try later.
will be displayed on GUI.

The procedure below will provide a user the steps to run On Demand Polling scripts from the E5-MS.

1. Select **On Demand Polling** under the **Link Utilization** tree node in the main menu on the left side of the E5-MS GUI page link as shown in [Figure 78: On Demand Polling](#)

On Demand Polling

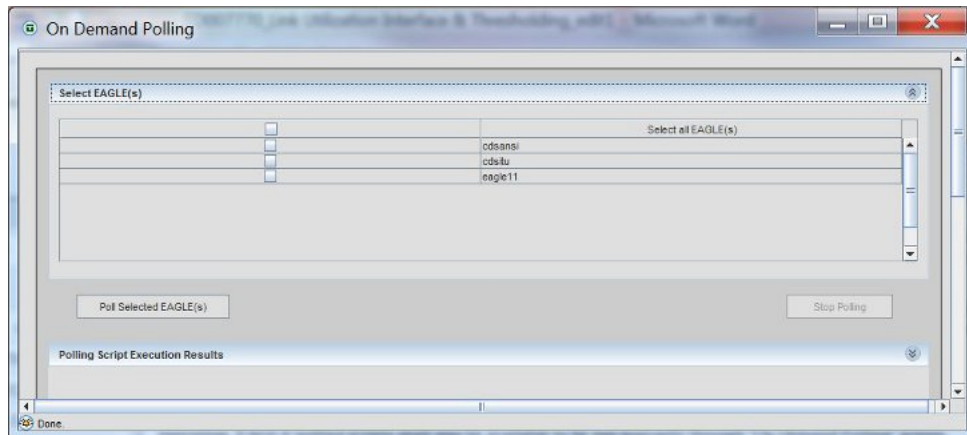


Figure 78: On Demand Polling

2. Click the check boxes from the **Select all EAGLE(s)** list which on-demand polling is being performed. A single, multiple, or all connected EAGLE systems may be selected.
3. Click on the **Poll Selected EAGLE(s)** button to begin polling.
 - The real-time status of EAGLE system polling script execution is displayed in the **Polling Script Execution Results** at the bottom of the screen.
 - While the on-demand execution for selected EAGLE system(s) is in progress, all check boxes and **Poll Selected EAGLE(s)** button are disabled.
 - If the another polling script starts execution of a scheduled EAGLE system polling script while the EAGLE system is being polled via an on-demand request, the scheduled script will not execute.
 - Once the polling of selected EAGLE system(s) is completed, the check boxes and the **Poll Selected EAGLE(s)** button will be enabled.
 - If no polling script is found, then instead of **Select all EAGLEs** checkbox, **No Polling scripts available!** message will be displayed on the GUI and both **Polling Selected EAGLE(s)** and **Stop Polling** buttons will be disabled.

The output of the polling is shown in [Figure 79: Polling Script Execution Results](#)

```

Polling Script Execution Results
eagle11 X
Successfully logged in to EAGLE 'eagle11!!'
> rept-stat-card

tokyostp11          EAGLE
rept-stat-card
Command entered at terminal #17.
;

Command Accepted - Processing
tokyostp11          EAGLE
CARD  VERSION    TYPE   GPL     PST      SST      AST
1101  134-071-011  LIMIT1 SS7HC   IS-NR    Active   -----
1102  134-071-011  LIMIT1 SS7HC   IS-NR    Active   -----
1105  134-071-011  DSM     SCCPHC  IS-ANR   MPS Unavl -----
1108  134-071-011  IPSM    IPSHC   IS-NR    Active   -----
1109  134-069-000  HIPR2   HIPR2   IS-NR    Active   -----
1110  134-069-000  HIPR2   HIPR2   IS-NR    Active   -----
1111  -----      ESENET  IPG     IS-ANR   Fault    -----

```

Figure 79: Polling Script Execution Results

4. Clicking the **Stop Polling** button to stop polling scripts execution of EAGLE system immediately and the login session with the EAGLE system will be terminated on the EAGLE system on which polling is in progress at that time.

The information message `Script execution stopped in EAGLE <CLLI>` will be display in the tab with the EAGLE name.

Thresholding Configuration

The Thresholding Configuration functionality is available upon successful installation of these modules:

- Measurements Module
- Fault Management
- Configuration Management Interface (CMI)
- Link Utilization Interface

The **Thresholding Configuration** feature provides the ability to enable or disable the three measurement types: link, linkset and card. Using this capacity information along with the measurements gathered from EAGLE system, the **Thresholding Configuration** feature calculates percent utilization for all the entities of the type link, linkset, and card. **Thresholding Configuration** allows configuration of thresholds by link, linkset, and card measurement types. For each measurement type, the threshold alarm value, alarm severity, and threshold clear value can be configured independently from the other measurement types. The alarms generated by **Thresholding Configuration** feature are visible on the **Alarms** screen under **Fault Management** in E5-MS.

Thresholding Configuration

Before performing this procedure, the user must be associated with a Usergroup that is authorized to use the **Link Utilization** application.

This procedure is used to sort the Threshold Alarm messages, Threshold Clear messages and Threshold Informational messages from the E5-MS.

1. Select **Thresholding Configuration** under the **Link Utilization** tree node in the main menu on the left side of the E5-MS GUI page link.

Thresholding Configuration

A screen will appear, as shown in Thresholding Configuration Screen.

<input type="checkbox"/> Enable All	Measurement Type	Threshold Alarm Value	Severity Level	Threshold Clear Value
<input checked="" type="checkbox"/>	CARD	75	Major	25
<input checked="" type="checkbox"/>	LINK	35	Minor	20
<input checked="" type="checkbox"/>	LINKSET	-Select-	Minor	-Select-

Submit

Done.

Figure 80: Thresholding Configuration Screen

2. **Enable** each Measurement Type within the check box or **Enable All** check box on the column header. By default, the check box on the column header and for all the three rows are unchecked i.e., the thresholding functionality is disabled for all the measurement types. **Measurement Type** contain three pre-populated entries - LINK, LINKSET and CARD one in each row.
3. Select the **Threshold Alarm Value** from a drop down values 1 to 99. This is the threshold value which the percent utilization calculated for the entities corresponding to the associated **Measurement Type** are compared. By default, value **Select** is populated in the drop down.
4. Select **Severity Level** from a drop down with the values **Select**, **Critical**, **Major** and **Minor**. By default, the value is set to **Select**.
If **Critical** selected, a pop up a confirmation box stating Are you sure you want to display a CRITICAL alarm when threshold is exceeded?
5. The **Threshold Clear Value** from the drop down values 1 to 99. This is the threshold value with which the percent utilization calculated for the entities, with outstanding **Threshold Alarms**, corresponding to the associated **Measurement Type** are compared. By default, value **Select** is populated in the drop down.
6. Click the **Submit** button at the bottom of the configuration table.
If all the values provided by the user are valid, then the configuration data is submitted and an informational message is displayed
Threshold configuration data successfully updated!

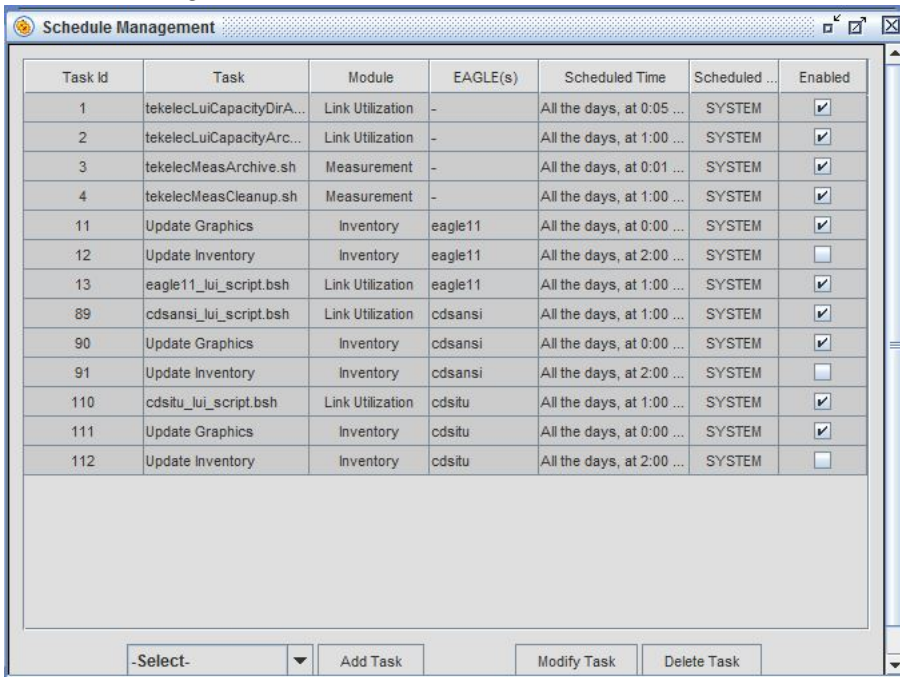
When the data on **Threshold Configuration** screen is entered incorrectly, the user clicks the **Submit** button appropriate error messages will occur if:

- The **Threshold Alarm Value** drop down for a measurement type contains **Select**. Error message Threshold alarm value for measurement type <measurement type> not selected!

- The **Threshold Clear Value** drop down for a measurement type contains **Select**. Error message Threshold clear value for measurement type <measurement type> not selected!
- The **Threshold Alarm Value** field contains a value, which is greater than or equal to the value in **Threshold Alarm Value**. Error message Threshold clear value will be greater than threshold alarm value!
- The **Severity Level** drop down for a measurement type contains **Select**. Error message The severity level for measurement type '<measurement type>' not selected!

Schedule Management

Schedule Management screen located in the tree node on the left side of the E5-MS GUI provides the same polling script and is scheduled to run at 01:10 AM every day. The frequency of polling script execution can be changed by modifying the date and time for the entry on **Schedule Management** screen. To disable polling, the user must remove the check from the box in the **Enabled** column on Schedule Management screen.



Task Id	Task	Module	EAGLE(s)	Scheduled Time	Scheduled ...	Enabled
1	tekelecLuiCapacityDirA...	Link Utilization	-	All the days, at 0:05 ...	SYSTEM	<input checked="" type="checkbox"/>
2	tekelecLuiCapacityArc...	Link Utilization	-	All the days, at 1:00 ...	SYSTEM	<input checked="" type="checkbox"/>
3	tekelecMeasArchive.sh	Measurement	-	All the days, at 0:01 ...	SYSTEM	<input checked="" type="checkbox"/>
4	tekelecMeasCleanup.sh	Measurement	-	All the days, at 1:00 ...	SYSTEM	<input checked="" type="checkbox"/>
11	Update Graphics	Inventory	eagle11	All the days, at 0:00 ...	SYSTEM	<input checked="" type="checkbox"/>
12	Update Inventory	Inventory	eagle11	All the days, at 2:00 ...	SYSTEM	<input type="checkbox"/>
13	eagle11_lui_script.bsh	Link Utilization	eagle11	All the days, at 1:00 ...	SYSTEM	<input checked="" type="checkbox"/>
89	cdsansi_lui_script.bsh	Link Utilization	cdsansi	All the days, at 1:00 ...	SYSTEM	<input checked="" type="checkbox"/>
90	Update Graphics	Inventory	cdsansi	All the days, at 0:00 ...	SYSTEM	<input checked="" type="checkbox"/>
91	Update Inventory	Inventory	cdsansi	All the days, at 2:00 ...	SYSTEM	<input type="checkbox"/>
110	cdsitu_lui_script.bsh	Link Utilization	cdsitu	All the days, at 1:00 ...	SYSTEM	<input checked="" type="checkbox"/>
111	Update Graphics	Inventory	cdsitu	All the days, at 0:00 ...	SYSTEM	<input checked="" type="checkbox"/>
112	Update Inventory	Inventory	cdsitu	All the days, at 2:00 ...	SYSTEM	<input type="checkbox"/>

Figure 81: Schedule Management

LUI Measurements Error and Informational Messages

The following error and informational messages are associated with the LUI Measurements feature.

Table 22: LUI Measurements Error and Informational Messages

Scenario	Error or Information Message
If there is no change in the configuration data and the check boxes corresponding to LINK , LINKSET , and CARD on the Threshold Configuration screen are already unchecked and the user clicks the Submit button.	No configuration data to update
When no constraint on the Threshold Configuration screen is violated and the user clicks the Submit button.	Threshold configuration data successfully updated!
The Threshold Alarm Value drop down for a measurement type contains Select .	Threshold alarm value for measurement type measurement type not selected!
The Threshold Clear Value drop down for a measurement type contains Select .	Threshold clear value for measurement type measurement type not selected!
The Threshold Clear Value field contains a value, which is greater than or equal to the value in Threshold Alarm Value field.	Threshold clear value cannot be greater than or equal to the threshold alarm value!
The Severity Level drop down for a measurement type contains Select .	The severity level for measurement type measurement type not selected!
In case E5-MS admin tries to remove an EAGLE from a usergroup which has Link Utilization operation assigned.	All EAGLE(s) are mandatory with Link Utilization operation.
In case E5-MS admin tries to remove either of command classes DATABASE or SYSTEM MAINT from a usergroup which has Link Utilization operation assigned.	Command classes DATABASE and SYSTEM MAINT are mandatory with Link Utilization operation.

Chapter 13

Northbound Interface (NBI)

Topics:

- [Overview.....169](#)
- [Functional Description.....169](#)
- [Northbound Interface GUI.....172](#)
- [NBI Agent Configuration GUI.....177](#)

This chapter provides information about the E5-MS Northbound Interface, which is a feature of the E5-MS product that forwards alarms from EAGLE, EPAP, LSMS, and the E5-MS to one or more client Network Management Systems.

Overview

The Northbound Interface application is an optional feature to the E5-MS that processes alarms received by the E5-MS from the EAGLE, EPAP, and LSMS systems. If this application is grayed out in the E5-MS from the Tools icon at the top of the E5-MS GUI, the client or user does not have the application available. The feature forwards events to NMS(s) in the form of SNMP v2c traps (SNMPv1 for LSMS). The FTP North Bound Interface allows E5-MS raw measurement reports to be forwarded to a database.

Alarms forwarded through the SNMP interfaces include:

- Alarms collected on the Southbound interfaces (Eagle, EPAP, and LSMS alarms)
- E5-MS alarms
- Alarms generated by features such as EAGLE EMS Measurements Based Threshold Alarms Tier 1.

NBI is able to support trap forwarding to NMS at a rate of 112 alarms per second. The rate has been derived for 14 mated pair of EAGLE(s) (i.e. 28 EAGLE(s)) with each sending alarms to E5-MS at a rate of 4 alarms per second

A (Secured) FTP NBI is offered on the E5-MS system. This interface allows the "export" of the measurement reports collected from the different elements managed.

An additional enhancement is offered with North Bound Interfaces for an additional filtering criteria. To the existing resource, sub-resource, severity and acknowledgement, you can add the UAM/UIM Number and the date/time of the event to this list.

Functional Description

The Northbound Interface processes alarms received by the EAGLE as well as alarms generated within the E5-MS. The E5-MS forwards the latest event for each (unique combination of) resource and sub-resource available with it to a NMS on receipt of a resynchronization request in the form of SET request. The resynchronization occurs in following manner:

1. NMS sends a SNMP SET request (that sets an object value to 1) indicating request for event resynchronization.
2. NBI halts normal forwarding of autonomous events to the requesting NMS. However, these autonomous events continue to be stored in the queue as outstanding autonomous events.
3. NBI fetches open events from alert table with timestamp less than equal to the time when normal forwarding was halted and forward them to the NMS as SNMP v2c traps after checking them against matching/filtering patterns.
4. After the resync process is complete, NBI sends a trap indicating the completion of resync process.
5. NBI forwards all the outstanding autonomous events, after checking them against matching/filtering patterns, received during this period to the NMS on a FIFO basis from the queue.
6. The object value is reset to 0 and normal trap forwarding is resumed.

Autonomous Events Trap Forwarding

NBI SNMP agent forwards all autonomous events received at E5-MS in form of SNMP v2c traps to all configured NMS, once the events are filtered using matching/filtering patterns. A NBI circular queue is maintained at E5-MS for storing autonomous events. One thread per NMS is maintained for forwarding autonomous events. Each thread maintains its own head on the circular queue; this is required to ensure that processing for one NMS do not interfere with other NMS configured. Three states are maintained per NMS as follows Normal, Resync and Transition mode. Autonomous event are forwarded in normal mode. Other modes are discussed in resynchronization.

The SNMP v2c traps forwarded to northbound NMS(s) are as per Oracle's TEKELEC EAGLE EMS MIB definition and have the following varbinds:

- alertTime - timestamp when E5-MS system received the event for the managed sub-domain.
- alertResourceName - provides the source of the alert in a human readable form.
- alertSubResourceName - provides the sub-source of the alert in a human readable form.
- alertSeverity - defines severity of the alert.
- alertAcknowledgeMode - indicates whether the alert is acknowledged or not.
- alertTextMessage - the message body of the alert.
- alertSequenceNumber - incrementing sequence number allowing NMS to determine if an event has been missed.

All the traps are forwarded to the NMS(s) on respective ports as configured in NBI. The trap header includes the community string as configured in NBI for that particular NMS.

Only those autonomous events which pass matching/filtering criteria as per rule defined in [Northbound Interface GUI](#) are forwarded by E5-MS to NMS.

All autonomous events are forwarded by E5-MS to a particular NMS if no matching/filtering criteria are configured in NBI for that NMS. Status Update events generated at the E5-MS are not be forwarded to NMS.

EAGLE inventory discovery events (for e.g. discovery/addition of Frame, Shelf, CARD etc.) are not be forwarded to NMS.

The E5-MS generates heartbeat traps and send it to all the NMS(s) periodically to indicate that the connection is still up. The periodicity may be different for different NMS(s) due to the heartbeat value configured in the NBI. No response is needed from NMS for the heartbeat trap.

Heartbeat Trap

NBI SNMP agent sends a heartbeat trap i.e. system alive message to NMS at configured interval. This interval is configurable from the NBI GUI. Each NMS can set the value of heartbeat interval as per there requirement. A separate thread gets spawned per NMS for sending heartbeat trap.

Resynchronization

If the NMS gets out of sync with E5-MS, the E5-MS NBI SNMP agent provides provision of listening to an SNMP set request from NMS. When receiving a SNMP set request, the E5-MS triggers resynchronization if another SNMP set request is not under progress at the NMS. E5-MS SNMP agent switches to resync mode for that NMS, during which following steps are performed:

- Autonomous events are buffered in queue and are not processed.
- Resync start trap is sent to NMS.
- Active alarms are picked from DB which are less than or equal to resync trigger time and are send as resync traps once the alarms get filtered using matching/filtering patterns.
- Resync stop trap is sent to NMS.
- Mode gets toggled from 'resync' to 'transition'. In transition mode, outstanding autonomous events get sent to NMS.
- Once all outstanding autonomous events gets sent then SNMP agent toggles mode from 'transition' to 'normal'.

E5-MS SNMP Agent Configuration

E5-MS provides a GUI for configuring SNMP agent read and write community. These community strings authenticates NMS Get/Set request to E5-MS agent. The GUI is launched from the menu screen as shown in NBI Tree Node. This is available to only authorized users having **NBI Agent Configuration** security operation assigned. NBI agent by default shall listen for SNMP Get/Set request on 8002 port which shall not be configurable.

<u>T</u> ools	<u>L</u> ook And Feel	<u>W</u> indow
<u>S</u> ecurity Administration		Alt-S
Change Password		
Themes		
Eagle Discovery		
Eagle Inventory		
LSMS Discovery		
EPAP Discovery		
Report Designer		
Reporting Studio		
NBI		
NBI Agent Configuration		
NBI FTP Configuration		
License Details		
E5-MS Notifications		
E5-MS Notifications Settings		

Figure 82: NBI Tree Node

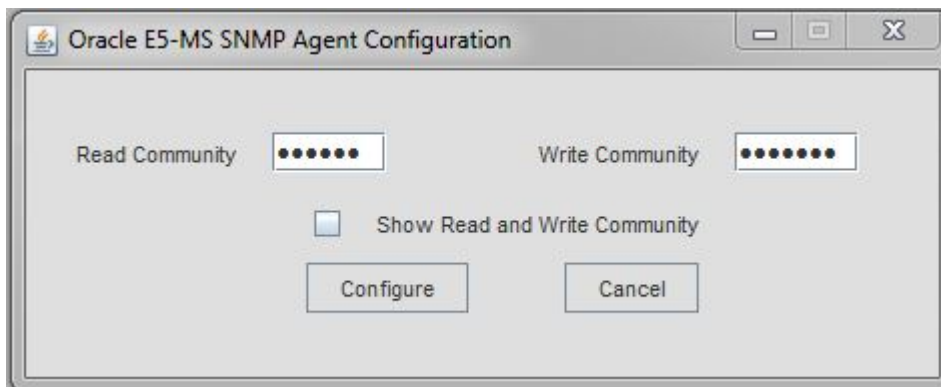


Figure 83: NBI Agent Configuration

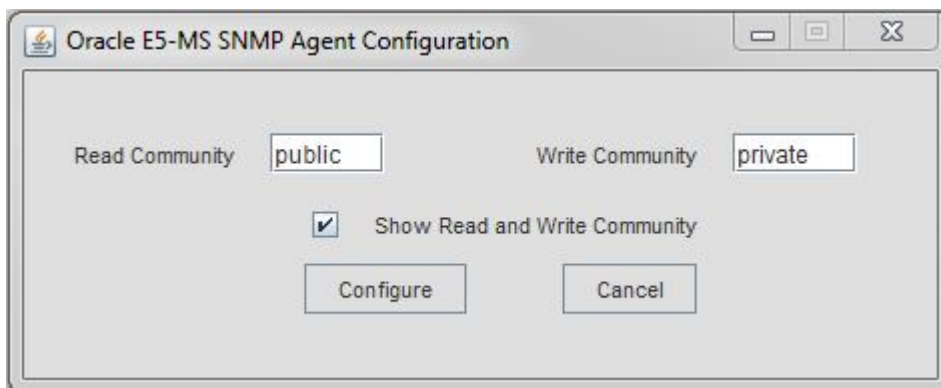


Figure 84: NBI Agent Configuration Plain Text

Functional Limitations

The functionality usage differences between the E5-MS and the existing EAGLE EMS is due to the underlying framework changes; however, all the function remains intact.

- A maximum of 10 Network Management Systems (NMS(s)) can be configured with NBI.

Note: If the clients tries to configure more than 10 NMSs, the error message `Limit for number of NMSs i.e. 10 is already reached!`

- The `QUEUESIZE` will accommodate twice the number of events expected to be queued in duration of 2 hours i.e., 2,000,000 event at an alarm rate of 180events/sec. Once a 2 million event threshold is met, there will be a loss of events.

Northbound Interface GUI

A Northbound Interface (NBI) GUI provides provision to configure an NMS along with matching/filtering patterns. These configurations are used by NBI module to send autonomous/resync events received at E5-MS to NMS. Autonomous/resync events are filtered using matching/filtering patterns before they are sent to NMS.

The E5-MS SNMP NBI GUI provides access to two collapsible panels, **Existing NMS(s)** and **NMS Configuration**. The user can collapse and expand each panel by clicking on its title bar.

The screenshot displays two panels from the E5-MS SNMP NBI GUI. The top panel, titled "Existing NMS(s)", contains a table with the following data:

NMS Label	Host Name/IP	Community	Port
Test1	10.25.24.50	public	162
Eagle2	10.25.24.51	public	162
Eagle3	10.25.26.6	public	162
Test2	10.26.13.135	public	162

The bottom panel, titled "NMS Configuration", contains the following fields and options:

- NMS Name*:** Text input field.
- Community*:** Text input field.
- IP*:** Radio button (selected).
- Host Name*:** Radio button.
- HeartBeat(sec)*:** Dropdown menu with value 60.
- Port*:** Text input field.
- Match/Filter Criteria:** A section with a checkbox and a table of criteria.

Criteria	Operation	Value
Resource:	Equal	
SubResource:	Equal	
Severity:	Equal	CRITICAL MAJOR MINOR WARNING INFO CLEAR
Acknowledge:	Equal	UNACKNOWLEDGE
UAM/UIM:	Equal	

At the bottom of the NMS Configuration panel are four buttons: Add, Modify, Delete, and Reset.

Figure 85: E5-MS SNMP NBI GUI

NMS Configuration Data

The NMS Configuration is located within the E5-MS SNMP NBI screen. The mandatory data fields are recognized with an asterisk(*) to Add a NMSs The following field must be filled:

1. NMS Name: A logical name for the NMS.
2. Hostname or IP: Depending upon the radio button selected a unique IP address or hostname of SNMP Manager to receive Traps.

3. Community: SNMP Community contained in Traps.
4. Port: Destination UDP port.
5. Heartbeat: Number of seconds between Heartbeat (i.e. system alive message) trap.

The Add button at the bottom of the screen is available once the screen is launched. The Modify, Delete and Reset buttons are shaded out until the user makes their selection from the Existing NMS(s).

NMS Configuration Element Rules

Element	Validation Rules
NMS Name* Field	<ul style="list-style-type: none"> • Only alphanumeric characters, hyphen and underscore are allowed. • It must have an alphabet as its first character. • Length is between 5 to 20 characters. <p>Invalid rules generate one of the following error messages:</p> <ul style="list-style-type: none"> • NMS name can contain only alphanumeric characters, hyphen and underscore! • NMS name can contain a minimum of 5 and a maximum of 20 characters. • NMS name must have an alphabet as its first character.
Community* Field	<ul style="list-style-type: none"> • String length cannot exceed 127 characters. • Blank string not allowed. <p>Invalid rules generate one of the following error messages:</p> <ul style="list-style-type: none"> • Community string is blank. • Community string length cannot exceed 127 characters.
IP*	<ul style="list-style-type: none"> • Blank is not allowed. • Valid IP address. <p>Invalid rules generate one of the following error messages:</p> <ul style="list-style-type: none"> • Invalid IP Address. Valid IP address format is '0-255.0-255.0-255.0-255'. • IP Address is blank!
Host name*	<ul style="list-style-type: none"> • Composed of series of labels concatenated with dots. For e.g. "en.wikipedia.org" • Each label must be between 1 and 63 characters long. • The entire hostname (including the delimiting dots) has a maximum of 255 characters. • Hostname labels may contain only the ASCII letters 'a' through 'z' (in a case-insensitive manner), the digits '0' through '9', and the hyphen ('-'). • No other symbols, punctuation characters, or white space are permitted.

Element	Validation Rules
	Invalid rules generate one of the following error message: <ul style="list-style-type: none"> • Invalid Host Name.
Heartbeat(sec)*	The ability to configure heartbeat (in seconds) is through heartbeat combo box (textbox cum drop-down) on NBI Configuration Interface. The user can either select a value from the drop-down or enter a value in the textbox. The heartbeat combo box will list the following entries- 60, 120, 300, 600, 900, 1800, 3600, 5400 and 7200. <ul style="list-style-type: none"> • Only numeric value between 5 and 7200 are allowed. • Blank is not allowed Invalid rules generate one of the following error message: <ul style="list-style-type: none"> • Heartbeat is blank. • Heartbeat can contain only numeric value between 5 and 7200.
Port	<ul style="list-style-type: none"> • Only numeric value between 0 and 65535 is allowed. • Blank is not allowed. Invalid rules generate one of the following error message: <ul style="list-style-type: none"> • Port number is blank. • Port number can contain only numeric value between 1025 and 65535. It can also be 162.

Match/Filter Criteria Data

Matching/Filtering Criteria is disabled by default. Checkbox is provided to either enable all criteria in one go or individually enable required criteria. Enabling **Matching/Filtering Criteria** set **Operation** to **Equal** by default.

The following are optional search **Criteria** of the alarms:

- **Resource:** Source of alarm.
- **Sub-resource:** Physical/logical component of source on which the alarm was actually raised.
- **Severity:** Criticality of alarm.
- **Acknowledge:** Alarm is acknowledged or not at E5-MS.
- **UAM/UIM:** UAM/UIM number of alarm received from EAGLE/EPAP/LSMS.

The **Operation** fields have the option of **Equal** or **Not Equal** values and use semicolons (;) to assistance in the filtering. The asterisk (*) can be use the **Resource** and **SubResource** criteria, such as *XXXX, XXX* and *XXX*.

Rules to send an autonomous/resync event to a NMS are as follows:

- Logical AND (&&) operation are performed to all criteria configured, matching (i.e. operation = Equal) and filtering (i.e. operation = Not Equal).
- Logical OR (|) operation are performed between multiple values configured per criteria

- Values other than ones specified in match criteria (i.e. Equal operation) shall automatically become filtering criteria and vice versa.

Match/Filter Criteria Element Rules

TIP: When you hover the mouse over the fields for a rule message will appear: Please enter values in format X or X-X, X-X;X-X and where X can be numeric. For wildcard search please use *.

Criteria	Operation	Value Rules
Resource	Equal or Not Equal	<ul style="list-style-type: none"> • Blank is not allowed • Multiple resources can be separated via (;) semicolon character • Special characters underscore (_), hyphen (-) and asterisk (*) are allowed. <p>Note: The asterisk (*) can be use for example *XXXX, XXX* and *XXX*.</p> <p>Invalid rules generate one of the following error message Resource criteria can contain (;) separated alphanumeric characters and special characters: (_), (-) and (*) (As a begin or last character or single *)"</p>
SubResource	Equal or Not Equal	<ul style="list-style-type: none"> • Blank is not allowed • Multiple resources can be separated via (;) semicolon character • Special characters underscore (_), hyphen (-) and asterisk (*) are allowed. <p>Note: The asterisk (*) can be use for example *XXXX, XXX* and *XXX*.</p> <p>Invalid rules generate one of the following error messages:</p> <ul style="list-style-type: none"> • Cannot add an empty string as Sub-resource in Match/Filter pattern. • NMS Sub Resource can contain (;) separated alphanumeric chars and special chars: (_), (-), (,), (/) and (*) (As a beginning and last character or single *)
Severity	Equal or Not Equal	<p>Severity levels:</p> <ul style="list-style-type: none"> • Critical • Major • Minor • Warning • Info • Clear <p>Note: User can select multiple severities at a time either matching or filtering criteria.</p>
Acknowledge	Equal or Not Equal	<p>Only applicable to resync events and not to autonomous events as Acknowledge/Unacknowledge is an E5-MS operation. Autonomous</p>

Criteria	Operation	Value Rules
		event trap forwarding are not impacted in case this criterion is configured.
UAM/UIM	Equal or Not Equal	<ul style="list-style-type: none"> • All UAM/UIM can be matched/filtered by specifying asterisk (*) • Multiple UAM/UIM can be specified semicolon separated as follows X;Y; A-B;Z • UAM/UIM range can be specified as A-B • Asterisk can't be clubbed with any other pattern • UAM/UIM cannot be blank • All UAM/UIM are in range 1-6917529027643179008 • 'From' value of UAM/UIM should be less than 'To' value in case UAM/UIM range is specified <p>Invalid rules generate one of the following error messages:</p> <ul style="list-style-type: none"> • UAM/UIM cannot be blank. • Any range of UIM/UAM can't be blank. • MAXIMUM NUMBER OF CHARACTERS is 200. • Invalid input, UAM/UIM should be in range 1-1500. • 'From' value of UAM/UIM should be less than 'To' value of UAM/UIM.

NBI Agent Configuration GUI

Figure 82: NBI Tree Node GUI is available to users with authorized access from the System Administrator, as shown in NBI Agent Configuration Tree node. As shown in *Figure 83: NBI Agent Configuration* is launched. The GUI is used to configure NBI agent read and write community strings. The read and write community text fields will blot out as soon as the user entered the strings.

Appendix

A

E5-MS System Administration

Topics:

- *Security Administration.....179*
- *Setting Up an E5-MS Workstation.....179*
- *Setting the Time Zone.....179*
- *Creating the E5-MS SSL Certificate.....180*
- *Security Administration Screen.....181*
- *Management of Usergroups and Users.....182*
- *User Management.....190*
- *Password Management.....193*
- *Login Restrictions Management.....196*
- *Password GUI.....197*
- *Account Recovery.....199*

This appendix describes the GUI and text-based user interface that performs E5-MS configuration and initialization.

Security Administration

The E5-MS customer is in charge of the system administration and the OS administration. Updates to the OS with the latest security patches will not impact the software behavior.

The customers will provide hardware and operating system, and have ownership of the root account or any privileged accounts (Group Users). Oracle requires a privileged account to perform installation, configuration, maintenance, support, and upgrades. It is recommended that the customer give privileges to Oracle personnel according to their needs/requirements but the customer will be the system administrator of the platform.

The default settings (including password) of the software components delivered by Oracle follow strong security rules (i.e complex passwords).

The E5-MS OEM components are configured to ensure the maximum security. For instance, if several levels of security are possible, the most secured parameters or options (for instance, logging levels, permissions granularity) are used.

Setting Up an E5-MS Workstation

The customer workstation serving as a client PC must meet certain criteria.

Screen Resolution

For optimum usability, the workstation must have a minimum resolution of 800x600 pixels and a minimum color depth of 16 thousand colors per pixel.

Compatible Browsers

The E5-MS can be viewed using either of the following web browsers provided by the customer:

- Microsoft® Internet Explorer version 8.0 or later
- Mozilla Firefox® version 16 or later.

Setting the Time Zone

If the time zone for E5-MS is not set properly, use the following procedure to set it. Use `system-config-date` to set the time zone.

1. Set the server to time zone X (for example, IST).

³ Microsoft is a registered trademark of the Microsoft Corporation.

⁴ Firefox is a registered trademark of the Mozilla Foundation.

2. Start the E5-MS server by using the `service e5msService start` command.
3. Launch the E5-MS client and perform resynchronization on a configured EAGLE.
4. Verify that the E5-MS timestamp on the Alarms GUI reflects time zone X.
5. Use the `system-config-date` command to change the server time zone to Y (for example, CDT).
6. Stop the E5-MS server by using the `service e5msService stop` command.
7. Start the E5-MS server by using the `service e5msService start` command.
8. Launch the E5-MS client.
Due to E5-MS server restart, resynchronization is automatically triggered for the added EAGLE(s).
9. Validate that the E5-MS timestamp on the Alarms GUI now reflects time zone Y.

Creating the E5-MS SSL Certificate

To create the SSL certificate needed for HTTPS-based access for E5-MS, execute the `E5MSCertificateCreationScript.sh` script present in the `/Tekelec/WebNMS/bin` directory. During execution of the script, provide the appropriate input (fitting the constraints) as shown in **bold** in the sample script execution below.

```
[root@e5ms8 bin]# cd /Tekelec/WebNMS/bin
[root@e5ms8 bin]# sh E5MSCertificateCreationScript.sh

Welcome to E5-MS SSL Certificate creation wizard!!!

Please provide E5-MS home path (Absolute path till 'WebNMS' directory e.g.
/Tekelec/WebNMS): /Tekelec/WebNMS

Please provide the country name (e.g. US)-
(Must not be empty, permitted characters - alphabets and space): US

Please provide the state name (e.g. North Carolina)-
(Must not be empty, permitted characters - alphabets and space): North Carolina

Please provide the organization name (e.g. Oracle)-
(Must not be empty, permitted characters - alphanumeric, underscore, dot and
space): Oracle

Please provide the organization unit name (e.g. E5MS)-
(Must not be empty, permitted characters - alphanumeric, underscore, dot and
space): E5MS

Please provide the keystore password -
(Must not be empty, length at least six, space not allowed, permitted characters-
alphanumeric, !, @ and #):<provide a password fitting the constraints>
Please provide E5MS root user's password (used for E5MS client login):<>

Trying to generate encrypted password for keystore and trust store...

Creating certificates for BE in localhost server.
Certificate stored in file </Tekelec/WebNMS/Certs/server.cer>
Certificate was added to keystore
The Certificates and key files were created in /Tekelec/WebNMS/Certs and copied
into the respective conf directories
Done.
```

```
Updating keystore and trust store password in transportProvider.conf file...  
Passwords successfully updated.
```

Note: The default E5-MS root user password used for client login is 'public'. So, for a fresh installation, that password should be supplied when asked in the script. For an upgrade scenario where the root user password has been changed by the customer, the updated password should be supplied when asked in the script.

Security Administration Screen

The E5-MS security module is centered on providing excessive security to E5-MS. Security management provides the administrator with the ability to configure and set various rules and constraints related to user passwords, user session validity, and user account validity. Some constraints are the same for all users and some are configured separately for each user.

Once the System Administrator is logged into the E5-MS, they can access the Security Administration application by selecting the **Security Administration** option under the **Tools** menu on the E5-MS client menu bar (or pressing **ALT+S** on the E5-MS client window), as shown in [Figure 86: System Administration Tree Node](#).



Figure 86: System Administration Tree Node

The Security Administration GUI will display, as shown in [Figure 87: Security Administration Screen](#).

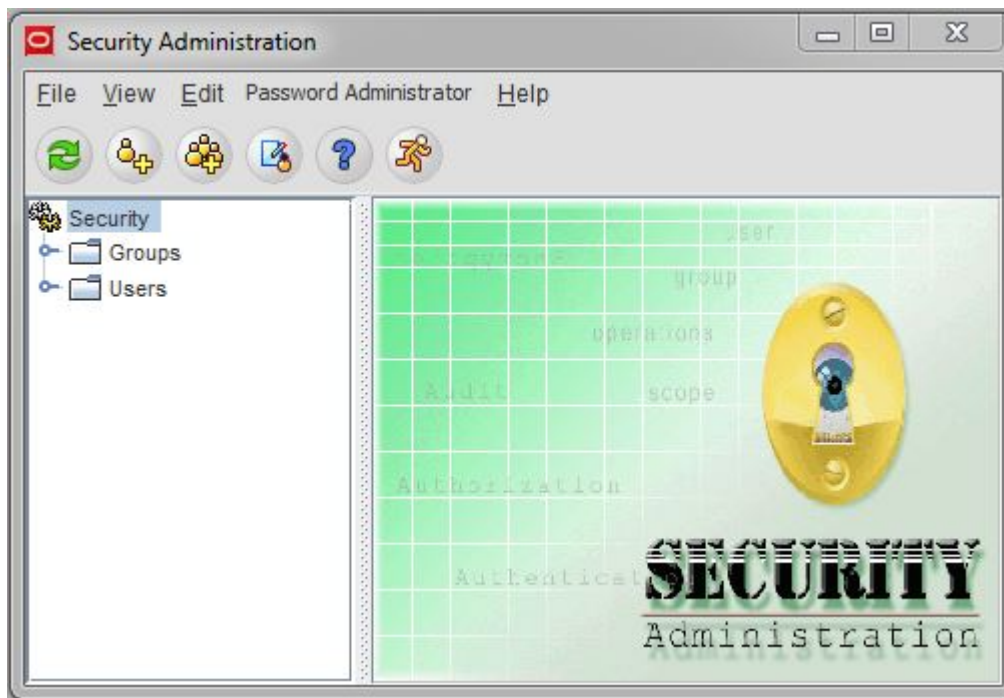


Figure 87: Security Administration Screen

This page is accessed by the System Administrator to set Usergroup and User access permissions.

Management of Usergroups and Users

The Security Administration GUI provides the System Administrator with the ability to manage E5-MS security. The E5-MS administrator creates new usergroups or new users to control different security levels of the E5-MS, by associating operations to usergroups. Once the user has logged in to the E5-MS client, all the operations available to the user are based on the usergroup to which the user belongs. The E5-MS administrator can configure various rules and constraints required to support password management in the E5-MS through the Security Administration GUI. The following sections provide detailed descriptions of the E5-MS security GUI and the procedures to create, modify, and delete usergroups and users.

The System Administrator can see all the existing Usergroups and Users after the **Security Administration** screen is open.

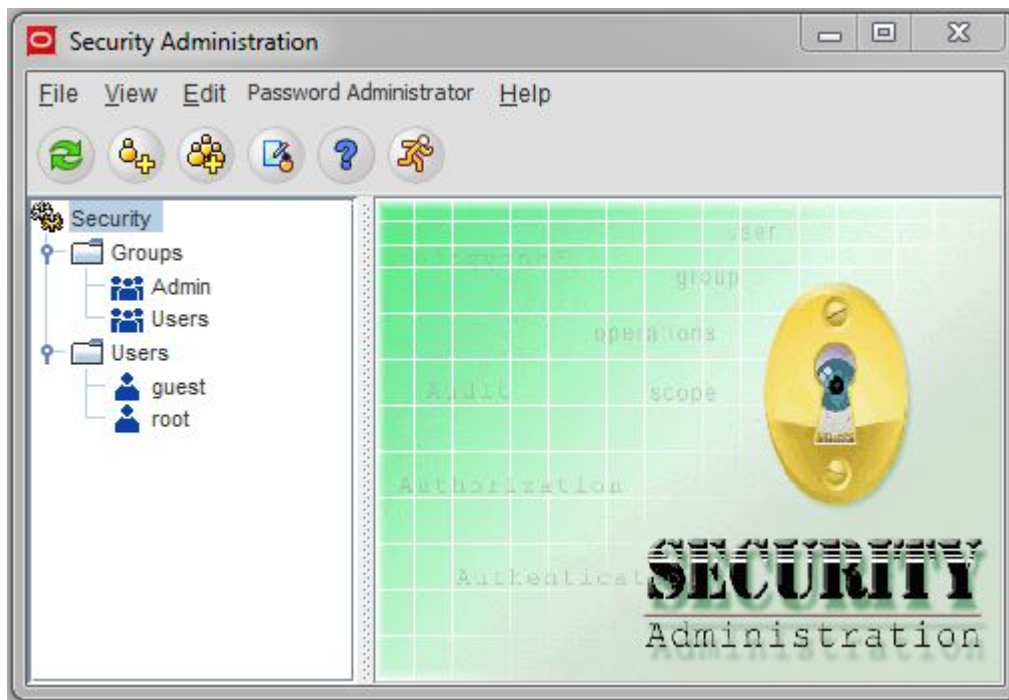


Figure 88: Security Administration Screen with Groups and Users

The System Administrator is responsible for adding and removing usergroups to and from the E5-MS. A usergroup **Admin** will always exist in the E5-MS, and all the operations are assigned by default. The **Admin** usergroup cannot be removed or deleted, and the assigned operations are not allowed to be modified. Attempting to delete the **Admin** usergroup will result in the following error message:


Usergroup Admin cannot be deleted!

Usergroup Management

This section includes the following procedures:

- *Create a Usergroup*
- *View a Usergroup*
- *Modify a Usergroup*
- *Delete a Usergroup*


Create New Usergroup

The **AddGroup** option is accessed by clicking on the icon symbol  or right clicking the usergroup tree on the left side of the Security Administration screen.

Create a Usergroup

Only the E5-MS System Administrators can create Usergroups.

This procedure describes how a System Administrator adds a Usergroup.

1. Click the icon symbol **Addgroup**  or right click the usergroup tree on the left side of the **Security Administration** screen.

A page similar to [Figure 89: Groups Wizard screen](#) appears.



Figure 89: Groups Wizard screen

2. Enter the name of the new Usergroup to be created in the **Enter the group name (*)** field.
The new Usergroup name must be unique within the E5-MS. Existing Usergroup names are listed in the left pane under **Groups**. The new Usergroup name must meet the following constraints:
 - The name must have at least 3 characters.
 - Only alphanumeric characters (0-9, a-z, A-Z) and spaces are allowed.**Note:** Before clicking Next, read the guidelines outlined on the Groups Wizard screen.
3. Click the **Next** button. A page similar to [Figure 90: Usergroup Attributes](#) is displayed.

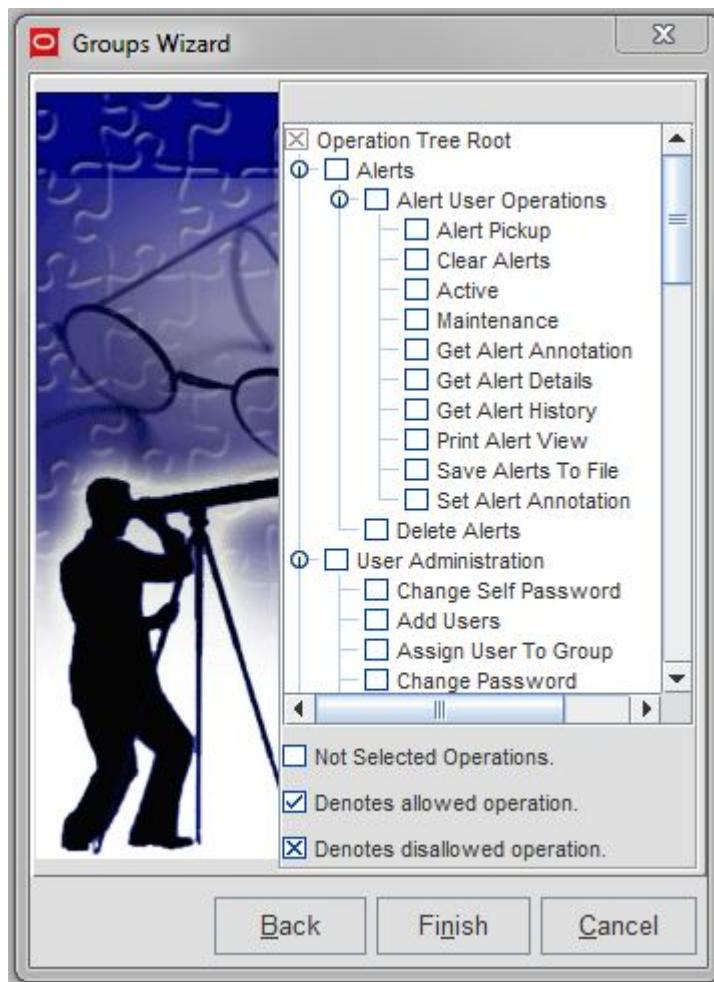


Figure 90: Usergroup Attributes

Assign Users to a Usergroup

This procedure describes how a System Administrator assigns Users to a **Usergroup**. To perform this procedure, the System Administrator clicks the **Setting Users** button available under the **Members** tab.

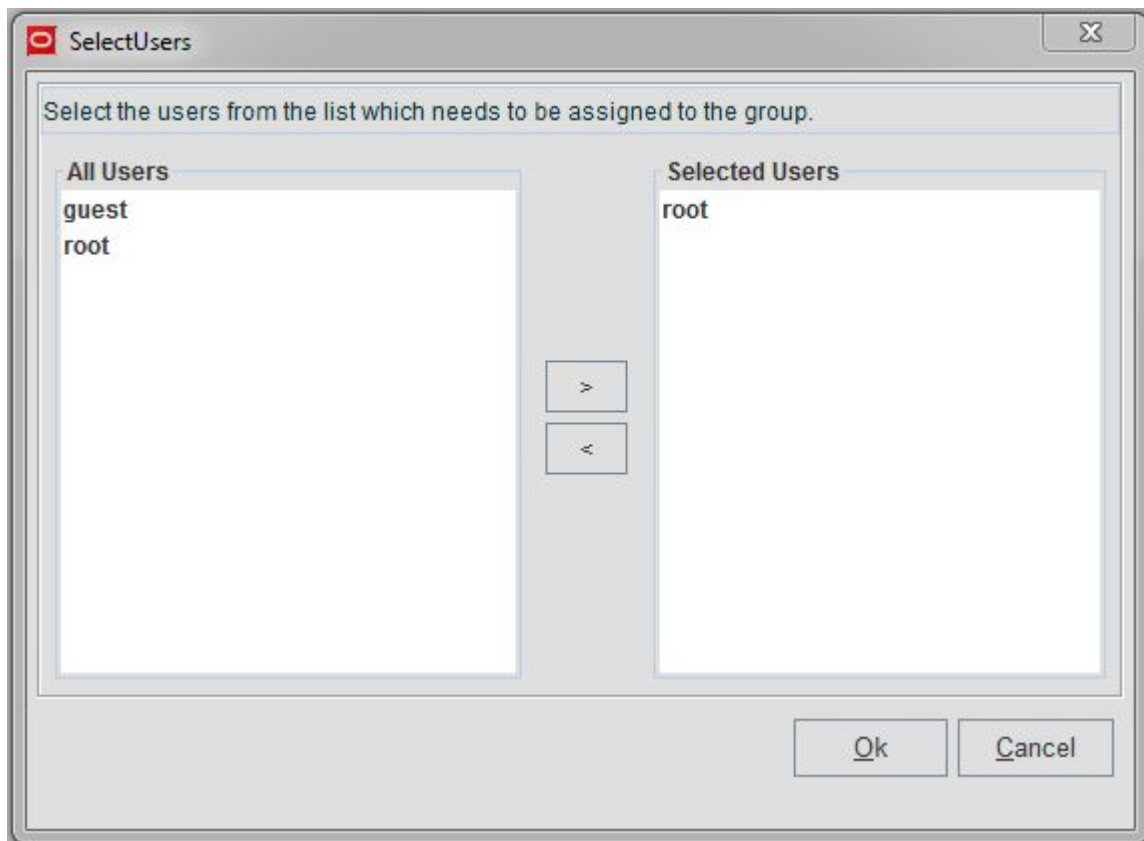


Figure 91: Select Users

As shown in [Figure 91: Select Users](#), all users are listed on the left side of the screen. The users assigned to the usergroup are listed on the right side of the screen. There are arrows in the middle to move users to the right or the left panes.

1. Select the user(s) from the list to the left.
2. Click the arrow pointing right to add the user(s) to the Selected Users pane.

Assign Attributes to a Usergroup

This procedure describes how a System Administrator assigns attributes to a usergroup, as shown in [Figure 92: Permitted Operations for Group](#).

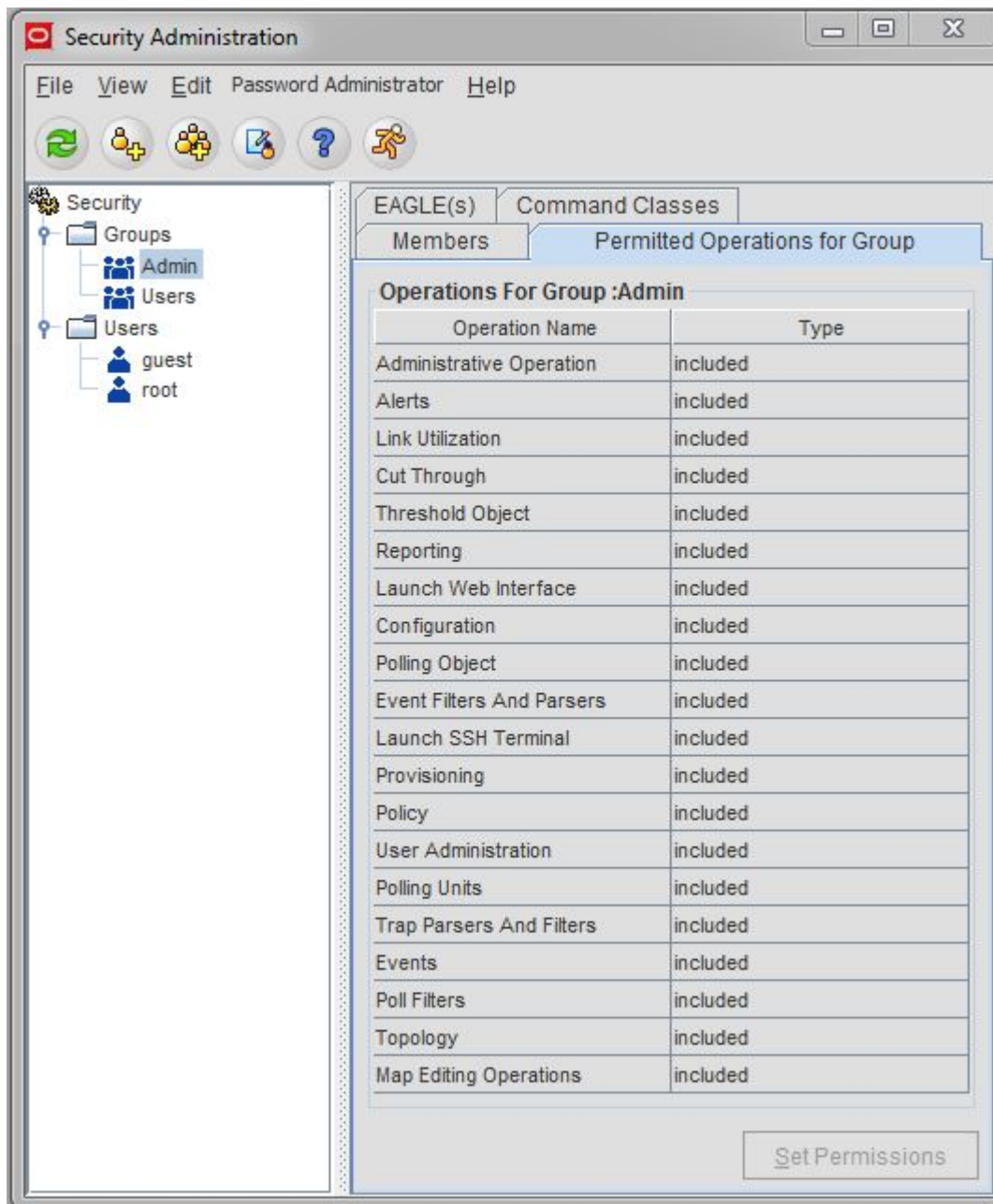


Figure 92: Permitted Operations for Group

All E5-MS operations are listed under Operation Name. The operations assigned to the usergroup are listed as included and those discarded are excluded. The **Set Permissions** button at the bottom of the screen will allow the System Administrator to assign or remove from the existing assignments.

1. Click the **Set Permissions** button to open the **Assign Permissions** screen shown in [Figure 93: Assign Permissions Screen](#).

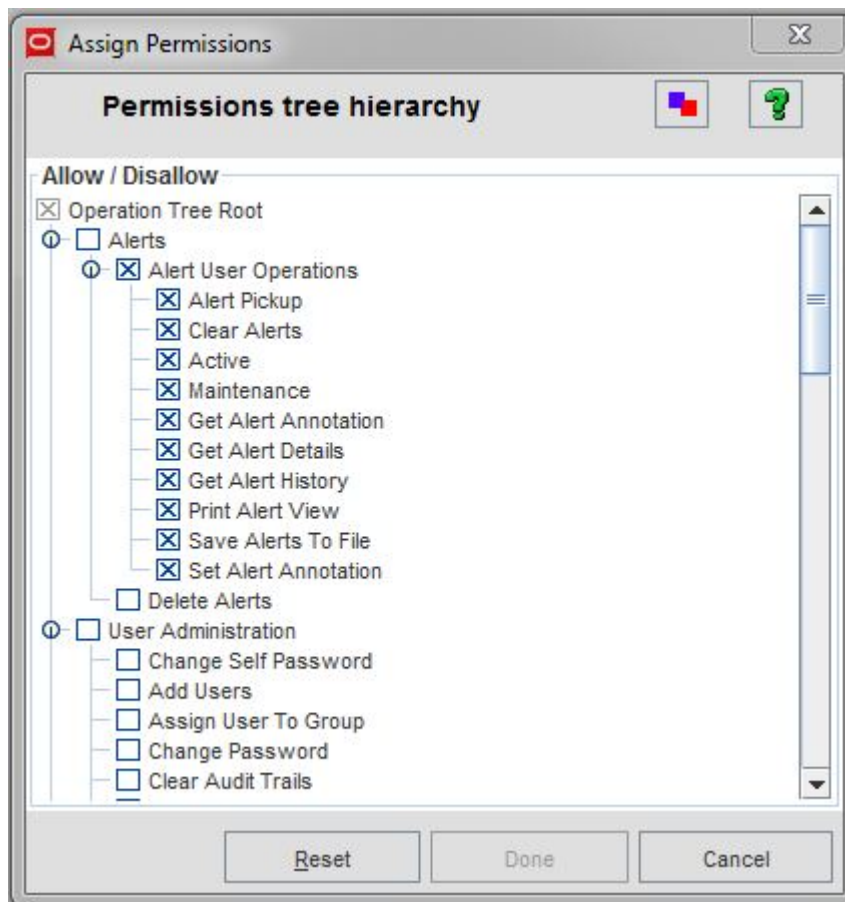


Figure 93: Assign Permissions Screen

The Permissions tree hierarchy is logically arranged in a tree structure with parent and child operations under the Operation Tree Root. There are operations within the tree that are parent/child nodes, parent/child/child nodes, and operations without child nodes.

2. Check the box next to the operations assigned to this new usergroup from the **Operation Tree Root**.
 - a) If parent nodes are assigned to a usergroup and its child node assignment is left blank, then that child node is assigned (even if the child node is left blank)
 - b) If a parent node is assigned/not assigned (left blank), then its child nodes can be assigned or discarded.
 - c) If a parent node is discarded, then by default all its child nodes are discarded.
 - d) If an operation is not assigned to a usergroup, it will be shaded out within the E5-MS GUI. This will prevent the user from accessing the operation.

Assign EAGLE(s) to a Usergroup

This procedure describes how a System Administrator assigns EAGLEs to a usergroup, as shown in [Figure 94: Select EAGLE\(s\)](#).

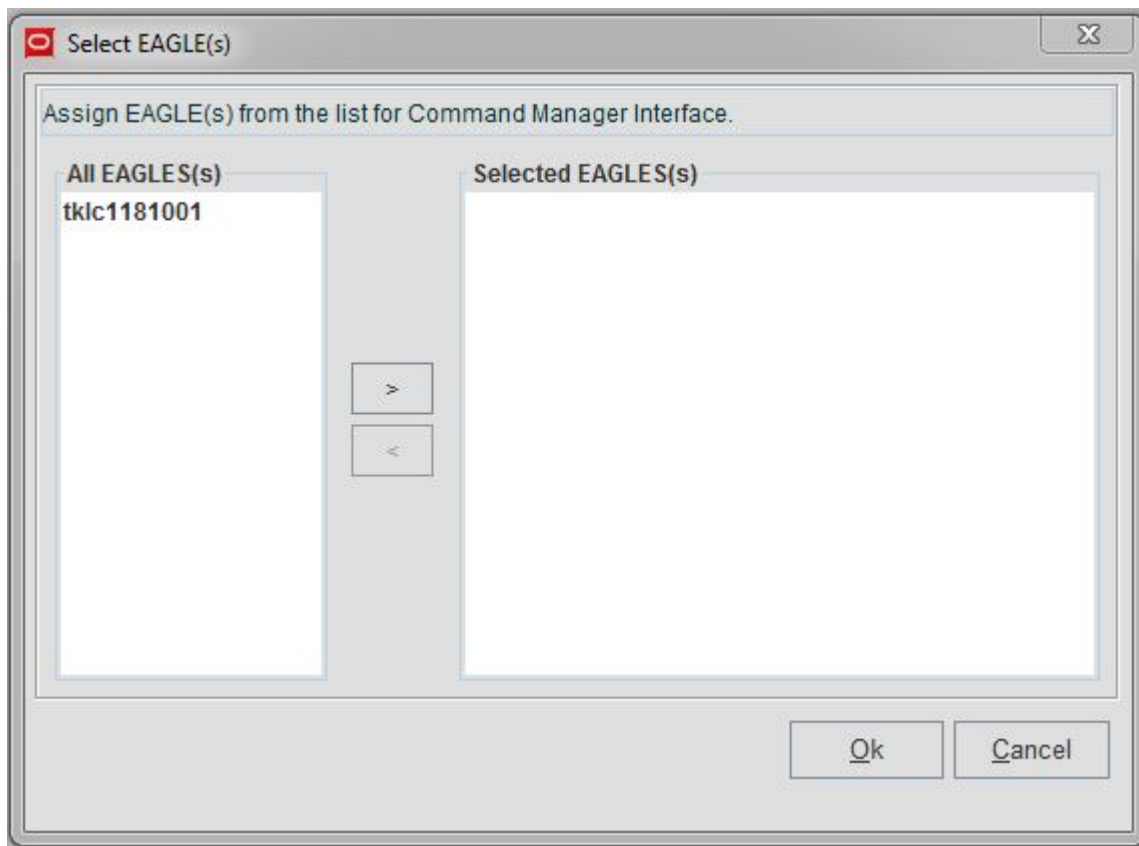


Figure 94: Select EAGLE(s)

All EAGLEs within the client's network are listed on the left side of the screen. The EAGLEs assigned to the usergroup are listed on the right side of the screen. There are arrows in the middle to move an EAGLE to the right or the left panes.

1. Select the EAGLE(s) from the list to the left.
2. Click the arrow pointing right to add the EAGLE(s) to the Selected EAGLE(s) pane.

Assign Command Classes to a Usergroup

This procedure describes how a System Administrator assigns Command Classes to a usergroup, as shown in [Figure 95: Select Command Classes](#).

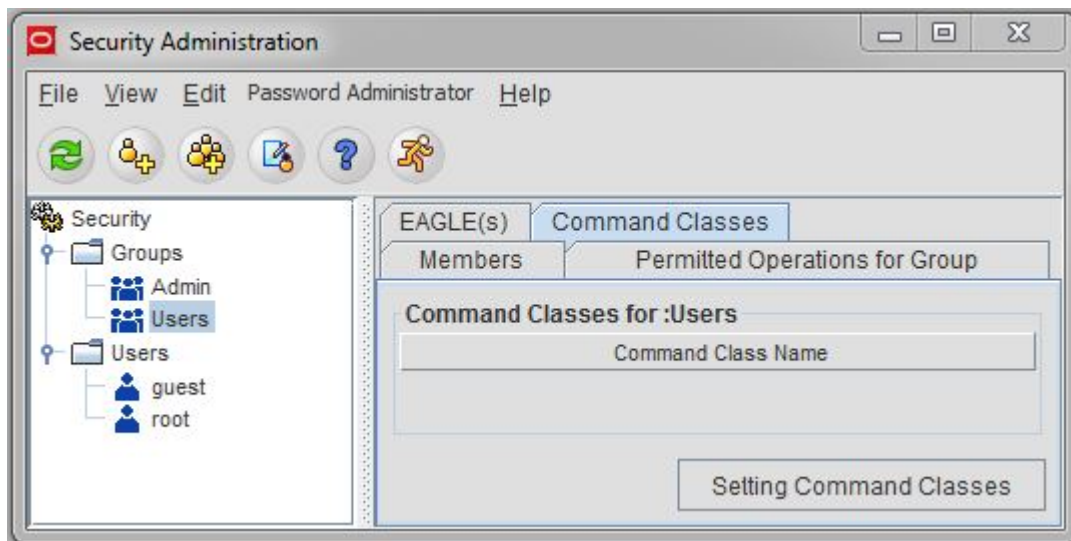


Figure 95: Select Command Classes

All Command Classes are listed on the left side of the screen. The Command Classes assigned to the usergroup are listed on the right side of the screen. There are arrows in the middle to move Command Classes to the right or the left panes.

1. Select the Command Classes from the list to the left.
2. Click the arrow pointing right to add the Command Classes to the Selected Command Classes pane.

The EAGLE(s) and Command Class cannot be modified by the assigned usergroup with access to the **Link Utilization** module.

If the E5-MS administrator tries to remove an EAGLE from a usergroup which has the **Link Utilization** module assigned, the operation is not allowed and the following error message is displayed:

```
All EAGLE(s) are mandatory with Link Utilization operation.
```

If the E5-MS administrator tries to remove either of the command classes DATABASE or SYSTEM MAINT from a usergroup assigned the Link Utilization operation, the operation is not allowed and the following error message is displayed:

```
Command classes DATABASE and SYSTEM MAINT are mandatory with Link Utilization operation.
```

User Management

An E5-MS user has access to the E5-MS only if the user is associated with an E5-MS usergroup. When the user belongs to the E5-MS Administrator usergroup, they can perform all the E5-MS operations. If the user does not belong to the E5-MS Administrator usergroup, they can perform only the operations associated with the user's usergroup. A user has access to the **Security Administration** GUI if the

Security Administration operation is assigned to the user. A user has access to user operations in the **Security Administration** window if the **User Administration** operation is assigned to the user.

This section describes the following procedures:

- *Create a new User*
- *Modify a User Profile*
- *Assign Permissions for a User*

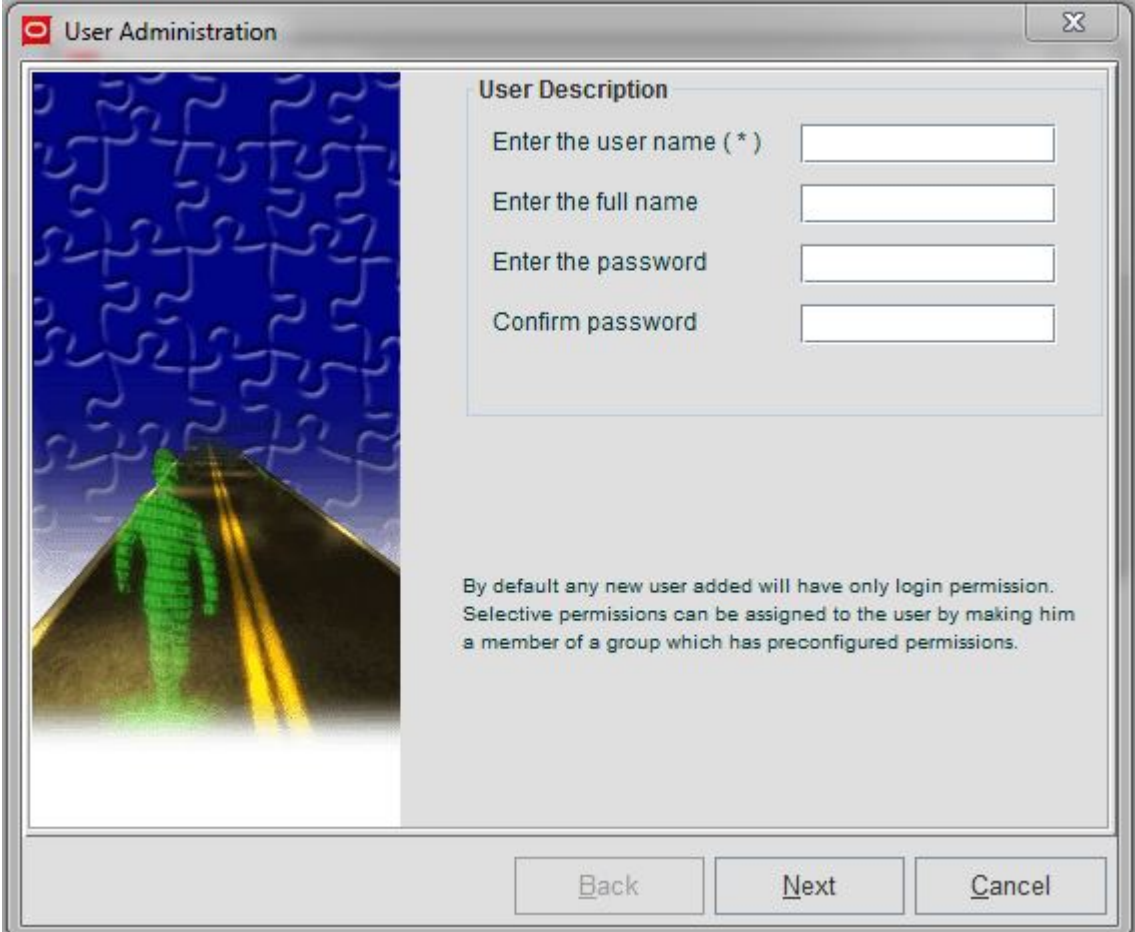
Add a User

Only E5-MS System Administrators can add new users.

This procedure describes how a System Administrator adds a user.

1. Click the **Addusers** icon (👤+) or right click the usergroup tree on the left side of the **Security Administration** screen.

A page similar to the one shown in [Figure 96: User Administration Screen](#) is displayed.



User Administration

User Description

Enter the user name (*)

Enter the full name

Enter the password

Confirm password

By default any new user added will have only login permission.
Selective permissions can be assigned to the user by making him
a member of a group which has preconfigured permissions.

Figure 96: User Administration Screen

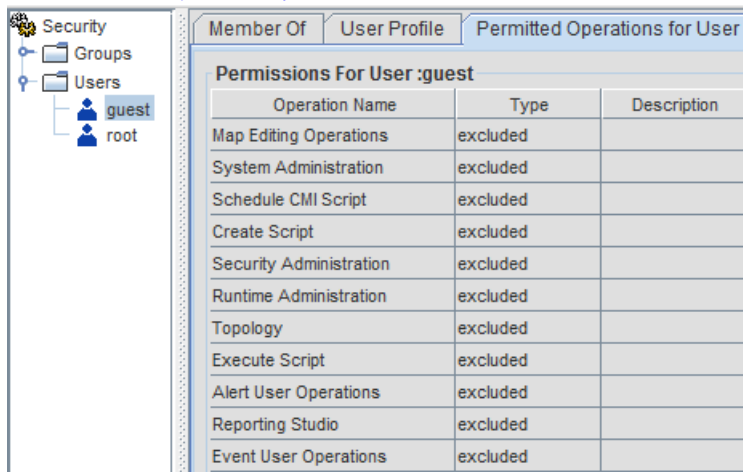
2. Enter the name in the **Enter the user name (*)** field.

This is the **UserID** the user will use to log in to the E5-MS. The user name must be unique within the E5-MS. The new user name must meet the following constraints:

- The name must have at least 3 characters.
 - Only alphanumeric characters (0-9, a-z, A-Z) and spaces are allowed.
3. Enter the name of the user in the **Enter the full name** field.
 4. Create a password for the new user. All the password constraints configured by the administrator are applicable to the password being set for a new user. Only a password satisfying all the constraints is accepted, and others are rejected with an error message displayed in the GUI. User accounts and passwords do not expire by default.

Assign Attributes to a User

This procedure describes how a System Administrator assigns attributes to a user, as shown in [Figure 97: Permitted Operations for User](#).



Operation Name	Type	Description
Map Editing Operations	excluded	
System Administration	excluded	
Schedule CMI Script	excluded	
Create Script	excluded	
Security Administration	excluded	
Runtime Administration	excluded	
Topology	excluded	
Execute Script	excluded	
Alert User Operations	excluded	
Reporting Studio	excluded	
Event User Operations	excluded	

Figure 97: Permitted Operations for User

All E5-MS operations are listed under Operation Name. The operations assigned to the user are listed as included and the operations discarded are excluded. Operation assignment to a user cannot be modified, since the operations of a user are set under usergroup operations.

Modify User Profile

This procedure describes how a System Administrator modifies a user profile.

The screenshot displays the 'User Profile' tab for the 'guest' user. The left-hand navigation pane shows a tree structure under 'Security' with 'Groups' (Admin, Users) and 'Users' (guest, root). The main content area has three tabs: 'Member Of', 'User Profile', and 'Permitted Operations for User'. The 'User Profile' tab is active, showing the following fields:

- Full Name of the User :guest**: A text input field containing 'guest'.
- Status for the User :guest**: A dropdown menu currently set to 'enabled'.
- Account expiry for :guest**: A field labeled 'This user account expires in' with a numeric input set to '0' and the unit 'Day(s)'.
- Password expiry for :guest**: A field labeled 'The password expires in' with a numeric input set to '0' and the unit 'Days(s)'.

Below these fields, there is instructional text: 'Please enter the number of days in which the user and/or the password expires... The values should be in the range of 0 to 999. A value zero indicates no expiry. Value if entered below or beyond the range will take the boundary value in range.' A 'Setting Profile' button is located at the bottom right of the form.

Figure 98: Modify User Profile

The System Administrator accesses the user profile from the **User Profile** tab. Fields under user profile are made active by selecting the **Setting Profile** option. User status is set to either **enable** or **disable**, and is enabled by default. If the user status is changed to **disable**, that user exists in the database but cannot log in to E5-MS. By default, a user account and password never expire.

Password Management

E5-MS security is centered on providing excessive security to E5-MS. The E5-MS security management application provides a System Administrator with the ability to configure and enforce various rules and constraints related to user password composition, user session validity, and user account validity. Some constraints are the same for all users while some are configurable separately for each user.

Password Encryption

To maintain a secured channel in network communication and to secure the storage of sensitive information like passwords, it is necessary to adopt a mechanism to withstand security attacks. E5-MS supports a cryptogram mechanism to ensure secured data communication. This is achieved with the help of RSA Data Security Algorithm for cryptography. RSA is a two-way encryption technique in

which the original message (plain text) is encrypted with a public key at the sender end. The encrypted plain text (cipher text) is received and decrypted with a private key at the receiver end. Only the receiver knows the private key and thus a foolproof communication mechanism is ensured.

Password Composition Management

To increase password security, user password composition is made complex. User passwords that follow all the password constraints as configured by the administrator are accepted, and otherwise a corresponding error message is displayed to the user. The following rules are applied to new passwords entered by the users:

1. Password should have the required minimum length (as configured by E5-MS Administrator).
2. Password length should be between 8 to 16 characters.
3. Password should contain required minimum number of alpha, numeric, and special characters (as configured by E5-MS Administrator).
4. Password should not contain associated username.

The E5-MS Administrator uses the GUI interface to configure the minimum required password length and the minimum number of alpha (A-Z, a-z), numeric (0-9), and special characters that should be present in a user password. These four attributes are stored in the database, with the default values as (8, 0, 0, 0) until the administrator modifies them. A user can change their password according to these attributes.

Password Constraint Configuration

An administrative operation named **Password Administration** is available on the **Security Administration** window of the E5-MS client. This operation is visible only if the user has permission to **Security Administration**. Clicking on the **Password Configuration** menu item under **Password Administration** launches the **Password Configuration** window. An E5-MS Administrator configures password composition and other password related constraints through this window.

Password Constraint Imposition

The user password is validated when a user/administrator changes the password. The following validation occurs for the new password:

1. Password should have the required minimum length (as configured by E5-MS Administrator).
2. Password length should be between 8 to 16 characters.
3. Password should contain required minimum number of alpha, numeric, and special characters (as configured by E5-MS Administrator).
4. Password should not contain associated username.
5. Password should not match any of the 'n' previously used passwords, where 'n' is the value configured by the EAGLE administrator.
6. Password should be modified only once within the minimum change interval configured for user password by the EAGLE administrator.

Password Change Management

To manage password changes, E5-MS manages two time period values, the Password Expiry period (separately for each E5-MS user) and the Notification period (for all users).

The Password Expiry period is the time after which a user password expires. Once a user password is set/reset, the Password Expiry period is decremented until the value of the password expiry period becomes zero. The notification period is the number of days prior to expiration of the password expiry period, from when the E5-MS starts notifying the user about the password expiration. Upon expiration of the password expiry period, the user's status is updated in the database to indicate the password

has expired. If a user with an expired password attempts to log in to E5-MS, the user is forced to reset their password. Once the user password is reset successfully, the user is allowed to log in with the new password.

To manage a user account, the E5-MS Administrator configures an Account Expiry period (separately for each E5-MS user). The Account Expiry period is the time after which a user account expires. Once a user account is created, the account expiry period of a user is decremented and updated in database. Once the value of the account expiry period becomes zero, the user's account status is updated in the database to show the account has expired, and the user cannot log in to E5-MS.

The E5-MS Administrator can set values for the account expiry and password expiry periods on a per user basis when a user profile is created. An administrator can also modify these values on a per user basis by editing a user's profile. The enforcement of account expiry or password expiry rules can be disabled by selecting the "never expires" option corresponding to the rule(s) when a user profile is created/modified. The value of the account expiry and password expiry periods are in the range 0 - 999. A value of 0 is equivalent to the "never expires" option, which disables the enforcement of the rule(s) on the user.






The Notification period value is configurable within the range 0 - 30 days by the E5-MS administrator. The same value is applicable to all users. If the remaining password expiry period for a user's password is less than or equal to the notification period, then warning messages are displayed after the user successfully logs in, indicating the number of days left before password expiration. Disabling the password expiry period for a user disables the enforcement of the notification period, and display of notification messages at login to E5-MS to that user. By default, this rule is disabled.

The E5-MS Administrator can restrict the number of previously used passwords for a user that cannot be reused as new passwords. The number of previously used passwords that cannot be reused are stored in a database and the value is modifiable by the E5-MS Administrator through a GUI interface. The E5-MS Administrator can disable the enforcement of this rule on all the E5-MS users by setting the value to zero (0) through the GUI Interface. By default this rule is disabled and value of number of previously used passwords that cannot be used again shall be zero (0). Up to 12 recently used passwords for every user are stored in the database. The passwords are stored as comma separated encrypted strings with the latest password at the end. When the number of passwords for a user stored in the database is 12 and a new password is to be stored in the database, then the oldest password is removed and the latest password is appended at the end. When a user password is modified, the encrypted password string is compared with the previously encrypted user password strings for that user stored in the database. If the new string matches any of the stored strings, the new password is rejected and an error message indicating the same is displayed on the GUI.

The E5-MS Administrator can configure a minimum password change interval for E5-MS users. An E5-MS user is allowed to change their password only once within this interval. If a user attempts to modify their password more than once within the configured time frame, a corresponding error message is displayed on the GUI Interface. A user can contact the E5-MS Administrator if it is required to change their password more than once during this period. The range of this interval is from 0 to 30 days, with the default being 0 days. The same value is applicable to all users.

User Status Icons

E5-MS provides the Administrator status icon of the user in the User Tree in security Administration window.

Icon	Description
	User account is enabled.
	User is disabled and cannot log in until he/she is re-enabled.
	User account has expired.
	User password has expired.
	User login is denied due to continuous unsuccessful login attempts.

Login Restrictions Management

This section presents procedures available for E5-MS System Administrator responsible for all the Usergroups and User access levels. The System Administrator will have access to all management operations.

When an E5-MS user logs in to E5-MS for the first time after the user has been created by the administrator, the E5-MS user is required to change their password to continue their login to E5-MS. Once their password has been successfully modified, the user can then continue their login to E5-MS.

An E5-MS Administrator can configure the maximum permissible number of wrong login attempts that can be made by an E5-MS user through a configuration file. Every time a user makes a wrong login attempt, the count of wrong login attempts for that user increments by one. If the number of wrong login attempts is within the permissible limit, when the user is able to successfully log in to E5-MS the count of wrong login attempts resets to 0. If the count of wrong login attempts made by a user equals the maximum permissible limit, the user account is locked and a corresponding message is displayed to the user. A user whose account is locked is not allowed to log in to E5-MS, and an attempt to do so results in an error message on the GUI. An E5-MS Administrator can disable the enforcement of this rule for all E5-MS users by setting the value of the number of wrong login attempts allowed to zero (0) in the configuration file. By default, the number of allowed wrong attempts is set to 5 in the configuration file.

An E5-MS Administrator can configure a lockout time (in minutes) through a configuration file, after which a user account is locked for being idle for this period. By default, this period is set to 30 minutes. The same value is applicable to all users. A 'Lock Screen' window is displayed where the locked user can enter their password to log in again to E5-MS. Once logged-in, the user can continue their E5-MS session.

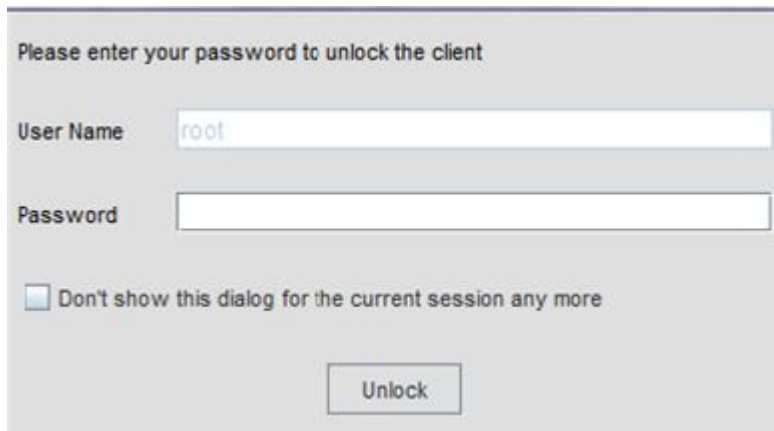
A screenshot of a lock screen dialog box. The title bar is not visible. The main text reads "Please enter your password to unlock the client". Below this, there are two input fields: "User Name" with the text "root" and "Password" which is empty. At the bottom left, there is a checkbox labeled "Don't show this dialog for the current session any more" which is currently unchecked. At the bottom center, there is a button labeled "Unlock".

Figure 99: Lock Screen

An E5-MS Administrator can configure the maximum permissible inactivity period (in minutes) through a configuration file, after which a user is terminated for being idle. By default, this period is set to 60 minutes. The same value is applicable to all users. The idle user's client session is terminated after this period, and a corresponding message is displayed to the user. The user is required to restart the client to start a new E5-MS session. The lockout time is less than the termination time, but if the administrator configures a termination time less than the lockout time, then the lockout functionality will not be in effect, and only the termination time is used.

An E5-MS Administrator can disable the login rights of another E5-MS user (except E5-MS Administrators) through the GUI interface. An E5-MS Administrator can disable a user while modifying the user's profile through the Security administrator window. When a user is disabled by an E5-MS Administrator, the status of that user is updated as disabled. The user information (usergroup and operation mappings) continues to exist in the database for the disabled user. A disabled user is not allowed to log in to E5-MS because the login rights of that user are disabled. An attempt to do so results in an error message on the GUI. When an E5-MS Administrator disables a user who is already logged in, the user is logged out of E5-MS and prompted with a corresponding message. Also, an E5-MS Administrator is not able to disable their own login rights.

Password GUI

Clicking 'Password Administration' on the Security Administration GUI opens up the 'Password Configuration' GUI on the E5-MS client. The Password Configuration GUI has two sections, 'Password Composition' and 'Password Restrictions'. A 'Disable All' check-box is also present on the GUI. All drop-downs on the GUI display the values that are present in the database for the respective fields.

The screenshot shows a 'Password Configuration' dialog box with a blue title bar and a close button. At the top, there is a checked checkbox labeled 'Disable All'. Below this, the 'Password Composition' section is enclosed in a rounded rectangle. It contains four rows, each with a checked checkbox and a label followed by a numeric input field with a dropdown arrow: 'Minimum length : 8', 'Minimum alpha characters : 0', 'Minimum numeric characters : 0', and 'Minimum special characters : 0'. A note below reads 'Note: Maximum allowed password length is 16.' The 'Password Restrictions' section follows, also in a rounded rectangle, with three rows: 'Number of old passwords that cannot be reused : 0', 'Minimum change interval for password : 0', and 'Password expiry notification period : 0'. A final note states 'Note: Selecting value '0' for a field is similar to disabling that field.' and a 'Submit' button is located at the bottom right.

Figure 100: Password Composition

This screenshot shows the same 'Password Configuration' dialog box, but with different values in the 'Password Restrictions' section. The 'Disable All' checkbox remains checked. In the 'Password Composition' section, the values are: 'Minimum length : 8', 'Minimum alpha characters : 1', 'Minimum numeric charecters : 2', and 'Minimum special charecters : 3'. The note below remains 'NOTE: Maximum allowed password length is 16.' In the 'Password Restrictions' section, the values are: 'Number of old password that cannot be reused : 5', 'Minimum change interval for user password : 5', and 'Expiry notification period : 7'. The 'Submit' button is still present at the bottom right.

Figure 101: Password Restrictions

Password Composition Section

In the 'Password Composition' section, an E5-MS Administrator can configure four constraints: 'Minimum Length', 'Minimum Alpha Characters', 'Minimum Numeric Characters', and 'Minimum Special Characters'.

Password Restrictions Section

In the 'Password Restrictions' section, an E5-MS Administrator can configure three restrictions: 'Number of Old Passwords that cannot be reused', 'Minimum Change Interval for user password', and 'Expiry Notification period'. The values configured for the three restrictions are applicable to all E5-MS users.

Disable Functionality

Functionality to disable all/some fields is provided on the 'Password Configuration' GUI, which disables enforcement of rules corresponding to the disabled fields for all E5-MS users, except for the minimum (8 characters) and maximum (16 characters) password constraints. Check boxes are provided corresponding to all the fields.

By default, all the constraints are disabled and the corresponding check boxes are checked and enabled. Selecting a check box disables the corresponding drop-down of the field. Multiple check boxes can be selected to disable multiple fields. No value corresponding to the disabled fields are updated in the database, when the page is submitted using 'Submit' button.

Drop-downs corresponding to the fields that have been disabled by an E5-MS Administrator or by default appear as disabled with the corresponding check boxes as selected. Selecting the 'Disable All' check box disables all the other check boxes present on the page, along with the corresponding drop-downs.

Password Configuration Data Submit

The 'Password Configuration' GUI contains a 'Submit' button at the bottom of the page. When clicking the 'Submit' button, the data selected in the drop-downs (except values in the disabled fields) is submitted and a message *"Password configuration data successfully updated by user: <username>."* is displayed on the GUI, indicating that the data has been updated in the database successfully.

The configuration data is not submitted in the following scenarios and a corresponding error message is displayed on the GUI:

1. When the total count of minimum required alpha, numeric, and special characters exceeds the minimum allowed password length as configured by an E5-MS Administrator.
2. When the minimum length constraint is disabled by an E5-MS Administrator and the total count of minimum required alpha, numeric, and special characters exceeds the maximum allowed password length (16).

Account Recovery

The E5-MS administrator can enable login rights of a user when their account is locked because of exceeding the permissible number of incorrect login attempts, when login rights have been disabled by the E5-MS administrator, or when the password has expired. An E5-MS administrator enables the login rights of such users by setting the user's status to 'enable' in the 'User Profile' window of the corresponding users. If no E5-MS administrator is able to log in to E5-MS because of password expiration or account locking, a password recovery mechanism is provided by Oracle Support to recover the E5-MS Administrator 'root' account.

E5-MS Administrator Password Recovery Mechanism

When the E5-MS administrator is not able to log in to E5-MS, the customer can request password recovery from Oracle Support. This topic describes the mechanism to recover the E5-MS administrator 'root' password.

1. E5-MS Administrator 'root' is in locked state or customer decides that they need 'root' password recovered.
2. Oracle Support representative either accesses the E5-MS remotely (if allowed by the customer) or travels to the customer site.
3. Once the Oracle Support representative has access to the E5-MS as described in step 2, the following sub-steps are performed (by the Oracle Support representative):
 - a. JRE_HOME
 - b. E5MS_HOME
4. Once the above specified parameters have been customized as per customer environment, the support representative shall execute the script providing the new password for 'root' administrator, when prompted for. This script resets 'root' administrator's password and, therefore the 'root' administrator can log in to E5-MS with the new password.

Note: Password configured via script shall not follow any password constraints.

5. On successful execution of script, start E5-MS server and log in to 'root' with new password.
6. Change the 'root' administrator's password after successful login to E5-MS.
7. Exit server login.
8. The Oracle Support representative provides the newly-created password of 'root' to the customer, and instructs them to log in to the E5-MS with 'root' user using that password and to change the 'root' administrator's password after successful login to E5-MS.
9. The customer shall immediately be required to change the password for the 'root' user account.
10. The customer is advised to reset the other (pre-existing) E5-MS user passwords while logged in as new 'root' Administrator.

Appendix B

E5-MS Backup and Restore

Topics:

- *Overview.....202*
- *System Requirement.....202*
- *Backup in E5-MS.....202*
- *Restore in E5-MS.....210*
- *File and their Locations.....211*

This appendix describes the configuration and execution of backup and restore for the E5-MS.

Overview

E5-MS is used to manage and monitor EAGLE, EPAP, and LSMS nodes in the network. E5-MS has database tables, configuration files and other data, that must to be backed up to take care of any data loss due to any reason. E5-MS provides both manual and daily automatic back up functionality. The scheduled backup interval can be configured as per user requirement. Backed up content can be restored by user manually whenever the need arise.

The System Administrators involved with the installation and configuration of E5-MS will manage the set up of the Backup and Restore.

Backup generates a copy of the existing configuration files, database tables and other data which can be used later to bring the E5-MS system to the previous configured state.

Restore uses a previously generated backup, bring the E5-MS system back to a state when the backup was generated.

System Requirement

Backup shall approximately require space equivalent to 100 MB + size of E5-MS database dump file. The size of E5-MS database dump file shall depend upon the size of E5-MS database. E5-MS database size shall be variable depending upon the number of EAGLEs being managed i.e. database size shall grow on the basis of deployed E5-MS configuration (Small, Medium, or Large).

Backup in E5-MS

Backup of the E5-MS system can be generated as per the requirement of the customer. Backup can be taken daily, weekly, day of the month etc. Oracle recommends daily backup so that the E5-MS can be restored to a state close to the disaster point.

By default, automatic (scheduled) backup of E5-MS will be configured. It will create backup of selected configuration data and database every day at 2 AM.

A user will also have the ability to create backup manually as well as update schedule as required by modifying the required files.

Backup Contents

All the required files and directories along with database will be backed up to preserve E5-MS state. As part of backup following E5-MS files and directories will get backed up:

- Directories: `conf/tekelec`, `users`, `commandManagerScripts`, `linkUtilizationScripts`, `reportingStudio`
- Files: `defaultconf/usernamePassword.conf`, `conf/clientparameters.conf`, `conf/securitydbData.xml`, `classes/hbnlib/hibernate.cfg.xml`, `classes/hbnlib/secondary/hibernate.cfg.xml`

Listed directories/files will be backed up as they are at the time of backup. The database tables will be backed up in a file named E5MS_Database_BackUp.sql.

Note: WebNMS backup does not consider empty directories for backup. So, the categories created by users in /opt/E5-MS/commandManager/scripts directory which do not have any scripts under them will not be backed up. Also it is suggested not to modify the content of files/directories to be backed up to ensure that upgrade process do not get impacted.

Automatic Backup

Configuration for Automatic Backup

The default configuration for automatic backup in E5-MS is given in /Tekelec/WebNMS/conf/BackUp.conf file. It is shown below:

```
<BACKUP
className="jdbc.MysqldumpBackup"
HOURL=" 2"
DAY_OF_THE_MONTH="*" />

<TABLES_TO_BACKUP
TABLES="ALL">
</TABLES_TO_BACKUP>
<FILES_TO_BACKUP
DIR_NAMES="conf/tekelec,users,commandManagerScripts,
linkUtilizationScripts,reportingStudio"
FILE_NAMES="defaultconf/usernamePassword.conf,
conf/clientparameters.conf,conf/securitydbData.xml,
classes/hbnlib/hibernate.cfg.xml,classes/hbnlib/secondary/hibernate.cfg.xml">
</FILES_TO_BACKUP>
```

The significance of entries in the above configuration in the BackUp.conf file is explained below:

```
HOURL=" 2"
```

The value indicates that the backup will be taken at 2 AM.

```
DAY_OF_THE_MONTH="*" /
```

The value indicates that backup will be generated daily.

```
<TABLES_TO_BACKUP
TABLES="ALL">
</TABLES_TO_BACKUP>
```

All database tables will be included in the backup.

```
<FILES_TO_BACKUP
DIR_NAMES="conf/tekelec,users,commandManagerScripts,
linkUtilizationScripts,reportingStudio"
FILE_NAMES="defaultconf/usernamePassword.conf,
conf/clientparameters.conf,conf/securitydbData.xml,
classes/hbnlib/hibernate.cfg.xml,
classes/hbnlib/secondary/hibernate.cfg.xml">
</FILES_TO_BACKUP>
```

All listed files and directories as mentioned in FILE_NAMES and DIR_NAMES tag respectively will be included in backup.

Configuring Default Backup Destination

A user will have the ability to update the backup destination as per his requirement by manually updating the directory path given for BACKUP_DESTINATION parameter in /Tekelec/WebNMS/conf/serverparameters.conf file. Following points must be taken care of while updating the same:

- While specifying the value (i.e. destination directory name), the absolute path should be specified and the directory path should exist.
- The path should be outside E5-MS home (/Tekelec/WebNMS). This is to ensure that the backup is not deleted in case of un-installation of E5-MS RPM.

Default Backup Destination

By default, the E5-MS backup will be created in the directory "/var/backup". This entry has been provided in /Tekelec/WebNMS/conf/serverparameters.conf file.

```
#Path of directory where backup of E5-MS will be taken
BACKUP_DESTINATION /var/backup
```

Manual Backup

A system user with privileges to execute /Tekelec/WebNMS/bin/backup/BackupDB.sh script will have the ability to take manual backup of E5-MS. The location where the backup will be generated can also be controlled by the user.

Manual backup on the default location

Manual backup of E5-MS for the default backup location /var/backup can be taken using the command given below:

```
# sh /Tekelec/WebNMS/bin/backup/BackupDB.sh
```

Manual backup on a desired location

It will also be possible to create backup at a desired location by providing the location as an argument to backup script as shown below. The directory provided by the user to create the backup should exist on the system before running the backup script, else backup might not work.

```
# sh /Tekelec/WebNMS/bin/backup/BackupDB.sh -d <Backup location>
```

For example:

```
# sh /Tekelec/WebNMS/bin/backup/BackupDB.sh -d /var/tklc/backup
```

The above command will generate a backup at location /var/tklc/backup.

Configuring Backup Schedule

A user will have the ability to update the default schedule value in /Tekelec/WebNMS/conf/BackUp.conf file manually to achieve backup as per user's own requirements. For this, there are multiple scheduling options available, shown in Table E5-MS Backup Scheduling Options, that provide a user great flexibility is scheduling the backups.

Note: Updating backup schedule will require a server restart for the changes to take impact.

E5-MS Backup Scheduling Options

The time at which the backup has to be executed, can be specified in any one of the following ways:

- Daily (for taking backup every day at 0200 hrs)
- Weekly (for taking backup on a fixed day every week (at 0200 hrs every Monday))
- Hour and Day_of_the_week (for taking backup at a fixed day(s) and time every week)
- Hour and Day_of_the_month (for taking backup at a fixed day(s) and time every month)

The following table provides examples as to how the above configuration options are used:

Scheduling Interval	Entry in BackUp.conf File
Daily	<pre><BACKUP className="jdbc.MysqldumpBackup" DAILY="true" /></pre>
Weekly	<pre><BACKUP className="jdbc.MysqldumpBackup" WEEKLY="true" /></pre>
Hour and Day_of_the_Week	<p>This parameter deals with two values - HOUR and DAY.</p> <p>The value for HOUR can be specified in comma separated form. The value can be any number from 1 to 24 (representing 24 hours).</p> <p>DAY_OF_THE_WEEK has also to be specified in comma-separated form. The DAY can be anything from SUN to SAT. Only the first three letters of the day have to be specified.</p> <p>For example, if backup is needed on Monday and Wednesday, it can be specified as shown below:</p> <p>Example:</p> <pre><BACKUP className="jdbc.MysqldumpBackup" HOUR="3,7" DAY_OF_THE_WEEK="MON,WED" /></pre>

Scheduling Interval	Entry in BackUp.conf File
Hour and Day_of_the_Month	<p>HOUR has to be specified as a list. For example, 2,5,22. It must be between 1 and 24.</p> <p>DAY_OF_THE_MONTH has to be given as a range (starting from 1 to a maximum of 31). The value of "*" is ALL.</p> <p>Example: To perform backup at HOUR 3,7 and DAY_OF_THE_MONTH 10-20 -</p> <pre data-bbox="776 533 1419 667" style="background-color: #f0f0f0; padding: 5px;"> <BACKUP className= " jdbc .MysqldumpBackup " HOUR= " 3 , 7 " DAY_OF_THE_MONTH= " 10 - 20 " /></pre>

Backup to an External Location

For better disaster recovery capability, it is recommended that backup should be taken to an external device. For this, the external device (e.g. NAS drive) should be mounted to the server. Once the device is successfully mounted, the admin shall need to use the device location for backup. In case of automatic backup (refer to Automatic Backup section) the admin shall need to update the backup destination manually in `/Tekelec/WebNMS/conf/serverparameters.conf` file (refer to Configuring default backup destination). In case of manual backup (refer to Manual Backup), the admin shall need to provide the device's location after the `-d` flag while running manual backup (refer to Manual backup on a desired location).

Normal Operations during Backup

When the backup process is executed, any operations should NOT be performed using the Clients until the backup process is complete.

When the backup process begins at the configured time, the following message (notification) shall be displayed on the status bar of E5-MS Client. A user will have to wait for the process to complete before performing any operations using the Client.

Backup operation is in progress. Please wait for sometime for your request to be processed by the server

Time taken in Backup

Backup shall approximately take about 5 minutes or more depending upon the size of E5-MS database. E5-MS database size shall be variable depending upon the number of EAGLEs being managed i.e. the deployed E5-MS configuration (Small, Medium or Large).

Status of Backup

The status of backup (automatic as well as manual) shall be logged in Audit Trails. A user with permission on 'User Audit' operation shall be able to view the audit messages showing start and completion of backup on 'User Audit' screen. Details of audit trails for various scenarios are below.

Scenario	Audit Trail Details					
	User Name	Operation Name	Audit Time	Status	Category	Description
Backup is started	SYSTEM	Backup Service	<time>	SUCCESS	E5-MS Backup	Backup is in progress
Backup completes successfully	SYSTEM	Backup Service	<time>	SUCCESS	E5-MS Backup	Backup is completed
Backup creation fails	SYSTEM	Backup Service	<time>	FAILURE	E5-MS Backup	Backup creation failed
Backup creation fails because of non-availability of space on backup location	SYSTEM	Backup Service	<time>	FAILURE	E5-MS Backup	Backup cannot be created, as there is not enough space left on the machine
Backup creation fails because of error in database connection	SYSTEM	Backup Service	<time>	FAILURE	E5-MS Backup	Backup creation failed due to database connection error

For manual backup, apart from the audit logs given above, the user shall also see the relevant log messages on console as shown in the Sample Outputs section.

Sample Outputs

Output while running Manual Backup

```
[root@e5ms2 backup]# sh BackupDB.sh -d /var/tklc/backup
```

```
Please wait! Backup of E5-MS is in progress...-
```

```
E5-MS database backup file "E5MS_Database_BackUp.sql"
successfully created.
```

```
Backup of directories successfully created.
```

```
E5-MS Backup is completed.
```

Output while Restoring from a Backup

```
[root@e5ms-12 backup]# sh RestoreDB.sh /var/backup/
E5MS_Database_BackUp.sql restore path :: /var/backup
```

```
WARNING! Attempting to restore the data!!! This will result in
losing your current data!!! Do you want to continue [y/n]?
```

```
y
```

```
Script will attempt to restore E5-MS database from the dump
file: /var/backup/E5MS_Database_BackUp.sql
```

```
E5-MS database restoration in progress...
```

```
Successfully restored E5-MS database.
```

```
The following files will be restored now to E5-MS:
```

```
/Tekelec/WebNMS//Tekelec/WebNMS/conf/tekelec
/Tekelec/WebNMS/conf/tekelec/lui.properties
/Tekelec/WebNMS/conf/tekelec/InventoryCommands.txt
/Tekelec/WebNMS/conf/tekelec/security.properties
/Tekelec/WebNMS/conf/tekelec/tekmeas.conf
/Tekelec/WebNMS/conf/tekelec/lui_template_script.txt
/Tekelec/WebNMS/conf/tekelec/ContinentZonalMap.xml
/Tekelec/WebNMS/conf/tekelec/CmiParameters.conf
/Tekelec/WebNMS/conf/tekelec/EagleCardNameNumMap.xml
/Tekelec/WebNMS/conf/tekelec/ModulesConf.xml
/Tekelec/WebNMS/conf/tekelec/common.config
/Tekelec/WebNMS/conf/tekelec/fault.properties
/Tekelec/WebNMS/conf/tekelec/NbiParameters.conf
/Tekelec/WebNMS/conf/tekelec/server_conf.properties
/Tekelec/WebNMS/conf/tekelec/reporting.properties
/Tekelec/WebNMS//Tekelec/WebNMS/users
/Tekelec/WebNMS//Tekelec/WebNMS/users/root
/Tekelec/WebNMS/users/root/toolbar.dtd
/Tekelec/WebNMS//Tekelec/WebNMS/users/root/listmenus
/Tekelec/WebNMS/users/root/listmenus/dummy.txt
/Tekelec/WebNMS/users/root/sysadminmenu.xml
/Tekelec/WebNMS//Tekelec/WebNMS/users/root/policymenus
/Tekelec/WebNMS/users/root/policymenus/nonperiodicpolicymenu.xml
/Tekelec/WebNMS/users/root/policymenus/periodicpolicymenu.xml
/Tekelec/WebNMS/users/root/AudioInfo.xml
/Tekelec/WebNMS/users/root/mibmenu.xml
/Tekelec/WebNMS/users/root/HomePageLayout.xml
/Tekelec/WebNMS/users/root/increments.conf
/Tekelec/WebNMS//Tekelec/WebNMS/users/root/mapmenus
/Tekelec/WebNMS/users/root/mapmenus/dummy.txt
/Tekelec/WebNMS/users/root/panelmenubar.dtd
/Tekelec/WebNMS/users/root/FramesInfo.conf
/Tekelec/WebNMS/users/root/alertsmenu.xml
/Tekelec/WebNMS/users/root/maptoolbar.xml
/Tekelec/WebNMS/users/root/clientparameters.conf
/Tekelec/WebNMS/users/root/framemenu.xml
/Tekelec/WebNMS/users/root/tllbrowsermenu.xml
/Tekelec/WebNMS/users/root/TreeOperations.xml
/Tekelec/WebNMS/users/root/Tree.xml
/Tekelec/WebNMS/users/root/maptoolbar.dtd
/Tekelec/WebNMS/users/root/frameoptions.xml
```



```

/Tekelec/WebNMS//Tekelec/WebNMS/users/guest
/Tekelec/WebNMS/users/guest/toolbar.dtd
/Tekelec/WebNMS//Tekelec/WebNMS/users/guest/listmenus
/Tekelec/WebNMS/users/guest/listmenus/dummy.txt
/Tekelec/WebNMS/users/guest/sysadminmenu.xml
/Tekelec/WebNMS//Tekelec/WebNMS/users/guest/policymenus
/Tekelec/WebNMS/users/guest/policymenus/nonperiodicpolicymenu.xml
/Tekelec/WebNMS/users/guest/policymenus/periodicpolicymenu.xml
/Tekelec/WebNMS/users/guest/AudioInfo.xml
/Tekelec/WebNMS/users/guest/mibmenu.xml
/Tekelec/WebNMS/users/guest/HomePageLayout.xml
/Tekelec/WebNMS/users/guest/increments.conf
/Tekelec/WebNMS//Tekelec/WebNMS/users/guest/mapmenus
/Tekelec/WebNMS/users/guest/mapmenus/dummy.txt
/Tekelec/WebNMS/users/guest/panelmenubar.dtd
/Tekelec/WebNMS/users/guest/alertsmenu.xml
/Tekelec/WebNMS/users/guest/maptoolbar.xml
/Tekelec/WebNMS//Tekelec/WebNMS/users/guest/state
/Tekelec/WebNMS/users/guest/state/dummy.txt
/Tekelec/WebNMS/users/guest/clientparameters.conf
/Tekelec/WebNMS/users/guest/framemenu.xml
/Tekelec/WebNMS/users/guest/tllbrowsermenu.xml
/Tekelec/WebNMS/users/guest/TreeOperations.xml
/Tekelec/WebNMS/users/guest/Tree.xml
/Tekelec/WebNMS/users/guest/maptoolbar.dtd
/Tekelec/WebNMS/users/guest/frameoptions.xml
/Tekelec/WebNMS//Tekelec/WebNMS/commandManagerScripts
/Tekelec/WebNMS//Tekelec/WebNMS/commandManagerScripts/kanav
/Tekelec/WebNMS//Tekelec/WebNMS/commandManagerScripts/kanav/Kanav
/Tekelec/WebNMS/commandManagerScripts/kanav/Kanav/kan.bsh
/Tekelec/WebNMS//Tekelec/WebNMS/commandManagerScripts/viv
/Tekelec/WebNMS//Tekelec/WebNMS/commandManagerScripts/usr4
/Tekelec/WebNMS//Tekelec/WebNMS/commandManagerScripts/usr4/default
/Tekelec/WebNMS/commandManagerScripts/usr4/default/scrl.bsh
/Tekelec/WebNMS//Tekelec/WebNMS/commandManagerScripts/usr4/cat1
/Tekelec/WebNMS/commandManagerScripts/usr4/cat1/scrl.bsh
/Tekelec/WebNMS/commandManagerScripts/usr4/cat1/scr4.bsh
/Tekelec/WebNMS//Tekelec/WebNMS/commandManagerScripts/arjun
/Tekelec/WebNMS//Tekelec/WebNMS/commandManagerScripts/arjun/default
/Tekelec/WebNMS/commandManagerScripts/arjun/default/hashhhh.bsh
/Tekelec/WebNMS//Tekelec/WebNMS/commandManagerScripts/k2
/Tekelec/WebNMS//Tekelec/WebNMS/commandManagerScripts/kan
/Tekelec/WebNMS/linkUtilizationScripts/aricentstp_lui_script.bsh
/Tekelec/WebNMS/linkUtilizationScripts/tekelecstp_lui_script.bsh
/Tekelec/WebNMS/linkUtilizationScripts/eagle9_lui_script.bsh
/Tekelec/WebNMS/linkUtilizationScripts/tklc9010801_lui_script.bsh
/Tekelec/WebNMS/linkUtilizationScripts/stpd1180801_lui_script.bsh
/Tekelec/WebNMS/linkUtilizationScripts/eale5_lui_script.bsh
/Tekelec/WebNMS/linkUtilizationScripts/tklc1071501_lui_script.bsh
/Tekelec/WebNMS/linkUtilizationScripts/eagle3_lui_script.bsh
/Tekelec/WebNMS/linkUtilizationScripts/pveagle03_lui_script.bsh
/Tekelec/WebNMS/linkUtilizationScripts/eagle8_lui_script.bsh
/Tekelec/WebNMS/linkUtilizationScripts/tklc1180601_lui_script.bsh
/Tekelec/WebNMS/linkUtilizationScripts/eagle6_lui_script.bsh
/Tekelec/WebNMS/linkUtilizationScripts/tklc1170501_lui_script.bsh
/Tekelec/WebNMS//Tekelec/WebNMS/reportingStudio
/Tekelec/WebNMS/reportingStudio/Alarms_SpecificDuration_WithSeverity.rpt
/Tekelec/WebNMS/reportingStudio/Resources_Top10_PerCount.rpt
/Tekelec/WebNMS/reportingStudio/Events_SpecificDuration_WithSeverity.rpt
/Tekelec/WebNMS/reportingStudio/
LinkReport_withErlang_PercentUtilization.rpt
/Tekelec/WebNMS/reportingStudio/All_Events.rpt
/Tekelec/WebNMS/reportingStudio/Alarms_Top10_PerCount.rpt
/Tekelec/WebNMS/reportingStudio/Alarms_Top10_PerSeverity.rpt

```

```

/Tekelec/WebNMS/reportingStudio/
Events_SpecificDuration_WithSeverity_UAM_Number.rpt
/Tekelec/WebNMS/reportingStudio/
Alarms_SpecificDuration_WithSeverity_UAM_Number.rpt
/Tekelec/WebNMS/reportingStudio/EventSummary_SpecificDuration.rpt
/Tekelec/WebNMS/reportingStudio/
CardReport_withErlang_PercentUtilization.rpt
/Tekelec/WebNMS/reportingStudio/Resources_Top10_PerSeverity.rpt
/Tekelec/WebNMS/reportingStudio/All_Alarms.rpt
/Tekelec/WebNMS/reportingStudio/Events_SpecificDuration.rpt
/Tekelec/WebNMS/reportingStudio/Inventory_OOSCards.rpt
/Tekelec/WebNMS/reportingStudio/
LinkSetReport_withErlang_PercentUtilization.rpt
/Tekelec/WebNMS/reportingStudio/Inventory_AllCards.rpt
/Tekelec/WebNMS/reportingStudio/Measurement_Systot_STP.rpt
/Tekelec/WebNMS/reportingStudio/Events_SpecificDate.rpt
/Tekelec/WebNMS/reportingStudio/Alarms_SpecificDate.rpt
/Tekelec/WebNMS/reportingStudio/AlarmSummary_SpecificDuration.rpt
/Tekelec/WebNMS/reportingStudio/Alarms_SpecificDuration.rpt
/Tekelec/WebNMS/defaultconf/usernamePassword.conf
/Tekelec/WebNMS/conf/securitydbData.xml
/Tekelec/WebNMS/classes/hbnlib/hibernate.cfg.xml
/Tekelec/WebNMS/classes/hbnlib/secondary/hibernate.cfg.xml
All the files & directories specified in the FILES_TO_RESTORE tag
are successfully restored

E5-MS successfully restored.

```

Restore in E5-MS

How to Restore from Existing Backup

A system user with privileges to execute `/Tekelec/WebNMS/bin/backup/RestoreDB.sh` script will have the ability to restore E5-MS system to a previous state by using the backup generated earlier. Before restoring the contents, E5-MS server must be shut down. This is because the restore script deletes the database tables and re-creates them using the database backup file.

Restoring from the default/any backup location

Restore can be executed using the backup at the default/any backup location by using the command given below

```

$> sh /Tekelec/WebNMS/bin/backup/RestoreDB.sh
<path of data filename>

```

For example, for restoring from default backup following command can be issued:

```

$> sh /Tekelec/WebNMS/bin/backup/RestoreDB.sh
/var/backup/E5MS_Database_BackUp.sql

```

Sample output of restore script execution is shown in Sample Outputs.

Default Restore Contents

The `RestoreDB.sh` script will use `/Tekelec/WebNMS/bin/backup/TablesToRestore.conf` to know what to restore (database and directories) using the configuration given below.

```
<RESTORE TABLES="ALL">
</RESTORE>

<FILES_TO_RESTORE
DIR_NAMES="conf/tekelec,users,commandManagerScripts,linkUtilizationScripts,
reportingStudio"
FILE_NAMES="defaultconf/usernamePassword.conf,
conf/clientparameters.conf,conf/securitydbData.xml,classes/hbnlib/hibernate.cfg.xml,classes/hbnlib/secondary/hibernate.cfg.xml">
</FILES_TO_RESTORE>
```

The significance of the entries in the above configuration in the `TablesToRestore.conf` file is explained below:

```
<RESTORE TABLES="ALL">
</RESTORE>
```

Restore all the database tables present in the backup.

```
<FILES_TO_RESTORE DIR_NAMES="conf/tekelec,users,
commandManagerScripts,linkUtilizationScripts, reportingStudio"
FILE_NAMES="defaultconf/usernamePassword.conf,
conf/clientparameters.conf,conf/securitydbData.xml,
classes/hbnlib/hibernate.cfg.xml,
classes/hbnlib/secondary/hibernate.cfg.xml">
</FILES_TO_RESTORE>
```

Restore all the files and directories listed in `FILE_NAMES` and `DIR_NAMES` tag respectively from the backup.

Time taken in Restore

Restore shall approximately take few minutes (for e.g. 10 to 15 mins for very small database) or more depending upon the size of backup. The backup size shall be variable depending upon the size of E5-MS database backup file.

The size of E5-MS database backup file shall depend upon the number of EAGLEs being managed i.e. the deployed E5-MS configuration (Small, Medium or Large).

Status of Restore

The status of restore shall be shown through relevant log messages on console shown in Sample Outputs.

File and their Locations

The following files are used during backup and restore.

Table 23: Backup and Restore related Files and Directories

File/Directory	Description
/Tekelec/WebNMS/conf/BackUp.conf	The configuration file where backup contents and schedule are listed. It is recommended not to change backup content as it may create issues with upgrade process.
/Tekelec/WebNMS/conf/serverparameters.conf	File where the directory for backup is mentioned.
/Tekelec/WebNMS/bin/backup/BackupDB.sh	Script to be used to manually generate E5-MS backup.
/Tekelec/WebNMS/bin/backup/ResotreDB.sh	Script to be used to restore the E5-MS from a previously generated backup.
/Tekelec/WebNMS/bin/backup/TablesToRestore.conf	The configuration file where restore contents are listed for restore. It is recommended not to change restore content as it may create issues with upgrade process.

Appendix C

E5-MS Failover

Topics:

- *Overview.....214*
- *Failover Setup.....217*
- *Licensing.....232*
- *Limitations.....232*

This appendix describes the failover for the E5-MS.

Overview

In E5-MS, failover support is provided by providing two redundant servers configured as primary and standby servers. In failover setup, the primary and standby servers should have access to the replicated database. MySQL is used as the database for E5-MS and the MySQL data files are stored in the /Tekelec/WebNMS/mysql/data directory.

The WebNMS configuration files are overwritten from the primary server onto the standby server once every BACKUP_INTERVAL, if configured. There is no GUI to make changes to these configuration files; any changes will have to be done manually.

During the failover period, while the standby server comes up to assume the responsibilities of the primary server, alarms and other intermediary data would be lost.

Requirements

Database replication should be set up between the primary and standby E5-MS server databases before implementing failover. Refer to [How to Set Up Failover](#) for the procedure.

Primary Server

The server that starts first (between the two servers) becomes the primary server. In the database, details regarding the primary and standby servers are maintained in a table named BEFailOver. Refer to [Befailover Table](#) for details about the table. At a configured regular time interval, the primary server updates the BEFailOver table about its presence with a count named LASTCOUNT. With every update the count gets incremented. The periodic interval at which the primary has to update the database regarding its presence is known as HEART_BEAT_INTERVAL. If HEART_BEAT_INTERVAL is configured as 60 seconds, the primary server will update the BEFailOver table every 60 seconds. This interval is configurable. Refer to [Files and Location in FAILOVER](#).

Standby Server

When a server is started, if no standby server is already registered with the primary server, the primary server registers this server as the standby server. At any time, only one primary server and one standby server can be configured. If a second standby server is started, the primary server will refuse registration. When the primary server registers a standby server, it makes an entry regarding the registration in the database.

Similar to the primary, the standby server updates the BEFailOver table about its presence at a specified periodic interval (HEART_BEAT_INTERVAL) in the LASTCOUNT which gets incremented with every update. The primary server monitors the LASTCOUNT of standby server as per the FAIL_OVER_INTERVAL. When the standby fails to update the LASTCOUNT, the primary assumes that the standby had failed and it cancels its registration as well as its entries from the BEFailOver table. This would enable E5-MS to connect a new standby server. It is important here to note that a new standby server will be able to register with the primary only when replication between the existing servers is stopped and failover is setup between the primary and the new standby server.

Client

During failover, a pop-up is shown to already logged in users stating that the connection to the primary server is lost and the client is trying to connect to the standby server. Until the failover process is complete a user will not be able to use E5-MS.

The pop-up message shown is " Connection lost to primary server <primary server hostname> at :9090. Now client is trying to connect secondary server <secondary server hostname> at :9090"

Failover Process

When the primary server fails, it fails to update the LASTCOUNT. The standby server keeps monitoring the primary's LASTCOUNT at a specified periodic interval known as FAIL_OVER_INTERVAL. The default value for FAIL_OVER_INTERVAL is 60 seconds. If FAIL_OVER_INTERVAL is configured as 50 seconds, the standby will monitor the primary's LASTCOUNT every 50 seconds. Every time, when the standby server looks up the LASTCOUNT, it compares the previous and present counts. When the primary server fails to update the LASTCOUNT, consecutive counts will be the same and the standby assumes that the primary had failed. Here, a parameter named RETRY_COUNT, the default value for RETRY_COUNT is 3, comes into play which enables the user to specify the number of times the standby has to check the primary's LASTCOUNT (when the primary fails to update the LASTCOUNT) before assuming that the primary had failed.

Once the standby server finds that the primary had failed, it immediately changes its mode as PRIMARY and assumes all the functions that were being performed by the hitherto primary server.

To check if the failover process is successful, check for the SERVERROLE column in the BEFailover table. Whereas any end user will be able to connect to the standby server, the new active server, on successful switchover.

After switchover, when the old primary server is started it registers as the new standby server.

For the default entries configured, E5-MS takes around 2 minutes for a successful switchover. During the failover interval alarms and other intermediary data would be lost.

Manual Failover

Once both the primary and standby servers are started in their respective modes, manually stop the primary server by the following command.

```
$> sh Shutdown.sh root public
```

After some time (based on FAIL_OVER_INTERVAL and RETRY_COUNT), the stand-by server will become primary server.

Please note that if the server just shutdown is started before the standby has taken the role of primary it may lead to erroneous situation breaking replication setup between two MySQL servers. Such an action is highly unadvisable

Files and Location in FAILOVER

The following files are used for failover process.

Directory/File	Description
/Tekelec/WebNMS/bin/startnms.sh	<p>The script file is used to start E5-MS server. For failover, the value of a property <code>-Djava.awt.headless</code> is modified from <code>-Djava.awt.headless=false</code> to <code>-Djava.awt.headless=true</code>.</p> <p>This change has already been done in the file and no manual changes are required while creating failover setup.</p> <p>For more details, visit: http://www.oracle.com/technetwork/articles/javase/headless-136834.html</p>
/Tekelec/WebNMS/bin/startMySQL.sh	<p>The script file is used to pass arguments to the MySQL server that are necessary to implement database replication.</p> <p>This file needs to be updated manually in case failover needs to be set up, and the changes required are part of the failover setup procedure described in How to Set Up Failover.</p>
/Tekelec/WebNMS/conf/serverparameters.conf	<p>A property DB_REPLICATION with value true has been added to this file to enable database replication for E5-MS.</p> <p>No manual changes are required for this file during the failover setup procedure.</p>
/Tekelec/WebNMS/conf/Failover.xml	<p>The values for HEART_BEAT_INTERVAL, FAIL_OVER_INTERVAL, BACKUP_INTERVAL, and RETRY_COUNT can be configured from this file. The default values for these parameters are 60 (seconds), 80 (seconds), 3600 (seconds) and 3, respectively. A user can optimize these values as per the network performance.</p> <p>The E5-MS configuration files/directories which are to be backed up are also specified in this file as follows:</p> <pre><INCLUDE> <!-- Entries for conf & users folders have been removed as they are taken care of by Zoho--> <DIR name="images"/> <DIR name="html"/> <DIR name="icons"/> <DIR name="commandManagerScripts"/> <DIR name="linkUtilizationScripts"/> <DIR name="reportingStudio"/> <FILE name="apache/tomcat/conf/server.keystore"/> </INCLUDE></pre> <p>Note: Any changes made in the Failover.xml file would be effective only after server restart.</p>

Directory/File	Description
/Tekelec/WebNMS/classes/hbplib/hibernate.cfg.xml	<p>The following c3p0 entries have been un-commented:</p> <pre><property name="hibernate.c3p0.acquireRetryAttempts">2</property> <property name="hibernate.c3p0.acquireRetryDelay">3000</property> <property name="hibernate.c3p0.breakAfterAcquireFailure">>false</property></pre> <p>Also, you need to replace the value localhost with the server's hostname in the following connection URL. This update needs to be done manually in case failover needs to be set up and is part of the failover setup procedure described in How to Set Up Failover.</p> <pre><property name="connection.url">jdbc:mysql://localhost /WebNmsDB?dumpQueriesOnException= true&jdbcCompliantTruncation=false</property></pre>
/Tekelec/WebNMS/classes/hbplib/secondary/hibernate.cfg.xml	<p>This file is an exact replica of the file above except for the hostname entry is for the standby server. This update needs to be done manually.</p>
/Tekelec/WebNMS/jre/lib/security/java.policy	<p>The following entries have been appended to the file:</p> <pre>permission java.awt.AWTPermission ".*"; permission java.security.SecurityPermission "createAccessControlContext"; permission java.net.SocketPermission "*.1024-65535","connect,accept,resolve,listen";</pre> <p>For details go to: http://docs.oracle.com/javase/1.5.0/docs/guide/security/permissions.html</p>

Failover Setup

To set up failover between the primary and standby servers, database replication is a must. Refer to [How to Set Up Failover](#) for failover setup.

After failover setup is created between the primary and standby servers, when shutting down a server, MySQL is not stopped and database replication keeps working. However, when one or both the servers go down in an outage or power failure in such a way that MySQL is also shut down, the databases will have to be synchronized. Refer to [Synchronizing Databases](#).

In the case of failed connectivity between primary and secondary, the secondary would be unable to read the last count of the primary and will assume the role of the primary while the primary will de-register the secondary and continue as primary.

How to Set Up Failover

For setting up failover, one of the servers can be assumed to be the **Primary** server and the other the **Standby** server.

Before proceeding with setting up of failover, the following details should be known:

- MySQL root user's password for both the primary and standby servers. The default password is **public**.
 - Hostnames for both the primary and standby servers. In the following procedure, for illustration purposes, these values are called **primary server hostname** and **standby server hostname** respectively.
1. Log into the primary E5-MS server using user **root**.
 2. In the system's hosts file, add the DNS entries for both the primary and standby servers as shown:

```
<PRIMARY SERVER IP> <PRIMARY SERVER HOSTNAME>
<STANDBY SERVER IP> <STANDBY SERVER HOSTNAME>
```

For example:

```
10.248.10.25 e5ms8
10.248.10.21 e5ms9
```

On CentOS, the hosts file is placed in the `/etc` directory.

3. Replace the *localhost* value in the following statement in the `/Tekelec/WebNMS/classes/hbplib/hibernate.cfg.xml` file with the hostname of the server:

```
<property name="connection.url">jdbc:mysql://localhost/WebNmsDB?dump
QueriesOnException=true&jdbcCompliantTruncation=false
</property>
```

For example:

```
<property name="connection.url">jdbc:mysql://e5ms7/WebNmsDB?dump
QueriesOnException=true&jdbcCompliantTruncation=false
</property>
```

4. Move to directory `/Tekelec/WebNMS/bin`:

```
cd /Tekelec/WebNMS/bin
```

5. Change the server-id value in the `startMySQL.sh` file. Any number in the range 1 to $2^{32}-1$ can be used as the value for server-id:

```
Update the value:
--server-id=1

To:
--server-id=<new value>
```

6. Start the MySQL server by invoking the `startMySQL.sh` script:

```
sh startMySQL.sh

# bin/safe_mysqld: line 199: my_print_defaults: command not found
bin/safe_mysqld: line 204: my_print_defaults: command not found
nohup: redirecting stderr to stdout
Starting mysqld daemon with databases from /Tekelec/WebNMS/mysql/data
```

7. Move to the `/Tekelec/WebNMS/mysql/bin` directory:

```
cd /Tekelec/WebNMS/mysql/bin
```

8. Connect to the MySQL client by executing `mysql` in the `/Tekelec/WebNMS/mysql/bin` directory. Provide the password for the MySQL root user when prompted. The default password is **public**.

```
./mysql -uroot -p<password>

Warning: Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 125
Server version: 5.6.18-enterprise-commercial-advanced-log MySQL Enterprise Server
 - Advanced Edition (Commercial)

Copyright (c) 2000, 2014, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.
Other names may be trademarks of their respective owners.

mysql>
```

9. Log into the standby E5-MS server using user **root**.
 10. In the system's hosts file, add the DNS entries for both the primary and standby servers as shown:

```
<PRIMARY SERVER IP> <PRIMARY SERVER HOSTNAME>
<STANDBY SERVER IP> <STANDBY SERVER HOSTNAME>

For example:

10.248.10.25 e5ms8
10.248.10.21 e5ms9
```

On CentOS, the hosts file is placed in the `/etc` directory.

11. Replace the *localhost* value in the following statement in the `/Tekelec/WebNMS/classes/hbplib/hibernate.cfg.xml` file with the hostname of the server:

```
<property name="connection.url">jdbc:mysql://localhost/WebNmsDB?dump
QueriesOnException=true&jdbcCompliantTruncation=false
</property>

For example:

<property name="connection.url">jdbc:mysql://e5ms8/WebNmsDB?dump
QueriesOnException=true&jdbcCompliantTruncation=false
</property>
```

12. Move to directory `/Tekelec/WebNMS/bin`:

```
cd /Tekelec/WebNMS/bin
```

13. Change the server-id value in the `startMySQL.sh` file. Any number in the range 1 to $2^{32}-1$ can be used as the value for server-id. However, the value used must not be same as the value used on the primary server.

```
Update the value:
--server-id=1

To:
--server-id=<new value>
```

14. Start the MySQL server by invoking the `startMySQL.sh` script:

```
sh startMySQL.sh

# bin/safe_mysqld: line 199: my_print_defaults: command not found
bin/safe_mysqld: line 204: my_print_defaults: command not found
nohup: redirecting stderr to stdout
Starting mysqld daemon with databases from /Tekelec/WebNMS/mysql/data
```

15. Move to the `/Tekelec/WebNMS/mysql/bin` directory:

```
cd /Tekelec/WebNMS/mysql/bin
```

16. Connect to the MySQL client by executing `mysql` in the `/Tekelec/WebNMS/mysql/bin` directory. Provide the password for the MySQL root user when prompted. The default password is **public**.

```
./mysql -uroot -p<password>

Warning: Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 125
Server version: 5.6.18-enterprise-commercial-advanced-log MySQL Enterprise Server
 - Advanced Edition (Commercial)

Copyright (c) 2000, 2014, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.
Other names may be trademarks of their respective owners.

mysql>
```

17. Take a backup of the database from the primary server and restore the database on the standby server:

- a. Run the `/Tekelec/WebNMS/bin/backup/BackupDB.sh` script on the primary server.
- b. Tar the contents of `/var/backup` directory:

```
cd /var/backup
tar cvf /tmp/backup.tar *
```

- c. Transfer the tar file created above to the standby server:

```
scp /tmp/backup.tar root@<secondaryserverip>:/tmp/
```

- d. Restore the tar file on the standby machine:

```
cd /var/backup
tar xvf /tmp/backup.tar
cd /Tekelec/WebNMS/bin/backup/
./RestoreDB.sh /var/backup/E5MS_Database_BackUp.sql
```

18. Execute the following five MySQL commands on the primary server. Replace the italicized values by the actual values.

Note: In the CREATE USER command, the values for *<primary replication user>* and *<primary replication user password>* can be provided as intended by the user. However, both these values should be noted to be used later in the GRANT REPLICATION SLAVE command.

```
GRANT ALL PRIVILEGES ON *.* TO root@'<primary server hostname>' IDENTIFIED BY
'<primary server's mysql root user password>';

GRANT ALL PRIVILEGES ON *.* TO root@'<standby server hostname>' IDENTIFIED BY
'<standby server's mysql root user password>';

CREATE USER '<primary replication user>'@'localhost' IDENTIFIED BY '<primary
replication user password>';

GRANT REPLICATION SLAVE ON *.* TO '<primary replication user>'@'<standby server
hostname>' IDENTIFIED BY '<primary replication user password>';

FLUSH PRIVILEGES;

For example, if the primary server hostname is e5ms7 and the standby server
hostname is e5ms8:

GRANT ALL PRIVILEGES ON *.* TO root@'e5ms7' IDENTIFIED BY 'public';

GRANT ALL PRIVILEGES ON *.* TO root@'e5ms8' IDENTIFIED BY 'public';

CREATE USER 'e5ms7user'@'localhost' IDENTIFIED BY 'e5ms7@123';

GRANT REPLICATION SLAVE ON *.* TO 'e5ms7user'@'e5ms8' IDENTIFIED BY 'e5ms7@123';

FLUSH PRIVILEGES;
```

19. Execute the following five MySQL commands on the standby server. Replace the italicized values by the actual values.

Note: In the CREATE USER command, the values for *<primary replication user>* and *<primary replication user password>* can be provided as intended by the user. However, both these values should be noted to be used later in the GRANT REPLICATION SLAVE command.

```
GRANT ALL PRIVILEGES ON *.* TO root@'<primary server hostname>' IDENTIFIED BY
'<primary server's mysql root user password>';

GRANT ALL PRIVILEGES ON *.* TO root@'<standby server hostname>' IDENTIFIED BY
'<standby server's mysql root user password>';

CREATE USER '<standby replication user>'@'localhost' IDENTIFIED BY '<standby
replication user password>';

GRANT REPLICATION SLAVE ON *.* TO '<standby replication user>'@'<primary server
```

```

hostname>' IDENTIFIED BY '<standby replication user password>';

FLUSH PRIVILEGES;

For example, if primary server hostname is e5ms7 and standby server hostname is
e5ms8:

GRANT ALL PRIVILEGES ON *.* TO root@'e5ms7' IDENTIFIED BY 'public';
GRANT ALL PRIVILEGES ON *.* TO root@'e5ms8' IDENTIFIED BY 'public';

CREATE USER 'e5ms8user'@'localhost' IDENTIFIED BY 'e5ms8@123';

GRANT REPLICATION SLAVE ON *.* TO 'e5ms8user'@'e5ms7' IDENTIFIED BY 'e5ms8@123';

FLUSH PRIVILEGES;

```

20. Run the SHOW MASTER STATUS command at the MySQL prompt on the primary server:

```

mysql> SHOW MASTER STATUS;
+-----+-----+-----+-----+
| File           | Position | Binlog_Do_DB | Binlog_Ignore_DB |
+-----+-----+-----+-----+
| log-bin.000004 |      545 | WebNmsDB     | mysql              |
+-----+-----+-----+-----+
1 row in set (0.00 sec)

```

Note the values for the File and Position columns, referred to later in the procedure as the PrimaryLogFile and PrimaryLogPosition.

21. Run the SHOW MASTER STATUS command at the MySQL prompt on the standby server:

```

mysql> SHOW MASTER STATUS;
+-----+-----+-----+-----+
| File           | Position | Binlog_Do_DB | Binlog_Ignore_DB |
+-----+-----+-----+-----+
| log-bin.000004 |      545 | WebNmsDB     | mysql              |
+-----+-----+-----+-----+
1 row in set (0.00 sec)

```

Note the values for the File and Position columns, referred to later in the procedure as the StandbyLogFile and StandbyLogPosition.

22. Execute the following two MySQL commands on the primary server. In the command, use the values for <StandbyLogPosition> and <StandbyLogFile> noted previously in this procedure.

```

CHANGE MASTER TO MASTER_HOST='<standby server hostname>', MASTER_PORT=3306,
MASTER_USER='<standby replication user>', MASTER_PASSWORD='<standby replication
user password>', MASTER_LOG_POS=<StandbyLogPosition>,
MASTER_LOG_FILE='<StandbyLogFile>';

START SLAVE;

```

23. Execute the following two MySQL commands on the standby server. In the command, replace the values for <PrimaryLogPosition> and <PrimaryLogFile> noted previously in this procedure.

```

CHANGE MASTER TO MASTER_HOST='<primary server hostname>', MASTER_PORT=3306,
MASTER_USER='<primary replication user>', MASTER_PASSWORD='<primary replication
user password>', MASTER_LOG_POS=<PrimaryLogPosition>,

```

```
MASTER_LOG_FILE='<PrimaryLogFile>';

START SLAVE;
```

24. Verify that replication has been set up correctly by executing the `SHOW SLAVE STATUS\G;` command at the MySQL client on the standby server.

Verify the **bold** values in the command output. Both should be **Yes** for correct replication setup.

```
SHOW SLAVE STATUS\G;

Output similar to the following is displayed -
***** 1. row *****
      Slave_IO_State: Waiting for master to send event
      Master_Host: e5ms7
      Master_User: e5ms7user
      Master_Port: 3306
      Connect_Retry: 60
      Master_Log_File: log-bin.000001
      Read_Master_Log_Pos: 98
      Relay_Log_File: relay-bin.000002
      Relay_Log_Pos: 233
      Relay_Master_Log_File: log-bin.000001
      Slave_IO_Running: Yes
      Slave_SQL_Running: Yes
      Replicate_Do_DB:
      Replicate_Ignore_DB:
      Replicate_Do_Table:
      Replicate_Ignore_Table:
      Replicate_Wild_Do_Table:
      Replicate_Wild_Ignore_Table:
      Last_Errno: 0
      Last_Error:
      Skip_Counter: 0
      Exec_Master_Log_Pos: 98
      Relay_Log_Space: 233
      Until_Condition: None
      Until_Log_File:
      Until_Log_Pos: 0
      Master_SSL_Allowed: No
      Master_SSL_CA_File:
      Master_SSL_CA_Path:
      Master_SSL_Cert:
      Master_SSL_Cipher:
      Master_SSL_Key:
      Seconds_Behind_Master: 0
1 row in set (0.00 sec)

ERROR:
No query specified
```

25. Verify that replication has been set up correctly by executing the `SHOW SLAVE STATUS\G;` command at the MySQL client on the primary server.

Verify the **bold** values in the command output. Both should be **Yes** for correct replication setup.

```
SHOW SLAVE STATUS \G;

Output similar to the following is displayed -
***** 1. row *****
```

```

Slave_IO_State: Waiting for master to send event
Master_Host: e5ms8
Master_User: e5ms8user
Master_Port: 3306
Connect_Retry: 60
Master_Log_File: log-bin.000001
Read_Master_Log_Pos: 98
Relay_Log_File: relay-bin.000002
Relay_Log_Pos: 233
Relay_Master_Log_File: log-bin.000001
Slave_IO_Running: Yes
Slave_SQL_Running: Yes
Replicate_Do_DB:
Replicate_Ignore_DB:
Replicate_Do_Table:
Replicate_Ignore_Table:
Replicate_Wild_Do_Table:
Replicate_Wild_Ignore_Table:
Last_Errno: 0
Last_Error:
Skip_Counter: 0
Exec_Master_Log_Pos: 98
Relay_Log_Space: 233
Until_Condition: None
Until_Log_File:
Until_Log_Pos: 0
Master_SSL_Allowed: No
Master_SSL_CA_File:
Master_SSL_CA_Path:
Master_SSL_Cert:
Master_SSL_Cipher:
Master_SSL_Key:
Seconds_Behind_Master: 0
1 row in set (0.00 sec)

ERROR:
No query specified

```

Note: The entries for primary and standby servers must also be done on the client machines' hosts file. On a Windows machine, the hosts file is in the C:\Windows\System32\drivers\etc folder.

Synchronizing Databases

Case 1: Both Servers Fail Simultaneously

1. Execute `startMySQL.sh` on both servers once they are up.
2. Login to MySQL.
3. Execute `STOP SLAVE` on both the servers.
4. Execute `START SLAVE` on the standby server.
5. Check if the SLAVE started properly. Execute `SHOW SLAVE STATUS`.

Slave_IO_Running: Yes

Slave_SQL_Running: Yes

Two lines to check are shown above; both these columns should contain **Yes**.

6. Execute `START SLAVE` on primary.
7. Check if the SLAVE started properly. Execute `SHOW SLAVE STATUS`.

Slave_IO_Running: Yes

Slave_SQL_Running: Yes

Two lines to check are shown above; both these columns should contain **Yes**.

Once the above mentioned lines contain **Yes** for both the servers, replication is complete and the databases are in sync.

Case 2: Standby Server Fails or Standby Server Machine Is Shut Down

1. Execute STOP SLAVE on the primary server.
2. Execute `startMySQL.sh` on the standby server once it is up.
3. Execute START SLAVE on the primary server.
4. Check if the SLAVE started properly. Execute SHOW SLAVE STATUS.

Slave_IO_Running: Yes

Slave_SQL_Running: Yes

Two lines to check are shown above; both these columns should contain **Yes**.

Once the above mentioned lines contain **Yes** for both the servers, replication is complete and the databases are in sync.

Case 3: Primary Server Fails or Primary Server Machine Is Shut Down

It is important to note that in case the primary server fails, the standby server takes its place as an Active server.

1. Execute STOP SLAVE on the new Active server (previously standby, before primary failed).
2. Execute `startMySQL.sh` on the restarted server once it is up.
3. Execute START SLAVE on the new Active server.
4. Check if the SLAVE started properly. Execute SHOW SLAVE STATUS.

Slave_IO_Running: Yes

Slave_SQL_Running: Yes

Two lines to check are shown above; both these columns should contain **Yes**.

Once the above mentioned lines contain **Yes** for both the servers, replication is complete and the databases are in sync.

Once the databases are synchronized, start the failed E5-MS server(s).

Befailover Table

The BEFailover table consists of the following columns:

Field Name	Type	Constraints	Description
HOSTADDRES	varchar(50)		Host's Address
NMSBEPORT	int(11)		WebNMS BE port
RMIREGISTRYPORT	int(11)		WebNMS registry port number

Field Name	Type	Constraints	Description
LASTCOUNT	bigint(20)		Value incremented after every HEART_BEAT_INTERVAL
SERVERROLE	varchar(10)	Can have one of the below values PRIMARY(States that this server is the primary server), STANDBY(States that this server is the standby server), FAILED(States that this server is not responding), and SHUTDOWN(States that this server is shutdown),	Describes the present role for a host.
STANDBYSERVERNAME	varchar(50)		Host address for standby server. Please note that this field shows the standby server host address only in case when the server was primary, has been shutdown and the standby has taken over as primary. This entry is used by the server to re-connect to the STANDBYSERVERNAME as and when this server comes up again

Tables Replicated

All E5-MS tables are replicated. Some of these important WebNMS tables are described below:

Table Name	Purpose
ANNOTATION	This table has the details on Alert Annotation and Alert History.
Alert	This table stores Web NMS Alert related properties.
AttributeAudit	This table contains the audit at the attribute level and contains information, like the number of retries, ending time of execution, etc.
AuthAudit	This table is used to store the log information regarding the authentication and authorization

Table Name	Purpose
	operations of a user in order to keep track of the operations performed by various users logged into the network.
BeFailOver	This table is used to store information for primary and standby servers
CORBANode	<p>The discovered CORBA object is mapped to the CORBANode. The properties are given in the corbaseed.file in <Web NMS Home>/conf directory.</p> <p>The CORBA Node object with the above mentioned properties is stored in the topology database. Only after the discovered device is stored in the topology database as a managed object, WebNMS starts managing the CORBA device.</p>
ConfigAttributes	The attributes defined in a particular task are stored in this table
configProvider	This contains the entries which are created by reading the configprovider.xml file and also contains the list of provider for the protocols used for configuring the device.
ConfigTaskDetails	This also contains the task related details like the total number of attributes contained in a task, type of the attribute namely, group, table, columnar, etc.
ConfigTasks	Whenever a task gets defined, it gets stored in this table. This contains information like name of the task, protocol to be used when executing the task, etc. It also stores information like whether or not rollback is needed, the rollback document, etc.
DataCollectionAttributes	This table holds the details about the data collection criteria, which you specify in the Data Collection tag, for the PolledData of a PollingObject. This includes a property of the ManagedObject compared with a value and only when that criteria satisfies, PolledData will be created and data collection done.
DeviceAudit	This table is used to store the device level audit details. This contains information, like device name, task name, starting time of execution, ending time of execution, etc. This also contains the status of configuration i.e., Success or Failure
DeviceList	Many devices can be grouped together so that the task can be executed over the group of devices at

Table Name	Purpose
	a later point of time. This grouping of devices are stored in this table.
DeviceListDetails	This contains the common properties of the device, like port to be used for configuration, value for timeout, retries, etc.
DeviceUserProps	This table contains the user properties specified for the device, like COMMUNITY in case of SNMP.
Event	The event table stores Web NMS Event related properties.
GroupTable	The aggregate (or group) relationship is modeled in the database using the Group Table.
IpAddress	This table represents an IP interface.
ManagedGroupObject	The aggregate (or group) relationship is modeled in the database using the Group Table.
ManagedObject	The ManagedObject Table is the core database object. It stores the Managed Objects and their properties or attributes. This base table contains all the basic elements required by NMS to manage an object, e.g., name, status, type, etc., An object that has been discovered will have an entry in the ManagedObject table, and the other corresponding tables based on the type of the Managed Object. The other tables that may have entries of a discovered Managed Object are Node Table, Network Table, Interface Table, etc.,
MapContainer	The following table gives you the attributes that are specific to MapContainers. The MapContainer object also consists of all the attributes that are listed as MapSymbol.
MapDB	This table consists all the map entries and their properties.
MapGroup	There are no specific attributes for MapGroup. The MapContainer object also consists of all the attributes that are listed as MapSymbol.
MapLink	The following table gives you the attributes that are specific to MapLinks. The MapLink object also consists of all the attributes that are listed as MapSymbol.
MapSymbol	The following table gives you the attributes of MapSymbols. All the attributes present in this table are also common to MapContainer, MapLink, and MapGroup objects.

Table Name	Purpose
NamedViewToAuthorizedViewTable	This table is used to stores the Named View defined for a particular view.
Network	This table represents an IP network.
Node	This table represents an IP Node.
OperationsTreeTable	This table is used to represent the tree hierarchy of the Operations. This information is used when assigning an Operation to a View where all the children for an Operation are also assigned to that View
PendingDevices	Similar to storing the pending tasks, the pending devices over which configuration has to be performed is stored in this table.
PendingTasks	When the ConfigServer is shut down, the list of pending tasks available for execution at the time of shut down are stored in this table. Whenever the server gets restarted, it reads this table and starts the configuration again.
PolledData	This is the table used for storing the PolledData. It contains the details such as name of the PolledData, Agent that has to be polled, data that has to be collected, whether multiple or not, etc. These details form the basis for data collection.
Polling Attributes	This table stores the match criteria details of PollingObject. The match criteria specification allows you to filter only the desired ManagedObjects.
PollingObjects	This table stores information about the PollingObject. It contains only two fields: name, and status
Providers	This table holds information about the protocol providers for data collection. The provider name and its associated class file name are stored.
STATSDATA	When Web NMS is started, the polling units will be stored in the PolledData table. After data collection, the collected data will be stored in the STATSDATA table if the type of the collected value is long.
STRINGDATA	When Web NMS is started, the polling units will be stored in the PolledData table. After data collection, the collected data will be stored in the STRINGDATA table if the type of the collected value is string.

Table Name	Purpose
SnmpInterface	This table stores additional information on the IP interface for nodes supporting SNMP
SnmpNode	This table stores additional information for nodes supporting SNMP.
TL1Interface	<p>The IP address of the Network Interface Card present in the TL1 Node is the TL1 Interface present in the TL1 Node. The properties of the TL1 Interface are given in the t11seed.file in <Web NMS Home>/conf directory,</p> <p>The TL1 Interface is created with the above mentioned properties and stored in the topology database as a TL1 Interface object. The values of the properties are fetched from t11seed.file and the device. The status polling of the TL1 device is dealt by the Topology module. This module uses the STATPOLLCOMMAND property in the TL1 Interface object, to query the status of the TL1 Interface and in turn the status of the TL1 Node.</p>
TL1Node	The discovered TL1 object is mapped to the TL1 Node. The properties are given in the t11seed.file file in <Web NMS Home>/conf directory
TaskAudit	This table is used to store the task level audit details. This contains information like task name, submitted time, device list, etc.
TaskToDeviceListMap	When a task is defined and devices are associated, the mapping between the tasks and device lists are stored in this table.
ThresholdObjects	This table holds information about the thresholds which you create for monitoring the collected data. Details such as threshold type, threshold value, etc. are stored in this table.
TopoObject	The TopoObject is the base class of all IP objects in the Topology database. The TopoObject table stores all the common set of Network, Node, Interface or IpAddress Objects
UserGroupTable	This table is used to store the assigned group of each user. A user can be present in more than one group
UserPasswordTable	This table maintains the user name and the password for the user
ViewPropertiesTable	The ViewPropertiesTable maps a view name to the properties of objects

Table Name	Purpose
ViewToOperationsTable	The ViewToOperations table maps the View Name to the corresponding operations. The Operation Name and the type of operation for a given View Name will be stored here.
ViewsToGroupTable	This table assigns a View Name to a Group, which specifies the access for the Group

E5-MS Custom Replicated Tables

Table Name	Purpose
Tek_Secu_MapUserGrpEagleNode	This table contains the associations between user groups and eagles
Tek_Secu_MapUsergrpCmdClass	This table contains the associations between user groups and eagle command classes
Tek_Secu_PasswordConfig	This table stores the password configuration.
Tek_Secu_UserInfo	This table contains the basic user information.
Tek_inventory_card	This table consists of entries for eagle cards.
Tek_inventory_eagleNode	This table consists of entries for eagle nodes.
Tek_inventory_frame	This table consists of entries for eagle frames.
Tek_inventory_shelf	This table consists of entries for eagle shelves.
Tek_inventory_slot	This table consists of entries for eagle slots.
tek_cmi_cmd_param_lookup	This table contains eagle command parameters whose values need to be looked up from a fixed set of values, maintained in this table.
tek_cmi_cmd_param_map	This table contains mapping between eagle commands and their parameters.
tek_cmi_cmd_param_validation	This table contains validation rules applicable on various command parameters.
tek_cmi_cmd_param_values	This table contains command parameter values.
tek_cmi_cmd_params	This table contains all command parameters.
tek_cmi_cmdclass_cmd_map	This table maps command classes to commands.
tek_cmi_cmdclasses	This table contains command classes.
tek_cmi_commands	This table contains command.
tek_lui_config_data	This table contains the thresh-holding values.
tek_lui_link_data	This table contains link data.

Table Name	Purpose
tek_lui_measurements	This table contains the state and utilization details for various entities.
tek_lui_slk_capacity	This table contains capacity data.
tek_lui_slk_capacity_arch	This is an archive table for capacity data.
tek_lui_slk_reptstatcard	This table contains parsed rept-stat-card output.
tek_scheduler_task	This table contains all the E5-MS tasks, and related attributes, scheduled by E5-MS scheduler interface.
tekelec_meas_headers	This table contains CSV file's header information.
tekelec_meas_reports	This table contains the number and type of supported reports.

Licensing

Failover in E5-MS is enabled via a valid E5-MS license only. Failover is FAK controlled, however MySQL replication cannot be controlled through licensing.

Both primary and standby servers will require separate licenses, as licenses are tied to the system's MAC address.

Limitations

1. Unlike MySQL data replication which synchronizes the Primary and Standby E5-MS servers every second, the conf file which are not present in MySQL table are synchronized every 1 hour (default configured BACKUP_INTERVAL is 3600 seconds). Note that the configuration file changes may not be as frequent. Once the configuration is set after the installation at the customer site, configuration change might be done rarely on need basis (once in many days). The configuration done in primary will be replicated in the standby after every hour. If configuration change was done in a conf file after last synchronization and failover happens due to a power failure (or any abrupt condition due to which conf file replication can't be ensured), the last configuration change will not be available in the standby server after standby takes over as the Primary server. Please note that most of the configuration file changes do not come into effect while server is up. So, in case of failover for any change in the configuration files to take effect, both the primary and standby servers should be restarted.

Note: The changes made in the primary server configuration files will be reflected to standby's configuration files once they are copied to the standby after the BACKUP_INTERVAL, or you can make the change manually at both the servers.

2. In case of failover, a pop-up for lost connection is shown on the client, which also shows that the client is trying to connect to the standby server. The jar file of the E5-MS server is required at the client's cache for the client to automatically connect to server. During first time failover, when the

client has not connected to the standby server even once, the jar file of secondary will not be present in client's cache. Hence the user has to manually connect to the new Active E5-MS server. Once the jars of Active and Standby servers are present in the Client cache, manual intervention will not be required any further. The client will automatically connect to the new active server after the failover/switchback.

3. In case of manual failover, when the Active server is manually stopped, if the stopped server is re-started before the standby server takes over as the new Active server, started server registers itself as the primary server and also de-registers the already registered standby server (the standby servers entry is removed from the BEFailover table). In such a case, failover will fail and the standby server will have to be manually stopped and then restarted, such that it registers with the primary server, again.
4. The Eagles would need to have the IP of the standby server configured as FTP server so that it continues to send measurement reports to the standby once the primary has gone down.
5. The SNMP-enabled EAGLE, EPAP, and LSMS would need to have the IP of both the primary and standby servers configured as SNMP hosts so that they are able to send traps to the standby server once the primary server goes down.
6. I-net Clear is a separate stand-alone installation and any I-net configuration data will not be available on the standby server and will have to be done manually.
7. In case of failed connectivity between primary and standby, the standby would be unable to read the last count of the primary and will assume the role of the primary while the primary will de-register the secondary and continue as primary. Manual intervention would be required to resolve this issue.
8. The clients, which are not logged in during failover, will have to manually connect to the new active server.
9. If the number of retry counts is configured as n in hibernate.cfg.xml files, E5-MS allows $n+1$ retries. As per WebNMS this behavior is by design. Also, E5-MS will try indefinitely to connect to the failed primary server, if the value is set to '0' or less.

Appendix D

E5-MS Database Password Change

Topics:

- [E5-MS Database Password Change for Standalone Server.....235](#)
- [E5-MS Database Password Change for Failover Setup.....236](#)

This appendix describes the process to change the E5-MS database password. The internal database is pre-configured with a password that you can change to prevent unauthorized access to the database from the command line. This appendix contains password change procedures for a standalone server and for a failover setup.

E5-MS Database Password Change for Standalone Server

This procedure describes how to change the E5-MS database password for a standalone server.

1. Shut down the E5-MS server:

```
service e5msService stop
```

2. Start MySQL by using `/Tekelec/WebNMS/bin/startMySQL.sh`:

```
sh startMySQL.sh
```

3. Update the MySQL root user's password by using following steps:

1. Log in to MySQL as the root user with its current password:

```
[root@e5ms-12 bin]# ./mysql -u root -p
Enter password:
Warning: Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 125
Server version: 5.6.18-enterprise-commercial-advanced-log MySQL Enterprise Server
 - Advanced Edition (Commercial)

Copyright (c) 2000, 2014, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective owners.
```

2. Set mysql as the database:

```
mysql> use mysql;
```

3. Set the new password for the root user and flush:

```
mysql> SET PASSWORD FOR 'root'@'localhost' = PASSWORD('hello');
Query OK, 0 rows affected (0.00 sec)
mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)
```

4. Commit the change and exit MySQL:

```
mysql> commit;
Query OK, 0 rows affected (0.00 sec)
mysql> exit
Bye
```

4. Stop MySQL by using `/Tekelec/WebNMS/bin/stopMySQL.sh`:

When prompted for the password, supply the new password set in step 3.

```
[root@e5ms-12 bin]# sh stopMySQL.sh
Enter Password:
STOPPING server from pid file /Tekelec/WebNMS/mysql/data/e5ms-12.pid
130910 00:45:26 mysqld ended
```

5. Execute the `/Tekelec/WebNMS/bin/E5MSConfigurationScript.sh` script to update the new MySQL root user's password in E5-MS:

```
# sh E5MSConfigurationScript.sh
Please enter E5-MS home path.(Absolute path till WebNMS directory)
/Tekelec/WebNMS/
Press 1 To update current system username and password in E5-MS
2 To update current mysql root user's password in E5-MS
3 To Exit
Your Choice (1, 2 or 3): 2
Enter new password for MySQL root user: hello
Do you want to proceed with the entered password? (y/n) y
MySQL Password updated successfully.
```

6. Start the E5-MS server:

```
service e5msService start
```

E5-MS Database Password Change for Failover Setup

To update the MySQL user's password for a failover setup, first stop replication, then update the MySQL root user's password, and then set up replication again between the servers. Use the following steps:

1. Stop database replication between the servers by using the following commands on both the primary and standby servers:

1. Log in to MySQL as the root user using its current password:

```
[root@e5ms-12 bin]# ./mysql -u root -p

Enter password:

Warning: Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 125
Server version: 5.6.18-enterprise-commercial-advanced-log MySQL Enterprise Server
- Advanced Edition (Commercial)

Copyright (c) 2000, 2014, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective owners.
```

2. STOP SLAVE;
3. RESET SLAVE;
4. QUIT

2. Shut down the standby server and then the primary server by using the following command:

```
# service e5msService stop
Stopping E5-MS server...
MySQL not stopped for failover
Done.
```

3. On each server, follow steps 3 to 5 in [E5-MS Database Password Change for Standalone Server](#) to update the MySQL root user's password.
4. Follow steps 18 to 25 in [How to Set Up Failover](#) to set up replication again between the two servers.
5. Start the primary server:

```
service e5msService start
```

6. Start the standby server:

```
service e5msService start
```

Appendix E

EPAP Support Messages

Topics:

- [Error/Informational Messages for EPAP Support.....239](#)

This appendix lists the error and informational messages for E5-MS support of EPAP.

Error/Informational Messages for EPAP Support

The error and informational messages for E5-MS support of EPAP are listed in [Table 24: Error/Informational Messages for EPAP Support](#). EPAP <A/B/' '> can be decoded as follows:

EPAP A	Used for messages referring to EPAP A configurations in the case of the PROV and Non PROV EPAP types
EPAP B	Used for messages referring to EPAP B configurations in the case of the PROV and Non PROV EPAP types
EPAP	Used for messages referring to EPAP configurations in the case of the PDB Only EPAP type

Table 24: Error/Informational Messages for EPAP Support

S No.	Error/Information Messages
1	EPAP <A/B/' '> name can contain only alphanumeric characters, hyphen and underscore!
2	EPAP <A/B/' '> name can contain a minimum of 5 and a maximum of 20 characters!
3	EPAP <A/B/' '> name must have an alphabet as its first character!
4	EPAP <A/B/' '> read community string is blank!
5	EPAP <A/B/' '> read community string length cannot exceed 20 characters!
6	EPAP <A/B/' '> IP address provided is invalid! Valid IP address format is '0-255.0-255.0-255.0-255'.
7	EPAP <A/B/' '> IP address is blank!
8	EPAP <A/B/' '> port number is blank!
9	EPAP <A/B/' '> port number can contain only numeric value between 0 and 65535!
10	EPAP <A/B/' '> login name can contain only alphanumeric characters, hyphen and underscore!
11	EPAP <A/B/' '> login name can contain a minimum of 5 and a maximum of 20 characters!
12	EPAP <A/B/' '> login name must have an alphabet as its first character!
13	EPAP <A/B/' '> login password string is blank!
14	EPAP <A/B/' '> login password string length cannot exceed 20 characters!
15	EPAP <A/B/' '> description field length cannot exceed 200 characters!
16	EPAP addition request has been sent to server. Please wait for status.
17	EPAP '<EPAP A IP>' discovery failed! Reason: <REASON>. Please resolve the issue and retry.
18	EPAP modification request has been sent to server. Please wait for status.
19	EPAP '<EPAP A IP >' modified by user '<USER NAME>'.

20	EPAP '<EPAP A IP >' added by user '<USER NAME>'.
21	EPAP '<EPAP A IP>' modification failed! Reason: <REASON>. Please resolve the issue and retry.
22	Both EPAP A and EPAP B status cannot be 'Active' simultaneously!
23	EPAP deletion request has been sent to server. Please wait for status.
24	EPAP '<EPAP A IP>' deleted by user '<USER NAME>'.
25	EPAP '<EPAP A IP>' deletion failed! Reason: <REASON>. Please resolve the issue and retry.
26	Provisioning, SNMP/SSH and Web IP address cannot be same in 'PDB Only' EPAP!
27	EPAP A and EPAP B IP address cannot be same in 'PROV' and 'Non PROV' EPAP!
28	Please fill up all mandatory fields before proceeding!
29	Alarm resynchronization initiated for EPAP: <EPAP name> by user: <USER NAME>!
30	Alarm resynchronization completed for EPAP: <EPAP NAME> initiated by user: <USER NAME>!
31	Alarm resynchronization failed for EPAP: <EPAP NAME> initiated by user: <USER NAME>! Reason: <REASON> Please resolve the issue and try again.
32	E5-MS cannot connect to EPAP: <EPAP NAME> for receiving alarms! Please check the connection.
33	Invalid selection for 'PDB Only' EPAP type!
34	EPAP added to E5-MS.
35	Received 'resyncRequiredTrap' from EPAP for alarm resynchronization.
36	Regaining connection.
37	Warm start of E5-MS server.
38	Automatic alarm resynchronization completed for EPAP <EPAP NAME>.
39	Automatic alarm resynchronization failed for EPAP! Reason: <REASON> Please resolve the issue and try again.
40	Automatic alarm resynchronization failed for EPAP: <EPAP NAME>! Reason: <REASON> Please resolve the issue and try again.
41	Buffer overflows during southbound resynchronization for EPAP: <EPAP NAME>! This could result in loss of alarms.
42	EPAP '<EPAP A IP>' modification failed! Reason: No field was changed during modification operation. Please resolve the issue and retry.
43	EPAP <A/B/' '> write community string is blank!
44	EPAP <A/B/' '> write community string length cannot exceed 20 characters!
45	EPAP <SNMP/SSH or Provisioning or Web> IP address provided is invalid! Valid IP address format is '0-255.0-255.0-255.0-255'.

46	EPAP <SNMP/SSH or Provisioning or Web> IP address is blank!
----	---

▶Fault Management GUI Custom Views◀

Topics:

- *Working with Custom Views.....243*
- *Filter Field Descriptions for Network Events Custom View.....260*
- *Filter Field Descriptions for Alarms Custom View.....261*
- *Tips and Tricks for Using Custom Views.....264*

▶ This appendix describes the use of custom views for events/alarms in the Fault Management GUI.◀

▶ Working with Custom Views ◀

▶ The events/alarms in the Network Events/Alarms view can be numerous and make it difficult to identify events/alarms of interest. A search can be performed to locate particular events/alarms, but when a lot of events/alarms satisfy a certain set of criteria, it can be helpful to create a *Custom View*. A custom view specifies filter criteria that result in the display of only the subset of events/alarms that meet the specified filter criteria, eliminating the need to perform a search every time. ◀

▶ Custom views, once created, continue to be updated and navigable for additions/deletions of events/alarms based on the filter criteria until the client is closed. The user can either save views or remove them. ◀

▶ Adding a New Custom View ◀

▶ This procedure describes how to add/create a custom view for events/alarms by specifying the desired filtering criteria and providing a name for the view. Multiple custom views can be created to display a variety of information.

To add a new custom view, perform following steps:



1. Click on the Network Events or Alarms node in the left navigation pane.
2. Use either of the following two methods to create a custom view:
 - From the **Custom Views** menu in the top menu bar, choose **Add Custom View** as shown in [Figure 102: Add Custom View By Using Menu Bar](#).

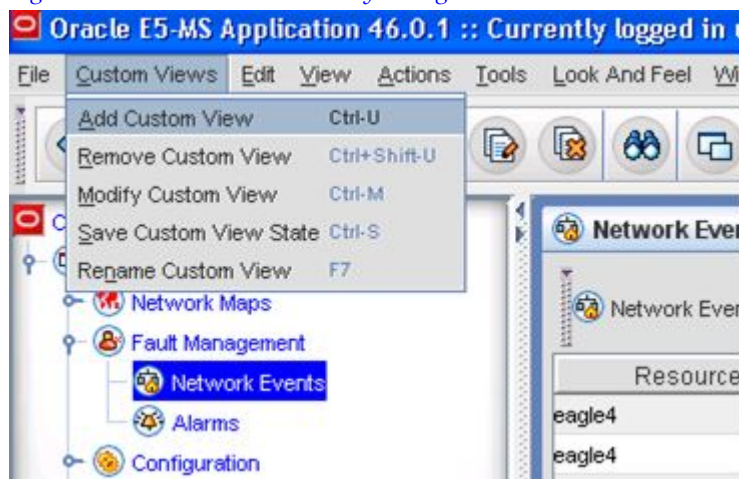


Figure 102: Add Custom View By Using Menu Bar

- Right-click on the node (Network Events or Alarms) in the left navigation pane, and choose **Custom Views > Add Custom View** as shown in [Figure 103: Add Custom View By Using Left Navigation Pane](#).

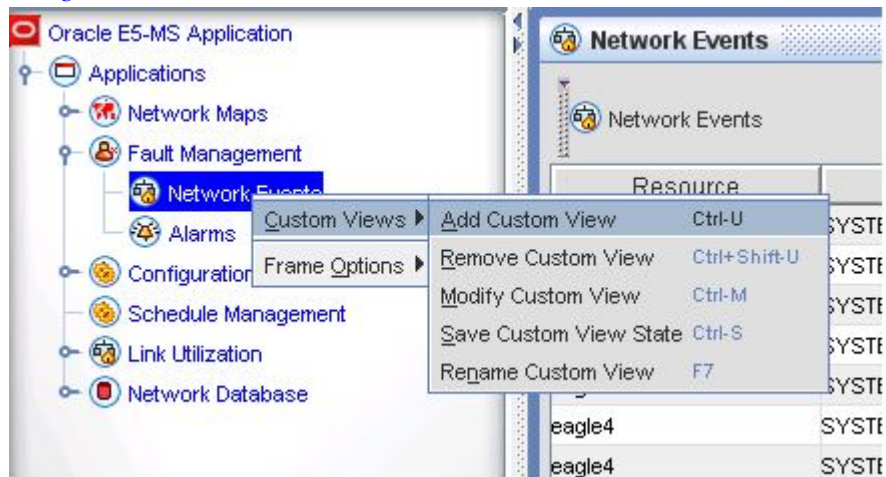


Figure 103: Add Custom View By Using Left Navigation Pane

If the Network Events node was selected, then a **Show object with these Properties** dialog box with the title **Specify Event Filter Criteria** is displayed, as shown in [Figure 104: Specify Event Filter Criteria](#). If the Alarms node was selected, then a **Show object with these Properties** dialog box with the title **Specify alarm filter criteria** is displayed, as shown in [Figure 105: Specify Alarm Filter Criteria](#).

Show objects with these Properties

Specify Event Filter Criteria

Properties | Tree Node Properties

Filter View Name: Network Events0

ParentName: Network Events

Severity: all

Message:

Category:

Network:

Node:

Entity:

Resource:

Sub-Resource:

Protocol:

UAM/UIM/MRN Number:

From Date/Time (E5-MS Timestamp): , : : .

To Date/Time (E5-MS Timestamp): , : : .

From Date/Time (Device Time Stamp): , : : .

To Date/Time (Device Time Stamp): , : : .

Event Age: Any Time

Select Props To View | Additional Criteria

Apply Filter | Close | Help

Figure 104: Specify Event Filter Criteria

Show objects with these properties [X]

Specify alarm filter criteria

Filter View Name: Alarms0

Parent name: Alarms

Severity: all

Previous severity: all

Owner: []

Category: []

Group: []

Message: []

Entity: []

Resource: []

Sub-Resource: []

Protocol: []

UAM/UM/MRN Number: []

From Date/Time (E5-MS Timestamp): [] [] [] [] [] [] [] [] [] []

To Date/Time (E5-MS Timestamp): [] [] [] [] [] [] [] [] [] []

From Date/Time (created): [] [] [] [] [] [] [] [] [] []

To Date/Time (created): [] [] [] [] [] [] [] [] [] []

From Date/Time (Device Time Stamp): [] [] [] [] [] [] [] [] [] []

To Date/Time (Device Time Stamp): [] [] [] [] [] [] [] [] [] []

From Date/Time (Acknowledgement Time): [] [] [] [] [] [] [] [] [] []

To Date/Time (Acknowledgement Time): [] [] [] [] [] [] [] [] [] []

GroupViewMode: none

Alarm age (modified time): Any [] [] Time

[Select props to view] [Additional criteria]

[Apply filter] [Close] [Help]

Figure 105: Specify Alarm Filter Criteria

- Specify the custom view name in the **Filter View Name** field and the match criteria to be used to filter the data in the **Properties** pane.

One or more filter fields can be specified; if more than one field is specified, then an AND operation is applied on the fields. For a description of the various fields available in this window, see [Filter Field Descriptions for Network Events Custom View](#) and [Filter Field Descriptions for Alarms Custom View](#).

- Optionally, select the fields (columns) that should be visible in the resulting custom view.

To perform this step, see [Controlling the Fields Displayed In a Custom View](#). This step can be skipped if no changes to the default visible fields (columns) are needed.

- Click **Apply Filter**.

The custom view is created with the name specified. A new node is shown under the Network Events/Alarms node in the left navigation pane, and the custom view shows the events/alarms as per the user-specified filter criteria (see [Figure 106: Custom View for Network Events](#) and [Figure 107: Custom View for Alarms](#)).

Resource	Severity	Message
eagle4	Critical	[R] DEIR ...
eagle4	Critical	[R] MPS ...
eagle4	Critical	[R] MPS ...
eagle4	Critical	[R] SCCP...
eagle4	Critical	[R] Node ...
eagle4	Critical	[R] DPC i...
eagle4	Critical	[R] DPC i...
eagle4	Critical	[R] DPC i...
eagle4	Critical	[R] DPC i...
eagle4	Critical	[R] DPC i...
eagle4	Critical	[R] DPC i...
eagle4	Critical	[R] DPC i...
eagle4	Critical	[R] DPC i...
eagle4	Critical	[R] DPC i...

Figure 106: Custom View for Network Events

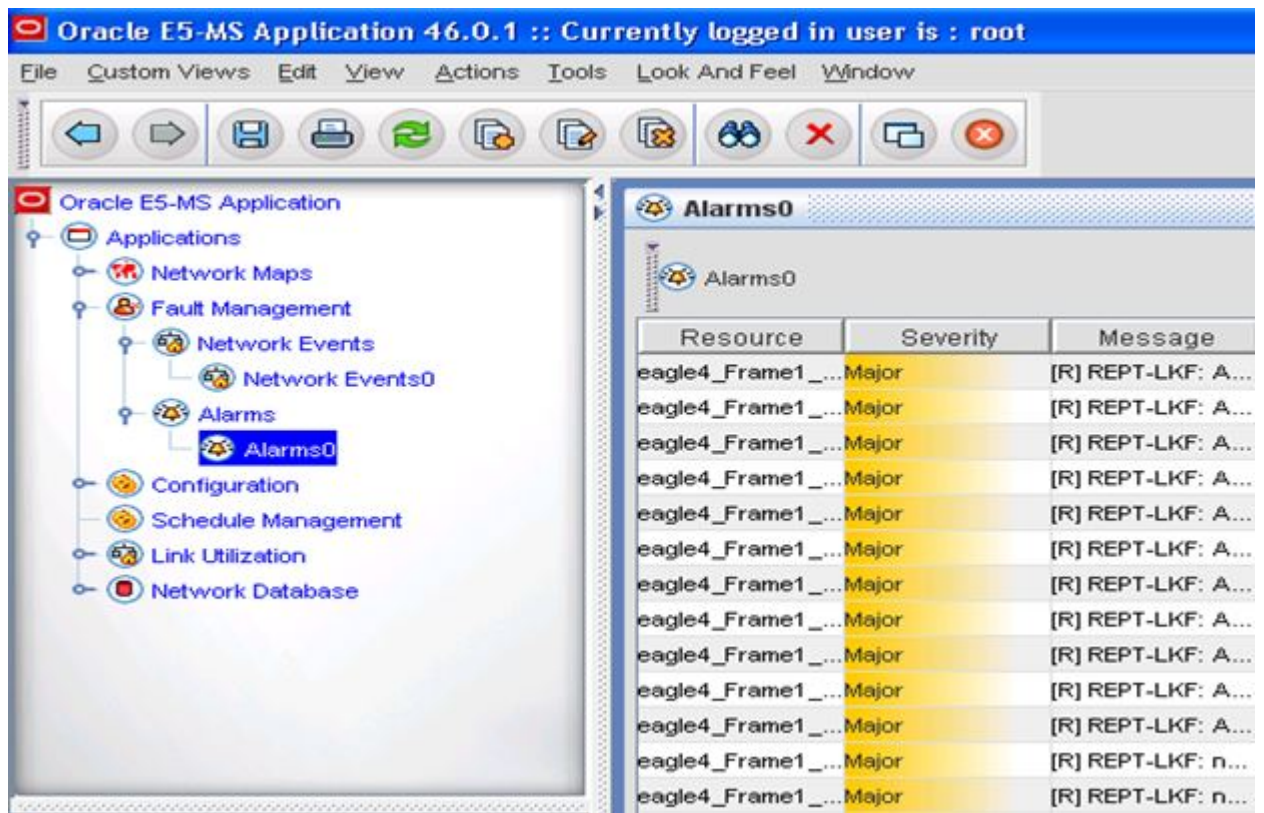


Figure 107: Custom View for Alarms

Note:

Child views can be created under a parent node. For example, a custom view named *Master* (parent node) might show only events/alarms that are in *Major* status, and under this *Master* view the user can create child views, such as *M1* and *M2*. *M1* and *M2* can each have a different set of criteria, such as only events/alarms from particular EAGLE nodes. Deleting the *Master* view will delete all the child views under it.



► Modifying a Custom View ◀

► This procedure describes how to modify a previously created custom view to expand or limit the information displayed in the custom view.

To modify an existing custom view, perform following steps:



1. Click on the custom view node under the Network Events or Alarms node in the left navigation pane.

2. Perform either of the following two procedures to modify the custom view:

- From the **Custom Views** menu in the top menu bar, choose **Modify Custom View** as shown in [Figure 108: Modify Custom View By Using Menu Bar](#).

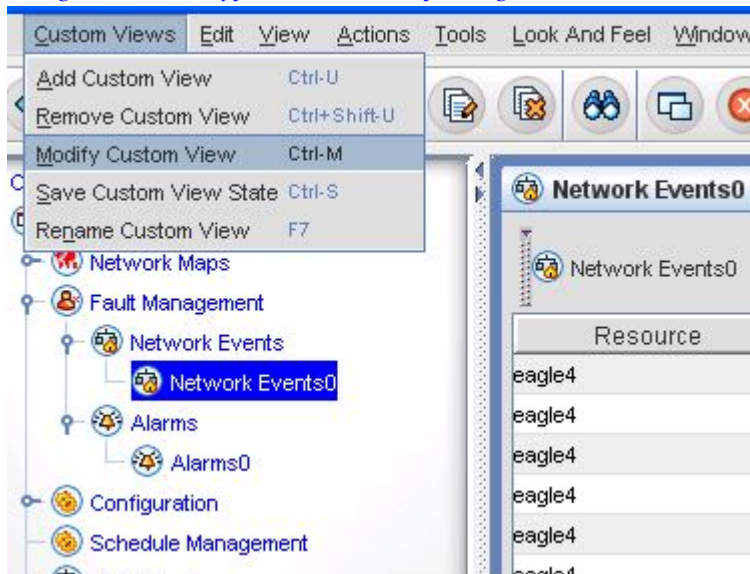


Figure 108: Modify Custom View By Using Menu Bar

- Right-click on the custom view node under the Network Events or Alarms node in the left navigation pane, and choose **Custom Views > Modify Custom View** as shown in [Figure 109: Modify Custom View By Using Left Navigation Pane](#).

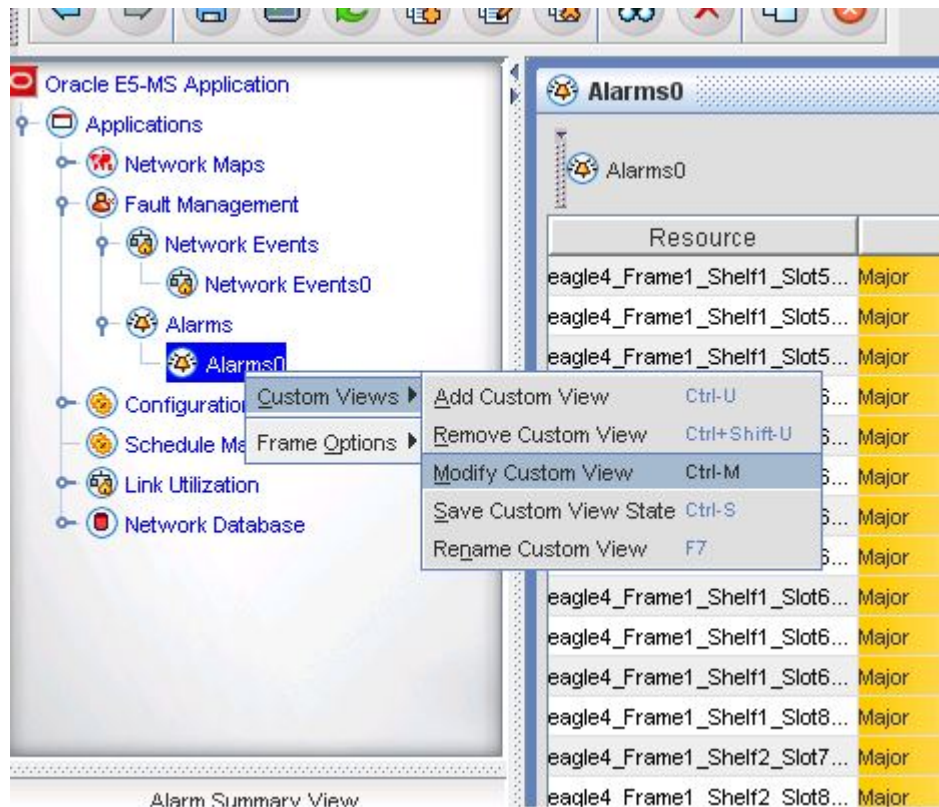


Figure 109: Modify Custom View By Using Left Navigation Pane

Depending upon whether the custom view is an events/alarms view, the corresponding **Show object with these Properties** dialog box with title "Specify Event Filter Criteria" or "Specify alarm filter criteria" is displayed.

- Follow steps 3 to 5 in *Adding a New Custom View* to modify the custom view as required.



▶ Saving a Custom View ◀

▶ This procedure describes how to save the current state of the custom view, such as the order of the columns, the sorted alarms, and the first and the last viewed alarms.

To save an existing custom view, perform the following steps:



- Click on the custom view node under Network Events/Alarms node in the left navigation pane.
- Perform either of the following two procedures to save the custom view:
 - From the **Custom Views** menu in the top menu bar, choose **Save Custom View State** as shown in *Figure 110: Saving Custom View By Using Menu Bar*.

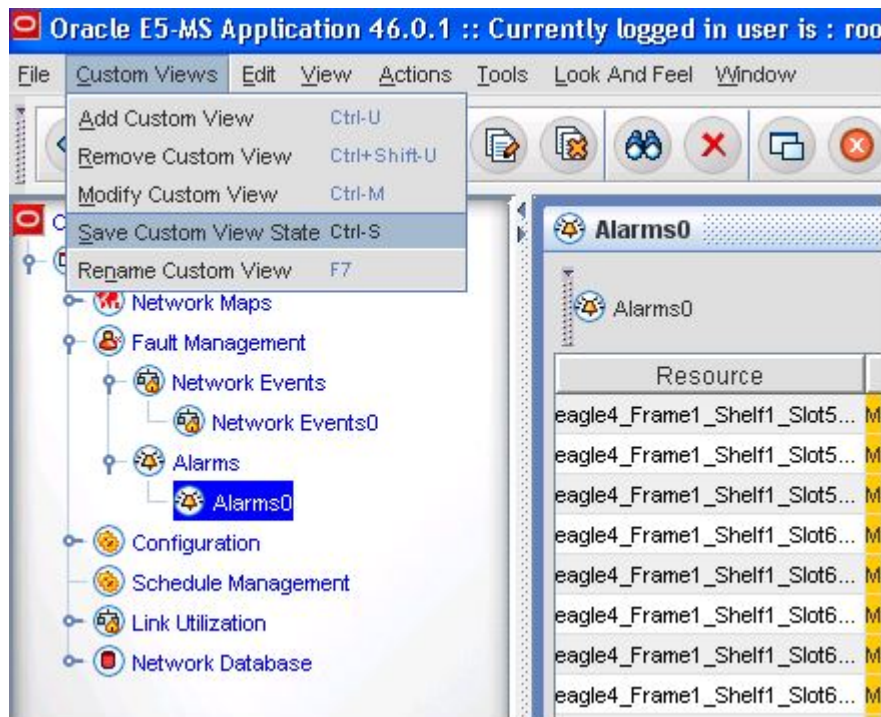


Figure 110: Saving Custom View By Using Menu Bar

- Right-click on the custom view node under the Network Events or Alarms node in the left navigation pane, and choose **Custom Views > Save Custom View State** as shown in [Figure 111: Saving Custom View By Using Left Navigation Pane](#).

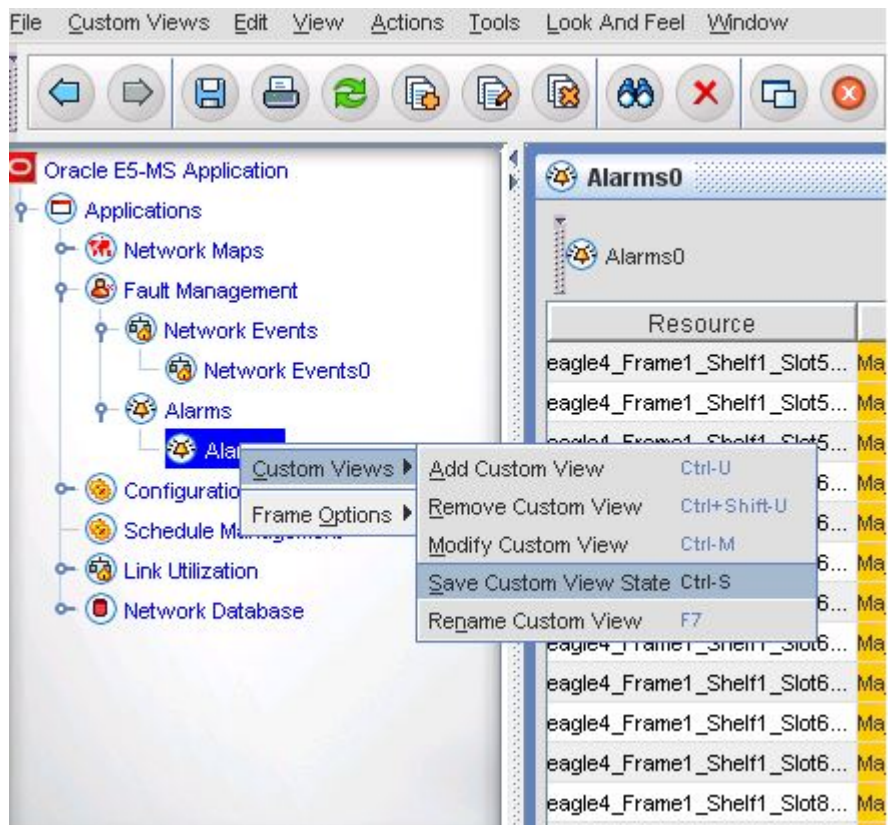


Figure 111: Saving Custom View By Using Left Navigation Pane



A message that the custom view has been saved is displayed in the status bar at the bottom left side on the GUI, as shown in *Figure 112: Custom View Saved Successfully*.



Figure 112: Custom View Saved Successfully



▶Deleting a Custom View◀

- ▶ This procedure describes how to delete an existing custom view.

Perform the following steps to delete a custom view:



1. Click on the custom view node under the Network Events or Alarms node in the left navigation pane.
2. Perform either of the following two procedures to delete the custom view:
 - From the **Custom Views** menu in the top menu bar, choose **Remove Custom View** as shown in *Figure 113: Deleting a Custom View By Using Menu Bar*.

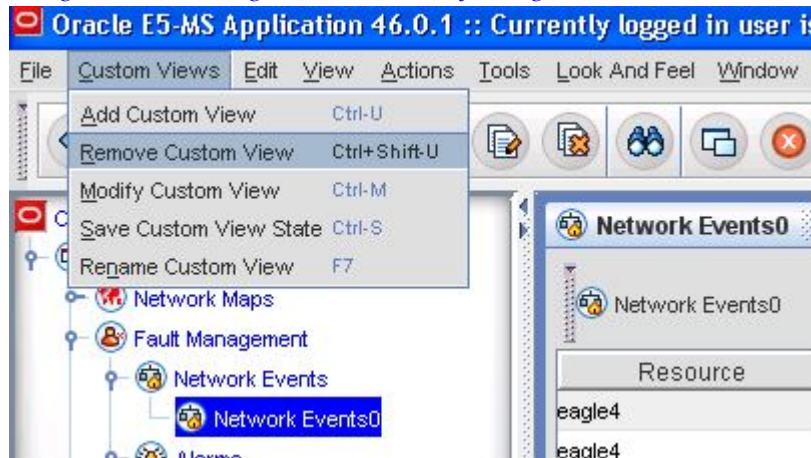


Figure 113: Deleting a Custom View By Using Menu Bar

- Right-click on the custom view node under the Network Events/Alarms node in the left navigation pane, and choose **Custom Views > Remove Custom View** as shown in *Figure 114: Deleting a Custom View By Using Left Navigation Pane*.

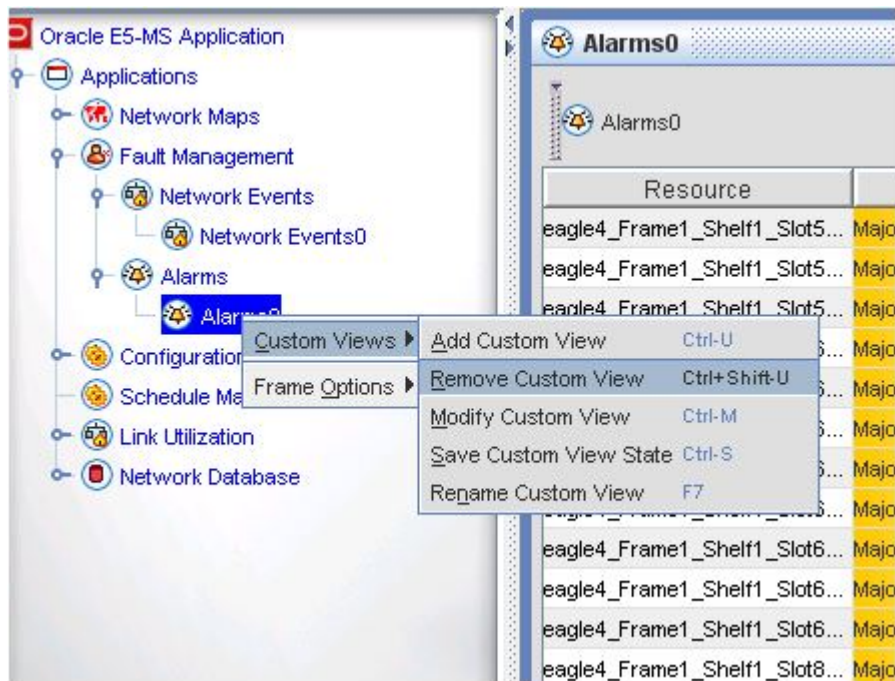


Figure 114: Deleting a Custom View By Using Left Navigation Pane

3. Click **Yes** in the confirmation box to delete the custom view.

Note:

Deleting a parent custom view also deletes any child custom views added under the parent view (as described in [Adding a New Custom View](#)).



▶ Renaming a Custom View ◀

- ▶ This procedure describes how to rename an existing custom view.

Perform the following steps to rename a custom view:



1. Click on the custom view node under the Network Events or Alarms node in the left navigation pane.
2. Perform either of the following two procedures to rename the custom view:
 - From the **Custom Views** menu in the top menu bar, choose **Rename Custom View** as shown in [Figure 115: Rename a Custom View By Using Menu Bar](#).

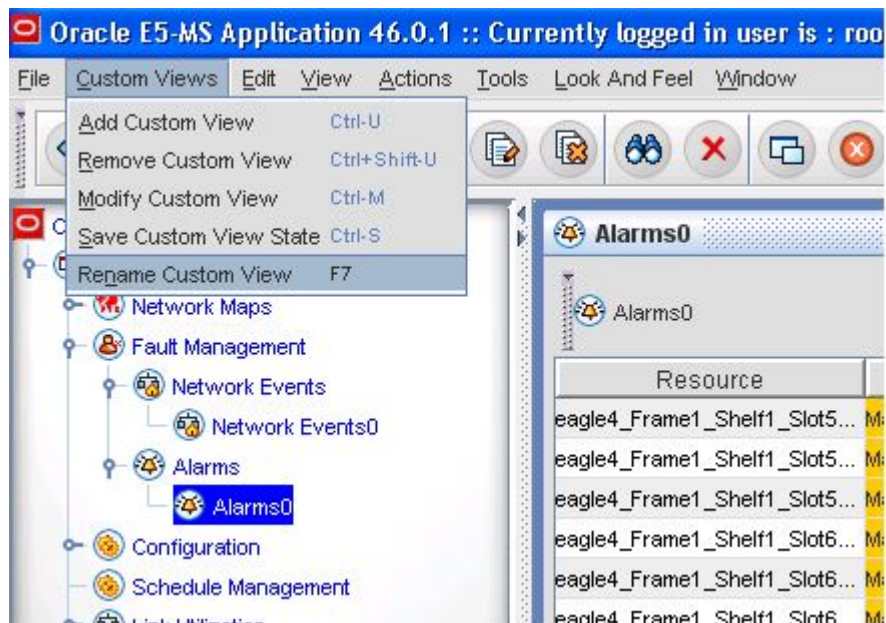


Figure 115: Rename a Custom View By Using Menu Bar

- Right-click on the custom view node under the Network Events/Alarms node in the left navigation pane, and choose **Custom Views > Rename Custom View** as shown in [Figure 116: Rename a Custom View By Using Left Navigation Pane](#).

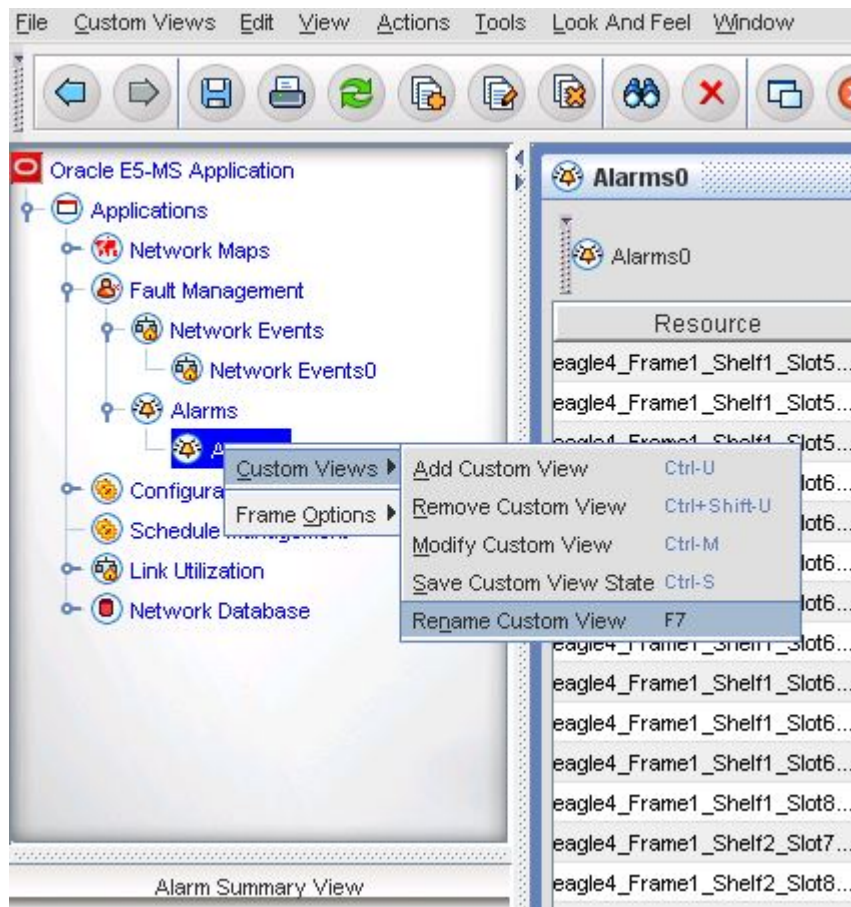


Figure 116: Rename a Custom View By Using Left Navigation Pane

3. Type the new name for custom view as shown in [Figure 117: Entering a New Name for a Custom View](#), and press **Enter**.

Note: To retain the existing name and not proceed with renaming, press the **Esc** key.

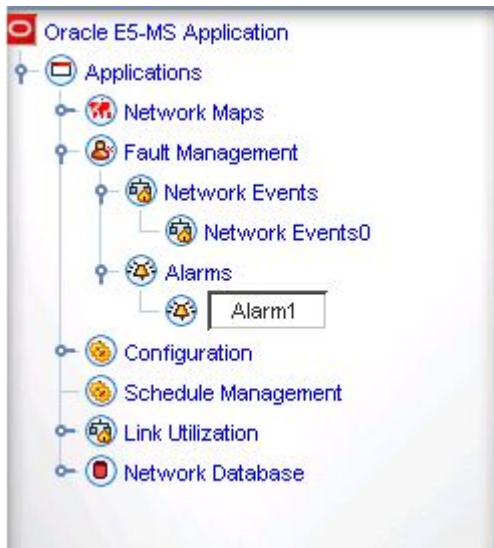


Figure 117: Entering a New Name for a Custom View



▶ Controlling the Fields Displayed In a Custom View ◀

▶ This procedure describes how to control which fields should be displayed in a custom view.

Perform the following steps:



1. During custom view creation/modification, on the **Show object with these Properties** dialog box shown in [Figure 104: Specify Event Filter Criteria](#) and [Figure 105: Specify Alarm Filter Criteria](#), click the **Select Props To View** button.

The **Select Table Columns** dialog box is displayed, as shown in [Figure 118: Selecting Table Columns for Network Events](#) and [Figure 119: Selecting Table Columns for Alarms](#). The selected fields are the columns that can be seen in the resulting custom view.

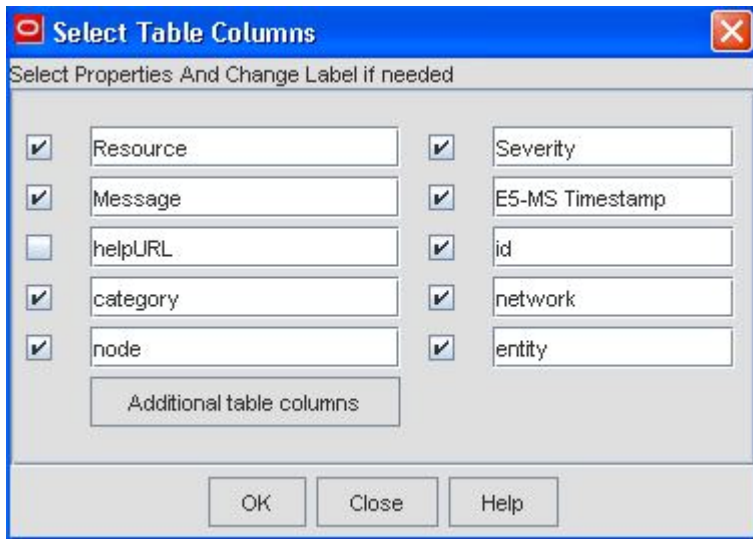


Figure 118: Selecting Table Columns for Network Events

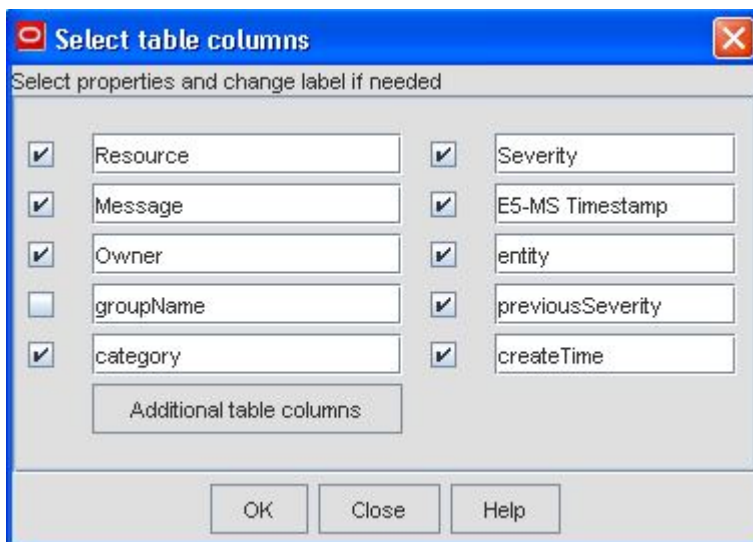


Figure 119: Selecting Table Columns for Alarms

2. Select the columns to display or hide as follows:
 - To display a column, check the check box next to the column name.
 - To hide a column, clear the check box next to the column name.
3. To view additional table columns, click the **Additional table columns** button shown in *Figure 118: Selecting Table Columns for Network Events* and *Figure 119: Selecting Table Columns for Alarms*.

The **User defined table columns** dialog box is displayed, as shown in *Figure 120: Specifying Additional Table Columns for Network Events* and *Figure 121: Specifying Additional Table Columns for Alarms*.

Display Name	Property Name
X UAM/UIM/MRN Number	eventid
X Device Time Stamp	deviceTimeStamp
X Sub-Resource	subresource
X Protocol	protocol

Figure 120: Specifying Additional Table Columns for Network Events

Display Name	Property Name
X UAM/UIM/MRN Number	alarmid
X Count	count
X Acknowledgement Time	AckDate
X Device Time Stamp	deviceTimeStamp
X Sub-Resource	subresource
X Protocol	protocol

Figure 121: Specifying Additional Table Columns for Alarms

4. Enter the display name and corresponding property name in the **Display Name** and **Property Name** fields exactly as shown in *Figure 120: Specifying Additional Table Columns for Network Events* and *Figure 121: Specifying Additional Table Columns for Alarms*.
5. Click **OK** on the **User defined table columns** dialog box.
6. Click **OK** in the **Select Props To View** dialog box.



► Filter Field Descriptions for Network Events Custom View ◀



S. No.	Property	Description
1.	Filter View Name	Specify the name for the custom view being created or modified. If no value is specified in this field, the custom views are created with default values, such as Network Events0, Network Events1, and Network Events2.
2.	Parent Name	Use the drop-down box to choose the parent tree node under which the custom view should be placed. The criteria set for the parent custom view are automatically used for the child custom view, so only additional criteria for the child custom view must be specified.
3.	Severity	From the editable drop-down box, choose the event severity on which events are to be filtered in the custom view. For multiple severities, type the severity values separated by a comma (for example: Major, Info).
4.	Message	Specify all or part of a message associated with the events that you want to view.
5	Category	Specify the category of the events that you want to view (for example: EAGLE, EPAP, and so on).
6	Network	-
7	Node	-
8	Entity	Specify the name of the failed entity (that is primarily responsible for the event) on which events are to be filtered. Note: To create a filter for an entity value that includes a comma (,), create the filter using an asterisk in place of the comma. A filter created with the comma will not work.
9	Resource	Specify the resource of the event on which events are to be filtered.
10	Sub-resource	Specify the sub-resource of the event on which events are to be filtered. Note: To create a filter for a sub-resource value that includes a comma (,), create the filter using an asterisk in place of the comma. A filter created with the comma will not work.
11	Protocol	Specify the protocol of the event on which events are to be filtered.
12	UAM/UIM/MRN Number	Specify the event ID of the event on which events are to be filtered. Note: To filter based on an event ID that begins with zero, do not include the leading zero. A filter that includes the leading zero will not work.
13	From Date/Time (E5-MS Timestamp)	Events that occur after the time specified in this ModTime (modified time) field [Month, Date, Year, Hour, Min, Sec, AM/PM] are displayed in the custom view.

14	To Date (E5-MS Timestamp)	Events that occur up to the time specified in this ModTime (modified time) field [Month, Date, Year, Hour, Min, Sec, AM/PM] are displayed in the custom view.
15	Event Age	<p>Specify the age of the event on which events are to be filtered. The age of an event denotes the time elapsed since the last modification of the event in the E5-MS system.</p> <p>By default, the value specified is Any, whereby events of all ages are displayed.</p> <p>Other options are minutes, hours, days, today, and yesterday.</p> <p>Example:</p> <p>Age in hrs > 1 displays all the events that are more than an hour old. After this custom view is created, the events are dynamically added to the view as they satisfy the criteria of being more than an hour old. Set the minutes in which the custom view should be refreshed in Refresh period in minutes (by default, it is set as 1 minute). After setting the refresh period, the server sends data automatically at the time interval specified.</p>



► Filter Field Descriptions for Alarms Custom View ◀



S. No.	Property	Description
1.	Filter View Name	Specify the name for the custom view being created or modified. If no value is specified in this field, default values such as Alarms0, Alarms1, and Alarms2 are used.
2.	Parent Name	<p>Use the drop-down box to choose the parent tree node under which the custom view should be placed.</p> <p>The criteria set for the parent custom view are automatically used for the child custom view, so only additional criteria for the child custom view must be specified.</p>
3.	Severity	<p>From the editable drop-down box, choose the severity on which alarms are to be filtered in the custom view.</p> <p>Tip: For multiple severities, type the severity values separated by a comma (for example: Major, Minor).</p>

4.	Previous severity	Use the editable drop-down box to choose the previous severity of the alarms to be viewed. For example, to view alarms that were previously minor and then became critical, select Minor in this field. Tip: For multiple severities, type the severity values separated by a comma (for example: Major, Minor).
5.	Owner	Specify the name of the owner with which the alarm is associated. Tip: To create a custom view for alarms that are unowned by any user, set the value as null. For multiple owners, specify owner names separated by a comma. Example: If the value is set as root , then only the alarms owned by root are displayed in the custom view.
6.	Category	Specify the category of the alarms to be viewed. For example, EAGLE, EPAP.
7.	Group	-
8.	Message	Specify all or part of a message associated with the alarms you want to view in the custom view. Example: If the message is specified as <i>Node Clear.</i> , then only alarms with this message are displayed in the custom view.
9.	Entity	Specify the name of the failed entity (that is primarily responsible for the alarm) on which alarms are to be filtered. Note: To create a filter for an entity value that includes a comma (,), create the filter using an asterisk in place of the comma. A filter created with the comma will not work.
10.	Resource	Specify the resource of the alarm on which alarms are to be filtered.
11.	Sub-resource	Specify the sub-resource of the alarm on which alarms are to be filtered. Note: To create a filter for a sub-resource value that includes a comma (,), create the filter using an asterisk in place of the comma. A filter created with the comma will not work.
12.	Protocol	Specify the protocol of the alarm on which alarms are to be filtered.
11.	UAM/UIM/MRN Number	Specify the alert ID of the alarm on which alarms are to be filtered. Note: To filter based on an ID that begins with zero, do not include the leading zero. A filter that includes the leading zero will not work.
12.	From Date/Time (E5-MS Timestamp)	The alarms modified after the time specified in this field [Month, Date, Year, Hour, Min, Sec, AM/PM] are displayed in the custom view.
13.	To Date/Time (E5-MS Timestamp)	The alarms modified up to the time specified in this field [Month, Date, Year, Hour, Min, Sec, AM/PM] are displayed in the custom view.

14.	From Date/Time (created)	The alarms generated after the time specified in this field [Month, Date, Year, Hour, Min, Sec, AM/PM] are displayed in the custom view.
15.	To Date/Time (created)	The alarms generated up to the time specified in this field [Month, Date, Year, Hour, Min, Sec, AM/PM] are displayed in the custom view.
16.	From Date/Time (Device Time Stamp)	The alarms generated after the time specified in this field [Month, Date, Year, Hour, Min, Sec, AM/PM] are displayed in the custom view.
17.	To Date/Time (Device Time Stamp)	The alarms generated up to the time specified in this field [Month, Date, Year, Hour, Min, Sec, AM/PM] are displayed in the custom view.
18.	From Date/Time (Acknowledgment Time)	The alarms acknowledged after the time specified in this field [Month, Date, Year, Hour, Min, Sec, AM/PM] are displayed in the custom view.
19.	To Date/Time (Acknowledgment Time)	The alarms acknowledged up to the time specified in this field [Month, Date, Year, Hour, Min, Sec, AM/PM] are displayed in the custom view.
20.	GroupViewMode	<p>From the drop-down box, choose the mode used to group the alarms in the custom view.</p> <p>max Alarms of maximum severity are grouped and displayed at the beginning of the list.</p> <p>latest The newest alarms are grouped and displayed at the beginning of the list.</p> <p>none The alarms are not grouped.</p>
21.	Alarm Age (modified time)	<p>Specify the age of the alarm on which alarms are to be filtered. Age of an alarm denotes the time elapsed since the last modification of the alarm in the E5-MS system.</p> <p>By default, the value specified is Any, whereby alarms of all ages are displayed.</p> <p>Other options are minutes, hours, days, today, and yesterday.</p> <p>Example: Age in hrs > 1 displays all the alarms that are more than an hour old. After this custom view is created, the alarms are dynamically added to the view as they satisfy the criteria of being more than an hour old. Set the minutes in which the custom view should be refreshed in Refresh period in minutes (by default, the refresh period is set as 1 minute). After setting the refresh period, the server sends data automatically at the time interval specified.</p>



► Tips and Tricks for Using Custom Views ◀

► Following are some tips to effectively use custom views: ◀



- E5-MS custom views support the AND operation when multiple fields are selected. Completing more fields results in a more limited and refined view.
- While adding a custom view, most of the properties listed are string-based properties. Additionally, Boolean properties are provided in drop-down boxes with the values **all**, **true**, and **false**. Choosing **all** results in the property not being taken into consideration. Selecting **true** or **false** results in the self-explanatory behavior.
- For string-based properties, the string value is absolutely matched. For example, the string **ENET** matches the exact word only.
- Status, Severity, etc. are also treated as strings. Hence, for a filter of Alarms with severity **critical**, simply specify '**crit***'.
- In Network Events and Alarms views, filtering based on time can be done by specifying the starting time and the ending time. The format in which the time is to be specified is as follows:

```
MON DD,YYYY HH:MM:SS AM/PM
```

For example:

```
Mar 27,2014 12:24:12 AM
```

- It is advisable to leave the fields blank that are not a necessary part of the filtering criteria.
- **Wildcard characters** can be used for effective filtering. The following table provides the wildcard characters that can be used.

Wildcard Character	Description
* (asterisk)	An asterisk is used to match zero or more characters. Examples: <ul style="list-style-type: none"> • To view all objects with names that start with test, specify the criterion as test*. • To view all objects that end with com, specify as *com.
! (exclamation mark)	An exclamation mark filters the search using the NOT operator. Examples: <ul style="list-style-type: none"> • To view all objects with names that do not start with test, specify the criterion as !test*. • To view all alarms except alarms with <i>Critical</i> and <i>Major</i> severity, specify as !war*, !cle* or !warning, !clear.
, (comma)	A comma is used for specifying multiple criteria for the same property. Example: To view objects named nms-server1 , nms-server2 , and nms-server3 , specify nms-server1,nms-server2,nms-server3 .

&& (two ampersands)	<p>Two ampersands are used when a single value should be matched with many patterns.</p> <p>Example: If all the objects with names starting with abc and ending with xyz are required, specify abc*&&*xyz*.</p>
<between> "value1" and "value2"	<p>This notation is used to retrieve objects with numeric values within a specific range.</p> <p>Example:</p> <p>To retrieve object names with a poll interval value ranging from 300 to 305, specify <between> 300 and 305.</p> <p>Note that the first number is smaller than the second number. Only the values in between the given values, including the limits, will be matched.</p>



E

EPAP EAGLE Provisioning Application Processor

F

FTP File Transfer Protocol
A client-server protocol that allows a user on one computer to transfer files to and from another computer over a TCP/IP network.
Feature Test Plan

G

GUI Graphical User Interface
The term given to that set of items and facilities which provide the user with a graphic means for manipulating screen data rather than being limited to character based commands.

L

LSMS Local Service Management System
An interface between the Number Portability Administration Center (NPAC) and the LNP service databases. The LSMS receives LNP data from the NPAC and downloads that data to the service databases. LNP data can be entered into the LSMS database. The data can then be downloaded to the LNP service databases and to the NPAC.

S

STP Signal Transfer Point

S

The STP is a special high-speed switch for signaling messages in SS7 networks. The STP routes core INAP communication between the Service Switching Point (SSP) and the Service Control Point (SCP) over the network.

Spanning Tree Protocol