Oracle® Communications EAGLE Element Management System

Interface User's Guide

Release 47.0
F96529-06
October 2025

Oracle Communications EAGLE Element Management System Interface User's Guide, Release 47.0

F96529-06

Contents

5 EAGLE Discovery Application

6 OCEEMS Support of EPAP Alarms via SNMP Feed

11 Configuration Management Interface

12 Link Utilization Interface

13 Northbound Interface (NBI)

A Decoupling OCEEMS from EAGLE

B OCEEMS System Administration

C OCEEMS Backup and Restore

D OCEEMS Failover

What’s New in This Guide

This section introduces the documentation updates for Release 47.0 in Oracle Communications EAGLE Element Management System Interface User's Guide.

Release 47.0 - F96529-06 - October 2025

There are no updates in this document for this release.

Release 47.0 - F96529-05 - September 2025

There are no updates in this document for this release.

Release 47.0 - F96529-03 - February 2025

- Added a note about the steps to be performed during the upgrade procedure in the How to Restore from Existing Backup section.
- Added a note about auto/manual resynchronization in the Resynchronization Mechanism section.
- Added the Configuring LDAP Client on EMS 47.0 section to list the steps to configure the LDAP client.

Release 47.0 - F96529-02 - September 2024

- Updated the information about EMS's compatibility with RHEL 8.x in the Hardware and Software Requirements section.

Release 47.0 - F96529-01 - June 2024

- Updated the release version to 47.0 in the entire document.
- Added Appendix I to add the following general procedures:
  - PDF Download Error from Reporting Studio: Network Error/Internet Connection Error
  - Truncated field shown in Reporting Studio Reports
  - Prune Binary Log Procedure
  - How to use savelogs in EMS
  - SSH Server CBC Mode Ciphers Enabled
  - Null is passed for a clisession is observed in the inventory logs
  - rsyslog configuration for transfer of system log files to remote server
- Added the Appendix Transport Exception while launching Application(.jnlp) to list the steps to be performed when a transport exception is observed while launching .jnlp application.
- Added a note about the testing of OCEEMS 47.x with OpenWebStart version 1.9 in the OCEEMS Login section.
- Removed the `REPT-STAT-IPTPS` command from the Polling Scripts Creation section as the polling script now consists of two EAGLE commands that run on the EAGLE to fetch link capacity data instead of three.
- Updated the information about Pause (10) function used in Edit Script Pane.
- Updated the overview in the OCEEMS Backup and Restore section to add the example of system administrator.

- Updated the note about modifying the content of files or directories to be backed up to ensure that the upgrade process does not get impacted in the Backup Contents section.
- Added the example of system user in the Manual Backup section.
- Updated the command to take manual backup of OCEEMS for the default backup location `/var/backup` in the Manual backup on the default location section.
- Replaced the backup script and its example in the Manual backup on a desired location section.
- Added the example for the system user name in the Manual backup on a desired location section.
- Updated the command for manual backup in the Output while running Manual Backup section in Manual backup on a desired location.
- Updated the command for restoring from backup in the Output while Restoring from a Backup section in Manual backup on a desired location.
- Added the example for system user name in the Manual backup on a desired location section.
- Updated the command for restoring from the default location in the Restoring from the default/any backup location section.
- Updated the i-net version to 23.x and the command to check if i-net 23.x is installed in the Checking if i-net 23.x is Installed section:
- Updated the i-net version to 23.x and the commands to start the i-net 23.x service in the Starting the i-net 23.x Service section.
- Updated the Hardware and Software Requirements section with the following:
  - Updated the SUN Netra Server X3-2 version 7.0 to 8.8
  - Updated the HP Gen8 version 7.0 to 8.8
  - Updated the information about the web browsers for the OCEEMS client
- Updated the Java version from 1.8 to 17 in the entire document
- Updated the Tools Submenu image in the Toolbar Icons section.
- Updated the Alarm Summary View image in the Alarm Summary View section.
- Updated the EAGLE Discovery Screen and EAGLE Discovery Screen for Existing Eagle(s) in the Discovery GUI section.
- Updated the EAGLE Discovery Example screen in the Sample Configuration Data for SNMP Connection to EAGLE section.
- Updated the Shelf View image and the information about the Shelf View in the Map Views section.
- Added the note about the manual refresh of the shelf terminal view in the Map Views section.
- Updated the Configure SNMP Agent Community screen and step 4 in the Sample Configuration Data for SNMP Connection to EPAP section.
- Updated the Send Command Search and Script Execution Result Screen screens in the Script Management section.
- Updated the steps to install the Reporting Studio in the Installation of Reporting Studio section.
- Updated the steps to configure the Reporting Studio in the Configuration of i-net Clear Reports section.

- Updated the steps to uninstall i-net 23.x in the Uninstalling i-net 23.x section.
- Added step 9 in the Add an EAGLE System section.
- Added the steps to select the SNMP version in the SNMP Version section.
- Updated step 5 in the Sample Configuration Data for SNMP Connection to EAGLE section.
- Updated the screenshot for EAGLE Release-specific CMI Schema in the Sample Configuration Data for SNMP Connection to EAGLE section.
- Updated the screenshots in the steps to install the CMI schema in the Installing the CMI Schema section.
- Updated the Current EAGLE Compatibility Version figure in the Current Compatible EAGLE Release with OCEEMS section.
- Updated the Moving Back (installing) to the Default EAGLE Release Schema figure in the Moving Back to the Default EAGLE Release Schema from the OCEEMS section.
- Updated the output of the script run to install the CMI schema in the Procedure to Decouple the CMI from EAGLE section.
- Updated the output of the script run to change the system user and its password in the Updating the System User and Password for OCEEMS section.
- Updated the command to log in to MySQL in the following sections:
  - MySQL Root User Password Change for Standalone Server
  - MySQL Root User Password Change for Failover Setup
  - How to Set Up Failover after Fresh Installation
  - How to Set Up Failover after Upgrade

1

Introduction

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 (OCEEMS).

Scope and Audience

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

- **OCEEMS** configuration and administration, and use of the OCEEMS Graphical User Interface (**GUI**).
- Use of the OCEEMS to configure and monitor an Oracle Communications EAGLE Signal Transfer Point (**STP**) in a network.
- Use of the OCEEMS 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 1-1 Admonishments

Icon	Description
	Danger: (This icon and text indicate the possibility of *personal injury*.)
	Warning: (This icon and text indicate the possibility of *equipment damage*.)
	Caution: (This icon and text indicate the possibility of *service interruption*.)
	Topple: (This icon and text indicate the possibility of *personal injury* and *equipment damage*.)

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.

OCEEMS Administration

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

OCEEMS Core Applications

- EAGLE Discovery Application describes how the EAGLE nodes are discovered in the network.
- OCEEMS Support of EPAP Alarms via SNMP Feed describes support for EPAP fault management.
- OCEEMS Support of LSMS Alarms via SNMP Feed describes support for LSMS fault management.
- Fault Management provides descriptions of the functions provided by the OCEEMS Fault Management Interface.
- Measurements Module provides information about the OCEEMS 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 OCEEMS Configuration Management Interface (CMI).
- Link Utilization Interface provides information about the OCEEMS Link Utilization Interface (LUI).
- Northbound Interface (NBI) provides information about the OCEEMS Northbound Interface.

Appendixes

- OCEEMS System Administration provides an overview of the embedded security management tool and interface available in the OCEEMS.
- OCEEMS Backup and Restore describes the configuration and execution of the backup and restore procedure for the OCEEMS.
- OCEEMS Failover describes the failover procedure for the OCEEMS.
- EPAP Support Messages lists the error and informational messages for OCEEMS support of EPAP fault management.
- Fault Management GUI Custom Views describes the use of custom views for events/alarms in the Fault Management GUI.
- Using the OCEEMS MIB Browser as an NMS Proxy describes how the MIB browser application bundled with OCEEMS can be used as a proxy for an NMS to verify SNMP v3 features like trap forwarding and resynchronization.

- Measurement Report Configuration on EAGLE provides the EAGLE commands needed to configure measurement reports.

()

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

Call the 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 registration and opening a support ticket.

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 () 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 related to this document, refer to the Oracle Help Center site. See Locate Product Documentation on the Oracle Help Center Site for more information on related product publications.

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 Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) 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 http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click `Industries`.
3. Under the Oracle Communications subheading, click the `Oracle Communications documentation` link.

   The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
4. Click on your Product and then the Release Number.

   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the `PDF` link, select `Save target as` (or similar command based on your browser), and save to a local folder.

2

OCEEMS Administration

The first part of this manual describes OCEEMS administration, initialization, and first configuration.

OCEEMS Administration

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

OCEEMS Functional Description describes OCEEMS platform, inventory, fault management, alarms, and measurement functions.

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

OCEEMS Initialization and First Configuration

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

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

> **Note**
>
> When the initialization and first configuration are complete, the OCEEMS GUI will be available for use.

OCEEMS Non-Root System User

Prior to OCEEMS 46.3, only the root super user could perform OCEEMS operations like start/stop/restart of the OCEEMS server and update of OCEEMS configuration files. Release 46.3 and above include a feature that removes the need of root privileges to run OCEEMS.

With this feature, the use of the root user is now limited to the OCEEMS installation/upgrade/uninstallation procedures only. During OCEEMS installation/upgrade, a non-root system user for OCEEMS operations is created, and thereafter only the configured non-root system user is used for further initial configuration of OCEEMS and for OCEEMS operations.

3
OCEEMS Functional Description

This chapter provides an overview of the OCEEMS.

OCEEMS Overview

The OCEEMS 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 OCEEMS 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, OCEEMS reports the discovery, physical and logical topology maps, centralized event management, graphs and statistical information of the EAGLE system.

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

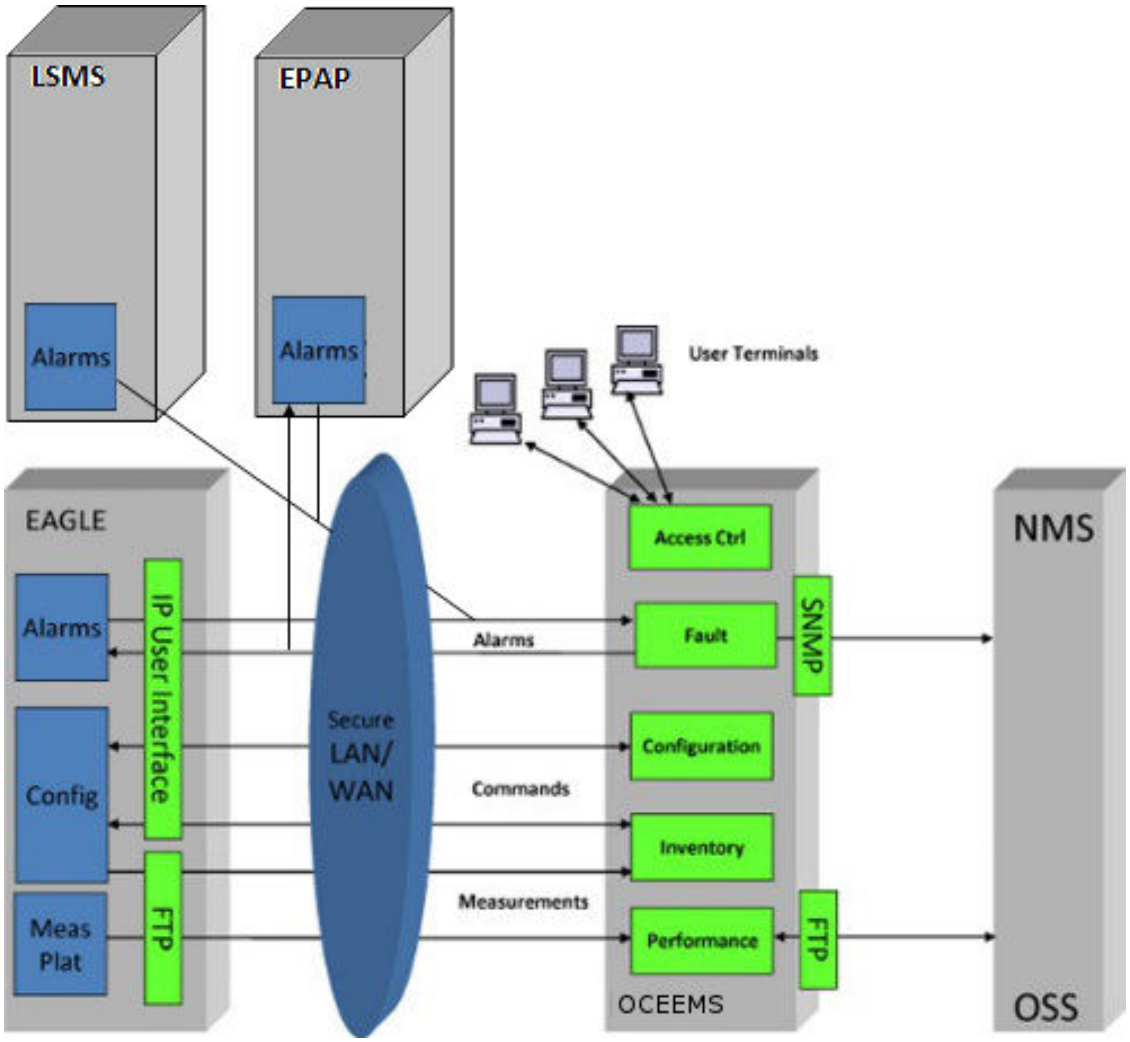
The System Administrator is provided a Security Interface to enable user access at different levels of the OCEEMS and EAGLE systems. Once the System Administrator has set up the individual EAGLE commands, the user will have access to complex command scripts that can be created, managed, executed, and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

The **OCEEMS** provides a mechanism for forwarding alarms from EAGLE, EPAP, and LSMS systems, and from the **OCEEMS** (including **OCEEMS** agents and interfaces) to a Northbound Interface. Alarms are synchronized between the OCEEMS and the monitored systems, upon request from the Northbound Interface.

OCEEMS Architecture

A general OCEEMS setup is shown in Figure 3-1:

Figure 3-1 OCEEMS Architecture



OCEEMS Applications

The OCEEMS **GUI** displays a view of the global network down to the card level with event-filtering capabilities. When outages occur, the OCEEMS 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 OCEEMS 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 OCEEMS 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 OCEEMS northbound interface.
- **Fault Management**
  The OCEEMS 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 number of events stored in the DB are detailed in the Feature Description and documented. The Fault Management application and DB support a minimum of 200 entries per second: 200 TPS. The alarm/event rate supported are documented. all required communication between EAGLE systems and the OCEEMS system.
- **Measurements Module**
  The OCEEMS Measurement Module parses measurement files received from the EAGLE **Measurements Platform Agent**, and then transfers the data to the OCEEMS 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 OCEEMS database. The data is used to create reports.

- **Security Administration**
  The OCEEMS customer is in charge of the system administration and the OS administration. The System Administrator is the owner of the root account and the non-root system user for OCEEMS operations, and is responsible for setting all privileges for group users.
- **Reporting Studio**
  The OCEEMS Reporting Studio is a reporting tool. The OCEEMS 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®. OCEEMS Users can create/update a report template as per their requirement.
- **Configuration Management Interface (CMI)**
  The OCEEMS 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 OCEEMS 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 OCEEMS activities, including EAGLE command script execution, all OCEEMS User activities, and all accesses to EAGLE systems
  - Create and manage custom command classes

  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 OCEEMS and EAGLE activity performed by the users, successful or not, are logged and documented.
- **Link Utilization Interface**
  The OCEEMS Link Utilization Interface (LUI) collects and stores link capacity information about EAGLE signaling links in the OCEEMS 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 optional OCEEMS Northbound Interface application converts alarms to SNMP alert traps and forwards them to client-registered Network Management Systems (NMS). Alerts can be synchronized between the OCEEMS and a Network Management System. The FTP Northbound Interface allows OCEEMS raw measurement reports to be forwarded to a database.
- **Backup and Restore**
  OCEEMS is used to manage and monitor EAGLE, EPAP, and LSMS nodes in the network. OCEEMS 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. The OCEEMS 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 OCEEMS, failover support is provided with two redundant servers configured as primary and standby servers. In the failover setup, the primary and standby servers have access to the replicated database. MySQL data files are kept in the `/Tekelec/Webnms/mysql/data` directory.

OCEEMS Security Tools

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

The OCEEMS 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).

The OCEEMS log files are protected from OCEEMS 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 OCEEMS users cannot modify the log files. For more information about log files, see *Purpose of OCEEMS Log Files* in *Upgrade/Install Guide*.

The OCEEMS 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 OCEEMS 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 (e.g., complex passwords).

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

For more information about OCEEMS security, see Security Administration Screen.

OCEEMS 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 OCEEMS client and managed EAGLE(s) could be on the other side of the firewall.

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

The ports used by OCEEMS, their type, and their purpose are provided in Table 3-1. All of these ports must be opened up on the firewall. None of the ports are encrypted.

> **Note**
>
> Ports for SSH (22), Telnet (23), SNMP (161), and SNMP v3 user discovery (1234 and 8002) must be opened bidirectionally.

Table 3-1 Ports Used by OCEEMS

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; OCEEMS 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	1234 (TCP)	Port for SNMP v3 user discovery by NMS for receiving traps from OCEEMS
10	2000 (TCP)	NMS BE port used for communication between BE and FE servers
11	2300 (TCP)	Config Server port
12	3306 (TCP)	MySQL
13	4500 (TCP)	SAS (SNMP Applet server) port In BE - FE combination, all SAS-related information is passed through a socket.
14	4567 (TCP)	Web NMS Client-Server communication port
15	8001 (UDP)	Web NMS Agent port
16	8002 (UDP)	Port for SNMP v3 user discovery by NMS and to receive SNMP set request from NMS after user discovery
17	8443 (TCP)	SSL connection port
18	9000 (TCP)	I-net Clear Reports server port
19	9999 (TCP)	SUM port
20	36001 (TCP)	NMS FE secondary port

Table 3-1 (Cont.) Ports Used by OCEEMS

S#	Port (Type)	Description
21	36002 (TCP)	Web NMS Client-Server communication port
22	36003 (TCP)	RMI Server Socket port
23	*Port Range* (TCP)	For the NBI FTP module to transfer measurement files from OCEEMS 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 OCEEMS server firewall as well.

Hardware and Software Requirements

OCEEMS was tested on the following platforms:

- VM running version 8.8
- EMS works with similar version of RHEL as that of Oracle Linux (OL 8).
- The OCEEMS server's `hosts` file (which is usually available in the `/etc` directory) must have an entry for the system's IP address and hostname (required for DNS name resolution). In a failover setup, both the primary and standby machines need entries for both systems' IP address and hostname. For example, for a setup where the primary server's IP address and hostname are `10.248.10.21` and `oceemspri` and the standby server's IP address and hostname are `10.248.10.22` and `oceemssec`, the following entries should be in the `/etc/hosts` file on both machines:

  ```
  10.248.10.21 oceemspri
  10.248.10.22 oceemssec
  ```

- To support IPv6-enabled EPAP devices, the machine on which OCEEMS is installed must be a dual stack (that is, able to communicate with other devices over both IPv4 and IPv6). In a failover setup, both servers must be dual stack.
- The `lsof` command is required by the OCEEMS Measurements module and should be installed on the system before OCEEMS is started. Verify its availability and install it if needed before starting the OCEEMS server.
- The hard disk partition where OCEEMS is installed must contain at least 500 GB of space, and the limit for the number of open files (ulimit -n) on the system should be configured to 65536
- Java 17 (64-bit) on the OCEEMS server system

  > **Note**
  >
  > In OCEEMS releases prior to 46.2, the JRE package required by OCEEMS was bundled with OCEEMS installation. However, starting with OCEEMS 46.2, OCEEMS no longer uses the bundled JRE package and requires JRE to be installed separately on the system. For the steps needed to install JRE on the system, see *Installation of Java Runtime for OCEEMS* in *Install/Upgrade Guide*.

- Java 17 on the machine where the OCEEMS client is used

- For a client machine to successfully render EAGLE card graphics and to be able to switch over from the primary server to the standby server during failover, the client machine's `hosts` file must have the hostname and IP address entries of the OCEEMS server. On a Windows-based client machine, the `hosts` file is located in the `C:\Windows\System32\drivers\etc` directory and the following entries should be added:
  - Standalone setup:

    ```
    <OCEEMS SERVER IP> <OCEEMS SERVER HOSTNAME>

    For example:

    10.248.10.25 oceems
    ```

  - Failover setup:

    ```
    <PRIMARY SERVER IP> <PRIMARY SERVER HOSTNAME>
    <STANDBY SERVER IP> <STANDBY SERVER HOSTNAME>

    For example:

    10.248.10.25 oceemspri
    10.248.10.21 oceemssec
    ```

- Either of the following web browsers for the OCEEMS client:
  - Microsoft® Edge Version 125.0.2535.51 (Official build) (64-bit) or later
  - Mozilla Firefox® Version 115.11.0 or later
  - Google Chrome Version 125.0.6422.112 (Official Build) (64-bit) or later

  > **Note**
  >
  > Your browser of choice should have Java and pop-ups enabled.

- For optimum usability, the OCEEMS client workstation should have a minimum resolution of 800x600 pixels and a minimum color depth of 16 thousand colors per pixel.

The OCEEMS is available in a tiered architecture using the following configurations:

- Small Network
  - Up to 4 Network Elements
  - Up to 5 concurrent users
  - CPU: 2 GHz minimum, single processor supported, dual processor recommended
  - Memory: 2 GB minimum, 16 GB recommended
  - Disk capacity: 500 GB minimum/recommended
- Medium Network
  - Up to 20 Network Elements
  - Up to 15 concurrent users
  - CPU: 2 GHz minimum, dual processor supported, quad processor recommended

  - Memory 8 GB minimum, 32 GB recommended
  - Disk capacity: 500 GB minimum, or more based on historical events recording requirements
- Large Network
  - Up to 50 Network Elements
  - Up to 25 concurrent users
  - CPU: 2 GHz minimum, dual processor supported, quad processor recommended
  - Memory 16 GB minimum, 64 GB recommended
  - Disk space: Determined based on historical events recording requirements

The following packages should also be manually downloaded and installed:

- Telnet/SSH
  For securely connecting to network elements like EAGLE, EPAP, and LSMS, the SSH service should be running on the OCEEMS machine. All network elements should communicate with OCEEMS over secure connections to provide a level of protection for the transported data. Optional features for secure communication are available and highly recommended for interfacing to EAGLEs.

  The TELNET application client is required and utilized as part of the connection to both secure and non-secure EAGLEs, so it needs to be installed on the OCEEMS server along with the SSH service and SSH client before installation of OCEEMS. If the target OS is Oracle Linux, the SSH service is enabled by default, so only the TELNET application package installation should be required on the server.
- FTP/SFTP
  For receiving measurement data (CSV files) from EAGLEs, the FTP/SFTP service should be running on the server. FTP is required for receiving measurement files from EAGLEs over a non-secure connection, and SFTP is required for receiving measurement files from EAGLEs over a secure connection.

  All network elements should communicate with OCEEMS over a secure connection, so use of FTP should be avoided as much as possible. If the target OS is Oracle Linux, SFTP is supported by default, so only FTP package installation should be needed (if required). In addition, when the machine supports SFTP, while configuring EAGLE for sending measurement data to OCEEMS using the `ent-ftp-serv` command, the `security` parameter must be turned **on**.

EAGLE Baseline Setup

The EAGLE must be equipped with the following:

- At least one IPSM card (up to 3 cards are supported)
- Terminal settings for alarm management:
  - Two terminals per IPSM are required
- Two MCPM cards for the Measurements Platform, or E5-based control cards (two E5-MASP assemblies and an E5-MDAL card) for E5-OAM Integrated Measurements
- A configured user to enable the OCEEMS Configuration Management Interface and the OCEEMS Inventory module to log in and execute commands and collect topology information

4

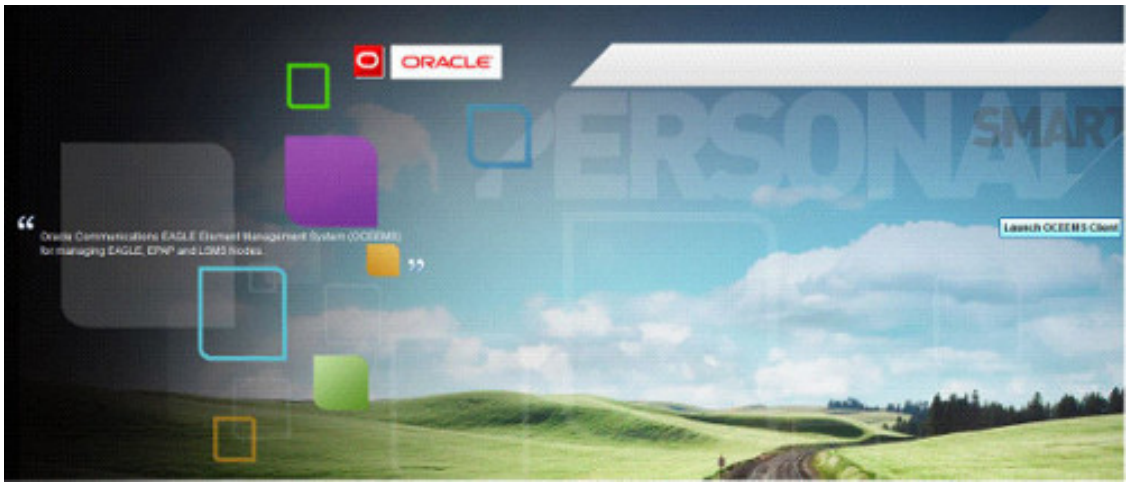
OCEEMS Graphical User Interface

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

Overview

The OCEEMS 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 OCEEMS and log in from a client workstation as shown in E5-MS Launch Screen.

Figure 4-1 OCEEMS Launch Screen



Please contact your System Administrator to assign the **OCEEMS Authentication** security operation.

OCEEMS Login

The OCEEMS login page is used to authenticate users of the OCEEMS.

Clients must upgrade their Java version to 64-bit Java 17 in order to open the OCEEMS GUI.

> **Note**
>
> OCEEMS 47.x is tested with OpenWebStart version 1.9 to open the downloaded jnlp file for OCEEMS GUI.

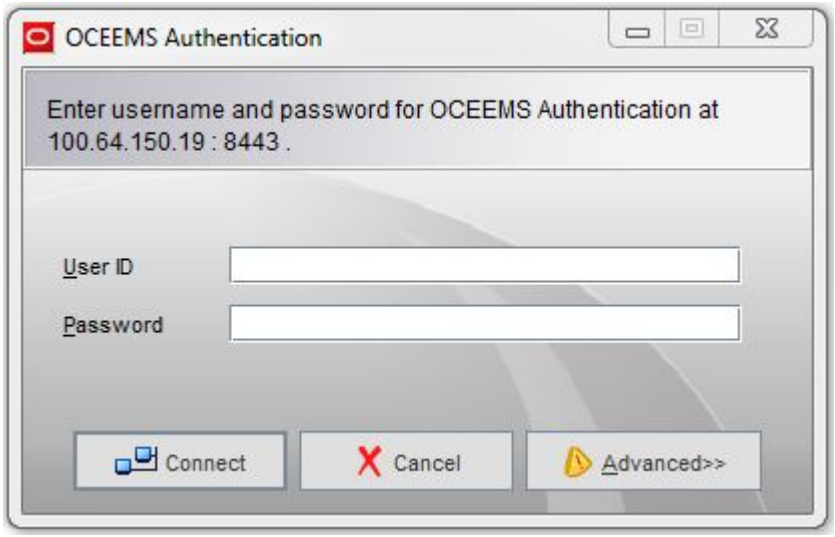
Logging In to OCEEMS

Please contact your System Administrator to assign the **OCEEMS** security operation.

This procedure describes how to log in to the OCEEMS.

1. Click **Launch OCEEMS Client** on the OCEEMS Launch screen (see E5-MS launch screen).
2. Enter the **User ID** and **Password** on the OCEEMS Authentication screen (see Figure 4-2).

Figure 4-2 OCEEMS Authentication Screen

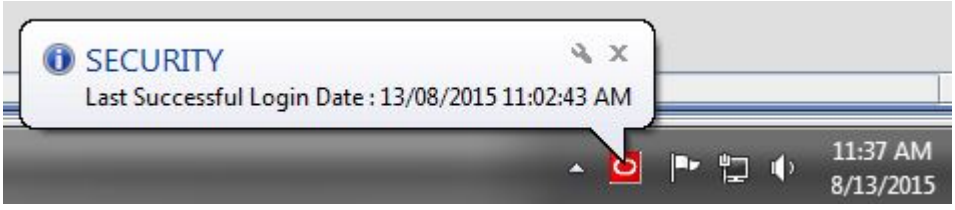


Please contact your System Administrator for your User ID and Password.

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

   If the user name and password entered in 2 are correct, the **OCEEMS user** is authenticated and notification is received on the lower right of the screen as shown in Figure 4-3.

Figure 4-3 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**.

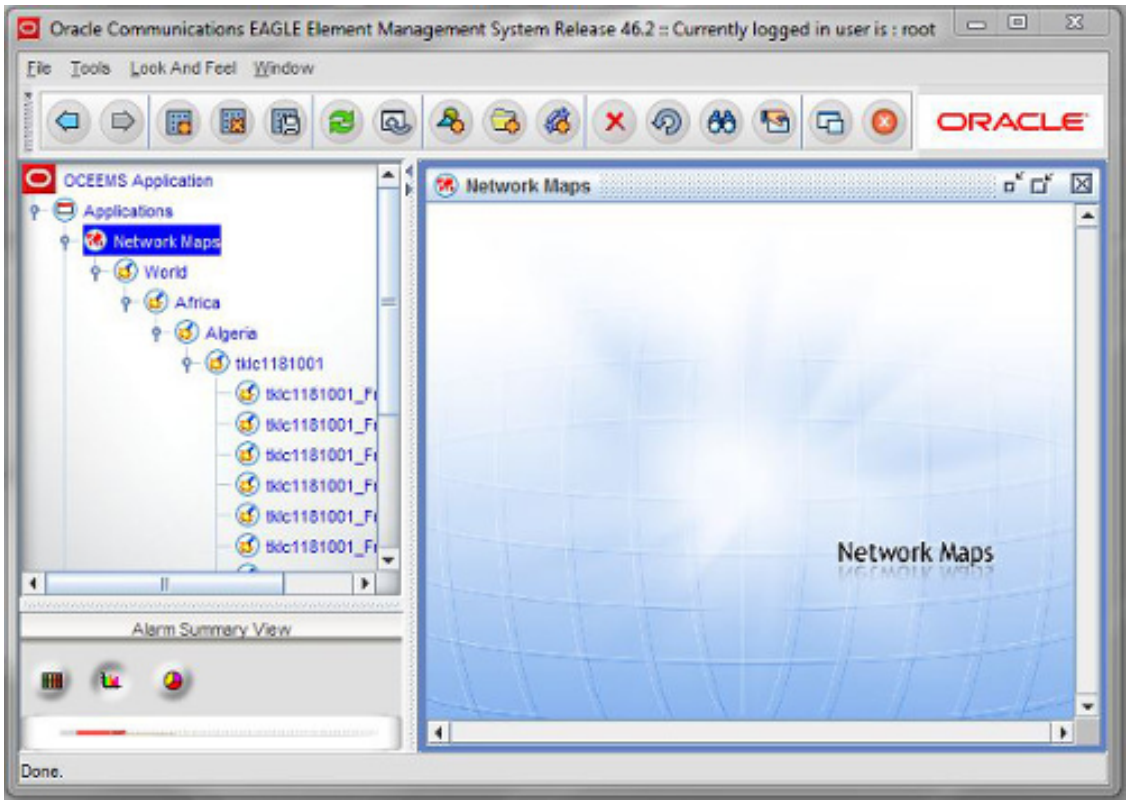
Login Page Elements

Element	Description
UserID Field	Enter your OCEEMS 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 OCEEMS.

OCEEMS Application Main View

After the user has access to the OCEEMS GUI, the OCEEMS application main screen is displayed:

Figure 4-4 OCEEMS Application Main Screen

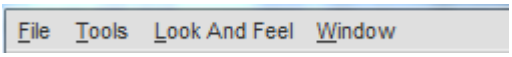


Menu Bar

The OCEEMS menu bar is the horizontal strip at the top of the OCEEMS GUI that contains available drop-down menus. It includes links to the specific OCEEMS 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 4-5 OCEEMS Menu Bar



Menu Bar Submenus

Main Menu Selection	Submenu
File	Back
	Forward
	Detach
	Close
	Close All
	Exit
Tools (only Security Administration has a keyboard shortcut available)	Security Administration
	Change Password
	Themes
	Eagle Discovery
	Eagle Inventory
	LSMS DIscovery
	EPAP Discovery
	Report Designer
	Reporting Studio
	NBI
	NBI Agent Configuration
	SNMP v3 Group Management
	SNMP v3 View Management
	NBI FTP Configuration
	License Details
	OCEEMS Notifications
	OCEEMS Notifications Settings
Look and Feel	Metal
	CDE Motif
	Windows
	Windows Classic
Window	Cascade
	Tile Horizontal
	Tile Vertical
	Save Location and Size
	Show Toolbar

Toolbar Icons

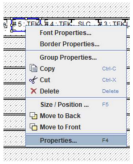
The toolbars are a set of icons that are part of the OCEEMS application. The common toolbar is easy-to-use and always available for performing common functions. Then there are several other toolbars associated with the application such as the:

- Map toolbar, which is viewed at the top of the OCEEMS 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

Figure 4-6 Tools Submenu

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

ICON	ICON Name	Description
	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 4-7 and Table 4-1.

Figure 4-7 Network Map Toolbar

Table 4-1 Network Map Toolbar Icons

ICON	ICON Name	Description
	Select Mode	Zooming In and Out
	Zoom Window	
	Zoom Mode	
	Zoom In	
	Zoom Out	
	Cut	Rearranging Map Symbols- There is a click, drag and drop capability on each map screen
	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 4-8 and Table 4-2.

Figure 4-8 Detached Network Map Toolbar

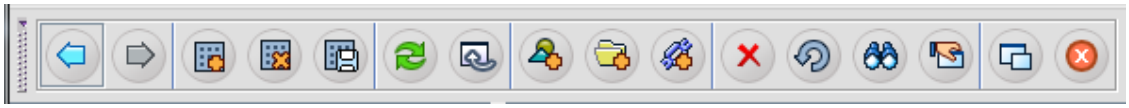


Table 4-2 Detached Network Map Toolbar Icons

ICON	ICON Name	Desciption
	Add Map	Adding Custom Maps
	Delete Map	Deleting Map Layout
	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 4-9 and Table 4-3.

Figure 4-9 Network Event Toolbar

Table 4-3 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	

Table 4-3 (Cont.) Network Event Toolbar Icons

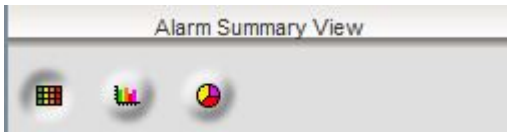
ICON	ICON Name	Description
	Remove Custom View	

Alarm Summary View

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

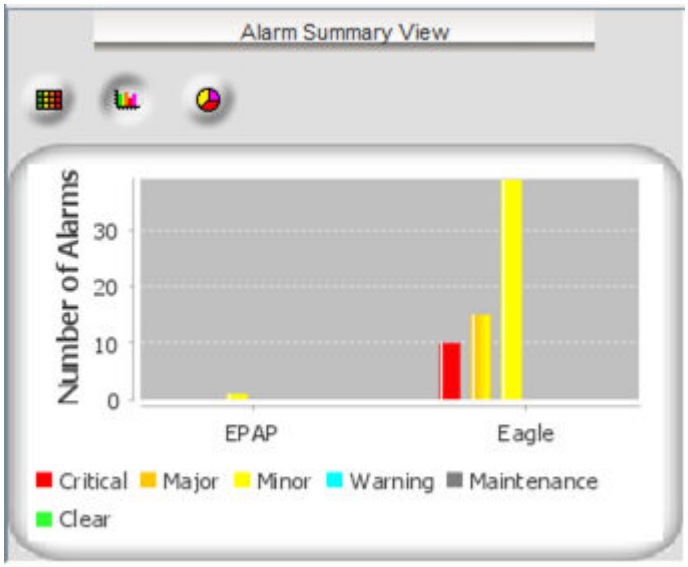
The three icons at the top of the Alarm Summary View are shown in Figure 4-10.

Figure 4-10 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 #unique_37/unique_37_Connect_42_V5512847.

Figure 4-11 Alarm Summary View



Alarm Severity Representation

Color	ICON Name
	Critical
	Major
	Minor
	Warning
	Maintenance
	Clear

5

EAGLE Discovery Application

This chapter provides information about the EAGLE Discovery application.

Overview

The OCEEMS has three elements of the inventory process:

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

EAGLE Discovery

The OCEEMS 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 OCEEMS 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 OCEEMS with the following data:

- Inventory data
- Map data

The OCEEMS 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 OCEEMS 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 Graphic**s operation is scheduled to run on 00:00 AM per day and **Update Inventory** are scheduled to run on 02:00 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 **OCEEMS GUI** menu bar.
2. Select **EAGLE Discovery** from the drop-down menu.

Figure 5-1 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.

OCEEMS 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 the OCEEMS database without performing any ping test. The user can perform discovery for a single EAGLE at a time.

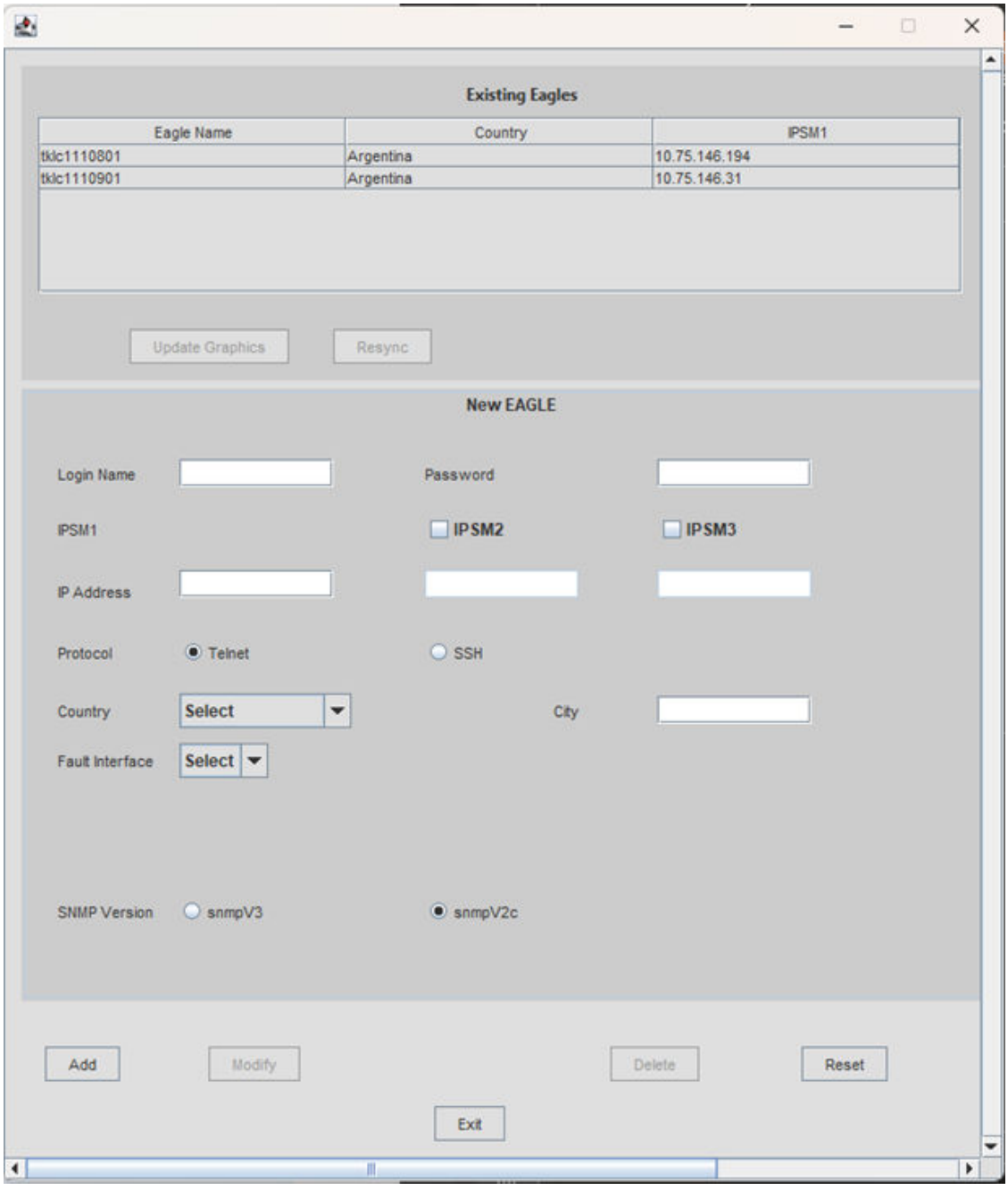
> **Note**
>
> No verification is performed to validate that the user configured EAGLE is an EAGLE or not. Only IP ping based mechanism is used for kicking off the discovery process.

Discovery GUI

The main functions of the EAGLE Discovery screen as shown in Figure 5-2 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.

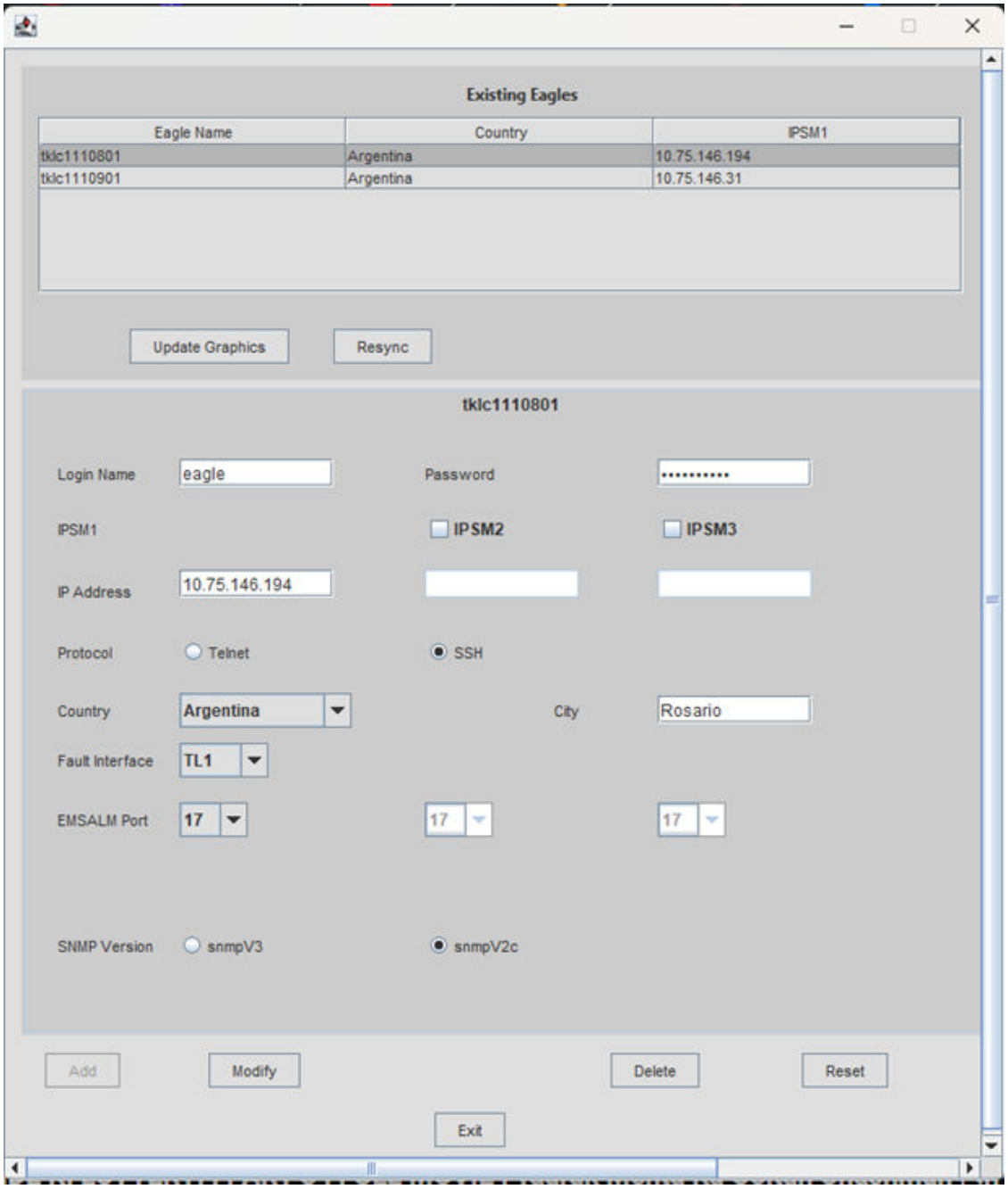
Figure 5-2 Eagle Discovery Screen



For the Existing EAGLE(s) listed in EAGLE Discovery screen, users can trigger a **Resync**hronization of alarms as shown in Figure 5-3.

> **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.

Figure 5-3 EAGLE Discovery Screen for Existing EAGLE(s)



Existing EAGLE(s)

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

The 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 the Chassis View. Update Graphics shall run a subset of Update Inventory commands. This update is pertaining to the specific EAGLE for which the user is fetching updates.

The EAGLE Discovery GUI shall support a minimum of 50 EAGLEs that can be configured in OCEEMS.

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

If the EAGLE Update graphics operation is successful, an OCEEMS information dialog box will appear stating `Graphics updated for EAGLE <EAGLE NAME>by user <USER NAME>.`

If the EAGLE Update graphics operation fails, an OCEEMS error message will appear stating `EAGLE <EAGLE NAME> graphics update failed! Reason: <REASON> Please resolve the issue and retry`

If the EAGLE Update Inventory operation is successful, an OCEEMS information dialog box will appear stating `Inventory updated for EAGLE <EAGLE NAME> by user <USER NAME>`.

If the EAGLE Update Inventory operation fails, an OCEEMS 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 OCEEMS management modules (like Fault, Configuration, and Security) 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 OCEEMS is connected.

1. Click **Tools** icon on the menu bar.
2. Select EAGLE Discovery.

   EAGLE Discovery screen pops up as shown in Figure 5-2
3. Type the name and password of the EAGLE in the 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 `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.
5. Enable the protocol by selecting either `Telnet` or `SSH`.
6. Select the country the EAGLE system is located in. Click the drop-down arrow to select the country.
   A country must be selected. If the country is not listed, select `Others` as shown in the following figure:

Figure 5-4 Country and City

There is no validation when selecting the country.

7. Enter the `City` the EAGLE system is located in, as shown in the above figure.

   There is no validation when the city is entered.

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

Figure 5-5 Fault Interface

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

Figure 5-6 EMSALM Port

If SNMP is selected in the following fields as shown in the following figure:

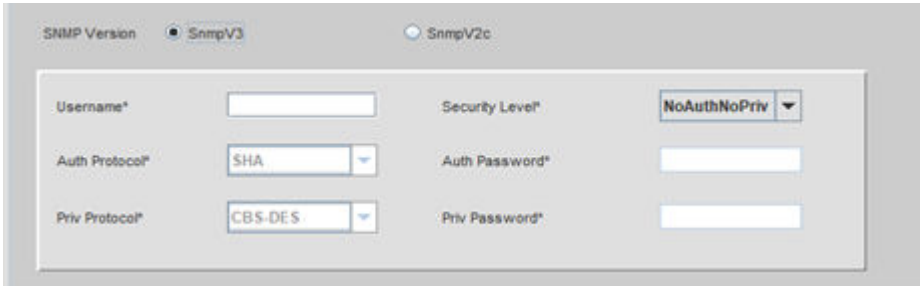
- `Read Community`
- `Write Community`
- `Active OAM IP`
- `Standby OAM IP`

Figure 5-7 SNMP as Fault Interface

9. Select **SNMP Version** (SnmpV2c is selected as default). If Snmpv3 is selected, the following fields will be displayed.

- Username
- Security Level
- Auth Protocol
- Priv Protocol
- Auth Password
- Priv Password

Figure 5-8 SNMP Parameters



10. Click the **Add** button at the bottom of the EAGLE Discovery screen.

    An OCEEMS 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 the OCEEMS 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.

Figure 5-9 IP Address

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

If the IPSM IP address is invalid, an OCEEMS 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 OCEEMS 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 for the protocol on the EAGLE are Telnet and **SSH**:

Figure 5-10 Protocol

Telnet is the protocol used for the Cut Through interface.

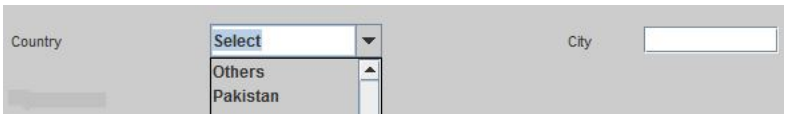
Country and City

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 5-11 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 5-12 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 5-13 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 5-14 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!`

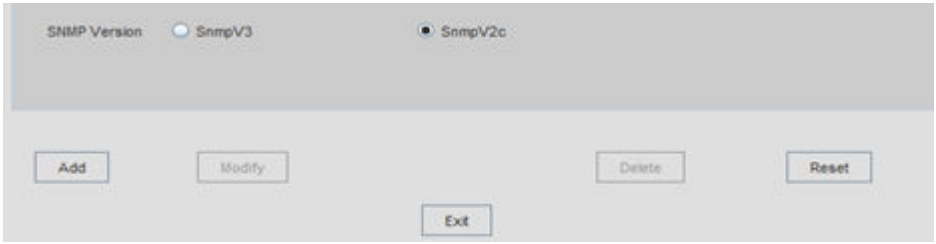
SNMP Version

Run the following steps to select the SNMP version:

For SnmpV2c:

1. Select SNMP Version as SnmpV3 or SnmpV2c. SnmpV2c is selected by default. As shown in SNMP Version.

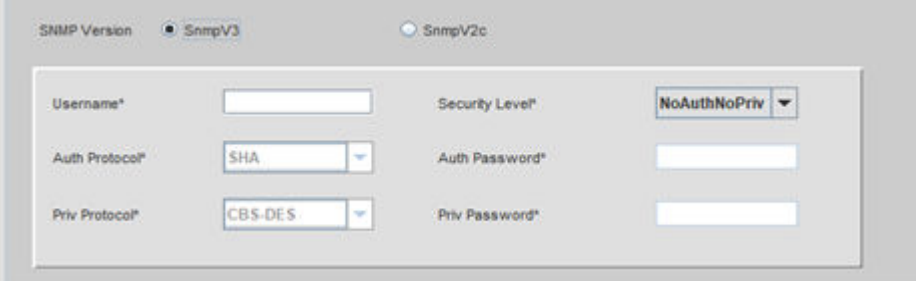
Figure 5-15 SnmpV2c



For SnmpV3:

1. Select **SnmpV3** version as shown in the following figure. The page will display the following fields:
   - Username
   - Security Level(NoAuthNoPriv/AuthNoPriv/AuthPriv)
   - Auth Protocol(SHA)
   - Priv Protocol(DES/AES)
   - Auth Password
   - Priv Password

Figure 5-16 SnmpV3



The following fields are required when the SNMPv3 radio button is selected:

For SnmpV3 user discovery, SNMP user name and security level are compulsory fields based on the selected security level. Users should observe the following UI scenarios:

- If Security Level is AuthPriv, then Auth Protocol, Auth Password, Priv Protocol & Priv Password are enabled.
- If Security Level is AuthNoPriv, then only Auth Protocol and Auth Password are enabled.
- If Security Level is NoAuthNoPriv, then no other fields are enabled.

Sample Configuration Data for SNMP Connection to EAGLE

This example shows configuration of EAGLE and OCEEMS for an SNMP connection to EAGLE.

SNMP Configuration on EAGLE

Use the following steps to configure EAGLE:

1. Log in to EAGLE via Telnet or SSH.
2. Check the current status of SNMPUIM on EAGLE by using the `rtrv-snmpopts` command:

```
> rtrv-snmpopts

    tklc1180801 16-08-02 05:28:17 MST  EAGLE 46.4.0.0.0-69.6.0
    rtrv-snmpopts
    Command entered at terminal #33.
;
Command Accepted - Processing
    tklc1180801 16-08-02 05:28:17 MST  EAGLE 46.4.0.0.0-69.6.0
    SNMP OPTIONS
    --------------------------------
    SNMPUIM    off
    GETCOMM    public
    SETCOMM    private
;
Command Executed
```

Also note the values for GETCOMM (Read Community) and SETCOMM (Write Community) for use in configuring OCEEMS for EAGLE discovery.

3. If SNMPUIM is OFF as shown above, turn it on by using the `chg-snmpopts:on=snmpuim` command:

```
> chg-snmpopts:on=snmpuim

    tklc1180801 16-08-02 05:28:40 MST  EAGLE 46.4.0.0.0-69.6.0
    chg-snmpopts:on=snmpuim
    Command entered at terminal #33.
;
Command Accepted - Processing
    tklc1180801 16-08-02 05:28:40 MST  EAGLE 46.4.0.0.0-69.6.0
    CHG-SNMPOPTS: MASP A - COMPLTD
;
Command Executed
```

4. Check the entries for the SNMP host by issuing the `rtrv-snmp-host` command:

```
> rtrv-snmp-host
    tklc1180801 16-08-02 05:27:48 MST  EAGLE 46.4.0.0.0-69.6.0
    rtrv-snmp-host
    Command entered at terminal #33.
            ;
Command Accepted - Processing
    tklc1180801 16-08-02 05:27:48 MST  EAGLE 46.4.0.0.0-69.6.0
    IPADDR   10.250.54.19
      HOST      nms160
      CMDPORT   161
      TRAPPORT  162
      HB        60
      TRAPCOMM  public
    SNMP HOST table is (1 of 2)  50% full
;
    tklc1180801 16-08-02 05:27:48 MST  EAGLE 46.4.0.0.0-69.6.0
;
Command Executed
```

5. Add an OCEEMS entry on the EAGLE, if not already present, by using the `ent-snmp-host` command with the ipaddr, version, protocol, and host parameters to specify the OCEEMS IP address and name. For example:
If SnmpV2c is selected at SNMP Version in Eagle discovery, run the following command:

```
ent-snmp-host:ipaddr=10.75.136.124:host=ems124:version=snmpv2c
Command Accepted -   Processing
tklc1110903 24-06-05 02:51:45 EST  EAGLE 47.1.0.0.0-79.32.0
7083.1321    CARD 1103     INFO      Eagle  RTDB Birthdate
Mismatch
           Report Date:24-06-05  Time:02:51:45\
;

tklc1110903 24-06-05 02:51:52 EST  EAGLE 47.1.0.0.0-79.32.0
7084.1321    CARD 1105     INFO      Eagle RTDB Birthdate
Mismatch
           Report Date:24-06-05  Time:02:51:52
;
```

```
tklc1110903 24-06-05 02:51:52 EST  EAGLE 47.1.0.0.0-79.32.0
ent-snmp-host:ipaddr=10.75.136.124:host=ems124:version=snmpv2c
Command entered at terminal #3.
;

tklc1110903 24-06-05 02:51:52 EST  EAGLE 47.1.0.0.0-79.32.0
SNMP HOST table is (2  of 2 ) 100% full
ENT-SNMP-HOST: MASP B - COMPLTD
;
```

If SnmpV3 is selected at SNMP version in Eagle discovery:

```
ent-snmp-
host:host=ems124:ipaddr=10.75.136.124:version=snmpv3:username=user2:secleve
l=authpriv:authprot=sha:privprot=des
Enter Auth Password :

Enter Priv Password :

Command Accepted -   Processing

tklc1110903 24-06-05 02:59:46 EST  EAGLE 47.1.0.0.0-79.32.0
7137.1321    CARD 1103     INFO      Eagle RTDB  Birthdate
Mismatch
Report Date:24-06-05  Time:02:59:46
;

tklc1110903 24-06-05 02:59:53 EST  EAGLE 47.1.0.0.0-79.32.0
7138.1321    CARD 1105     INFO      Eagle RTDB  Birthdate
Mismatch
Report Date:24-06-05  Time:02:59:53
;
```

6. Retrieve the OAM IP address by issuing the `rept-stat-card:loc=1113:mode=full` command:

```
> rept-stat-card:loc=1113:mode=full

    tklc1180801 16-08-02 05:28:59 MST  EAGLE 46.4.0.0.0-69.6.0
    rept-stat-card:loc=1113:mode=full
    Command entered at terminal #33.
;
Command Accepted - Processing
    tklc1180801 16-08-02 05:29:00 MST  EAGLE 46.4.0.0.0-69.6.0
    CARD   VERSION      TYPE      GPL        PST            SST        AST
    1113   139-006-000  E5MCAP    OAMHC      IS-NR          Active
-----
      ALARM STATUS       = No Alarms.
      BLMCAP  GPL version = 139-005-000
      IMT BUS A           = Conn
      IMT BUS B           = Conn
      CLOCK A             = Active
      CLOCK B             = Idle
      CLOCK I             = Idle
      MBD BIP STATUS      = Valid
```

```
     MOTHER BOARD ID     = E5-MCAP
      DBD STATUS          = Valid
      DBD TYPE            = 1G ENET
      DBD MEMORY SIZE     = 4096M
      HW VERIFICATION CODE = ----
      CURRENT TEMPERATURE   =  34C ( 94F)
      PEAK TEMPERATURE:     =  41C (106F)     [16-07-28 15:44]
      TROUBLE TEXT VER.  = Rev 136.7.2
      APPLICATION SERVICING
                                          MFC          MFC
      IPLNK STATUS
          IPLNK  IPADDR             STATUS     PST
          A      192.168.53.18      UP         IS-NR[Active OAM IP]

    Command Completed.
;
Command Executed
```

7. Retrieve the Standby OAM IP address by issuing the `rept-stat-card:loc=1113:mode=full:loc=1115` command:

```
> rept-stat-card:loc=1113:mode=full:loc=1115

    tklc1180801 16-08-02 05:29:06 MST  EAGLE 46.4.0.0.0-69.6.0
    rept-stat-card:loc=1113:mode=full:loc=1115
    Command entered at terminal #33.
;

Command Accepted - Processing
    tklc1180801 16-08-02 05:29:06 MST  EAGLE 46.4.0.0.0-69.6.0
    CARD   VERSION      TYPE      GPL        PST            SST        AST
    1115   139-006-000  E5MCAP    OAMHC      IS-NR          Standby
-----
      ALARM STATUS       = No Alarms.
      BLMCAP  GPL version = 139-005-000
      IMT BUS A           = Conn
      IMT BUS B           = Conn
      CLOCK A             = Active
      CLOCK B             = Idle
      CLOCK I             = Idle
      MBD BIP STATUS      = Valid
      MOTHER BOARD ID     = E5-MCAP
      DBD STATUS          = Valid
      DBD TYPE            = 1G ENET
      DBD MEMORY SIZE     = 4096M
      HW VERIFICATION CODE = ----
      CURRENT TEMPERATURE   =  35C ( 95F)
      PEAK TEMPERATURE:     =  41C (106F)     [16-07-28 14:25]
      TROUBLE TEXT VER.   = ----
      IPLNK STATUS
          IPLNK  IPADDR             STATUS     PST
          A      192.168.53.30      UP         IS-NR[Standby OAM IP]

    Command Completed.
```

```
;
Command Executed
```

SNMP Configuration on OCEEMS for EAGLE Discovery

Use the following steps to configure OCEEMS:

1. Log into the OCEEMS application.
2. Use the EAGLE Discovery GUI (**Tools**, and then **EAGLE Discovery**) and add the details for EAGLE as shown in the following figure:

Figure 5-17 Eagle Discovery Example

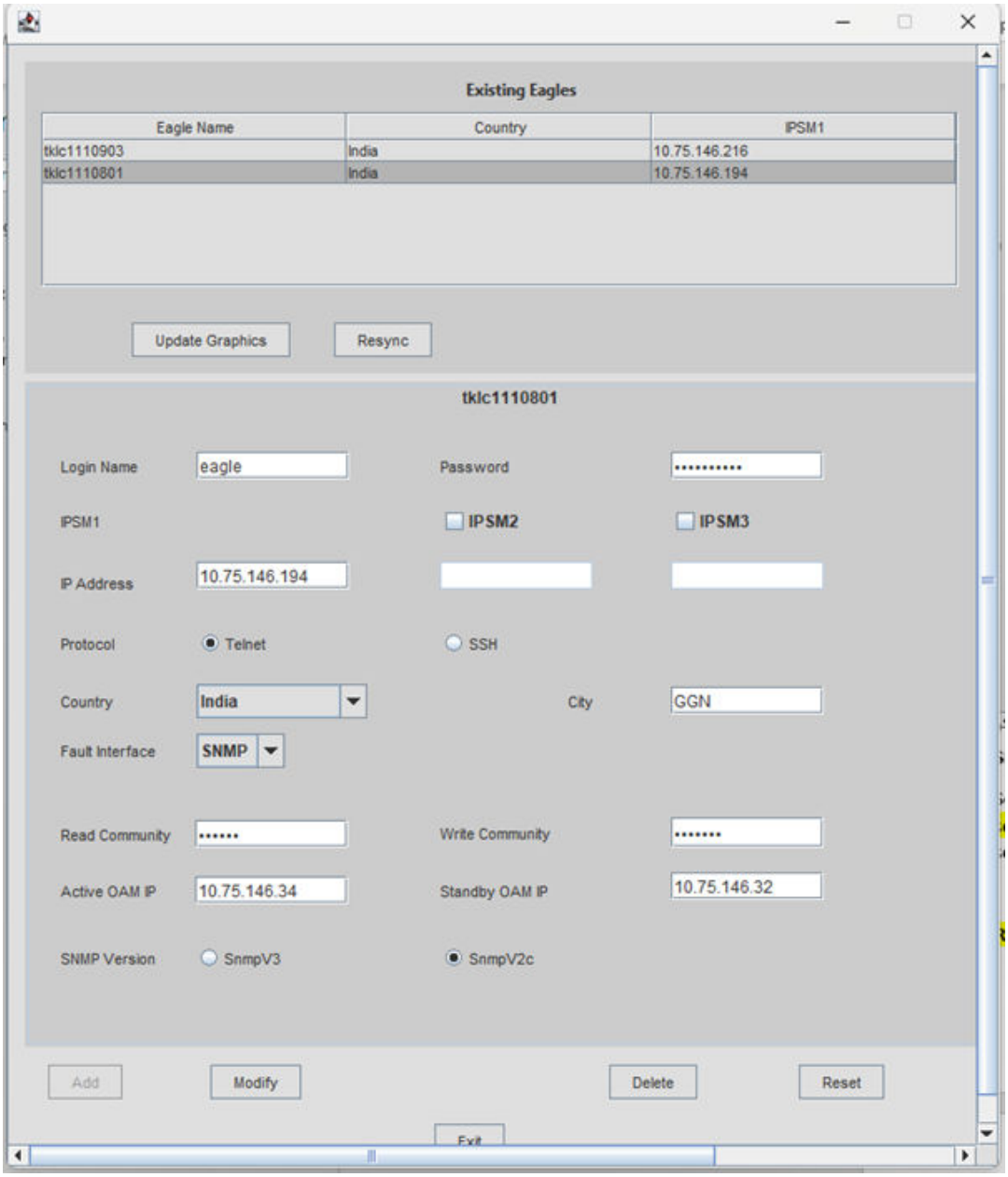
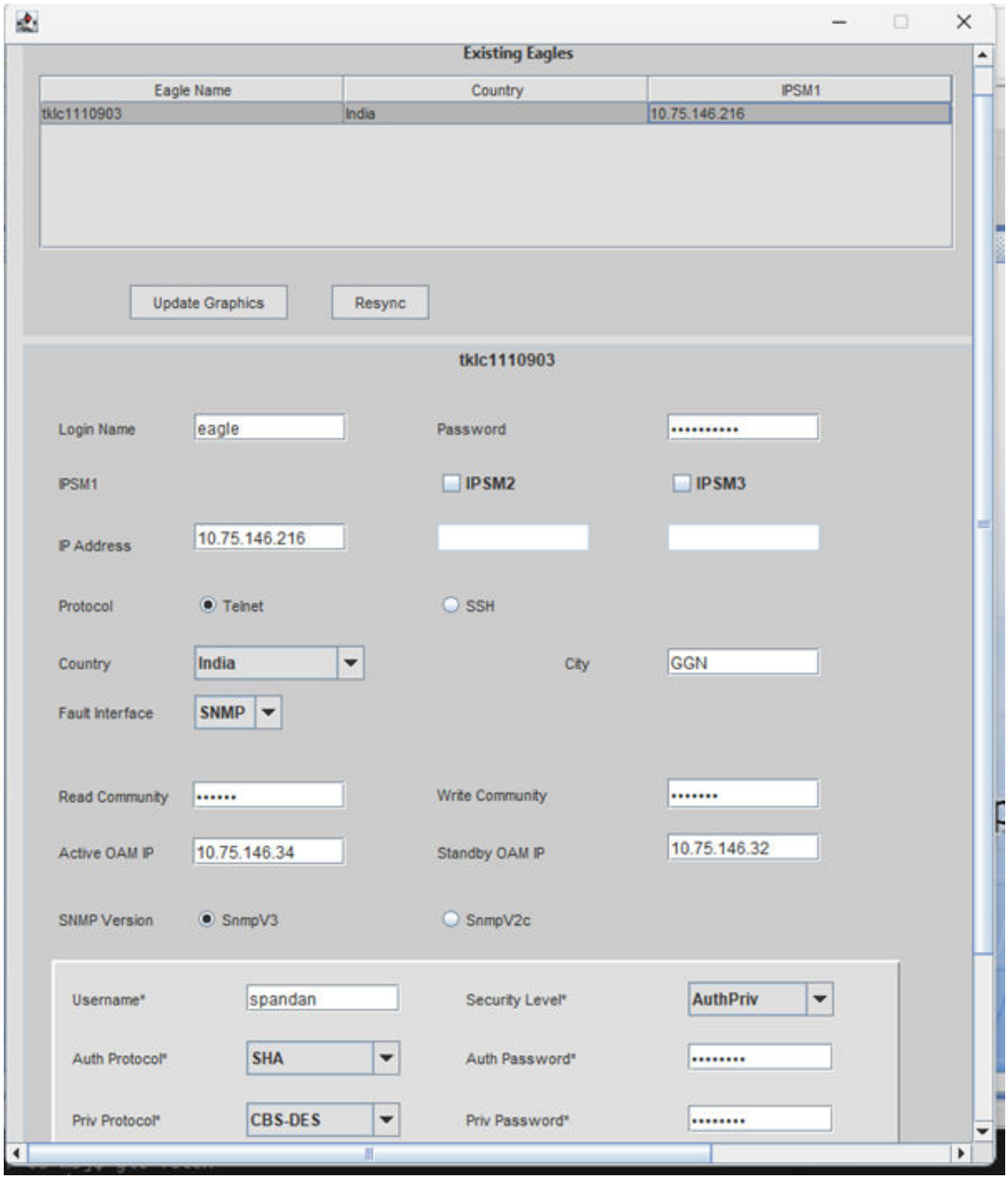


Figure 5-18 Eagle Discovery Example 2



Login Name/Password
Use the credentials that were used to log into the EAGLE in step 1 of SNMP Configuration on EAGLE.

IPSM
Multiple EAGLE IPSM entries can be added if configured on EAGLE.

Protocol
Select the protocol as configured on the EAGLE.

Country/City
Select the country and city where the EAGLE STP is installed.

Fault Interface
Select **SNMP**.

Read/Write Community
Enter the Read Community and Write Community as configured on the EAGLE, as shown in the `GETCOMM` and `SETCOMM` fields in the `rtrv-snmpopts` command output (see step 2 in SNMP Configuration on EAGLE).

Active/Standby OAM IP
Enter the `IPADDR` values from the `rept-stat-card:loc=1113:mode=full` command output and the `rept-stat-card:loc=1113:mode=full:loc=1115` command output, as shown in steps 6 and 7 in SNMP Configuration on EAGLE.

For information on selecting SNMP Version, see the SNMP Version section.

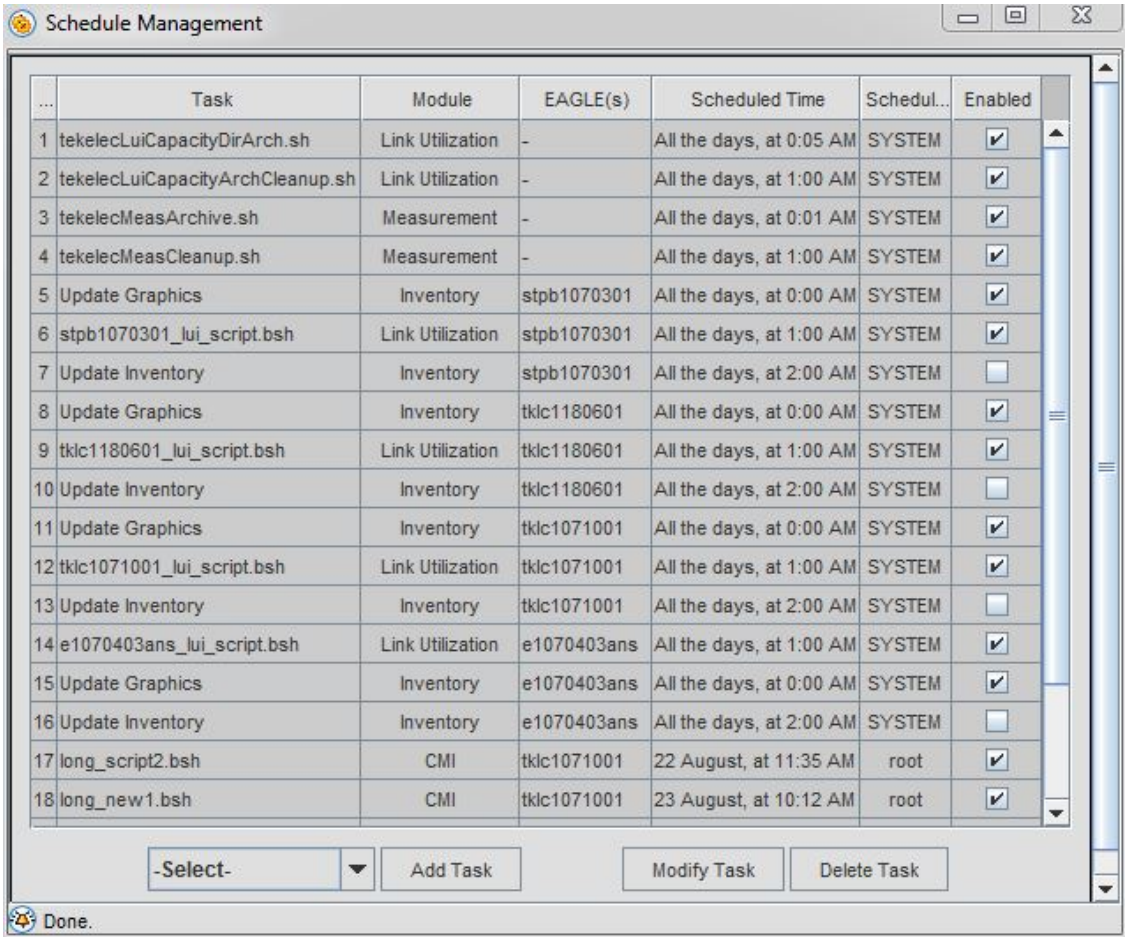
Schedule Management Screen

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

Schedule Management is located in the OCEEMS application tree node. The Schedule Management screen enables the user to set up 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 OCEEMS modules such as CMI, Security, and Fault Management.

For each EAGLE added to OCEEMS, two operations are automatically scheduled on the Schedule Management screen - **Update Inventory** and **Update Graphics**. By default, **Update Graphics** operations are scheduled to run at 00:00 AM each day and **Update Inventory** operations are scheduled to run at 02:00 AM each 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

Figure 5-19 Schedule Management Screen



Map Views

The EAGLE Discovery data provides the OCEEMS 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:

- World Level Map
- Continent Level Map
- Country Level Map
- Eagle Frame Map
- Chassis View
- Shelf View

Figure 5-20 World Level Map

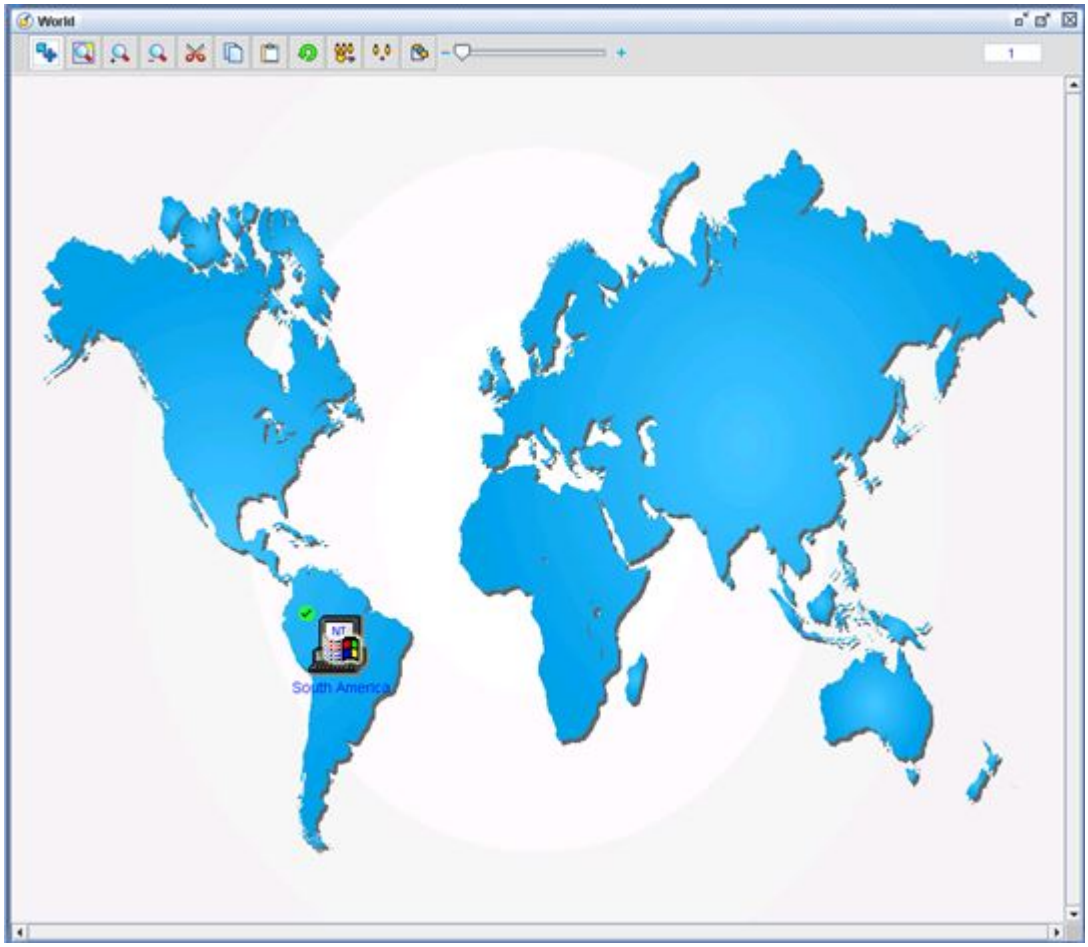


Figure 5-21 Continent Level Map

Figure 5-22 Country Level Map

Figure 5-23 Eagle Frame Map

Figure 5-24 Chassis View

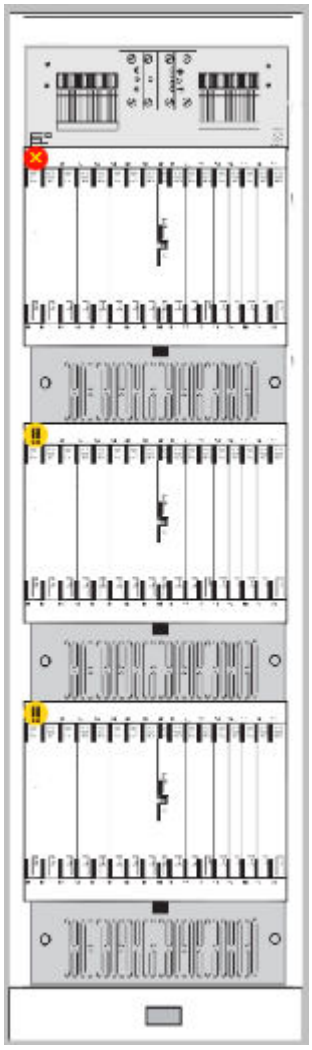
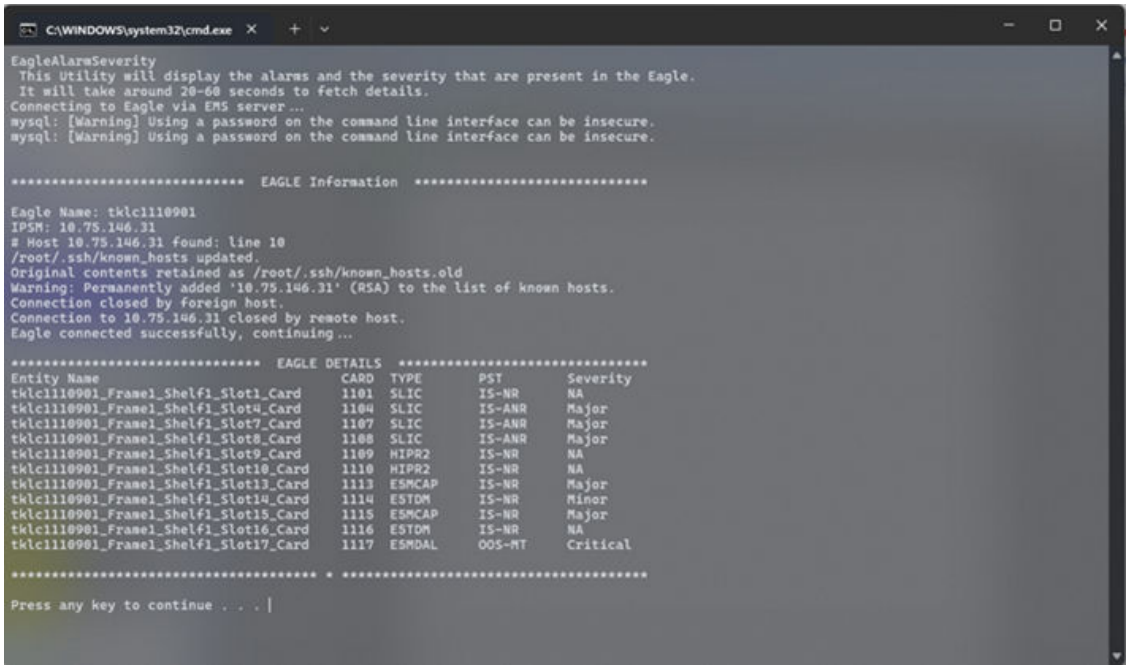


Figure 5-25 Shelf Terminal Pop-up View



Upon clicking the Shelf View, no further action is required. On clicking it, a terminal window will open and it will display the ALARM severity status of each card on the shelf. When you click it for the first time, it will pop up automatically. Upon clicking the Shelf View subsequently, you must manually refresh the view to display the pop up with the most up-to-date information. To refresh the view, click the refresh button.

> **Note**
>
> The manual refresh is only necessary from the second time onwards. Clicking the Shelf Terminal View for the first time will pop up without requiring additional actions.

Table 5-1 OCEEMS Maps List

Continent Map	Country Map
Africa	Algeria
	Cameroon
	Egypt
	Ghana
	Ivory Coast
	Kenya
	Mali
	Morocco
	Senegal
	Tunisia

Table 5-1 (Cont.) OCEEMS Maps List

Continent Map	Country Map
Asia	China
	India
	Indonesia
	Japan
	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
	Sweden
	Netherlands
	Romania
	Spain
	Switzerland
	UK

Table 5-1 (Cont.) OCEEMS Maps List

Continent Map	Country Map
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 OCEEMS

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

Perform the following steps on the OCEEMS 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 OCEEMS server for the changes to take effect.

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

Map View Features

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

The System Administrator must assign **Map Editing Operations** to a user to be able to save the edits.

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

> **Note**
>
> The chassis menu item limitation is as per the framework.

To navigate upwards (from lower to higher map view), the user needs to use the tree view. For example, while navigating from the EAGLE frame map to a Country map, use the tree view provided in the left side of OCEEMS main screen.

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

In the World map, symbol(s) correspond to continent(s) and other.

In the Continent map, symbol(s) correspond to country(s).

In the Country map, symbol(s) correspond to EAGLE(s).

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

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

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

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

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

The user is provided with a menu item on the chassis view to write certain editorial comments via the journal menu item.

The user is provided with a menu item on the chassis view to view card details.

The chassis view displays the last inventory update time in the 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 purposes.

> **Note**
>
> Only maps for which EAGLE discovery has been performed are available in the tree and map view.

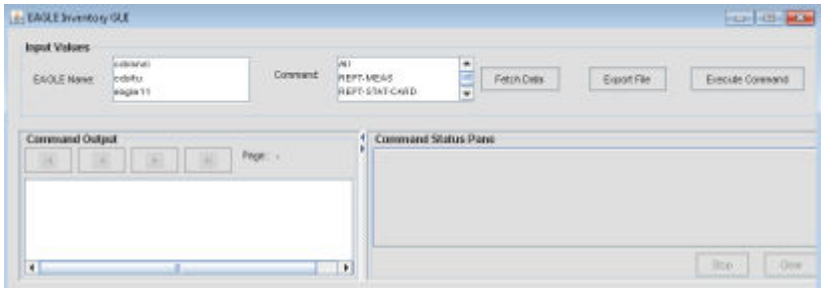
All maps and map symbols are supplied with OCEEMS itself and contain static images. However, users have the option to change the map images via the `ContinentZonalMap.xml` file available at `<OCEEMS_HOME>/conf/tekelec`. Any modifications to this file require server restart for the changes to take effect.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

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

Figure 5-26 EAGLE Inventory GUI



Authorized OCEEMS 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)

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

The 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 the Chassis View. Update Graphics shall run a subset of Update Inventory

commands. This update is pertaining to the specific EAGLE for which the user is fetching updates.

The EAGLE Discovery GUI shall support a minimum of 50 EAGLEs that can be configured in OCEEMS.

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

If the EAGLE Update graphics operation is successful, an OCEEMS information dialog box will appear stating `Graphics updated for EAGLE <EAGLE NAME>by user <USER NAME>.`

If the EAGLE Update graphics operation fails, an OCEEMS error message will appear stating `EAGLE <EAGLE NAME> graphics update failed! Reason: <REASON> Please resolve the issue and retry`

If the EAGLE Update Inventory operation is successful, an OCEEMS information dialog box will appear stating `Inventory updated for EAGLE <EAGLE NAME> by user <USER NAME>`.

If the EAGLE Update Inventory operation fails, an OCEEMS 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 OCEEMS management modules (like Fault, Configuration, and Security) 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 5-2 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`

Table 5-2 (Cont.) Inventory Commands

No.	For Each EAGLE System
16.	rtrv-scr-scrset
17.	rept-stat-db
18.	rtrv-gpl
19.	rept-stat-gpl
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
28.	rtrv-bip
29.	rtrv-card

6

OCEEMS Support of EPAP Alarms via SNMP Feed

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

Overview

OCEEMS Support of EPAP Alarms via SNMPv3 Feed enables the use of the OCEEMS to manage EPAP alarms through the following interfaces:

- Discovery
  The EPAP Discovery interface enables discovery and configuration of EPAP servers in the OCEEMS.
- Map
  The map interface displays discovered EPAP servers in the OCEEMS 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 OCEEMS is through an EPAP Discovery menu. EPAP Discovery is supported for both SNMPv2c and SNMPv3 protocols. EPAP nodes are then visible in the fault management menus and maps. The OCEEMS receives alarms from managed EPAP servers over the southbound SNMP interface. This alarm feed is processed by OCEEMS and presented to the user in the form of events and alarms. EPAP alarms can be forwarded on the OCEEMS northbound interface to one or more client Network Management Systems. OCEEMS users can monitor the EPAP alarm state and take relevant actions to maintain the EPAP servers in a healthy state.

For additional information about the EPAP configuration required, see *Configure EMS Server* and *Configure Alarm Feed* in *EPAP Administration Guide*.

> **Note**
>
> To support IPv6-enabled EPAP devices, the machine on which OCEEMS is installed must be a dual stack (that is, able to communicate with other devices over both IPv4 and IPv6). In a failover setup, both servers must be dual stack.

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)

OCEEMS supports both PDB single and segmented EPAPs.

The OCEEMS 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 OCEEMS menu bar, select **Tools**, and then **EPAP Discovery** to access the EPAP Discovery application and discover EPAP servers within your network. EPAP Discovery is supported for both SNMPv2c and SNMPv3 protocols. 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 OCEEMS with the alarm state for the selected (check boxes) EPAP nodes (for example, due to connection failure between OCEEMS and EPAP).
- EPAP Configuration
  This section includes the **Select EPAP Type** field, the **Select IP Version** radio buttons, and the other 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**, **Resync**, **Reset**, and **Exit** operations.

If the value selected for the **Select EPAP Type** field is **PDB Only**, the PDB Only EPAP Configuration (Auth/Priv) fields are displayed as shown in Figure 6-1.

Figure 6-1 PDB Only EPAP Configuration (Auth/Priv)

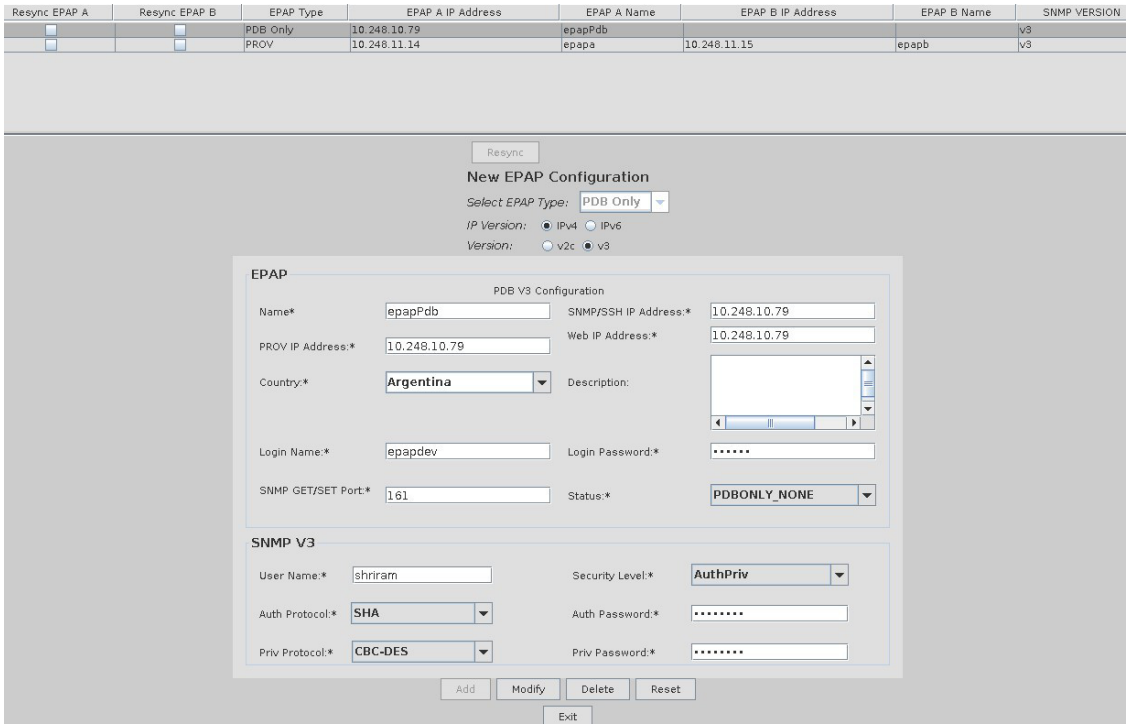


Figure 6-2 PDB Only EPAP Configuration (Auth/NoPriv)

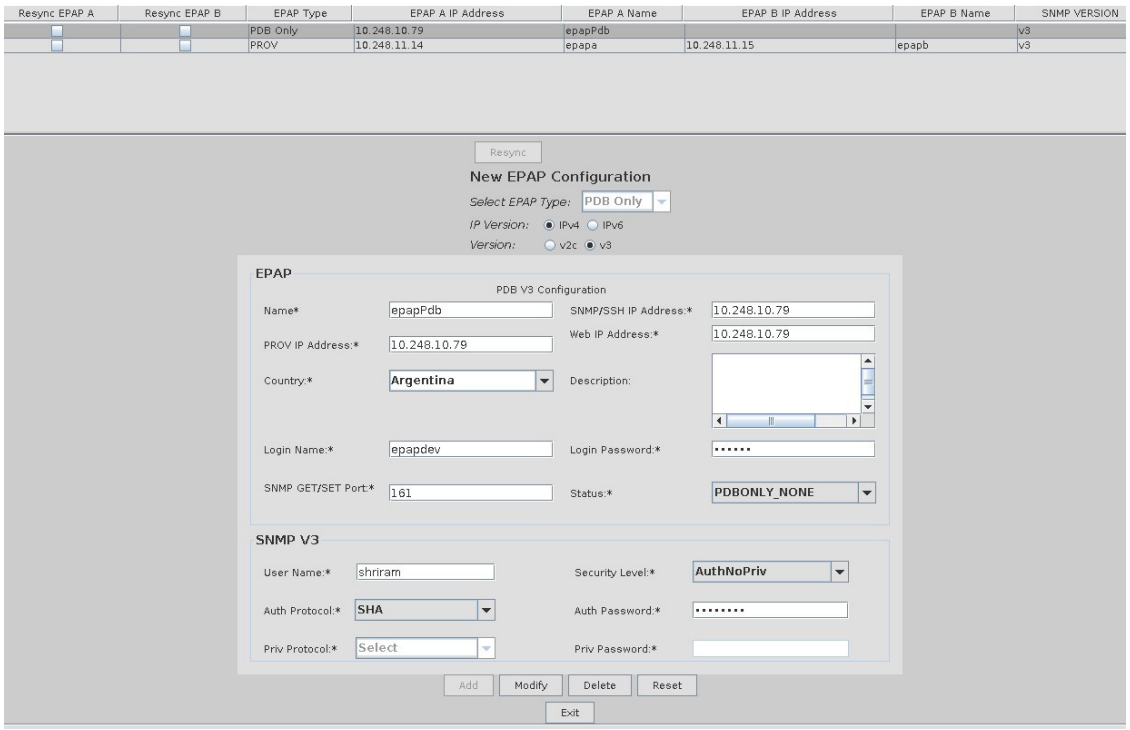
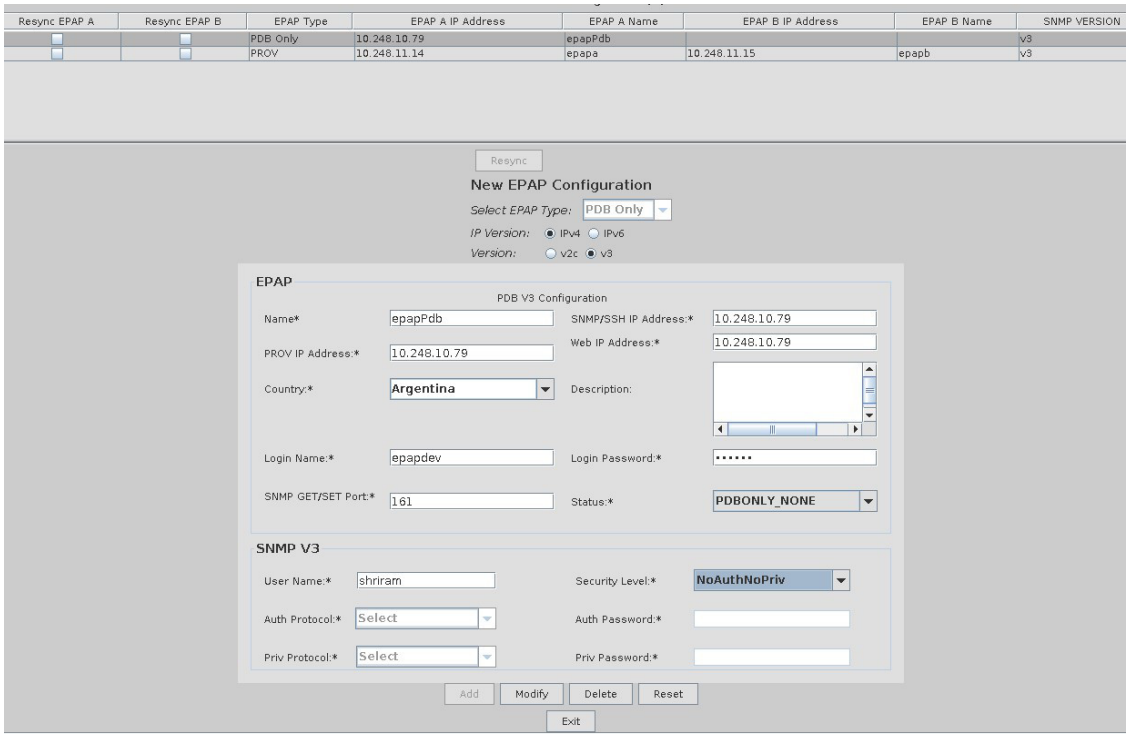


Figure 6-3 PDB Only EPAP Configuration (NoAuth/NoPriv)



As show in[Figure 6-1](#) and subsequent figures, 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 [V6] Address
Required IPv4 or IPv6 address used by EPAP for the SNMP interface. The IP version is set by the **Select IP Version** radio button.

PROV IP [V6] Address
Required IPv4 or IPv6 address used to provision EPAP. The IP version is set by the **Select IP Version** radio button.

Web IP [V6] Address
Required IPv4 or IPv6 address used by EPAP to access the web-based GUI. The IP version is set by the **Select IP Version** radio button.

> **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 OCEEMS; for information, see Adding a new country map to OCEEMS.

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 Get/Set Port
Required SNMP Agent Get/Set request port. Valid numeric values are 0 - 65535.

Status
Required current state of the EPAP server. OCEEMS 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 (Auth/Priv) fields are displayed as shown in Figure 6-4.

Figure 6-4 PROV/Non PROV EPAP Configuration (Auth/Priv)

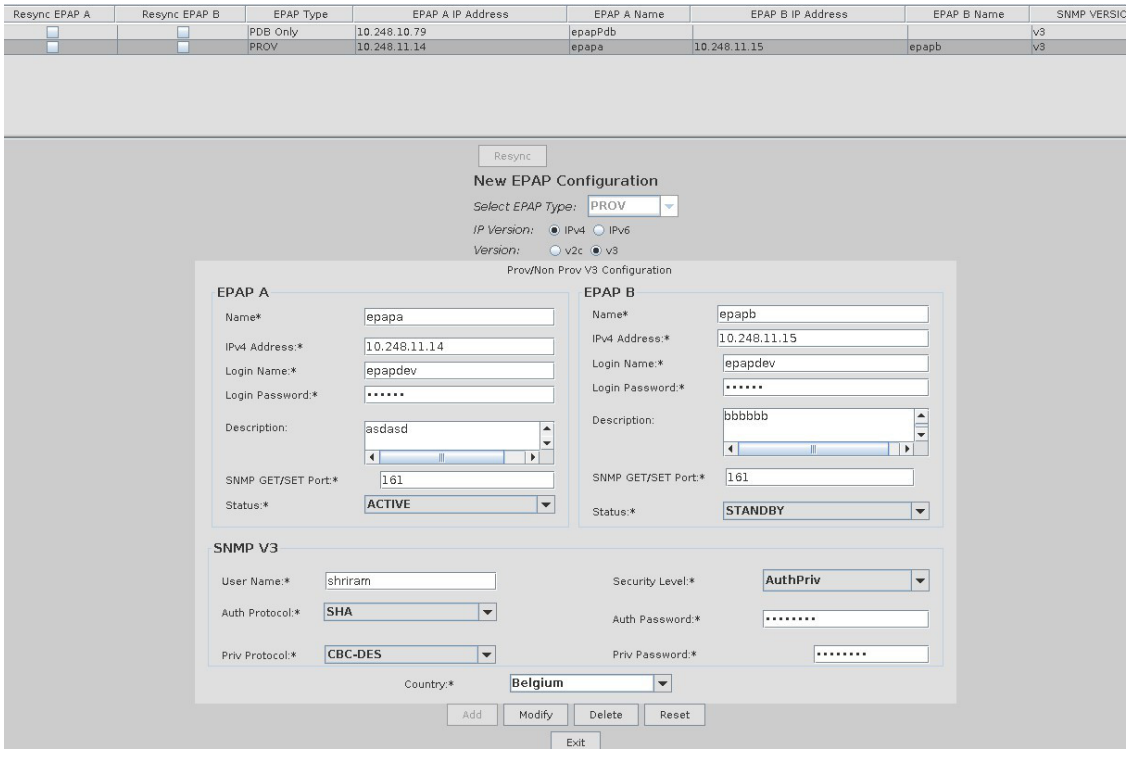


Figure 6-5 PROV/Non PROV EPAP Configuration (Auth/NoPriv)

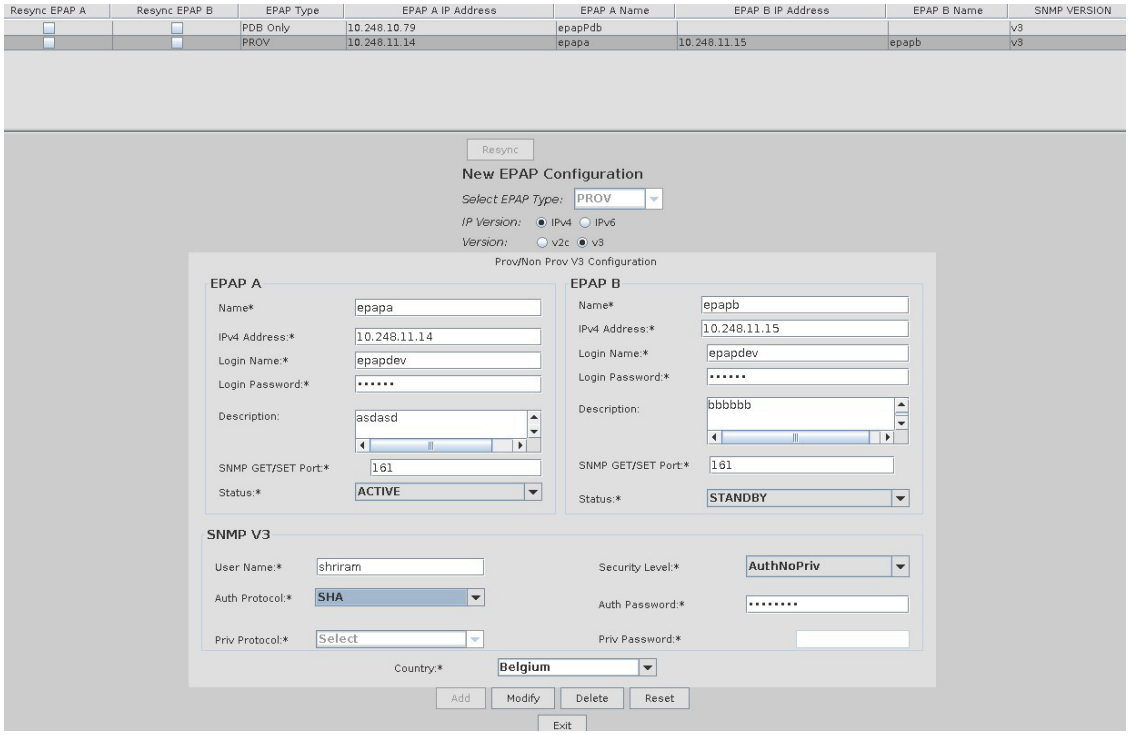
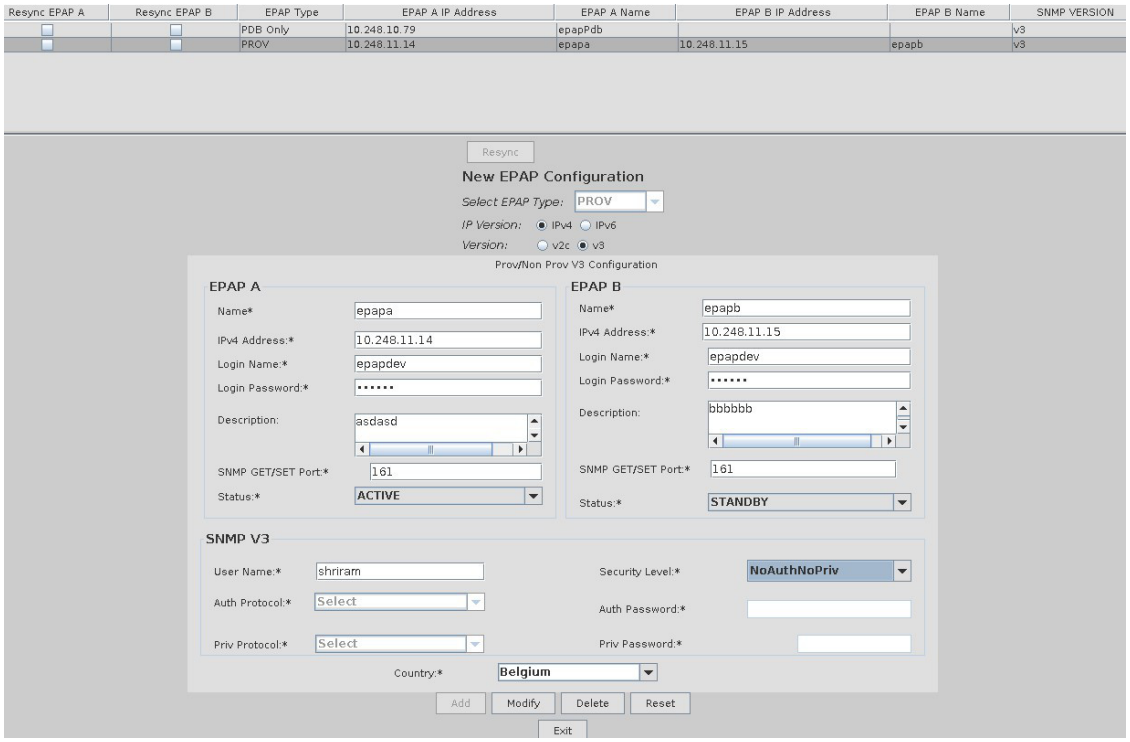


Figure 6-6 PROV/Non PROV EPAP Configuration (NoAuth/NoPriv)



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

Name
Required CLLI 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.

IPv4|v6 Address
Required IPv4 or IPv6 address for EPAP A and EPAP B. The IP version is set by the **Select IP Version** radio button.

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 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. OCEEMS 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 OCEEMS; for information, see Adding a new country map to OCEEMS.

SNMPv3 Discovery Required Fields

The following fields are required when the SNMPv3 radio button is selected:

User Name

Security Level (NoAuthNoPriv/AuthNoPriv/AuthPriv)

Auth Protocol (SHA)

Auth Password

Priv Protocol (DES/AES)

Priv Password

For SNMPv3 User Discovery, SNMP User Name and Security Level are compulsory fields based upon the selected Security Level. Users should observe the following UI scenarios:

- If Security Level is AuthPriv, then **Auth Protocol**, **Auth Password**, **Priv Protocol** & **Priv Password** are enabled.
- If Security Level is AuthNoPriv, then only **Auth Protocol** and **Auth Password** are enabled.
- If Security Level is NoAuthNoPriv, then no other fields are enabled.

Table 6-1 SNMPv3 Compliance Matrix

SNMPv3 User Security Level Configured on EPAP	SNMPv3 User Discovery on OCEEMS as AuthPriv	SNMPv3 User Discovery on OCEEMS as AuthNoPriv	SNMPv3 User Discovery on OCEEMS as NoAuthNoPriv
AuthPriv	Yes	No	No
AuthNoPriv	No	Yes	No
NoAuthNoPriv	No	No	Yes

Action Buttons

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

Add
The **Add** operation initiates the discovery process. While adding a EPAP, the user must provide details for the PROV, NON-PROV and PDB Only EPAP servers on the GUI. 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 OCEEMS 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 OCEEMS 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.

Database Tables

Table 6-2 stores all EPAP configuration data, including SNMPv3 User details and EPAP server details:

Table 6-2 Database Table - Tek_inventory_epapnode

Field Name	Type	Constraints	Description
MOID	bigint (20)	Primary Key	Auto generated Managed object ID
EPAPTYPE	varchar (10)		EPAP-A or EPAP-B or PDB Only
EPAPNAME	varchar (20)	Only alphanumeric characters, hyphen and underscore are allowed. It must have an alphabet as its first character. Length shall be between 5 to 20 characters. Must be unique.	EPAP Name

Table 6-2 (Cont.) Database Table - Tek_inventory_epapnode

Field Name	Type	Constraints	Description
EPAPIP	varchar (40)	Blank is not allowed. Should be a valid IP address. Must be unique.	EPAP IP
LOGINNAME	varchar (20)	Only alphanumeric characters, hyphen and underscore are allowed. It must have an alphabet as its first character. Length shall be between 5 to 20 characters.	EPAP server's login name
LOGINPWD	varchar (20)	String length cannot exceed 20 characters. Blank string not allowed.	EPAP login password
SNMPREAD	varchar (20)	String length cannot exceed 20 characters. Blank string not allowed.	EPAP SNMP-read protocol
SNMPWRITE	varchar (20)	String length cannot exceed 20 characters. Blank string not allowed.	EPAP SNMP-write protocol
PORT	int (11)	int length cannot exceed 11 characters. Blank port not allowed.	EPAP Port
STATUSSTRING	varchar (20)	String length cannot exceed 20 characters.	EPAP server's status
DESCRIPTION	varchar (200)	String length cannot exceed 200 characters.	EPAP description
COUNTRY	Varchar (40)	Length cannot exceed 200 characters.	Country where EPAP is deployed
PROVIP	varchar (40)	Length cannot exceed 40 characters.	EPAP Prov IP
WEBIP	varchar (40)	Length cannot exceed 40 characters	EPAP web IP
MATEDPAIR	varchar (20)	Length cannot exceed 20 characters	Name of the mated pair EPAP
ISEPAPA	bit (1)	Length cannot exceed 1 characters	EPAP SNMP version
IPADDVERSION	Varchar (2)	Length cannot exceed 2 characters	EPAP IP Address version (IPv4/IPv6)
SNMPV3USERNAME	Varchar (20)	Length cannot exceed 20 characters	EPAP SNMPv3 User Name (NULL in case of v2c)
SNMPV3SECURITYLEVEL	Varchar (20)	Length cannot exceed 20 characters	EPAP SNMPv3 Security Level (NULL in case of v2c)
SNMPV3AUTHPROTOCOL	Varchar (20)	Length cannot exceed 20 characters	EPAP SNMPv3 Auth Protocol Type (NULL in case of v2c)
SNMPV3AUTHPASSWORD	Varchar (100)	Length cannot exceed 20 characters	EPAP SNMPv3 Auth Password (NULL in case of v2c)

Table 6-2 (Cont.) Database Table - Tek_inventory_epapnode

Field Name	Type	Constraints	Description
SNMPV3PRIVPROTOCOL	Varchar (20)	Length cannot exceed 20 characters	EPAP SNMPv3 Privilege Protocol (NULL in case of v2c)
SNMPV3PRIVPASSWORD	varchar (100)	Length cannot exceed 20 characters	EPAP SNMPv3 Privilege Password (NULL in case of v2c)
VERSION	varchar (5)	Length cannot exceed 5 characters	EPAP version (v2c/v3)

Upon successful discovery of the LSMS Node, along with discovery of the SNMPv3 User, OCEEMS populates the USMTABLE, which contains SNMPv3 User details in encrypted format:

Table 6-3 Database Table - USMTABLE

Field Name	Type	Constraints	Description
DBKEY	VARCHAR (500)	Primary Key	Auto generated Managed object ID
HOST	VARCHAR (500)	Length cannot exceed 50 characters	Stores host IP
PORT	VARCHAR (5)	Length cannot exceed 5 characters	Stores port
ENGINENAME	VARCHAR (50)	Length cannot exceed 50 characters	Stores engine name
ENGINEID	VARCHAR (64)	Length cannot exceed 64 characters	Stores engine ID
USERNAME	VARCHAR (50)	Length cannot exceed 50 characters	Stores user name
SECURITYLEVEL	VARCHAR (5)	Length cannot exceed 5 characters	Stores security level
SECURITYNAME	VARCHAR (50)	Length cannot exceed 50 characters	Stores security name
AUTHPROTOCOL	VARCHAR (10)	Length cannot exceed 10 characters	Stores Auth Protocol type
AUTHPASSWORD	VARCHAR (255)	Length cannot exceed 255 characters	Stores Auth password
AUTHKEY	VARCHAR (255)	Length cannot exceed 255 characters	Stores Auth key
PRIVPROTOCOL	VARCHAR (10)	Length cannot exceed 10 characters	Stores Priv Protocol
PRIVPASSWORD	VARCHAR (255)	Length cannot exceed 255 characters	Stores priv Password
PRIVKEY	VARCHAR (255)	Length cannot exceed 255 characters	Stores Priv key ID
ENGINETIME	VARCHAR (10)	Length cannot exceed 10 characters	Stores enginetime
ENGINEBOOTS	VARCHAR (10)	Length cannot exceed 10 characters	Stores engineboots id

Table 6-3 (Cont.) Database Table - USMTABLE

Field Name	Type	Constraints	Description
LATESTRCVDENGTIME	VARCHAR (10)	Length cannot exceed 10 characters	Stores LATESTRCVDENGTIME
USMLOCALTIME	VARCHAR (30)	Length cannot exceed 30 characters	Stores USM local time

Table 6-4 Database Table - USERTABLE

Field Name	Type	Constraints	Description
DBKEY	VARCHAR (500)	Primary Key	Auto generated Managed object ID
HOST	VARCHAR (50)	Length cannot exceed 50 characters	Stores host IP
PORT	VARCHAR (5)	Length cannot exceed 5 characters	Stores EPAP port
ENGINENAME	VARCHAR (50)	Length cannot exceed 50 characters	Stores SNMPv3 engine name
USERNAME	VARCHAR (50)	Length cannot exceed 50 characters	Stores SNMPv3 username
AUTHPROTOCOL	VARCHAR (10)	Length cannot exceed 10 characters	Stores Auth Protocol of SNMPv3 user
AUTHPASSWORD	VARCHAR (255)	Length cannot exceed 255 characters	Stores Auth Password of SNMPv3 user
PRIVPROTOCOL	VARCHAR (10)	Length cannot exceed 10 characters	Stores Priv Protocol of SNMPv3 user
PRIVPASSWORD	VARCHAR (255)	Length cannot exceed 255 characters	Stores Priv Password of SNMPv3 user

Table 6-5 Database Table - ENGINETABLE

Field Name	Type	Constraints	Description
DBKEY	VARCHAR (500)	Primary Key	Auto generated Managed object ID
HOST	VARCHAR (50)	Length cannot exceed 50 characters	Stores host IP
PORT	VARCHAR (5)	Length cannot exceed 5 characters	Stores port
ENGINENAME	VARCHAR (50)	Length cannot exceed 50 characters	Stores engine name
ENGINEID	VARCHAR (64)	Length cannot exceed 64 characters	Stores engine ID
ENGINETIME	VARCHAR (10)	Length cannot exceed 10 characters	Stores enginetime
ENGINEBOOTS	VARCHAR (10)	Length cannot exceed 10 characters	Stores engineboots id

Sample Configuration Data for SNMP Connection to EPAP

This example shows configuration of EPAP and OCEEMS for an SNMP connection to EPAP.

SNMP Configuration on EPAP

Use the following steps to configure EPAP:

1. Log into EPAP via SSH.
2. Access the EPAP Configuration Menu:

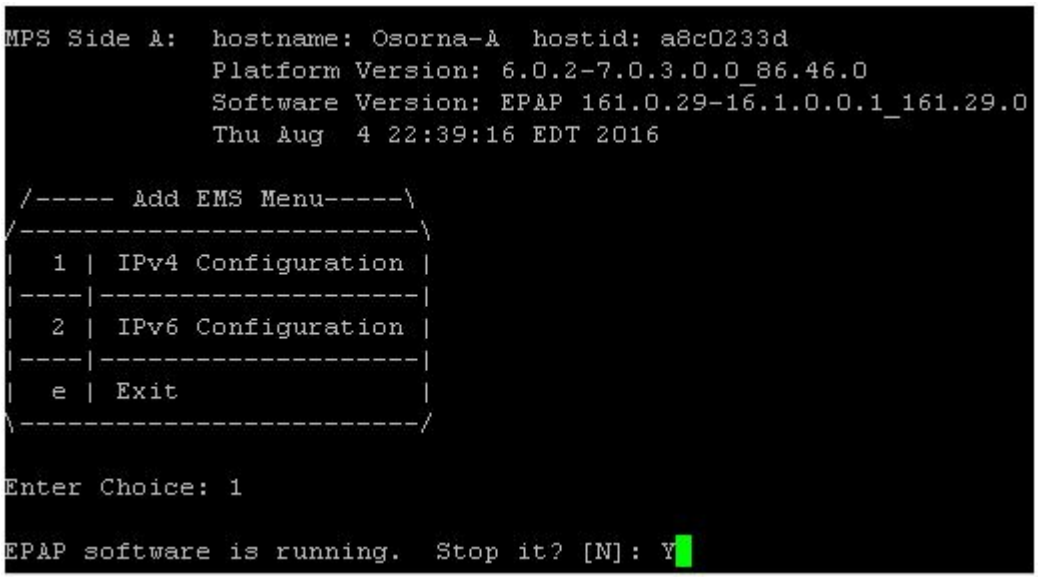
   ```
   $ sudo su – epapconfig
   ```

3. Enter choice **14** for Configure SNMP Agent Community, and provide the **SNMP Read Community** and **SNMP Write Community** strings as shown in #unique_41/unique_41_Connect_42_V6497078.

Figure 6-7 Configure SNMP Agent Community

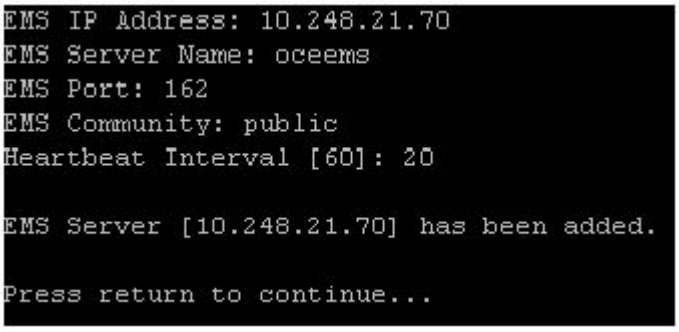
4. Enter choice **10** to SNMP configuration, followed by choice 5 to add an EMS server.
5. On the Add EMS Menu, select the type of configuration (**1** for IPv4 or **2** for IPv6) and stop the EPAP software if it is running, as shown in Figure 6-8.

Figure 6-8 Add EMS Menu



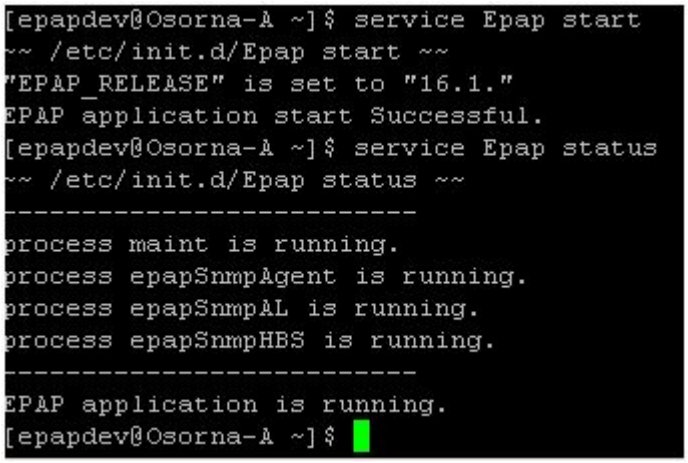
6. Enter the configuration details for the OCEEMS server, including the OCEEMS IP address, OCEEMS server name, the port for receiving SNMP traps (preferably 162), the community string, and the heartbeat time interval, as shown in Figure 6-9.

Figure 6-9 Sample Configuration Details for OCEEMS Server



7. Restart EPAP with the `service epap start` command, as shown in Figure 6-10.

Figure 6-10 Restarting EPAP

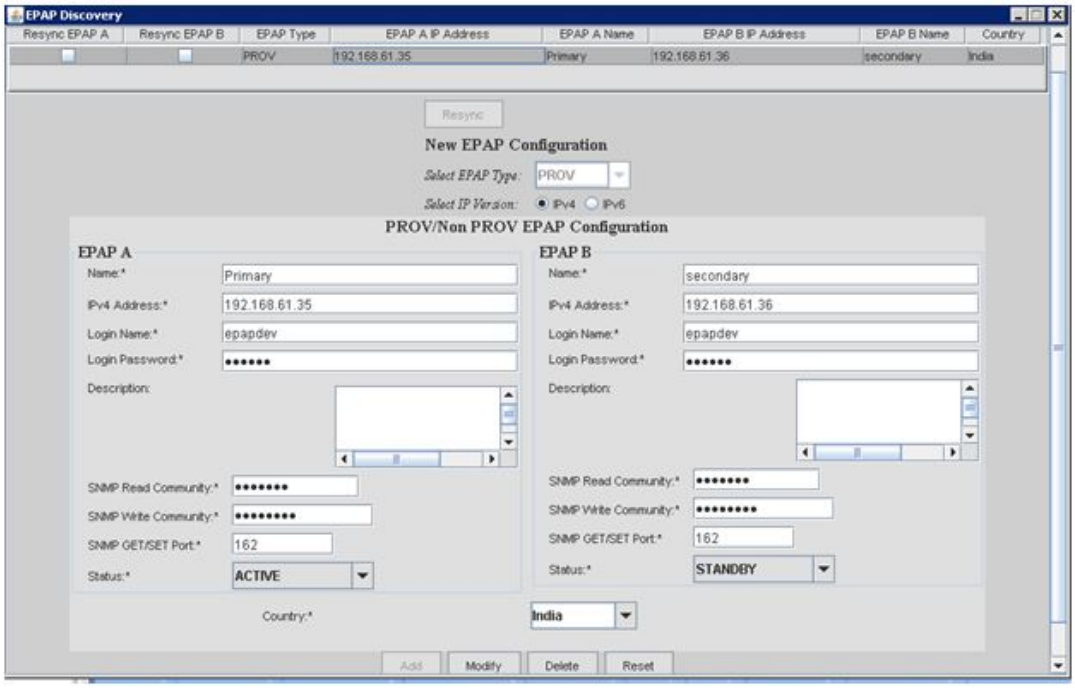


SNMP Configuration on OCEEMS for EPAP Discovery

Use the following steps to configure OCEEMS:

1. Log in to the OCEEMS application.
2. Use the EPAP Discovery GUI (**Tools**, and then **EPAP Discovery**) to add details for both the primary and standby EPAP servers, as shown in Figure 6-11.

Figure 6-11 Sample EPAP Discovery



For **Login Name** and **Login Password**, use the same credentials that were used to log into EPAP in step 1 in SNMP Configuration on EPAP.

For **SNMP Read Community**, **SNMP Write Community**, and **SNMP GET/SET Port**, use the same values that were configured in step 6 in SNMP Configuration on EPAP.

For EPAP **Status**, select the appropriate status (**Active**, **Standby**, **Force Standby**, **None**, **Up**, **Down**) for each server. The status can be checked on the EPAP side by using the `service Epap status` command.

Map Views

OCEEMS 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 6-12.

Figure 6-12 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 OCEEMS. For information, see Adding a new country map to OCEEMS.

For more information about map views, see Map View Features.

Cut Through Interface from Maps to EPAP

OCEEMS 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 OCEEMS user must provide login credentials on the launched interface.

Fault Management

The OCEEMS provides fault management support for EPAP on SNMPv3 over southbound Interface. SNMPv3 defines a user-based security mechanism that enables per-message authentication and encryption. OCEEMS works as SNMP Manager and EPAP acts as the SNMP Agent. Both the SNMP Agent & SNMP Manager need to maintain an entry for one another in order to exchange data. The OCEEMS fault management support for EPAP includes the following:

- Events and Alarms Viewer
- Event and Notification Details
- Alarm Acknowledgement and Clear
- Alarm Maintenance/Active Mode
- Northbound Interface
- Status Management

For general information about OCEEMS fault management, see Fault Management.

Events and Alarms Viewer

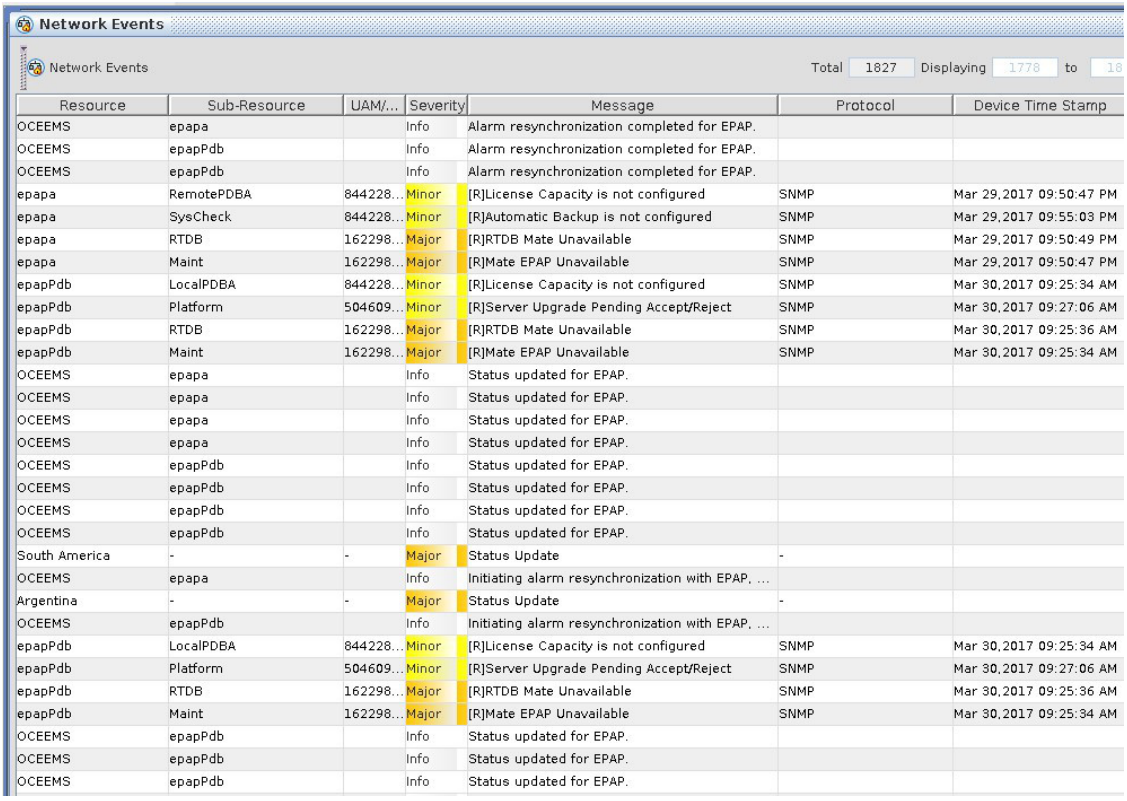
The alarms received from EPAP are displayed on the graphical maps and Text-Based interfaces. The SNMP traps received from EPAP are processed into events and displayed in the Network Events GUI in OCEEMS. Events that are associated with a defined pair event number are further processed into alarms and displayed in the Alarms GUI (**Fault Management**, and then **Alarms**) and map 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.

Alarms are only parsed by OCEEMS if they are valid alarms. Each trap received from EPAP is first validated against the entries present in USMTABLE for the EPAP SNMPv3 User. If the details present in the trap are authenticated by the USM Security Model, the traps are forwarded through OCEEMS trap filters and are parsed accordingly.

Network events received over SNMPv3 Protocol will have the protocol version set as SNMPv3 on the Network Events GUI.

Figure 6-13 EPAP Network Event GUI



Resource	Sub-Resource	UAM/...	Severity	Message	Protocol	Device Time Stamp
OCEEMS	epapa		Info	Alarm resynchronization completed for EPAP.		
OCEEMS	epapPdb		Info	Alarm resynchronization completed for EPAP.		
OCEEMS	epapPdb		Info	Alarm resynchronization completed for EPAP.		
epapa	RemotePDBA	844228...	Minor	[R]License Capacity is not configured	SNMP	Mar 29,2017 09:50:47 PM
epapa	SysCheck	844228...	Minor	[R]Automatic Backup is not configured	SNMP	Mar 29,2017 09:55:03 PM
epapa	RTDB	162298...	Major	[R]RTDB Mate Unavailable	SNMP	Mar 29,2017 09:50:49 PM
epapa	Maint	162298...	Major	[R]Mate EPAP Unavailable	SNMP	Mar 29,2017 09:50:47 PM
epapPdb	LocalPDBA	844228...	Minor	[R]License Capacity is not configured	SNMP	Mar 30,2017 09:25:34 AM
epapPdb	Platform	504609...	Minor	[R]Server Upgrade Pending Accept/Reject	SNMP	Mar 30,2017 09:27:06 AM
epapPdb	RTDB	162298...	Major	[R]RTDB Mate Unavailable	SNMP	Mar 30,2017 09:25:36 AM
epapPdb	Maint	162298...	Major	[R]Mate EPAP Unavailable	SNMP	Mar 30,2017 09:25:34 AM
OCEEMS	epapa		Info	Status updated for EPAP.		
OCEEMS	epapa		Info	Status updated for EPAP.		
OCEEMS	epapa		Info	Status updated for EPAP.		
OCEEMS	epapa		Info	Status updated for EPAP.		
OCEEMS	epapPdb		Info	Status updated for EPAP.		
OCEEMS	epapPdb		Info	Status updated for EPAP.		
OCEEMS	epapPdb		Info	Status updated for EPAP.		
OCEEMS	epapPdb		Info	Status updated for EPAP.		
South America	-	-	Major	Status Update	-	
OCEEMS	epapa		Info	Initiating alarm resynchronization with EPAP, ...		
Argentina	-	-	Major	Status Update	-	
OCEEMS	epapPdb		Info	Initiating alarm resynchronization with EPAP, ...		
epapPdb	LocalPDBA	844228...	Minor	[R]License Capacity is not configured	SNMP	Mar 30,2017 09:25:34 AM
epapPdb	Platform	504609...	Minor	[R]Server Upgrade Pending Accept/Reject	SNMP	Mar 30,2017 09:27:06 AM
epapPdb	RTDB	162298...	Major	[R]RTDB Mate Unavailable	SNMP	Mar 30,2017 09:25:36 AM
epapPdb	Maint	162298...	Major	[R]Mate EPAP Unavailable	SNMP	Mar 30,2017 09:25:34 AM
OCEEMS	epapPdb		Info	Status updated for EPAP.		
OCEEMS	epapPdb		Info	Status updated for EPAP.		
OCEEMS	epapPdb		Info	Status updated for EPAP.		

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.

OCEEMS automatically triggers southbound resynchronization under the scenarios listed in Table 6-6.

Table 6-6 Automatic Resynchronization Scenarios

Scenarios	Message
On EPAP addition	EPAP added to OCEEMS.
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 OCEEMS server.

Corresponding resynchronization events are raised along with client notifications:

- Automatic resynchronization initiated

Table 6-7 Event Details - Automatic Resynchronization Initiated

Element	Description
Source	OCEEMS
Sub Resource	<EPAP NAME>
Severity	Info
Category	Fault
Message	Initiating alarm resynchronization with EPAP.
Reason	See Table 6-6.

The following notification is sent:

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

- Automatic resynchronization successful

Table 6-8 Event Details - Automatic Resynchronization Successful

Element	Description
Source	OCEEMS
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 6-9 Event Details - Automatic Resynchronization Failure

Element	Description
Source	OCEEMS
Sub Resource	<EPAP NAME>
Severity	Info
Category	Fault
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 6-10 Event Details - Resynchronization Initiated by User

Element	Description
Source	OCEEMS
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 6-11 Event Details - Resynchronization Initiated by User Is Successful

Element	Description
Source	OCEEMS
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 6-12 Event Details - Resynchronization Initiated by User Has Failed

Element	Description
Source	OCEEMS
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 6-13 Event Details - Buffer Overflow During Southbound Resynchronization

Element	Description
Source	OCEEMS
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, OCEEMS 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 6-14 Event Details - Traps Buffer Overflow

Element	Description
Source	OCEEMS
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 OCEEMS fault management module listens for a heartbeat trap at a configured interval (default is 15 minutes) to verify connectivity with EPAP servers.

Table 6-15 Event Details - Heartbeat Trap Not Received at Configured Interval

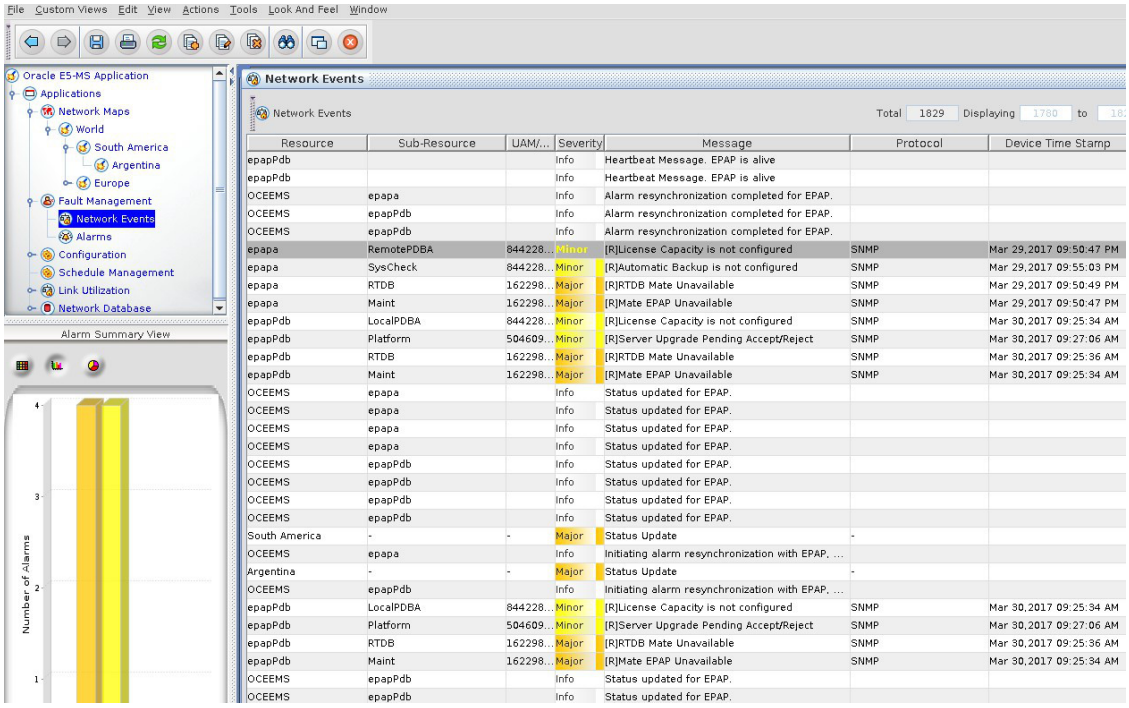
Element	Description
Source	OCEEMS
Sub Resource	AlarmMemory_<EPAP NAME>
Severity	Warning/Critical depending upon the alarm raised
Message	Cannot connect to EPAP for receiving alarms

OCEEMS notifies all active OCEEMS client sessions with the following message:

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

For a complete list of messages, see EPAP Support Messages.

Figure 6-14 EPAP Network Event Details GUI



Alarm Correlation and Aggregation

The OCEEMS fault management module applies correlation to only those EPAP events that have corresponding pair events of "clear" severity.

OCEEMS 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

OCEEMS 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 OCEEMS (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

OCEEMS 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 OCEEMS 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 OCEEMS, 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 OCEEMS, 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

OCEEMS 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 OCEEMS for incoming event
- Outgoing alertAcknowledgeMode = Acknowledge value as available in OCEEMS
- Outgoing alertTextMessage = As received in incoming event
- Outgoing alertSequenceNumber = Set by OCEEMS northbound interface module
- Outgoing alertSourceIp = As received in incoming event

Status Management

OCEEMS manages EPAP status as follows:

- OCEEMS 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 OCEEMS. 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.

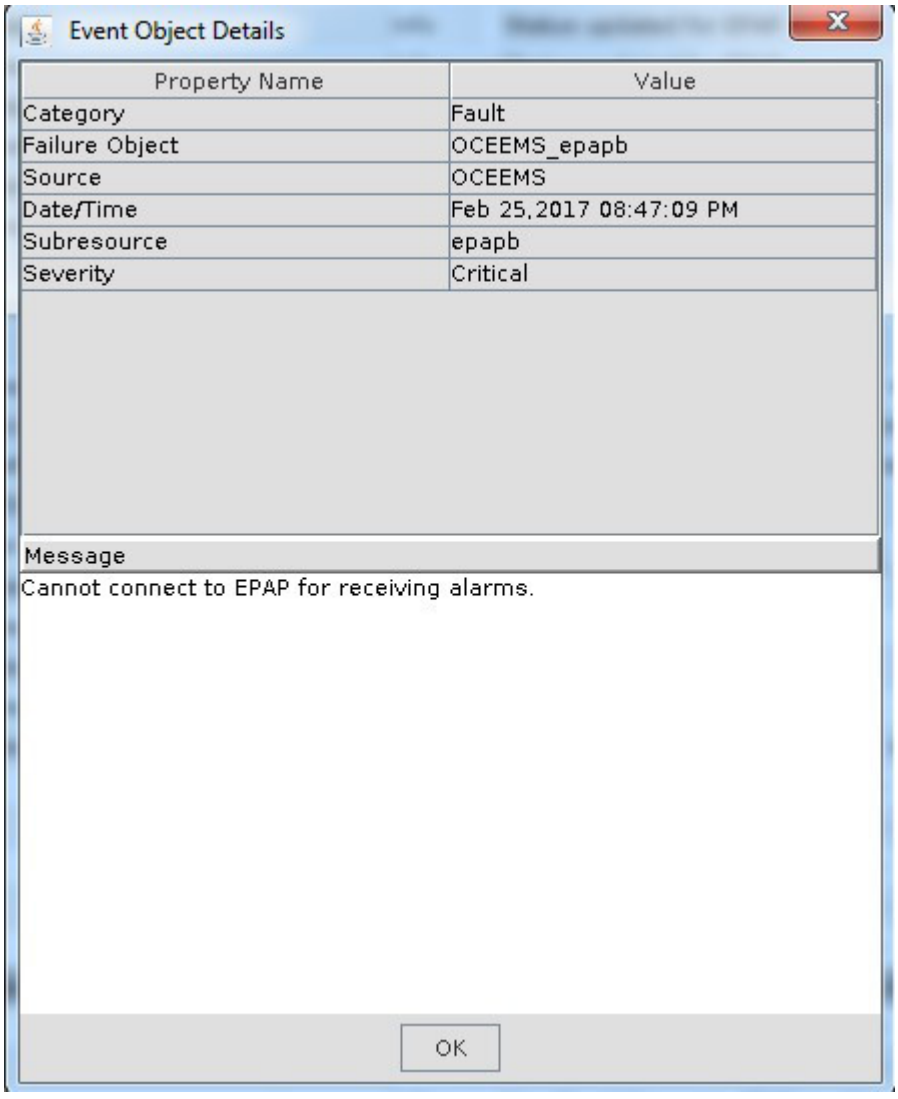
Heartbeat Support

OCEEMS Fault Management module listens for a 'heartbeat Trap' at configured intervals (default 15 minutes) to verify connectivity with the EPAP server. In the event that the specified trap is not received for the configured interval, a warning alarm will be raised, followed by a Critical alarm after each time the configured interval lapses. For each failed attempt at verifying connectivity with the EPAP server, OCEEMS will keep an incremental count.

Table 6-16 Event Details - Cannot Connect to EPAP

Element	Description
Source	OCEEMS
Sub Resource	<EPAP Name>
Severity	Critical
Message	Cannot connect to EPAP for receiving alarms

Figure 6-15 OCEEMS Raised Critical "Cannot connect to EPAP" Alarm



Resynchronization Mechanism

The OCEEMS supports Resync Mechanism during EPAP discovery (addition/modification) for users with resync privilege. The OCEEMS may fail to fetch the status of EPAP (failure getting the output of the EPAP status command `hastatus`). In this case, Resync Required Event is raised by the EPAP server. The OCEEMS addresses this request raised by the EPAP server.

Resync is executed on the OCEEMS for the following scenarios:

- A new EPAP is added by the user
- The SNMP version of an existing EPAP is being modified from v2c to v3 by the user
- The SNMP version of an existing EPAP is being modified from v3 to v2c by the user
- During the warm start of the OCEEMS server
- A Resync Request is raised by the EPAP Server
- Any field of the EPAP entry is modified

> **Note**
>
> The EPAP server may reject a Resync Request by the OCEEMS server if a Resync is already in progress.

EPAP Resync Option in Discovery GUI

The user can access the Resync option three different ways: by doing one of the following:

1. From the EPAP Discovery GUI and Maps area:

Figure 6-16 EPAP Resync Option in EPAP Discovery GUI

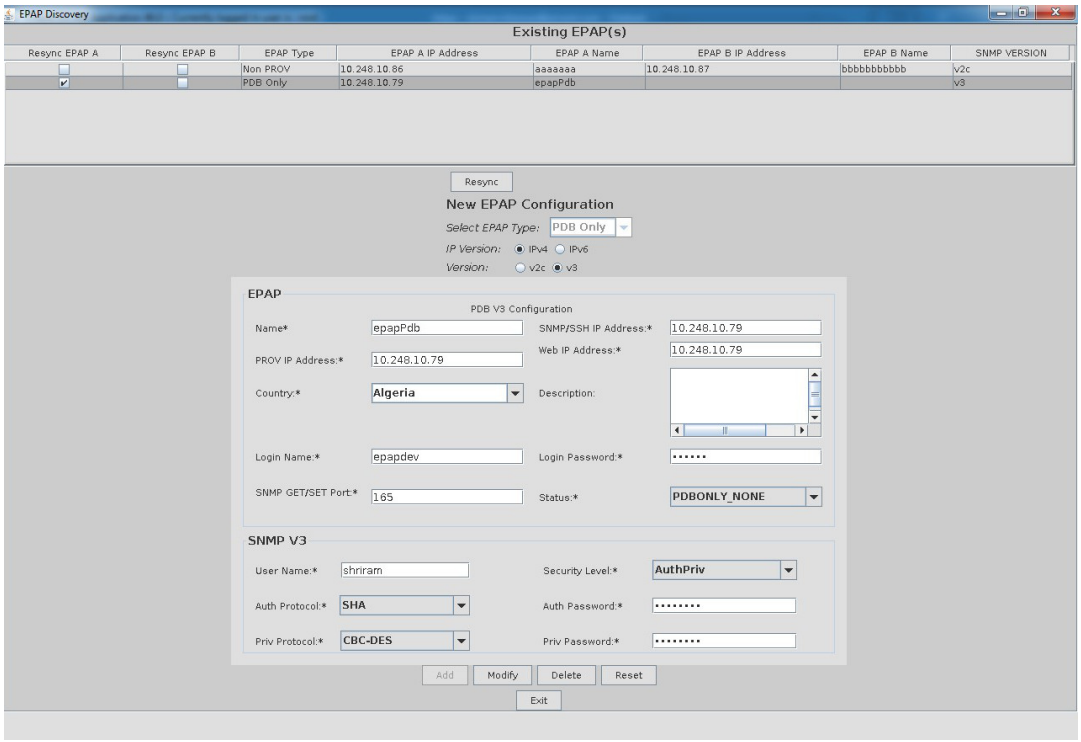
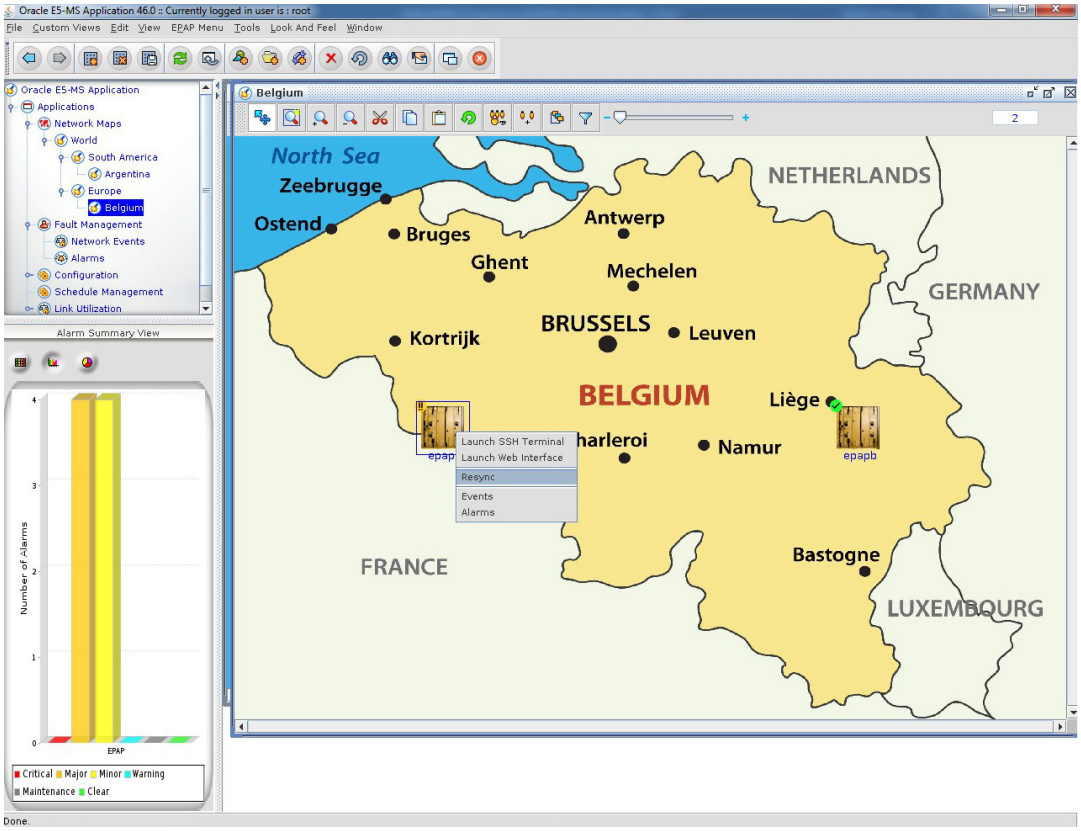
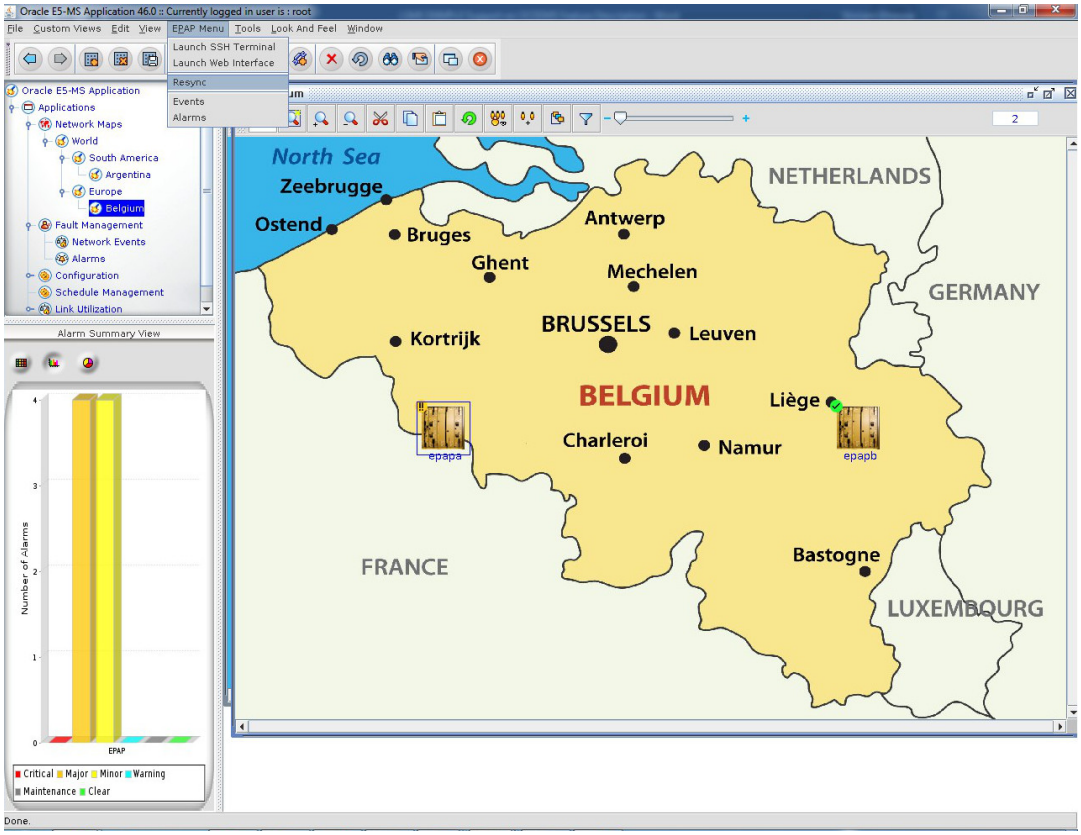


Figure 6-17 EPAP Resync Option in Maps Area



2. Right-clicking on the EPAP Node and selecting the **Resync** option:
3. Selecting the Resync option from the EPAP Menu bar when the EPAP Server Node is selected from Maps:

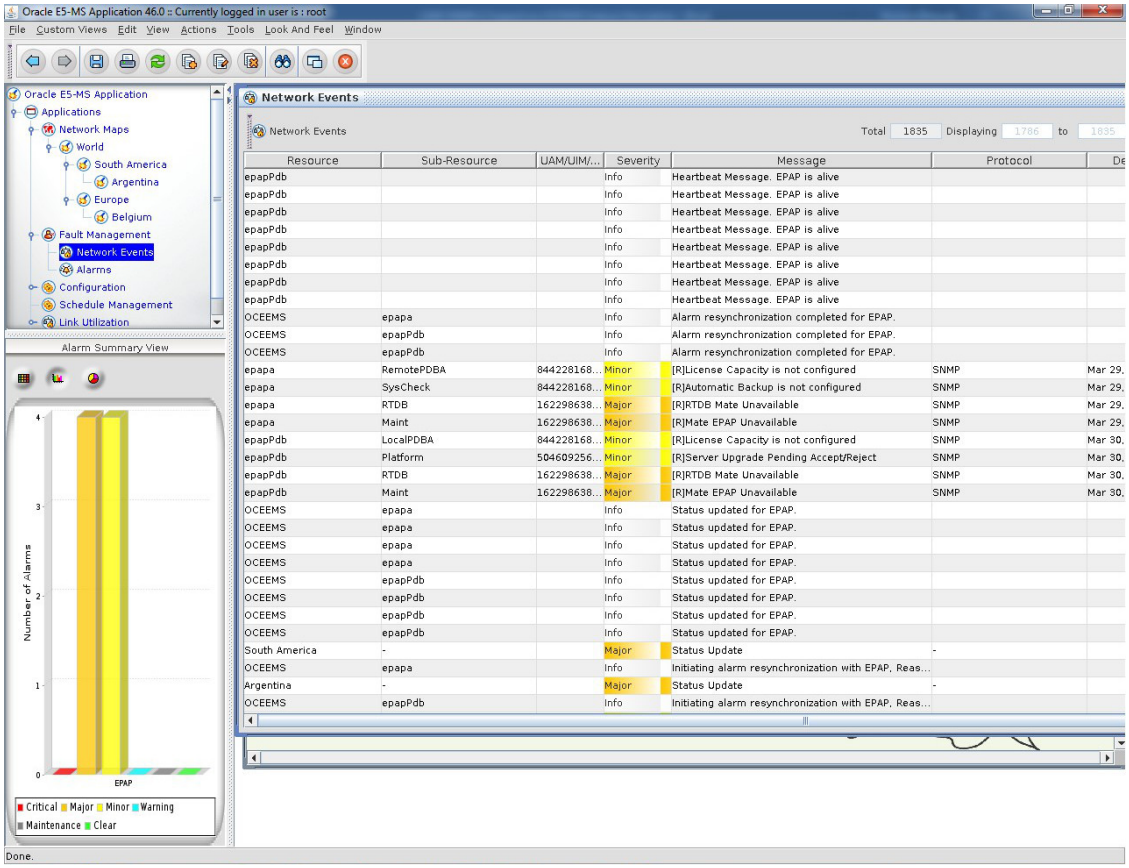
Figure 6-18 EPAP Resync Option in Maps - Menu Bar



The OCEEMS provides Resync capability on both primary and secondary EPAP servers concurrently by allowing the user to select the appropriate checkbox for the Resync that needs to be initiated.

The OCEEMS displays all resynced Alarms in the Network Events GUI with an R added to the start of the Message:

Figure 6-19 EPAP Alarm Resync



7

OCEEMS Support of LSMS Alarms via SNMP Feed

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

Overview

OCEEMS Support of LSMS Alarms via SNMPv3 Feed enables the use of the OCEEMS to manage LSMS alarms through the following interfaces:

- Discovery
  The LSMS Discovery interface enables discovery and configuration of LSMS servers in the OCEEMS.
- Map
  The map interface displays discovered LSMS servers in the OCEEMS 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 OCEEMS is through an LSMS Discovery menu. LSMS Discovery is supported for both SNMPv1 and SNMPv3 protocols. LSMS nodes are then visible in the fault management menus and maps. The OCEEMS 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 OCEEMS. This alarm feed is processed by OCEEMS and presented to the user in the form of events and alarms.

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

For additional information about the LSMS configuration required, see *Configuring an SNMP Agent* in *LSMS Alarms and Maintenance Guide*.

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 OCEEMS defines an LSMS node as follows:

- Each LSMS server is considered a node (2 servers = 2 nodes).
- The NAS is not visible to OCEEMS 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 OCEEMS 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 OCEEMS.

LSMS Discovery Menu

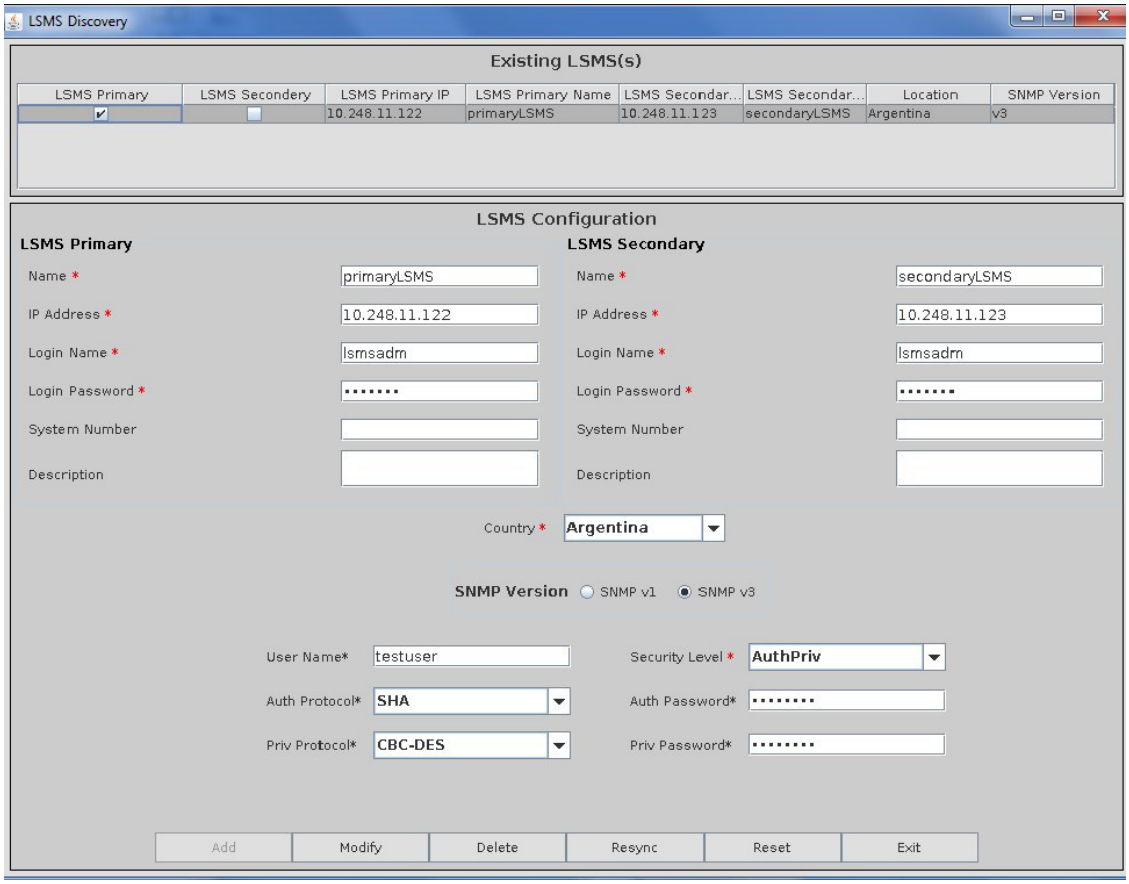
From the OCEEMS menu bar, select **Tools**, and then **LSMS Discovery** to access the LSMS Discovery application and discover LSMS servers within your network. LSMS Discovery is supported for both SNMPv1 and SNMPv3 protocols.

> **Note**
>
> **Tools**, and then **LSMS Discovery** is an available choice only for users who have permission to the **LSMS Discovery** administrative operation.

As shown in Figure 7-1, the LSMS Discovery screen contains the following sections:

- Existing LSMS(s)
  This section displays a list of previously added LSMS nodes; resync operation button is made available
- LSMS Configuration
  This section shows the required and optional fields used for LSMS discovery, along with SNMPv3 user Discovery fields. 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**, **Resync**,**Reset**, and **Exit** operations.

Figure 7-1 LSMS Discovery Screen (Auth/Priv)



> **Note**
>
> If SNMPv3 is chosen, then Resync option will be disabled.

Figure 7-2 LSMS Discovery Screen (Auth/NoPriv)

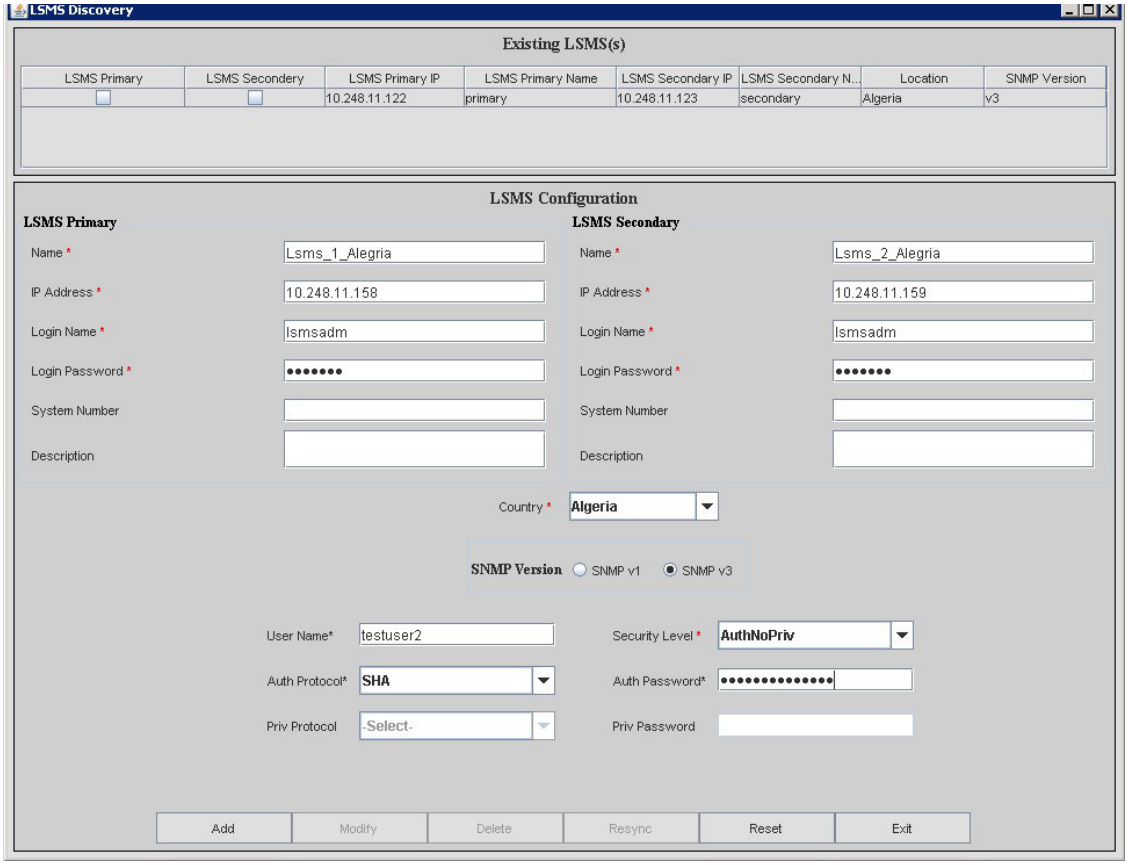
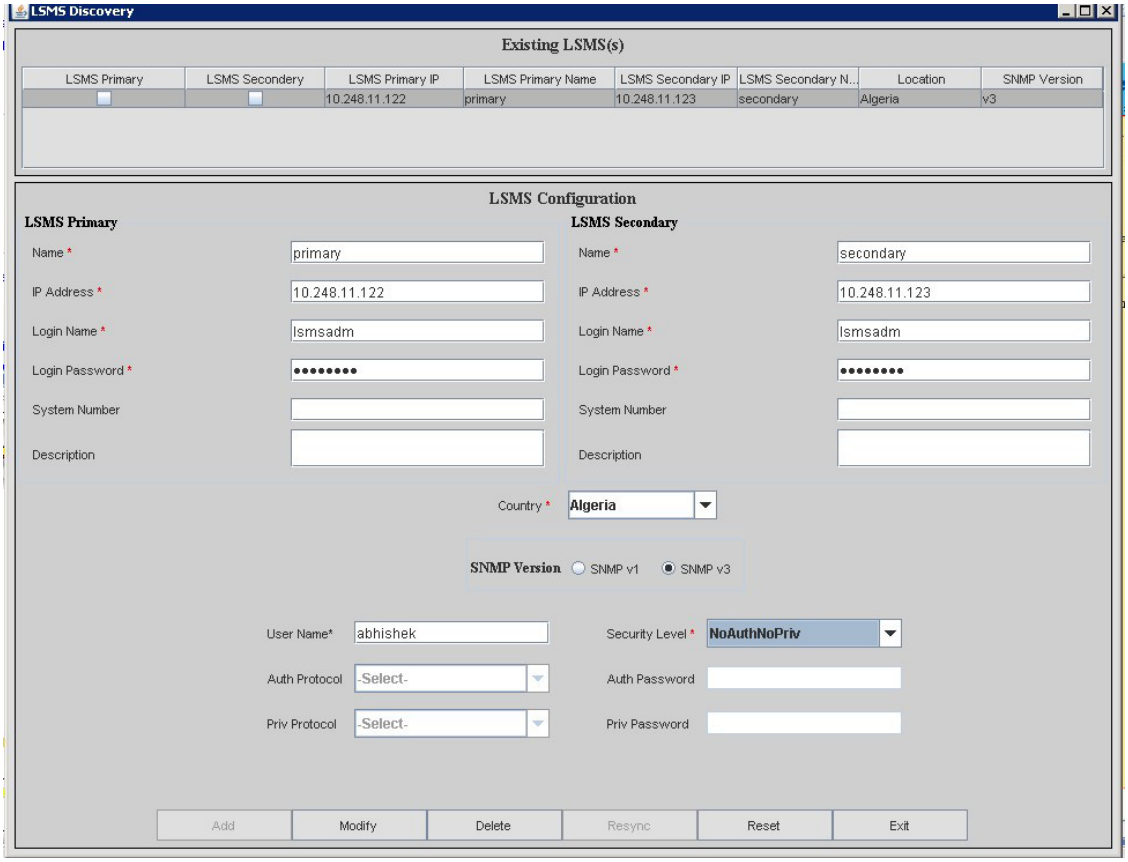


Figure 7-3 LSMS Discovery Screen (NoAuth/NoPriv)



As shown in Figure 7-1 and subsequent figures, the LSMS Discovery screen contains the following fields:

Name
Required **CLII** 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 OCEEMS 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 OCEEMS; for information, see Adding a new country map to OCEEMS.

SNMPv3 Discovery Required Fields

The following fields are required when the SNMPv3 radio button is selected:

User Name

Security Level (NoAuthNoPriv/AuthNoPriv/AuthPriv)

Auth Protocol (SHA)

Auth Password

Priv Protocol (DES/AES)

Priv Password

For SNMPv3 User Discovery, SNMP User Name and Security Level are compulsory fields based upon the selected Security Level. Users should observe the following UI scenarios:

- If Security Level is AuthPriv, then **Auth Protocol**, **Auth Password**, **Priv Protocol** & **Priv Password** are enabled.
- If Security Level is AuthNoPriv, then only **Auth Protocol** and **Auth Password** are enabled.
- If Security Level is NoAuthNoPriv, then no other fields are enabled.

Table 7-1 SNMPv3 Compliance Matrix

SNMPv3 User Security Level Configured on LSMS	SNMPv3 User Discovery on OCEEMS as AuthPriv	SNMPv3 User Discovery on OCEEMS as AuthNoPriv	SNMPv3 User Discovery on OCEEMS as NoAuthNoPriv
AuthPriv	Yes	No	No
AuthNoPriv	No	Yes	No
NoAuthNoPriv	No	No	Yes

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 OCEEMS 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 OCEEMS database. Upon successful deletion, LSMS nodes are removed from the Existing LSMS(s) section.

Resync
The **Resync** operation initiates a manual resync of the LSMS alarm state.

Reset
The **Reset** operation resets all LSMS Discovery configuration components to their default state.

Exit
The **Exit** operation exits the LSMS Discovery GUI.

Database Tables

Table 7-2 stores all LSMS configuration data, including SNMPv3 User details and LSMS server details:

Table 7-2 Database Table - Tek_inventory_lsmsnode

Field Name	Type	Constraints	Description
MOID	bigint(20)	Primary Key	Auto generated Managed object ID
LSMSTYPE	varchar(10)		Primary or Secondary
LSMSNAME	varchar(20)	Only alphanumeric characters, hyphen and underscore are allowed. It must have an alphabet as its first character. Length shall be between 5 to 20 characters. Must be unique.	LSMS Primary Name
LSMIIP	varchar(20)	Blank is not allowed. Should be a valid IP address. Must be unique.	LSMS IP
LSMSLOGINNAME	varchar(20)	Only alphanumeric characters, hyphen and underscore are allowed. It must have an alphabet as its first character. Length shall be between 5 to 20 characters.	LSMS server's login name
LSMSLOGINPWD	varchar(20)	String length cannot exceed 20 characters. Blank string not allowed.	LSMS login password
LSMSSTATUS	varchar(20)		LSMS server's status
LSMSSYSNUMBER	varchar(20)	String length cannot exceed 20 characters.	LSMS system number

Table 7-2 (Cont.) Database Table - Tek_inventory_lsmsnode

Field Name	Type	Constraints	Description
LSMSDESC	Varchar(200)	Length cannot exceed 200 characters.	Description about LSMS
LSMSCOUNTRY	varchar(40)		Country where LSMS is deployed
MATEDPAIR	varchar(20)		Name of the mated pair LSMS
LSMSSNMPVERSION	Varchar(2)		LSMS SNMP version
LSMSSNMPV3USERNAME	Varchar(20)		LSMS SNMPv3 User Name (NULL in case of v1)
LSMSSNMPV3SECURITY	Varchar(20)		LSMS SNMPv3 Security Level (NULL in case of v1)
LSMSSNMPV3AUTHTYPE	Varchar(20)		LSMS SNMPv3 Auth Protocol Type (NULL in case of v1)
LSMSSNMPV3AUTHPWD	Varchar(20)		LSMS SNMPv3 Auth Password (NULL in case of v1)
LSMSSNMPV3PRIVTYPE	Varchar(20)		LSMS SNMPv3 Privilege Protocol (NULL in case of v1)
LSMSSNMPV3PRIVPWD	Varchar(20)		LSMS SNMPv3 Privilege Password (NULL in case of v1)

Upon successful discovery of the LSMS Node, along with discovery of the SNMPv3 User, OCEEMS populates the USMTABLE, which contains SNMPv3 User details in encrypted format:

Table 7-3 Database Table - USMTABLE

Field Name	Type	Constraints	Description
DBKEY	VARCHAR(500)	Primary Key	Auto generated Managed object ID

Table 7-4 Database Table - USERTABLE

Field Name	Type	Constraints	Description
DBKEY	VARCHAR(500)	Primary Key	Auto generated Managed object ID
AUTHPASSWORD	VARCHAR(255)		Stores Auth Password of SNMPv3 user
PRIVPASSWORD	VARCHAR(255)		Stores Priv Password of SNMPv3 user

Table 7-5 Database Table - ENGINETABLE

Field Name	Type	Constraints	Description
DBKEY	VARCHAR(500)	Primary Key	Auto generated Managed object ID

Sample Configuration Data for SNMP Connection to LSMS

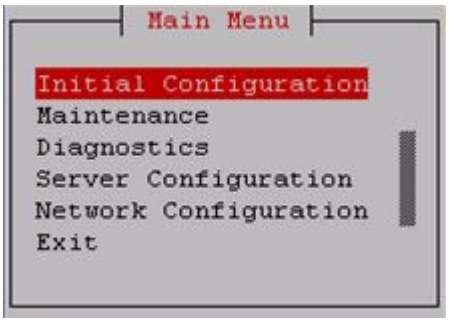
This example shows configuration of LSMS and OCEEMS for an SNMP connection to LSMS.

SNMP Configuration on LSMS

Use the following general steps to configure LSMS. For complete information about SNMP configuration on LSMS, see *Configuring the SNMP Agent* in the LSMS *Alarms and Maintenance Guide*.

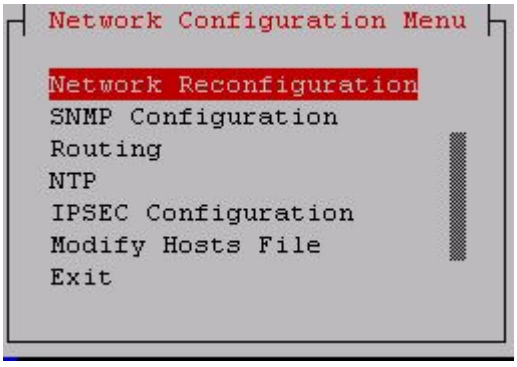
1. Log into LSMS via SSH.
2. Change the user to lsmsmgr to access the lsmsmgr user interface Main Menu:

Figure 7-4 Main Menu for lsmsmgr User Interface



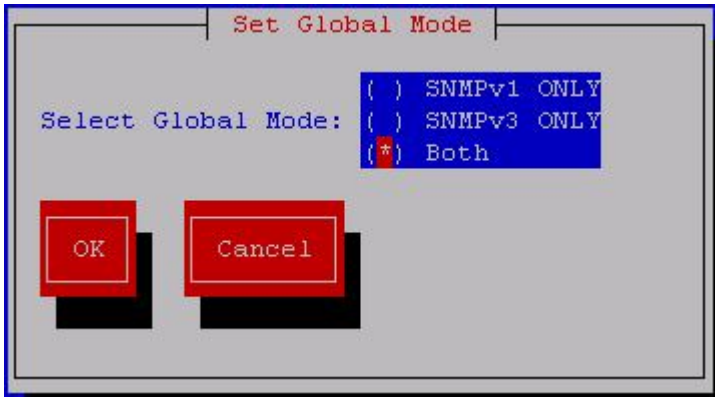
3. On the Main Menu, use the arrow keys to select **Network Configuration**.
The Network Configuration Menu is displayed:

Figure 7-5 Network Configuration Menu



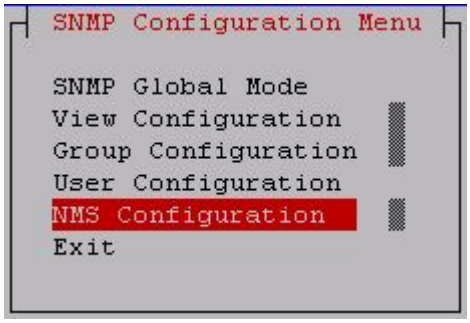
4. On the Network Configuration Menu, select **SNMP Configuration**.
5. On the SNMP Configuration Menu, select **SNMP Global Mode**.
The Set Global Mode screen is displayed to set the SNMP global mode:

Figure 7-6 Set Global Mode



6. To use SNMPv3, configure one or more SNMPv3 views (**SNMP Configuration**, and then **View Configuration**), one or more SNMPv3 groups (**SNMP Configuration**, and then **Group Configuration**) that use the SNMPv3 views, and one or more SNMPv3 users (**SNMP Configuration**, and then **User Configuration**) associated with the SNMPv3 groups. For details, see *Configuring the SNMP Agent* in the LSMS *Alarms and Maintenance Guide*.
7. On the SNMP Configuration Menu, select **NMS Configuration**:

Figure 7-7 NMS Configuration on the SNMP Configuration Menu

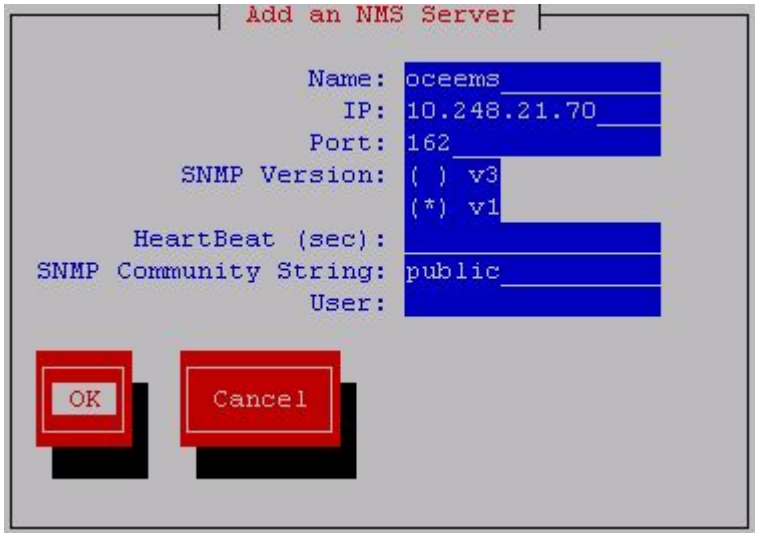


8. On the NMS Server Action Menu, select **Add NMS Server**:

Figure 7-8 Add NMS Server on the NMS Server Action Menu

9. On the Add an NMS Server screen, enter/select values for the OCEEMS **Name**, **IP** address, **Port**, and **SNMP Version** fields. For v3 specify the **HeartBeat** and **User** fields, and for v1 specify the **SNMP Community String** field.

Figure 7-9 Add an NMS Server



10. To see what has been configured, select **Show NMS Server** on the NMS Server Action Menu:

Figure 7-10 Show NMS Server on the NMS Server Action Menu

11. As shown in Figure 7-11, exit from the lsmsmgr configuration GUI by changing the user to lsmsadm (`su – lsmsadm`) and then start LSMS SNMP (`lsmsSNMP start`). If the Remote Monitoring feature is off as shown in Figure 7-11, turn it on (`dbcfginternal SNMP Y`) and again start LSMS SNMP (`lsmsSNMP start`).

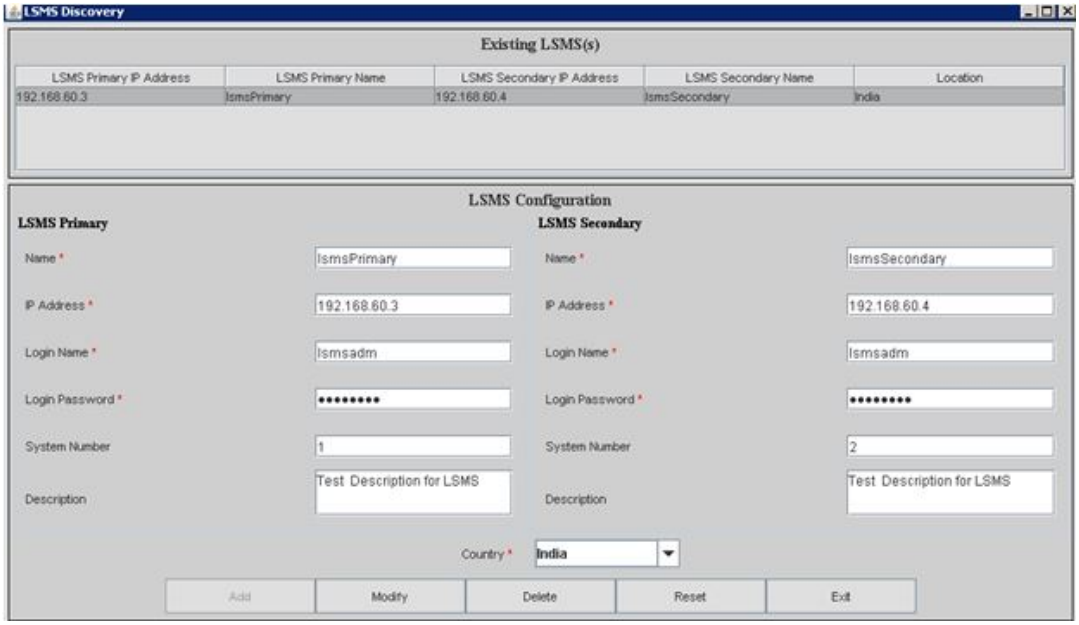
Figure 7-11 Starting LSMS SNMP

OCEEMS Configuration

Use the following steps to configure OCEEMS:

1. Log into the OCEEMS application.
2. Use the LSMS Discovery GUI (**Tools**, and then **LSMS Discovery**) and add details for both the primary and secondary LSMS servers, as shown in Figure 7-12.

Figure 7-12 Sample LSMS Discovery



For **Login Name** and **Login Password**, use the credentials that were used to log into LSMS in step 1 in SNMP Configuration on LSMS.

Map Views

OCEEMS 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 7-13.

Figure 7-13 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 OCEEMS. For information, see Adding a new country map to OCEEMS.

For information about map view features, see Map View Features.

Cut Through Interface from Maps to LSMS

OCEEMS 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 OCEEMS user must provide login credentials on the launched interface.

Fault Management

The OCEEMS provides fault management support for LSMS on SNMPv3 over southbound Interface. SNMPv3 defines a user-based security mechanism that enables per-message authentication and encryption. The OCEEMS works as the SNMP Manager and LSMS acts as the SNMP Agent. Both the SNMP Agent & SNMP Manager need to maintain an entry for one another in order to exchange data. Support for Fault Management 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 OCEEMS fault management, see Fault Management.

Events and Alarms Viewer

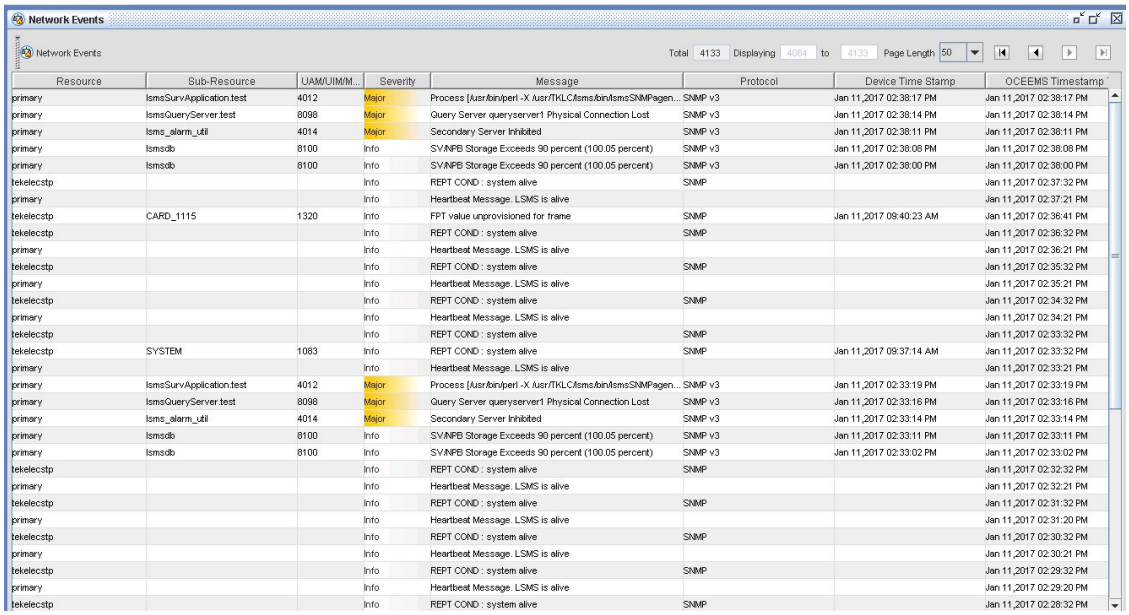
The alarms received from LSMS are displayed on the graphical maps and Text-Based interfaces. The SNMP traps received from LSMS are processed into events and displayed in the Network Events GUI in OCEEMS. Events that are associated with a defined pair event number are further processed into alarms and displayed in the Alarms GUI (**Fault Management**, and then **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.

Alarms are only parsed by OCEEMS if they are valid alarms. Each trap received from LSMS is first validated against the entries present in USMTABLE for the LSMS SNMPv3 User. If the details present in the trap are authenticated by the USM Security Model, the traps are forwarded through OCEEMS trap filters and are parsed accordingly.

Network events received over SNMPv3 Protocol will have the protocol version set as SNMPv3 on the Network Events GUI.

Figure 7-14 LSMS Network Event GUI



Event and Notification Details

- The OCEEMS fault management module applies correlation to only those LSMS events that have corresponding pair events of "clear" severity.
- OCEEMS buffers LSMS SNMPv3 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 (20 traps/sec for 5 minutes). If the buffer size is exceeded, a warning alarm is raised as follows:

Table 7-6 Event Details - Traps Buffer Overflow

Element	Description
Source	OCEEMS
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.

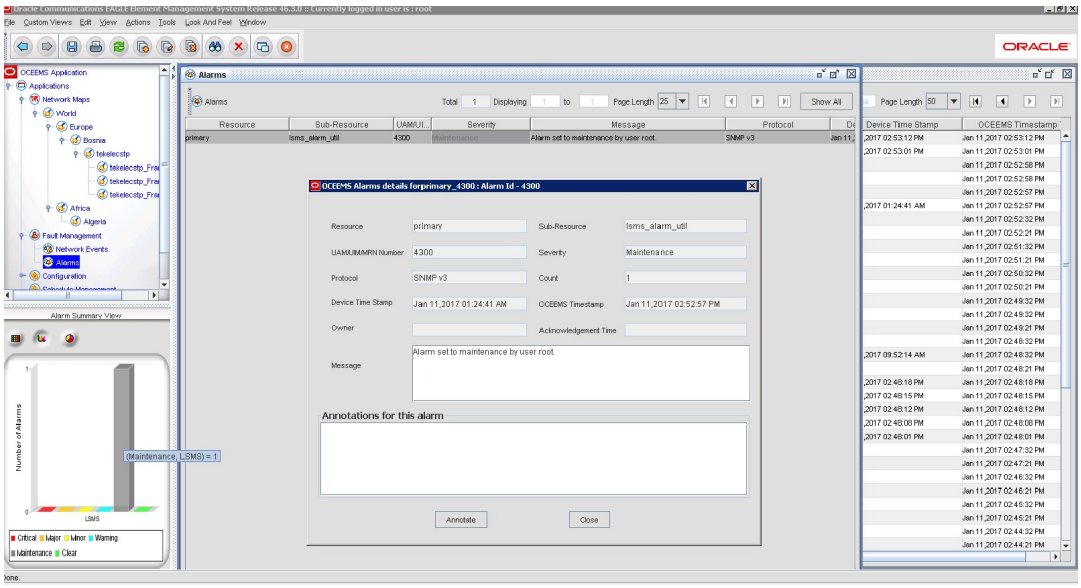
The buffer size (LSMS_QUEUE_MAX_SIZE) can be configured in the `fault.properties` file in the `/Tekelec/WebNMS/conf/tekelec` directory.

- OCEEMS 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 OCEEMS server. If OCEEMS cannot fetch the status of an LSMS node, the following critical alarm is raised:

Table 7-7 Event Details - Unable to Fetch LSMS Status

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

Figure 7-15 LSMS Network Event Details GUI



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

Table 7-8 OCEEMS Action When Status Cannot be Obtained

Scenario	OCEEMS Action
A new LSMS is being added by the user	The LSMS is not added to OCEEMS. 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 OCEEMS. This alarm must be manually cleared by the user.
During a warm start of the OCEEMS server	A critical alarm is raised. This alarm must be manually cleared by the user.
No "SwitchOverStarted" trap received, but "SwitchOverCompleted" trap received	A critical alarm is raised by the OCEEMS. This alarm must be manually cleared by the user.

Alarm Correlation and Aggregation

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

OCEEMS 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

OCEEMS 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 OCEEMS (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

OCEEMS 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 OCEEMS 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 OCEEMS, 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 OCEEMS, 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

OCEEMS extends the northbound interface feature to LSMS alarms. The northbound interface forwards alarms from LSMS to one or more client Network Management Systems. Incoming SNMPv3 events and the outgoing events are mapped as follows:

- Outgoing alertTime = As received in the incoming trap
- Outgoing alertResourceName = LSMS node name defined in OCEEMS
- Outgoing alertSubResourceName = As set by OCEEMS
- Outgoing alertSeverity = As set by OCEEMS
- Outgoing alertAcknowledgeMode = To be taken from OCEEMS Fault Management status
- Outgoing alertTextMessage = As set by OCEEMS
- Outgoing alertSequenceNumber = As set by OCEEMS

- Outgoing alertSourceIp = As set by OCEEMS

Status Management

OCEEMS manages LSMS status as follows:

- OCEEMS 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 OCEEMS server.
  For information about cases where OCEEMS might fail to fetch the status of LSMS see Table 7-8.
- 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 OCEEMS.
- 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 OCEEMS.
- On the map view, hovering the mouse over the LSMS node displays the current status of the LSMS server.

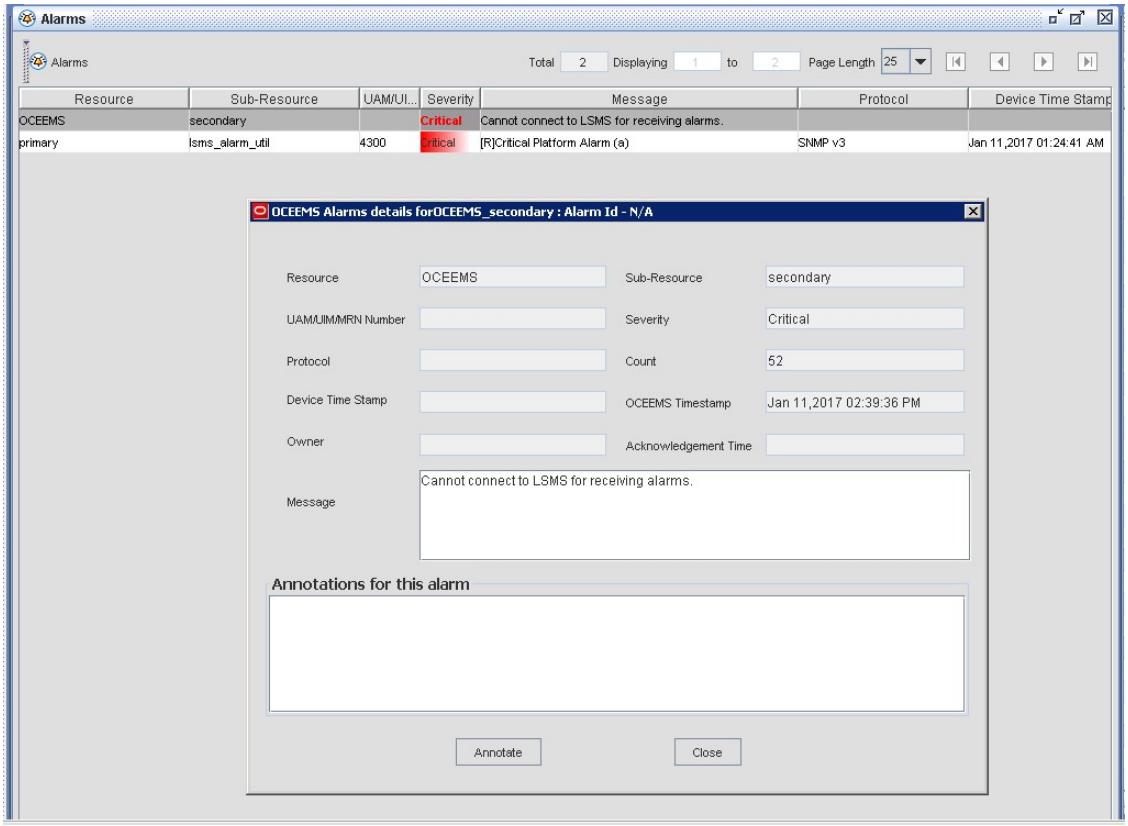
Heartbeat Support

OCEEMS Fault Management module listens for a 'heartbeat Trap' at configured intervals (default 15 minutes) to verify connectivity with the LSMS server. In the event that the specified trap is not received for the configured interval, a warning alarm will be raised, followed by a Critical alarm after each time the configured interval lapses. For each failed attempt at verifying connectivity with the LSMS server, OCEEMS will keep an incremental count.

Table 7-9 Event Details - Cannot Connect to LSMS

Element	Description
Source	OCEEMS
Sub Resource	<LSMS Name>
Severity	Critical
Message	Cannot connect to LSMS for receiving alarms

Figure 7-16 OCEEMS Raised Critical "Cannot connect to LSMS" Alarm



Resynchronization Mechanism

The OCEEMS supports Resync Mechanism during LSMS discovery (addition/modification) for users with resync privilege. The OCEEMS may fail to fetch the status of LSMS (failure getting the output of the LSMS status command `hastatus`). In this case, Resync Required Event is raised by the LSMS server. The OCEEMS addresses this request raised by the LSMS server.

Resync is executed on the OCEEMS for the following scenarios:

- A new LSMS is added by the user
- The SNMP version of an existing LSMS being modified from v1 to v3 by the user
- During the warm start of the OCEEMS server
- A Resync Request is raised by the LSMS Server

> **Note**
>
> - The EPAP server may reject a Resync Request by the OCEEMS server if a Resync is already in progress.
> - Auto/manual resync will pass for primary server but this will fail for secondary LSMS Server.

LSMS Resync Option in Discovery GUI

The user can access the Resync option three different ways: by doing one of the following:

1. From the LSMS Discovery GUI and Maps area:

Figure 7-17 LSMS Resync Option in LSMS Discovery GUI

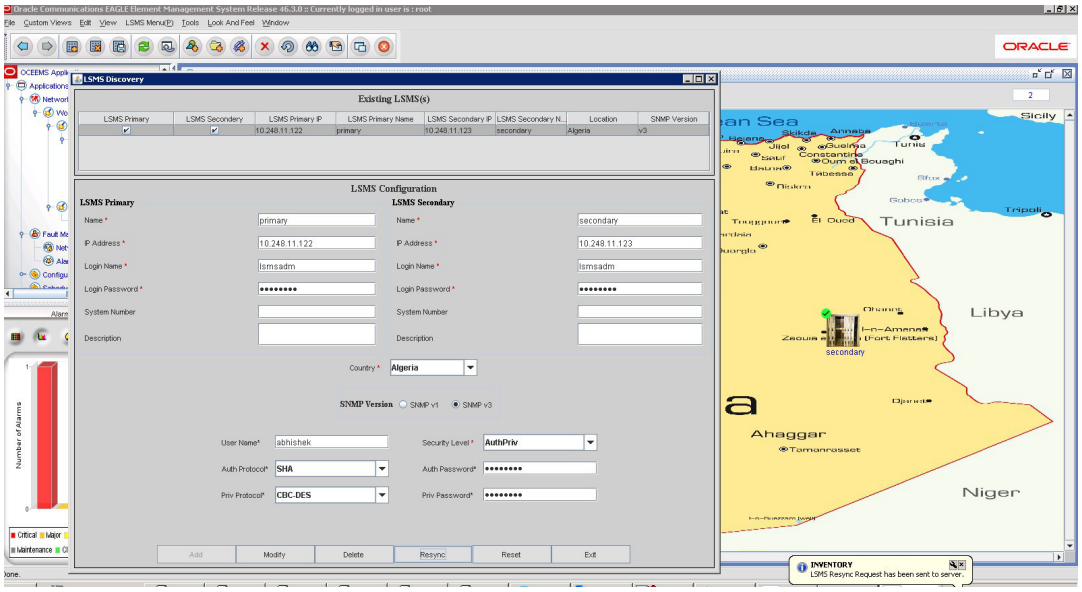
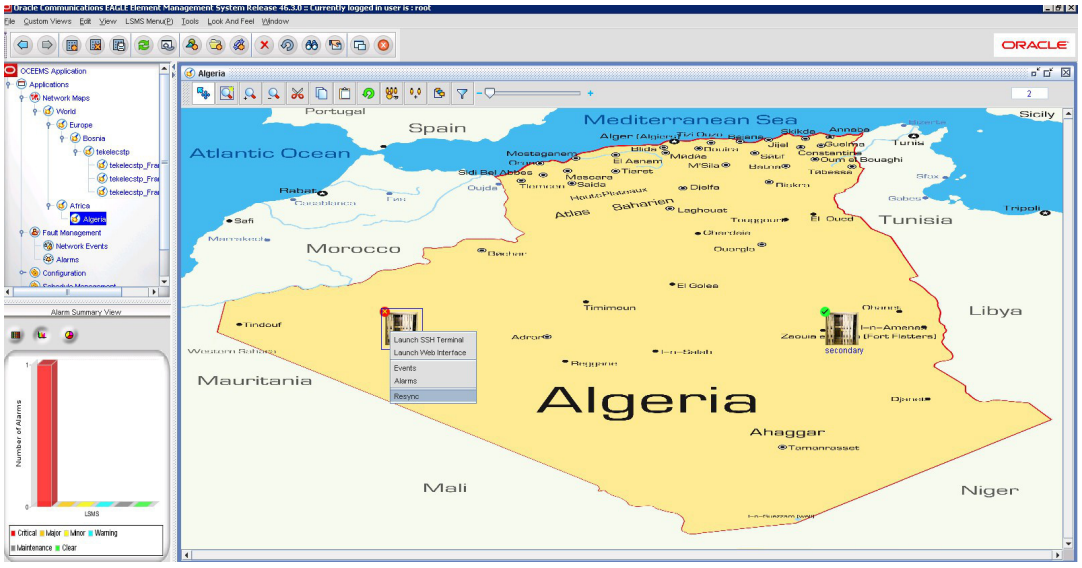
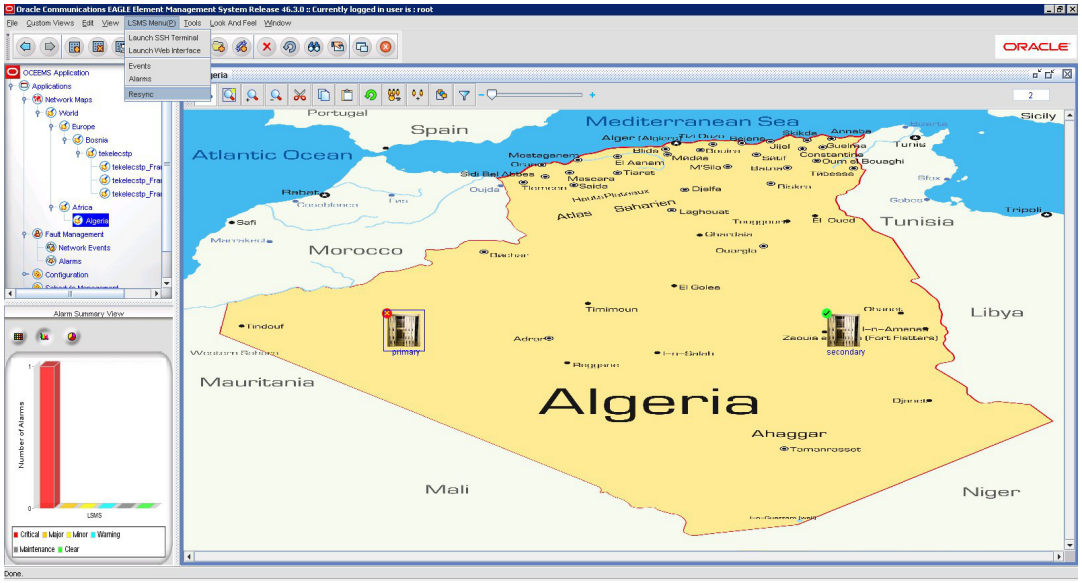


Figure 7-18 LSMS Resync Option in Maps Area



2. Right-clicking on the LSMS Node and selecting the **Resync** option:
3. Selecting the Resync option from the LSMS Menu bar when the LSMS Server Node is selected from Maps:

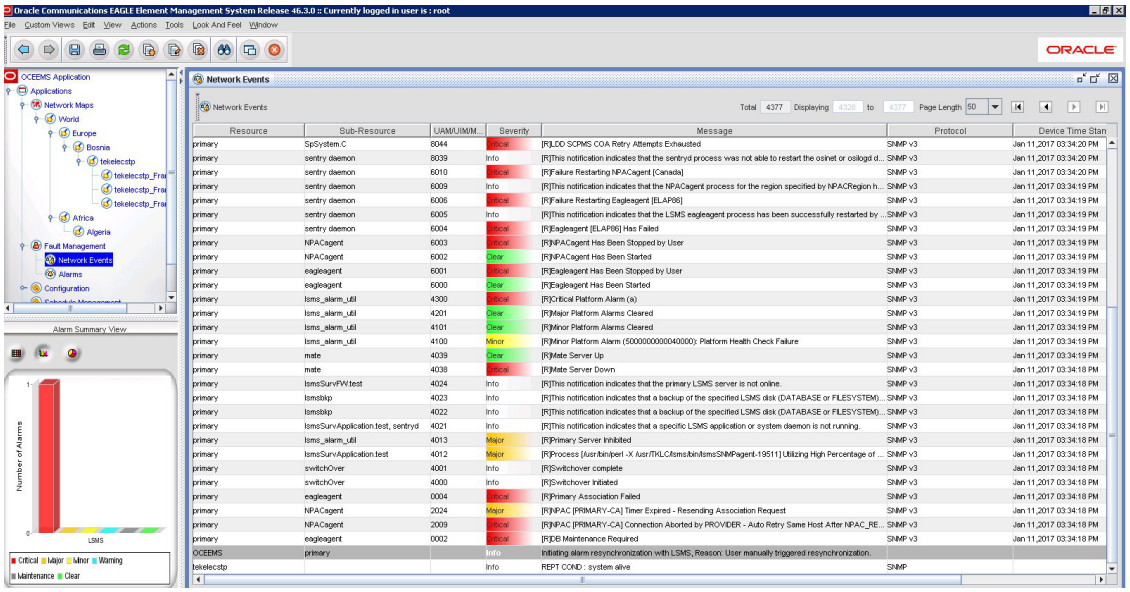
Figure 7-19 LSMS Resync Option in Maps - Menu Bar



The OCEEMS provides Resync capability on both primary and secondary LSMS servers concurrently by allowing the user to select the appropriate checkbox for the Resync that needs to be initiated.

The OCEEMS displays all resynced Alarms in the Network Events GUI with an R added to the start of the Message:

Figure 7-20 LSMS Alarm Resync



8
Fault Management

This chapter provides descriptions of the functions provided by the OCEEMS Fault Management Interface.

Overview

The Fault Management Interface enables users to monitor multiple EAGLE system alarm streams managed by OCEEMS. The Fault Management Interface gathers the EAGLE southbound information from the EAGLE Inventory application database, if the customer has the Inventory application available. The OCEEMS 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 OCEEMS 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.

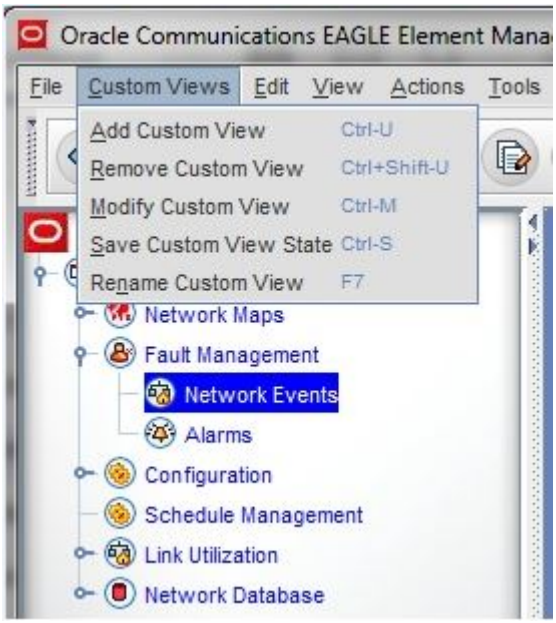
Functional Description

Fault management module can be divided into following features:

- **Alarm/Event Viewer**
  - OCEEMS 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**
  - OCEEMS fault management module applies correlation and aggregation rules (Table 8-1) 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**
  - OCEEMS 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 OCEEMS is out of sync with EAGLE alarm state (for e.g. due to connection failure between OCEEMS and EAGLE etc.). To resolve the out of sync scenarios, the OCEEMS has a southbound resynchronization feature which synchronizes the OCEEMS with the EAGLE alarm state.
- **Alarm Acknowledgement and Clear**
  - OCEEMS 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 fo the alarm.
  - Alarm clear operation clears an event for alarm in OCEEMS; however, this does not make any changes on EAGLE.
- **Alarm Maintenance mode**
  - OCEEMS 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 OCEEMS 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 OCEEMS 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 OCEEMS 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**
  - OCEEMS provides an automatic recovery from fault interface failure when EAGLE is TL1 enabled. If the OCEEMS 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 OCEEMS 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**
  - OCEEMS 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 OCEEMS, however, the southbound resynchronization at the OCEEMS fails as the resync request is sent to current active OAM IP. In this case a southbound resync fails at OCEEMS then resync request is sent to standby OAM IP. If resync is successful then the OCEEMS is switched between active and standby OAM in the database, unless there is a resync failure message sent to the client.
- **Custom Views**
  - OCEEMS provides a 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 the Alarms and Network Events views. In addition to the **Custom Views** pull-down menu shown in Figure 8-1, OCEEMS also provides a right-click menu option on the **Network Events** and **Alarms** nodes under **Fault Management** in the left panel.

Figure 8-1 Custom Views Menu



Status Update Alarms

The Status Update alarms are created by OCEEMS to aggregate the alarm status from the bottom of the network view to the top of network view. In the case of an EAGLE, the bottom-to-top view is **Slot (card location)**, and then **Shelf**, and then **Frame**, and then **EAGLE**, and then **Country**, and then **Continent**, and then **World**.

- OCEEMS generates Status Update alarms for all the slots (card locations) using the severity of alarms present on them. That is, if an alarm of Major severity exists on card location 1112, OCEEMS generates a Major severity Status Update alarm for slot 1112.
- A Status Update alarm is generated for a shelf using the highest severity of all the Status Update alarms generated for the slots belonging to that shelf.
- Similarly, Status Update alarms are generated for the rest of the levels (i.e., Frame, EAGLE, Country, Continent, and World) using this logic.

These alarms are then used to depict the alarm status of a network level on the OCEEMS GUI.

> **Note**
>
> Do not put alarms with message 'Status Update' in maintenance mode, as this will affect alarm aggregation and OCEEMS will not be able to correctly show alarm status on all the network levels.

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

OCEEMS 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	OCEEMS
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 OCEEMS
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.

Scenarios	Message
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.
OCEEMS shall send automatic resynchronization operation status notifications to all active OCEEMS 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 OCEEMS clients. Event details are as follows:

Fields	Description
Source	OCEEMS
Sub resource	<EAGLENAME>
Category	Fault
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

OCEEMS triggers resynchronization on the active OAM when SNMP FAK is enabled on the EAGLE. If resynchronization fails on the active OAM, then OCEEMS automatically triggers resynchronization on the standby OAM as configured during the EAGLE Add operation on the EAGLE Discovery GUI. If resynchronization is successful, then the active and standby OAM are switched on OCEEMS. Otherwise, error message `Alarm resynchronization failed for EAGLE: <EAGLENAME>` is displayed. Event details are as follows:

Fields	Description
Source	OCEEMS
Sub resource	<EAGLENAME>
Category	Fault
Severity	INFO

Fields	Description
Scenario and message	• 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 OCEEMS: - Switching of Active/Standby OAMs detected but data not updated. Reason: DB operation failed

> **Note**
>
> This functionality is applicable when EAGLE supports the SNMP southbound interface 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 8-1 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).

Table 8-1 (Cont.) Alarm Correlations Rules

Step #	Step	Severity	Resource	SubResource	Behavior on Alarms	Behavior on Network Events	Alarm Entry in database
3	Send SAME 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 SubResource as B	Minor	A	B	Major alarm (step3) is replaced by new Minor alarm (count is set to 1, severity is Minor, previous severity is Major).	New Minor alarm is displayed in Network Events (count is 1; severity is Minor while the old Minor (step1) and major event (step2, step 3) are still visible.	Update existing alarm entry in database for this minor alarm (count = 1, Severity = Minor, Previous severity = Major).
5	Send Same 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

OCEEMS 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 OCEEMS gets out of sync with EAGLE alarm state (for e.g. due to connection failure between OCEEMS and EAGLE etc.). To handle such cases, OCEEMS has a southbound resynchronization feature which gets OCEEMS 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 OCEEMS 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

OCEEMS 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

OCEEMS 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	OCEEMS
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.

OCEEMS 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 with for tracking and resolving. An email notification is sent to the assigned user.

Alarm Acknowledgement is located in the OCEEMS GUI by accessing **Edit**, and then **ACK/UNACK(P)**:

Figure 8-2 Alarm Acknowledgement

Alarm Clear is accessed the same way:

Figure 8-3 Alarm Clear

Alarm clear operation clears the alarm in OCEEMS; 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	Success Scenario: Alarm acknowledged for user <**User to whom alarm is assigned**> by < **User who assign alarm** > Failure scenarios : • 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 OCEEMS users. Email id of OCEEMS user and mail server configurations are picked from database.

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 OCEEMS users. The email id of OCEEMS user and mail server configurations are picked from database.

Alarm Clear Event

Clear Alert operation is available to only authorized OCEEMS 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	• Manual Clear: - Alarm cleared by OCEEMS user **<USERNAME>**. • Automatic Clear: - Alarm cleared by OCEEMS. • Maintenance Alarm changed to Active mode message - Maintenance alarm cleared by OCEEMS user **<USERNAME>**. • Buffer overflow alarm clear message - Buffer overflow alarm cleared by OCEEMS.

> **Note**
>
> Alarm clear operation triggered from OCEEMS 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 OCEEMS 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 OCEEMS, 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 OCEEMS 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 OCEEMS 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 OCEEMS 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 OCEEMS user assigned security operations Maintenance and Active mode.

Setup Alarm in Active Mode from Maintenance Mode

This is only available to authorized OCEEMS 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 OCEEMS 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

OCEEMS provides an automated mechanism to recover from fault interface failure in case EAGLE is TL1 enabled. If OCEEMS 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 OCEEMS 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 OCEEMS a fault scheduler gets started. This scheduler runs at one second interval to check OCEEMS Fault interface connectivity to all EAGLE(s).
3. Fault interface between OCEEMS and EAGLE is assumed connected; if UIM 1083 is not received at every 5 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:- OCEEMS is able to make session to IPSM card on EMSALM terminal
        i. If UIM 1083 is not received in 15 minutes, raise an alarm. Refer '**Alarm raising rule**.
        ii. Break the existing connection.
        iii. Recreate session with EAGLE.

i. If only one IPSM is available it is tried again.

ii. 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 (as in, if 3 IPSM are configured) then they are chosen in increasing order. For example, if the 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.

iii. Automatic Resync gets performed with EAGLE.

iv. Wait for UIM 1083 for 15 minutes again and go to step a.

b. Case 2: OCEEMS is not able to make session to any IPSM card on EMSALM terminal

i. OCEEMS can't connect to IPSM

ii. Wait for 15 minutes (i.e. inactive for that time).

iii. Raise an alarm, refer 'Alarm raising rule'.

iv. Retry connection with configured IPSMs.

i. If only one IPSM is configured then it is tried again.

v. If 2 or more IPSM are available then the next configured IPSM is tried before the current one which is IPSM1.

vi. 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	OCEEMS
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	OCEEMS
Sub Resource	<EAGLENAME>
Severity	Warning
Message	Connection failure detected on EMSALM <EMSALM> on IPSM IP <IPSM IP>

Note

In case OCEEMS 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	OCEEMS
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 `OCEEMS 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	OCEEMS
Sub Resource	AlarmMemory_<EPAP NAME>
Severity	Warning
Message	Cannot connect to EPAP for receiving alarms

- Critical Alarm Details:

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

OCEEMS notifies all active OCEEMS client sessions with the following message:

```
OCEEMS 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 OCEEMS 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 OCEEMS shall then get sync up with EAGLE heartbeat received time and shall check at appropriate time afterwards.

SNMP Active/Standby OAM Switching

OCEEMS 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 OCEEMS about the switch over. The OCEEMS 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 OCEEMS switches between active and standby OAM in database then resync failure message is sent to client.

Fault Management GUI

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

Network Events and Alarms Screens

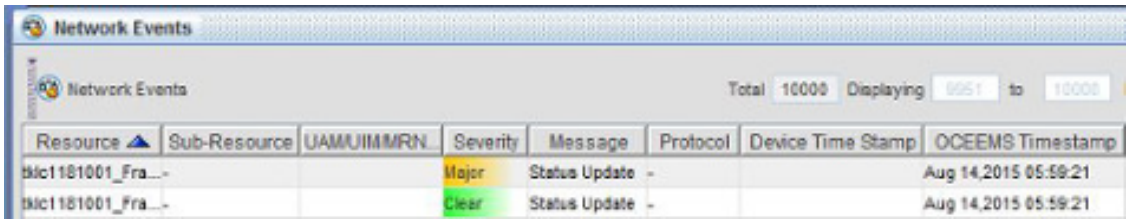
The **Network Events** and **Alarms**, screens are accessed from the **Fault Management** tree node on the left panel of the OCEEMS.

Figure 8-4 Fault Management Tree Node

Network Events

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

Figure 8-5 Historical Network Events



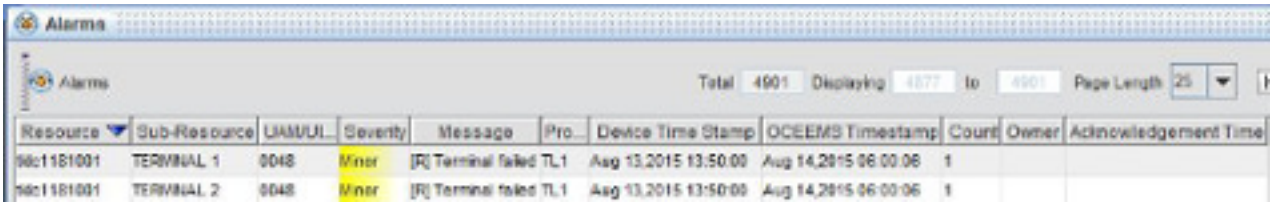
The Network Events display the following fields:

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

Alarms

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

Figure 8-6 Alarms Pane



The Alarms display the following fields:

- Resource
- Sub-Resource
- UAM/UIM/MRN Number
- Severity
- Message
- Protocol
- Device Timestamp
- OCEEMS 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
- OCEEMS 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:

- OCEEMS supports both 12-hour and 24-hour format for events and alarms. To switch between time formats, update the specified parameters in both of the following files to the desired time format and restart the server:
  - **SERVER_DATE_FORMAT=<TIMESTAMP FORMAT>** parameter in `/Tekelec/WebNMS/conf/tekelec/server_conf.properties`
  - **DATE_FORMAT=<TIMESTAMP FORMAT>** parameter in `/Tekelec/WebNMS/conf/clientparameters.conf`

  where **<TIMESTAMP FORMAT>** is one of the following values:

  ```
  MMM dd,yyyy HH\:mm\:ss (This enables 24-hour format)
  MMM dd,yyyy hh\:mm\:ss a (This enables 12-hour format)
  ```

- 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. OCEEMS fault management module supports both TL1 and SNMP southbound interfaces simultaneously.

> **Note**
>
> Through this requirement, OCEEMS is able to support a network where some EAGLEs are SNMP enabled and some are not.

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

OCEEMS listens to UAMs and UIMs and processes them into events in case the southbound protocol is TL1.

OCEEMS 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 = OCEEMS
- 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

OCEEMS listens for traps from multiple EAGLE(s) at configured trap port. OCEEMS listens to UAMs and UIMs received on EMSALM terminal configured by user in case southbound protocol is TL1. OCEEMS makes connection to EAGLE EMSALM terminal on successful EAGLE discovery and connection is terminated on deletion of EAGLE from OCEEMS inventory. OCEEMS 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.

OCEEMS 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 OCEEMS performs following steps:-

1. Case 1:- OCEEMS 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.
      i. If only one IPSM is available, is tried again.
      ii. 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.

iii. Automatic resynchronization gets performed with the EAGLE.

iv. Wait for UIM 1083 for 15 minutes again and continue as mentioned in Step a.

2. Case 2: OCEEMS is not able to make session to any IPSM card on EMSALM terminal
   a. OCEEMS cannnot 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.
      i. 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 OCEEMS for that EAGLE.

Following alarms are raised during IPSM switching as per 'Alarm Raising rule' mentioned in IPSM Switching Algorithm:

- Source = OCEEMS
- 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>.**

OCEEMS notifies all active OCEEMS client sessions about fault interface failure the message

```
OCEEMS 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 = OCEEMS
- 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.

OCEEMS 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. OCEEMS shall notify all active OCEEMS client sessions about fault interface failure the message

```
OCEEMS 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 OCEEMS for that EAGLE.

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

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

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

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

Alarm Reports

OCEEMS shall provide a reporter interface for generating fault management reports.

OCEEMS 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 OCEEMS:

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**.

9
Measurements Module

The chapter provides descriptions of the feature and functions of the OCEEMS 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

OCEEMS Measurements Platform module is used for parsing and management of EAGLE's performance data. The OCEEMS 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 OCEEMS. No separate key is needed for it. However, OCEEMS Measurements FTP module is licensed and a license must be purchase to use this feature.

Functional Description

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

The `lsof` command is required by the OCEEMS Measurements module and should be installed on the system before OCEEMS is started. Verify its availability and install it if needed before starting the OCEEMS server.

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

Input and output directories used by the Measurements platform module exist on the system before the module starts. The OCEEMS creates them during installation. The default path for the input directory is `/opt/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 To change the input directory, use the `inputDirectory` parameter in the `/Tekelec/WebNMS/conf/tekelec/common.config` file to set the location that OCEEMS scans for incoming measurement CSV files. If the `inputDirectory` parameter is modified while the OCEEMS 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 OCEEMS 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 OCEEMS 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, xxxxxxx_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 OCEEMS.
- 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 OCEEMS 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 is be 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 OCEEMS software installation is customer friendly and executable. The Measurement file collection and DB storage feature is a core function of OCEEMS and is installed together with all other core applications.

DataBase Overview

The OCEEMS 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.

These database tables are created during the installation of OCEEMS.

The EAGLE(s) connected to OCEEMS are configured to FTP their measurement files (CSV files) into a particular location, such as the default `input directory /opt/E5-MS/measurement/csvinput`, on the OCEEMS server. OCEEMS Measurement platform module scans the input directory for incoming measurement report files, parse the report files found, insert the measurement data into OCEEMS 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 CLLI mentioned in the file. In case, the value of CLLI 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 GTTACTION 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 GTTACTION 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 OCEEMS System Administrator through a configuration file (`/Tekelec/WebNMS/conf/tekelec/common.config`). Any changes done to the file are effective on OCEEMS 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. OCEEMS 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 OCEEMS 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 **tekelec_meas_headers** verified.
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 OCEEMS Measurements platform is dependent on the following two database tables:

- `tekelec_meas_headers`
  This table stores data related to measurement report generation such as 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), and time zone.
- `tekelec_meas_reports`
  This table is used to store the types of Measurement report files supported, their corresponding database table names, and the number of days after which the table is pruned.

The database tables are created during the installation of the OCEEMS. The Measurement module starts functioning when the OCEEMS server starts. The Measurement module database tables are removed when the OCEEMS is uninstalled.

Table 'tekelec_meas_headers'

The `tekelec_meas_headers` table is used by the Measurements module to store data related to measurement report generation such as the 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), and time zone. The table contains an auto-incremented key named **HEADERINDEX** that is used to map a report's header data to its measurement data in another table. The HEADERINDEX field is the primary key for each report file that is processed. The RPTTYPE field is linked to the corresponding RPTTYPE field of the tekelec_meas_reports table to determine the TABLE_NAME that is used for a report. The TABLE_NAME is then used along with the header data referenced by the HEADERINDEX to retrieve the report data and generate the report.

Field Name	Value	Description
HEADERINDEX	INTEGER, NOT NULL AUTO_INCREMENT, PRIMARY KEY	Primary key, 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 that is used to store data form the report file
DB_RETENTION_DAYS	INTEGER, NOT NULL	Data retention days for database table; data older than this is dropped

For more information, see Report Types Supported by Measurement Platform Module.

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 of the directory where measurement files need to be FTPed

Measurement Northbound FTP Module

OCEEMS 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 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

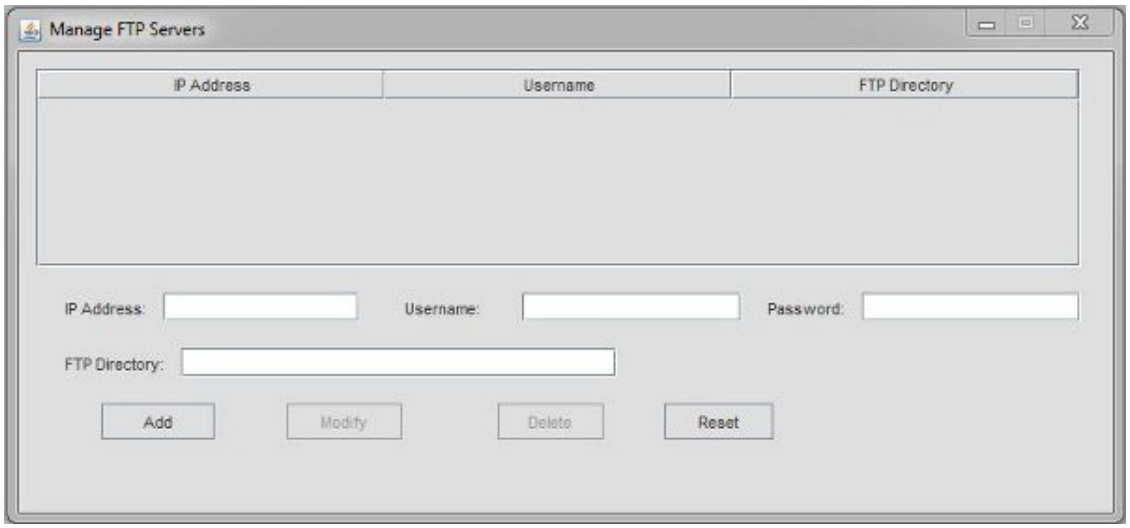
The System Administrator and all users assigned NBI FTP Configuration operation, have access to the measurement files by setting up a secure FTP IP address in the NBI FTP Configuration screen. You can access this screen from the main toolbar under the **Tools** menu.

Figure 9-1 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.
- Port - Port number to be used for FTPing the files.
- 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 9-2 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 popup 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 OCEEMS through FTP.
- The user in the **Username field** must have permission to create directory in the FTP directory so the OCEEMS can create directories in the FTP directory.

The output directory (`/var/E5-MS/measurement/csvoutput`) of OCEEMS Measurement platform module serves as the input directory for OCEEMS 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 OCEEMS 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 OCEEMS server. So, the directory structure for measurement files is similar to following:

- FTP Directory
  - EAGLE1
    - Date1
    - Date2

The logs of OCEEMS 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

Table 9-1 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 ENUM PER-ACL	TEK_MEAS_MTCD_ENUMACL	30
DAILY MAINTENANCE MEASUREMENTS ON ENUM PER-CARD	TEK_MEAS_MTCD_ENUMCARD	30
DAILY MAINTENANCE MEASUREMENTS ON ENUM PER-ENTITY	TEK_MEAS_MTCD_ENUMENTITY	30
DAILY MAINTENANCE MEASUREMENTS ON ENUM SYSTEM	TEK_MEAS_MTCD_ENUMSYS	30
DAILY MAINTENANCE MEASUREMENTS ON GTTACTION PER-PATH	TEK_MEAS_MTCD_GTTACTPATH	30
DAILY MAINTENANCE MEASUREMENTS ON GTTACTION 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_LNPSYSTM	30
DAILY MAINTENANCE MEASUREMENTS ON MAP SCREENING PATH	TEK_MEAS_MTCD_MAPPATH	30

Table 9-1 (Cont.) Report Types Supported by Measurement Platform Module

RPTTYPE	TABLE_NAME	DB_RETENTION DAYS
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_NPSYSTEM	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 SFTHROT	TEK_MEAS_MTCD_SFTHROT	30
DAILY MAINTENANCE MEASUREMENTS ON STP	TEK_MEAS_MTCD_STP	30
DAILY MAINTENANCE MEASUREMENTS ON STPLAN	TEK_MEAS_MTCD_STPLAN	30
DAILY MAINTENANCE MEASUREMENTS ON UA	TEK_MEAS_MTCD_UA	30
DAY-TO-HOUR AVAILABILITY MEASUREMENTS ON LINK	TEK_MEAS_DTHA_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

Table 9-1 (Cont.) Report Types Supported by Measurement Platform Module

RPTTYPE	TABLE_NAME	DB_RETENTION DAYS
HOURLY MAINTENANCE MEASUREMENTS ON EIR SYSTEM	TEK_MEAS_MTCH_EIR	14
HOURLY MAINTENANCE MEASUREMENTS ON ENUM PER-ACL	TEK_MEAS_MTCH_ENUMACL	14
HOURLY MAINTENANCE MEASUREMENTS ON ENUM PER-CARD	TEK_MEAS_MTCH_ENUMCARD	14
HOURLY MAINTENANCE MEASUREMENTS ON ENUM PER-ENTITY	TEK_MEAS_MTCH_ENUMENTITY	14
HOURLY MAINTENANCE MEASUREMENTS ON ENUM SYSTEM	TEK_MEAS_MTCH_ENUMSYS	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
HOURLY MAINTENANCE MEASUREMENTS ON LNP SSP	TEK_MEAS_MTCH_LNPSSP	14
HOURLY MAINTENANCE MEASUREMENTS ON LNP SYSTEM	TEK_MEAS_MTCH_LNPSYSTM	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_NPSYSTEM	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

Table 9-1 (Cont.) Report Types Supported by Measurement Platform Module

RPTTYPE	TABLE_NAME	DB_RETENTION DAYS
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
STP SYSTEM TOTAL MEASUREMENTS ON IDPR	TEK_MEAS_SYSTOT_IDPR	14
STP SYSTEM TOTAL MEASUREMENTS ON SFTHROT	TEK_MEAS_SYSTOT_SFTHROT	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

10
Reporting Studio

This chapter provides an overview of the **OCEEMS Reporting Studio**.

Overview

The default i-net Clear Reports remote interfaces is utilized for catering to the requirements of OCEEMS 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.

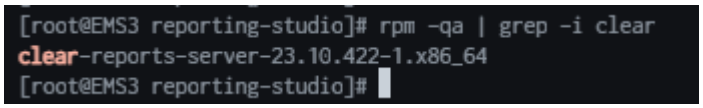
Checking if i-net 23.x is Installed

Run the following command with the 'root' user to check whether i-net 23.x is installed or not:

```
[root@EMS3 reporting-studio]# rpm -qa | grep -i clear
clear-reports-server-23.10.422-1.x86_64
[root@EMS3 reporting-studio]#
```

If the output is like “clear-reports-server-23.10.422-1.x86_64”, then it is installed, as shown below:

Figure 10-1 Checking if i-net is installed or not



If the output is blank, then i-net 23.x is not installed.

Starting the i-net 23.x Service

Complete this procedure to start the i-net 23.x service:

1. **Give permission to the non-root user (this needs to be run only once)**: Run the following commands from the root user to make sure that the non-root user has the permission to restart/start/stop/status clear-reports-service. Assuming the admin user name is emsadmuser, run the following command. UserID of adminuser name is different, replace emsadmuser with the admin username in the following commands.

   ```
   # echo 'emsadmuser ALL=(root) NOPASSWD: /sbin/service clear-reports
   restart' | sudo tee -a /etc/sudoers
   # echo 'emsadmuser ALL=(root) NOPASSWD: /sbin/service clear-reports start'
   | sudo tee -a /etc/sudoers
   # echo 'emsadmuser ALL=(root) NOPASSWD: /sbin/service clear-reports stop'
   | sudo tee -a /etc/sudoers
   ```

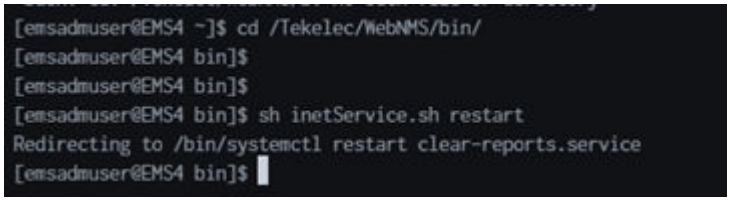
```
# echo 'emsadmuser ALL=(root) NOPASSWD: /sbin/service clear-reports
status' | sudo tee -a /etc/sudoers
```

Figure 10-2 Giving permission to non-root user to start/stop/restart clear-reports-server

2. Move to the directory `/Tekelec/WebNMS/bin` and run the script `inetService.sh start` with the non-root user, to start the i-net service.

```
# cd /Tekelec/WebNMS/bin
# sh inetService.sh start
```

Figure 10-3 Starting the i-net Service with Root User



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 OCEEMS 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 OCEEMS 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 OCEEMS, 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 10-4 Add User

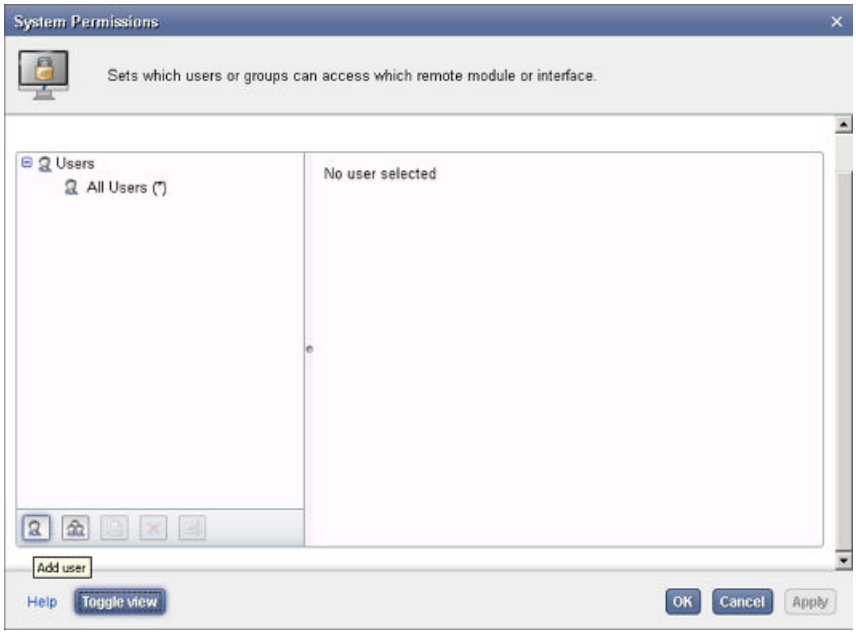
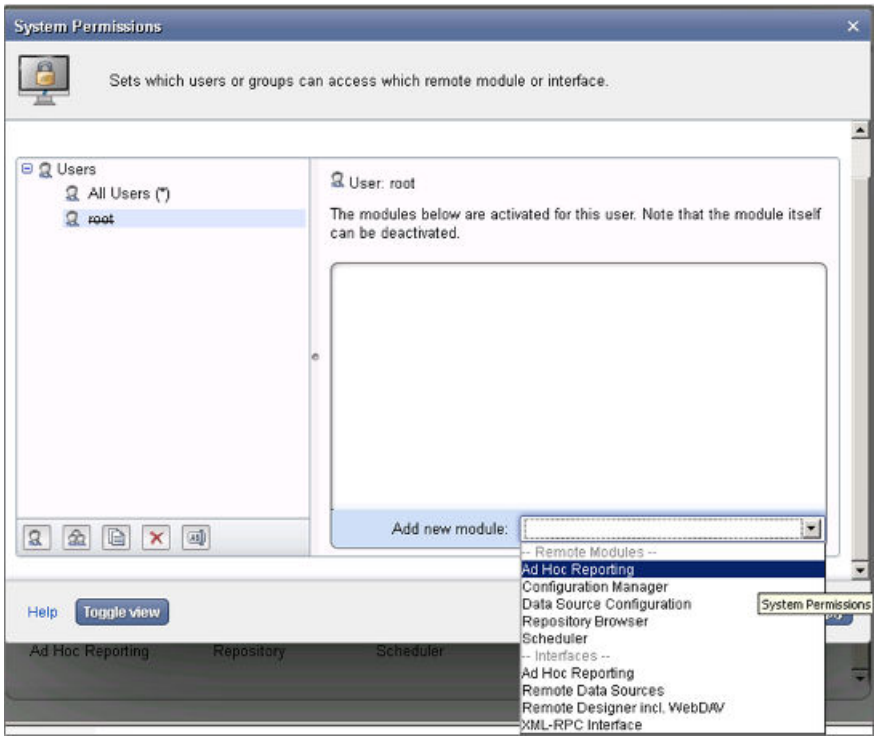


Figure 10-5 System Permissions



i-net Clear Reports Remote Interfaces

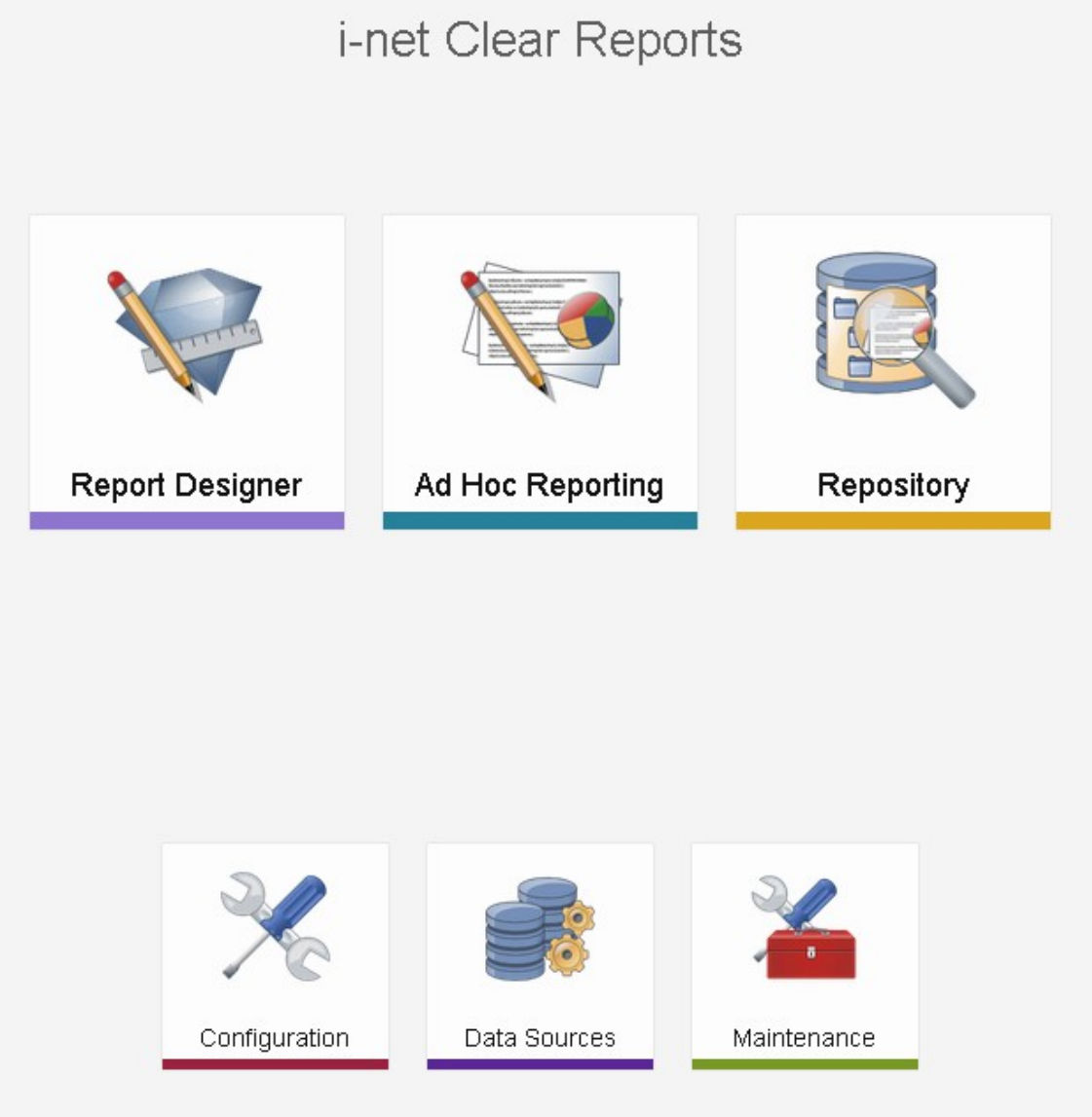
i-net Clear Reports provides following remote interfaces:

- **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.
- **Maintenance** - Provides access to maintenance configuration and tasks.
- **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.
- **Repository** - Provides access to the directory containing existing reporting templates.

Remote Interface

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

Figure 10-6 i-net Clear Report



Ad Hoc Reporting Interface

This chapter provides an overview of the EAGLE 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 10-7 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 10-8 Configuration Manager Interface

Post installation of i-net Clear Reports, it needs to be configured for use with OCEEMS. 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, OCEEMS database needs to be added as a data source to i-net Clear Reports for report generation using Data Source Configuration.

Figure 10-9 Data Source Configuration Interface

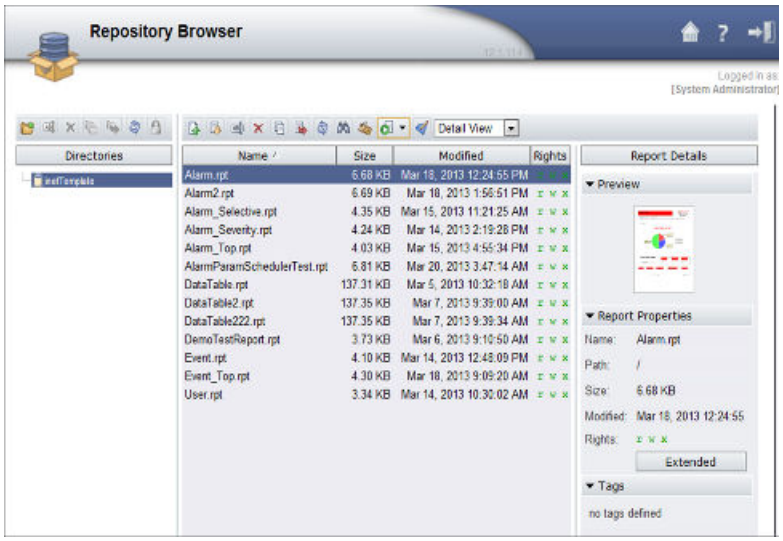
Repository Browser Interface

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 10-10 Repository Browser Interface



Task Planner Interface

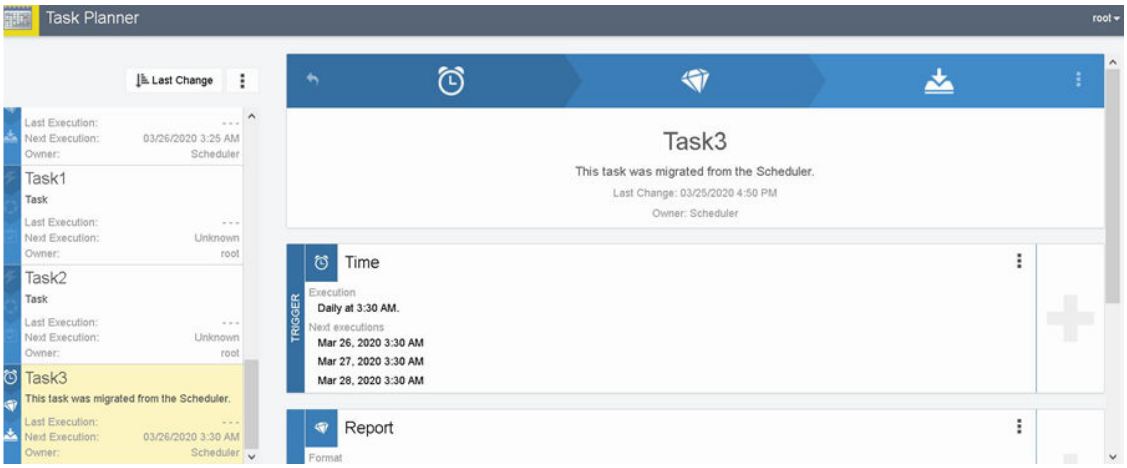
The Task Planner interface allows scheduling of report generation by creating named scheduled tasks.

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 FTPed or mailed to users. It also has provision of instant execution of a scheduled task.

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

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

Figure 10-11 Task Planner



Report Designer Interface

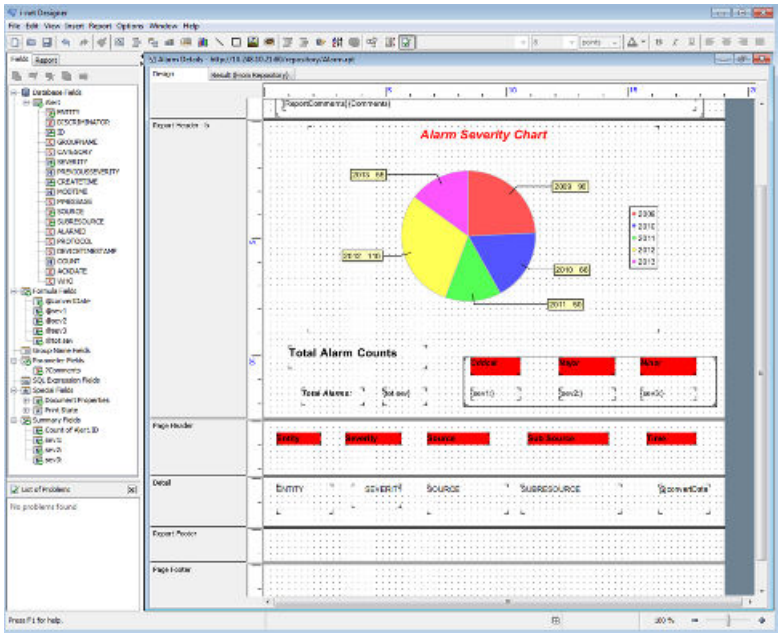
The Report Designer interface allows creating or editing a report template.

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 OCEEMS database while creating/updating report templates.

Figure 10-12 Report Designer



Installation of Reporting Studio

Complete this procedure to install the Reporting Studio for Release 47.0. These steps must be performed by super user **root**.

1. **Check port availability**: In the system, check whether the 9000 port is free. i-net Clear Reports run on port 9000. Run the following command:

   ```
   # netstat -tulpn|grep 9000
   ```

   a. If the output of the previous command is blank, as shown in the following output, skip to step 2:

   Figure 10-13 Blank output of netstat command

   ```
   [root@e5ms69 bin]# netstat -tulpn|grep 9000
   [root@e5ms69 bin]#
   ```

   b. If the output of the previous command displays the output shown below, then move to the step 2:

   ```
   tcp6 0 0 :::9000 :::* LISTEN 17869/java
   ```

   In the above output, the number 17869 is the PID of the process.

   Figure 10-14 Non-blank output of netstat command

   ```
   [root@e5ms69 inet17.1.146rpm]# netstat -tulpn|grep 9000
   tcp6       0      0 :::9000                 :::*                    LISTEN      17869/java
   [root@e5ms69 inet17.1.146rpm]#
   ```

2. Run the following command to kill the process initiated in step 1.b. For example, kill - 9 17869

```
# kill -9 <PID of the process at step 1.b>
```

3. Unzip the Reporting Studio zip file to the `reporting-studio` directory using the following command:

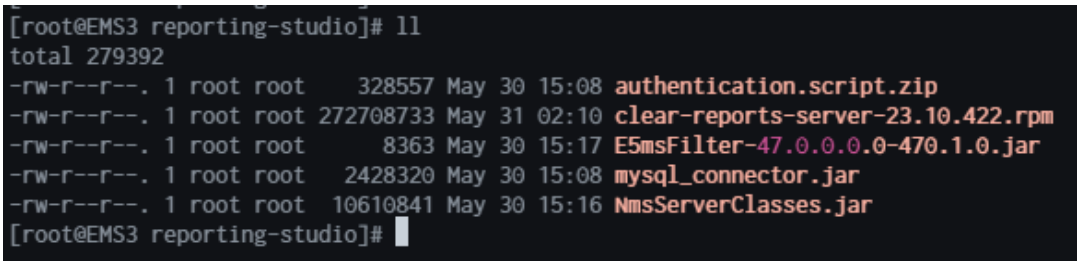
```
# unzip <reporting studio zip> -d reporting-studio
```

4. Move to the new `reporting-studio` directory created in step 3, and verify the contents of reporting studio zip file by running the following command:

```
# cd reporting-studio
# ll
```

5. Check all jars and scripts are available as per EMS and i-net release:

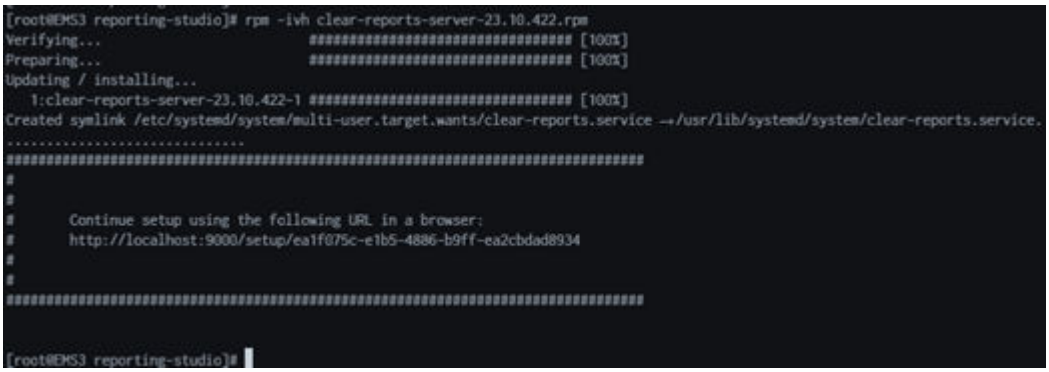
Figure 10-15 Contents of the Reporting Studio Zip



6. Once you are inside the same `reporting-studio` directory created in the above steps, install the i-net Clear Reports RPM by running the following command:

```
# rpm -ivh clear-reports-server-23.10.422.rpm
```

Figure 10-16 Installing clear-reports-server rpm



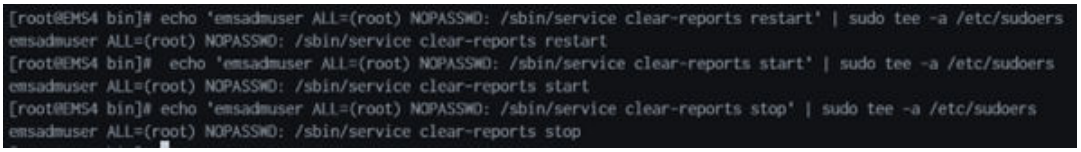
7. Copy jars and plug in to the same folder as done in following logs:

```
## cp NmsServerClasses.jar E5msFilter-47.0.0.0.0-470.1.0.jar /usr/share/i-
net-clear-reports/lib/
# cp mysql-connector-java.jar /usr/share/i-net-clear-reports/lib/driver/
# cp authentication.script.zip /usr/share/i-net-clear-reports/plugins/
```

8. Run the following commands from the root user to ensure that the non-root user has the permission to restart/start/stop/status clear-reports-service. Consider the admin user name is emsadmuser and run the following commands. UserID of adminuser name is different. Replace emsadmuser with the admin username in the following commands.

```
# echo 'emsadmuser ALL=(root) NOPASSWD: /sbin/service clear-reports
restart' | sudo tee -a /etc/sudoers
# echo 'emsadmuser ALL=(root) NOPASSWD: /sbin/service clear-reports start'
| sudo tee -a /etc/sudoers
# echo 'emsadmuser ALL=(root) NOPASSWD: /sbin/service clear-reports stop'
| sudo tee -a /etc/sudoers
# echo 'emsadmuser ALL=(root) NOPASSWD: /sbin/service clear-reports
status' | sudo tee -a /etc/sudoers
```

Figure 10-17 Giving permission to non-root user to start/stop/restart clear-reports-server



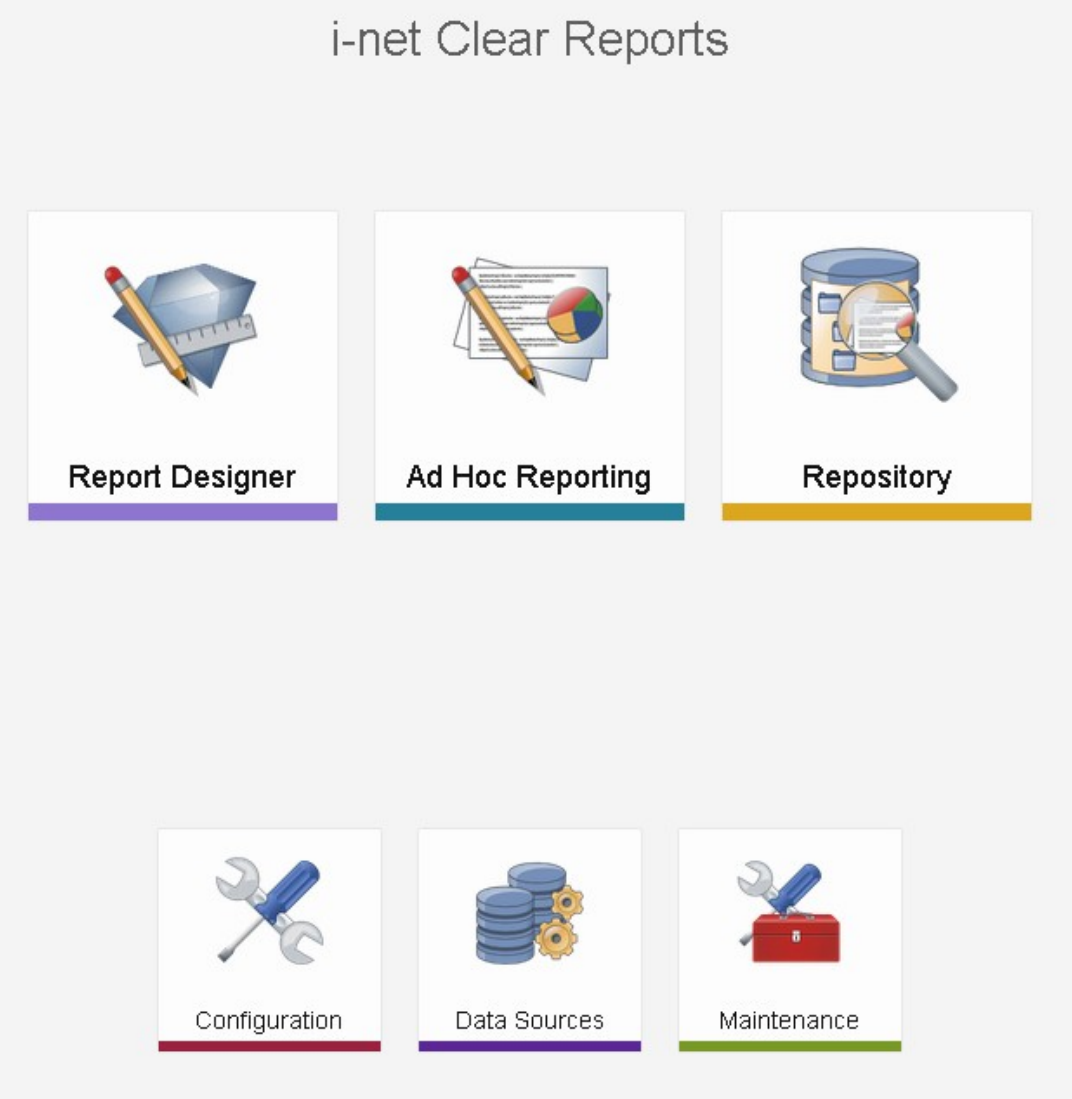
9. Move to the directory `/Tekelec/WebNMS/bin` and run the script `inetService.sh restart` with the non-root user to restart the i-net service.

```
# cd /Tekelec/WebNMS/bin
# sh inetService.sh restart
```

Figure 10-18 Restarting i-net server

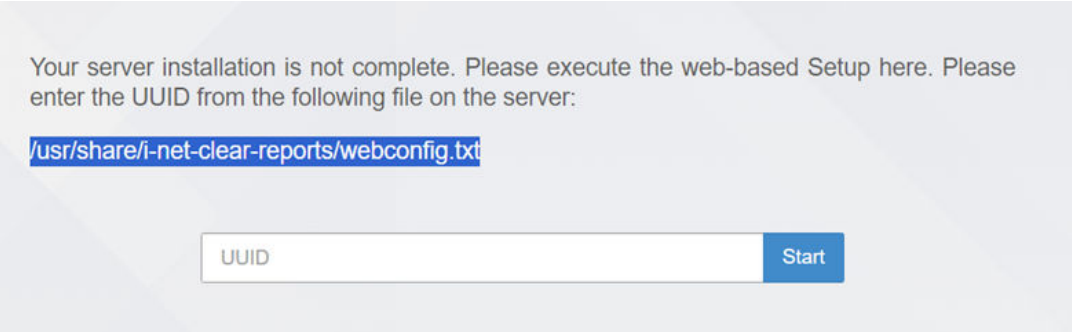
10. Go to a browser (preferably Chrome) and open the URL http://<IP Address of the Server>:9000. The following screen will open.

Figure 10-19 i-net Clear Reports home page



11. Click **Setup** on the i-net Clear Reports home page. It will open the i-net Clear Reports Setup window as shown below:

Figure 10-20 i-net Clear Reports Setup window



12. Log in with the non-root user and go to **i-net installation directory**. Run the following commands to view the contents of `webconfig.txt` file. Get UUID from `webconfig.txt`.

Copy the UUID value. After copying the UUID, paste it in the text box at the i-net Clear Reports Setup window in the browser.

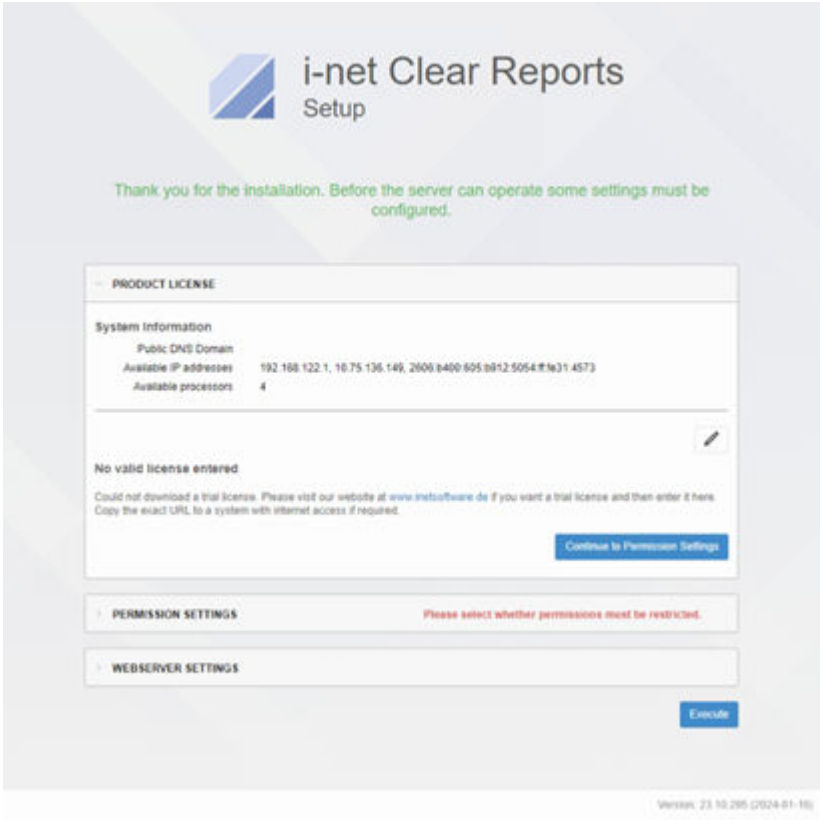
```
[emsadmuser@EMS3 bin]$ cat /usr/share/i-net-clear-reports/webconfig.txt
PROTOCOL http
ADDRESS localhost
PORT 9000
URL http://localhost:9000
UUID a0ec7aa0-5555-44da-95bd-63b4ea2732f0
[emsadmuser@EMS3 bin]$
```

13. Click the **Start** button as shown in the following figure, after pasting the UUID.

Figure 10-21 Pasting the UUID in the UUID text box

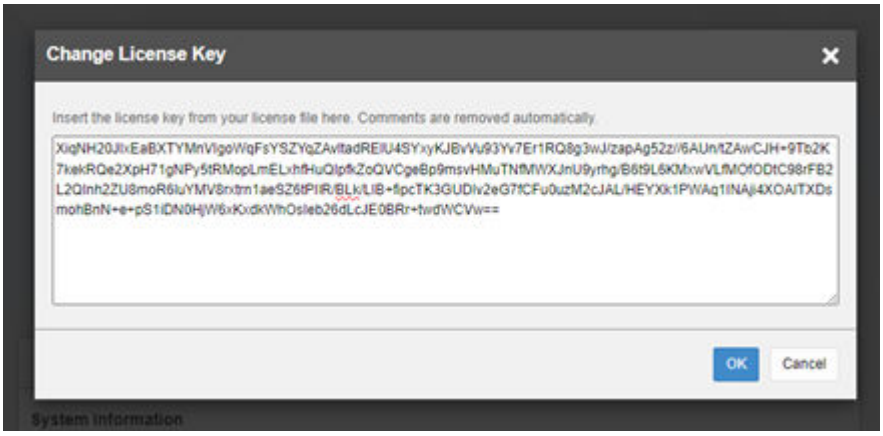
14. On clicking the **Start** button in the previous step, it will continue with the Setup and ask for the Product License, Permission Settings and Webserver Settings as shown below:

Figure 10-22 Product License and Webserver Settings



15. Enter the i-net Clear Reports 23.x Product License by clicking the **Edit** icon:

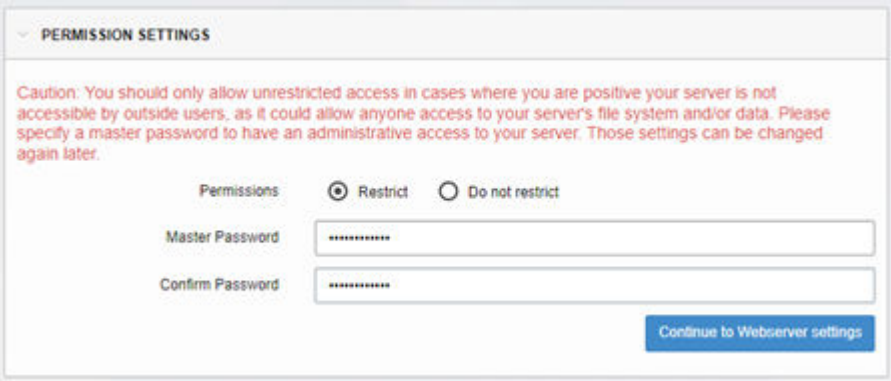
Figure 10-23 Entering the i-net Clear Report License



Click **OK** after entering the license.

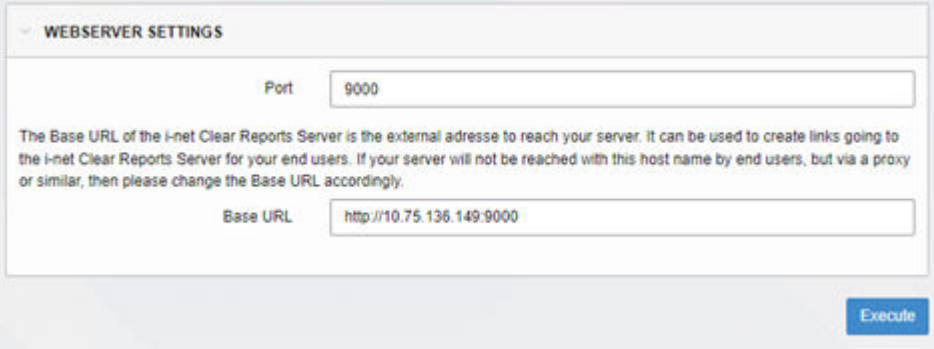
16. Click the **Continue to Permission Settings** button.
17. Click the **restrict radio** button and enter a Master password (using this password, master user will have unrestricted access):

Figure 10-24 Click Restrict on Permission Settings Page



18. Click **Continue to Webserver settings**.
19. Open the **Webserver Settings** and change the port from 80 to 9000 and update the base URL with http://<ip_of_the_EMS_server>:9000 as shown below:

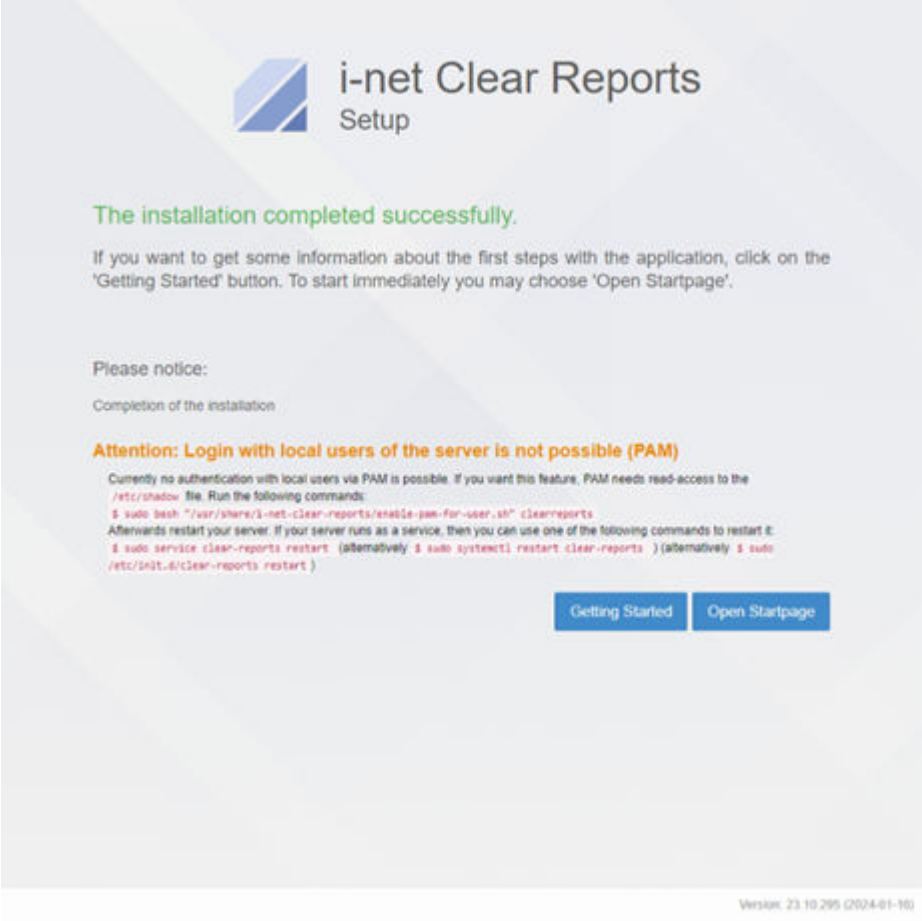
Figure 10-25 Changing the port



Click the **Execute** button as shown in above screenshot, after changing the port and the base URL.

20. After clicking the **Execute** button in the previous step, the i-net Clear Reports installation will be completed as shown below:

Figure 10-26 i-net Clear Reports installation completed



Configuration of i-net Clear Reports

> **Note**
>
> Once i-net Clear Reports configuration is done, it is not possible to open i-net by directly entering the URL (`<IP>:9000`) in the browser. Instead, i-net can be opened by opening E5-MS GUI, then Tools, and then Reporting Studio.

After the successful installation of i-net Clear Reports, it must be configured for use with OCEEMS. This configuration involves the following steps:

1. After the successful installation of i-net Clear Reports, run the below command assuming the admin user name is emsadmuser. UserID of adminuser name is different, replace emsadmuser with the admin username in the following commands.
   a. Run below commands on the EMS server CLI using the root user:

```
# sh /usr/share/i-net-clear-reports/enable-pam-for-user.sh clearreports
# su - emsadmuser
# cd /Tekelec/WebNMS/bin/
```

```
# sh inetService.sh restart
# sh inetService.sh status
```

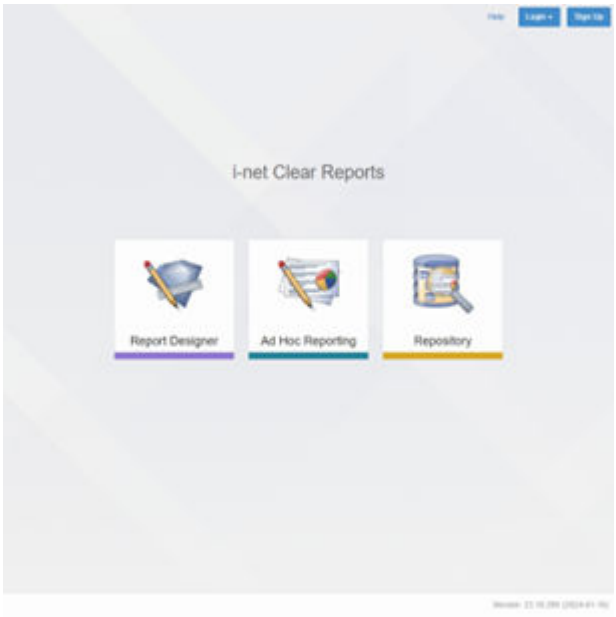
Figure 10-27 Giving permissions to Clear Reports User

b. Click **Open Startpage** to open the i-net Clear Reports Startpage.

Figure 10-28 Open StartPage

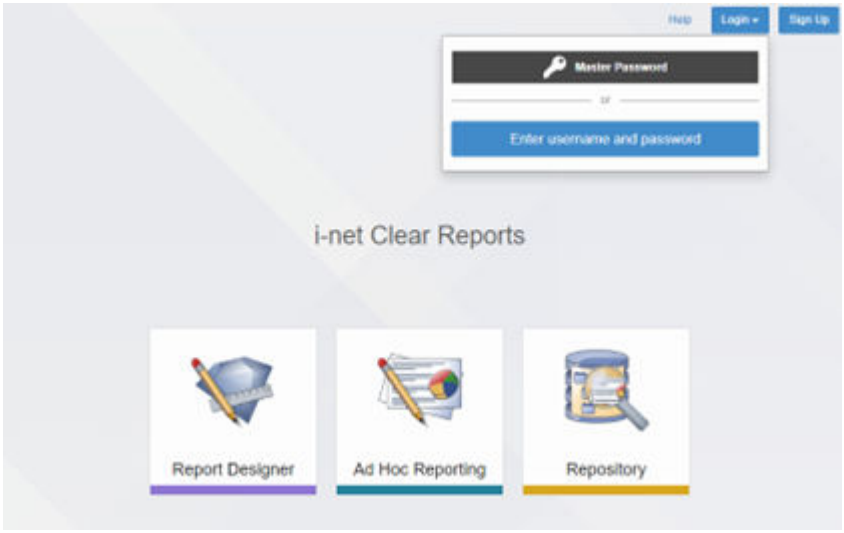
On clicking **Open Startpage**, the following window will appear:

Figure 10-29 i-net Clear Reports Start Page



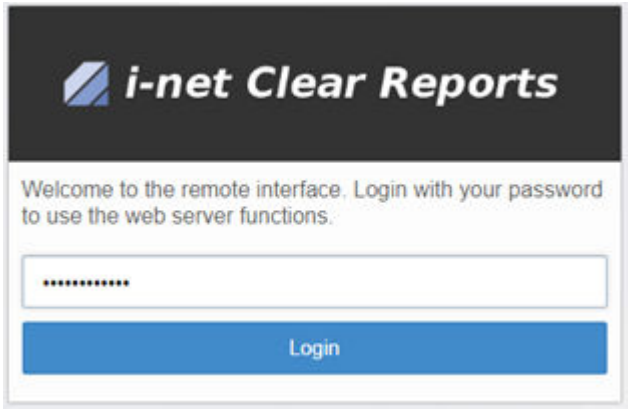
2. Click **Login** and then click **Master Password** as displayed in the following screenshot.

Figure 10-30 Master Password



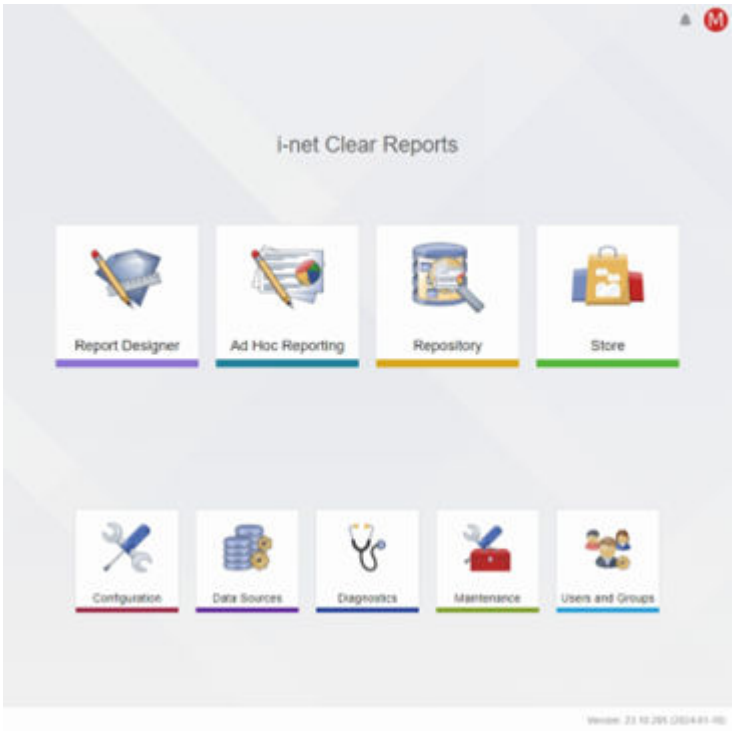
3. On clicking **Master Password** button, the following screen will appear. Enter the password created in step 17 of Section 2.2 and click **Login**.

Figure 10-31 Enter Master Password



On logging in, the following screen will appear:

Figure 10-32 i-net Clear Reports Page

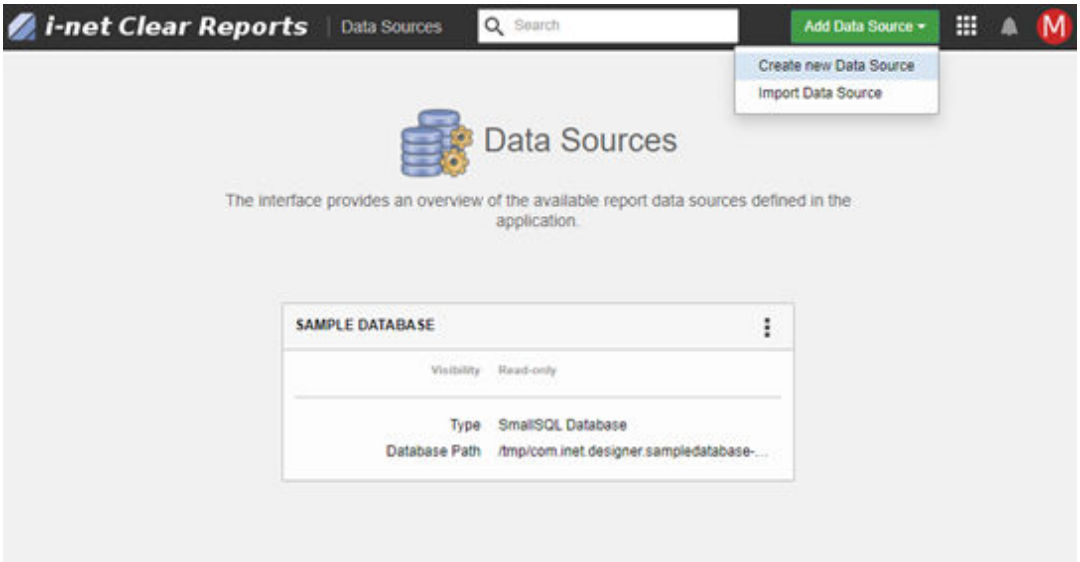


4. Click the **Data Sources** card.

Figure 10-33 Data Sources Page

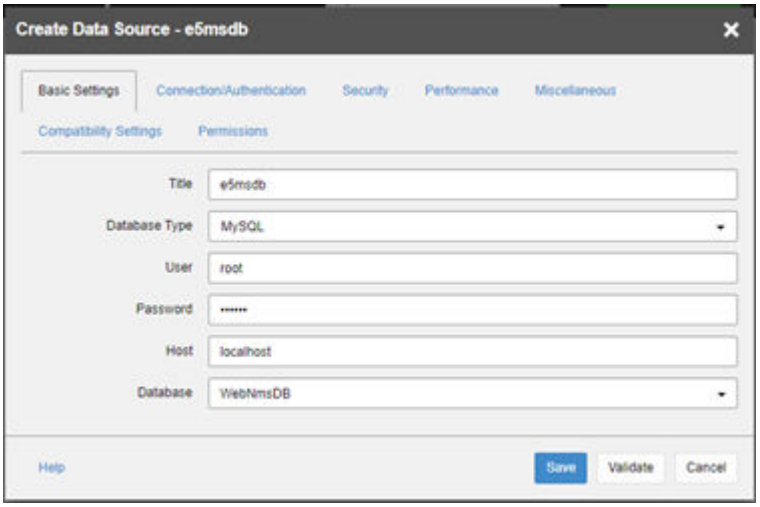
5. On clicking the Data Sources page, the following page will open. Click **Add Data Source** button on the Header, and select the **Create New Data Source** option from the drop-down.

Figure 10-34 Create New Data Source



The following pop-up will open. Enter the following details:

Figure 10-35 Create new database details

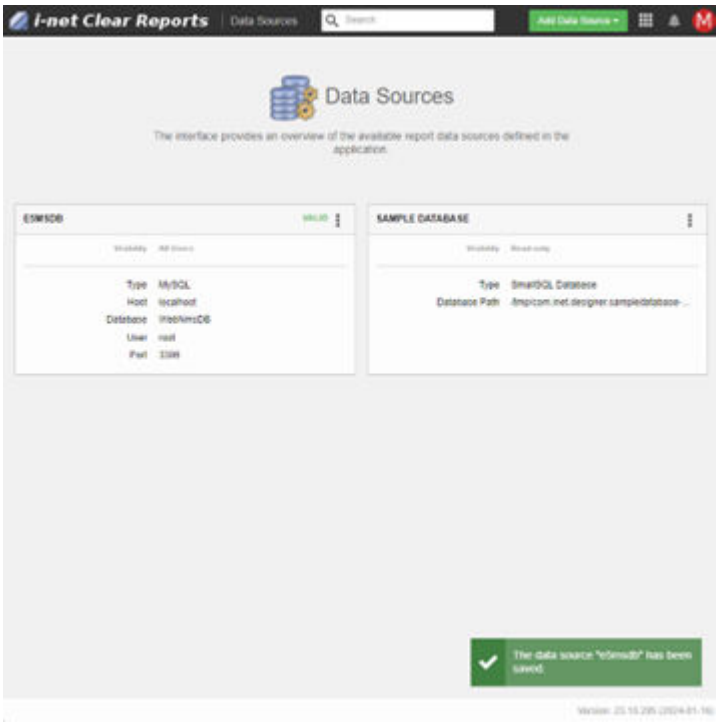


a. Click **Validate**.

b. Click **Save**.

The following screen will appear on the Data Sources page.

Figure 10-36 New data sources added

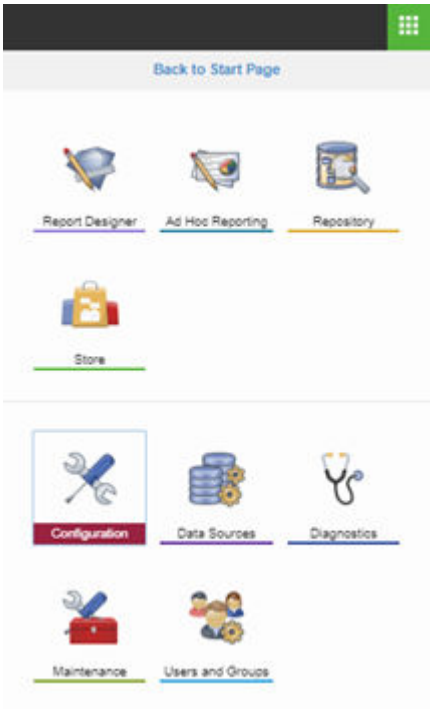


6. Click **Card Browser** option displayed on the header.

Figure 10-37 Card browser button

7. Click the **Configuration Card** as shown below.

Figure 10-38 Configuration Card

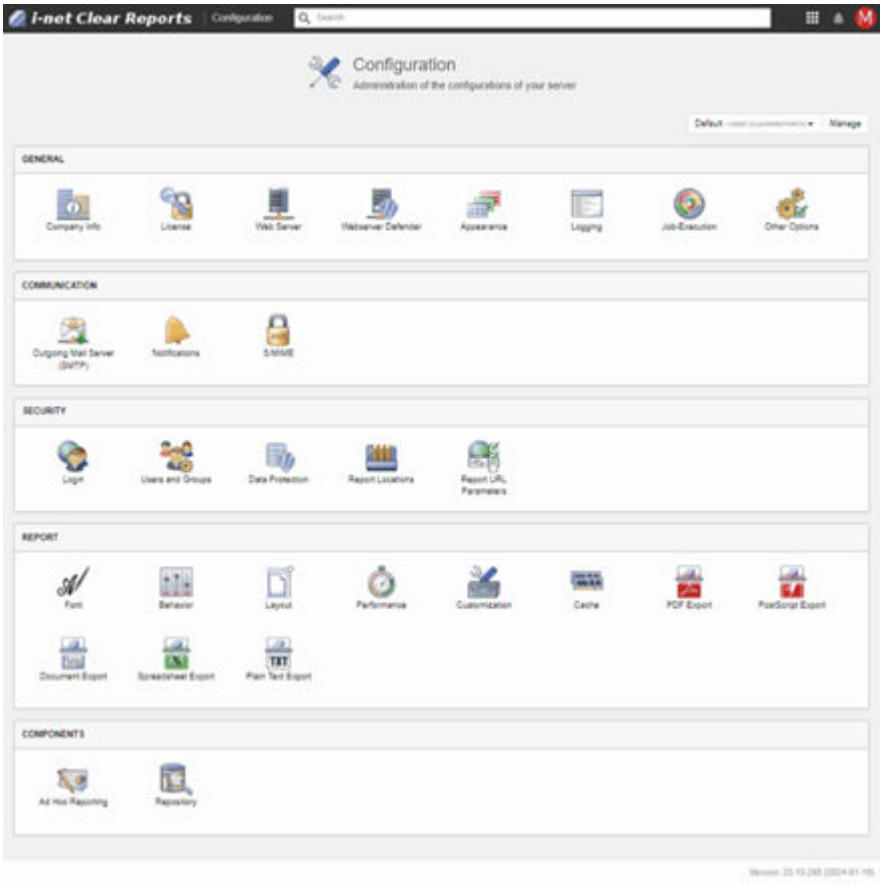


8. In the following page, click **User ("M")** on the right most and select the **Switch to Advanced View** option.

Figure 10-39 Switch to Advanced View

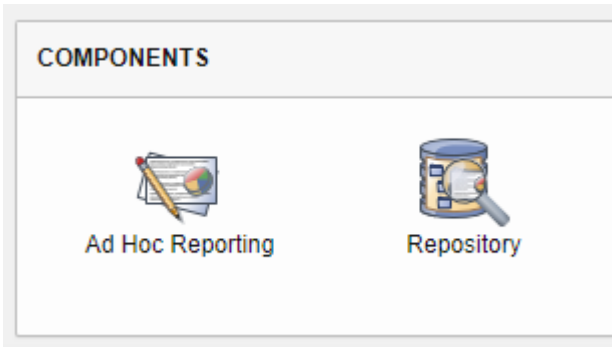
The advanced view of Configuration Page will appear as follows:

Figure 10-40 Advanced view of configuration page



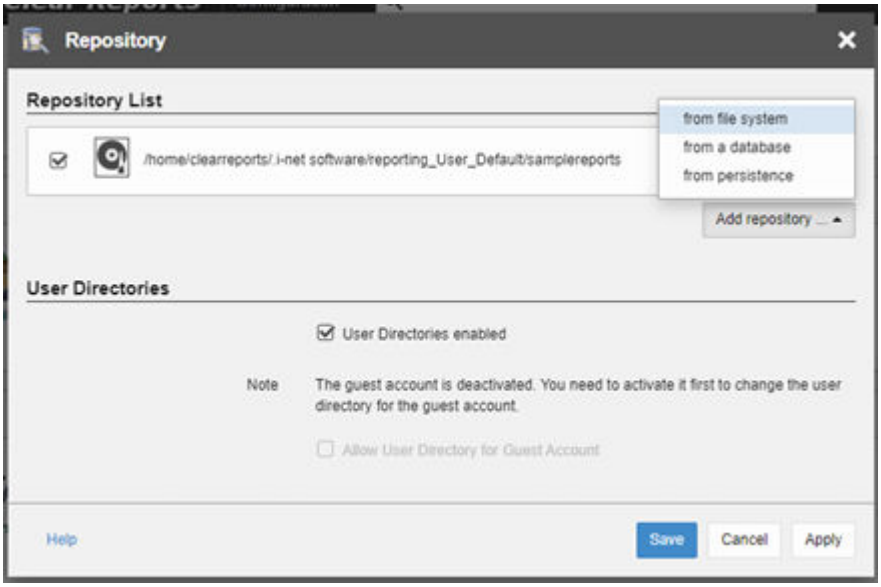
9. From the **Components** section, select **Repository**.

Figure 10-41 Select Repository



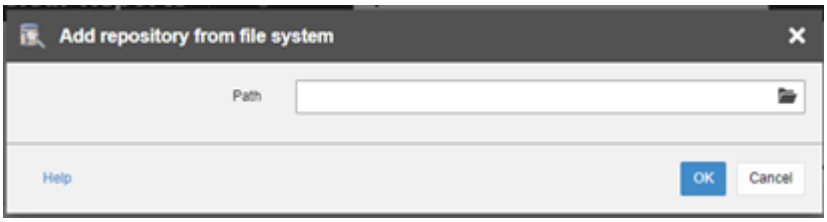
10. On selecting **Repository**, the following pop-up will appear. Click **Add repository** and select the **from file system** option.

Figure 10-42 Add Repository



The following screen will appear.

Figure 10-43 Adding the repository



11. Run the following command from the EMS server CLI from the root user. Considering the admin user name as emsadmuser, run the following command. UserID of adminuser name is different. Replace emsadmuser with the admin username in the following commands.

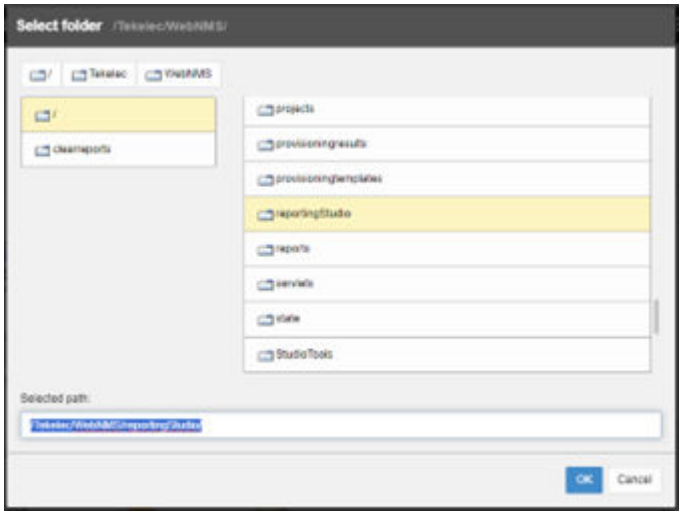
```
usermod -a -G emsadm clearreports
su – emsadmuser
/Tekelec/WebNMS/bin/inetService.sh restart
```

Output:

```
[root@EMS4 ~]# usermod -a -G emsadm clearreports
[root@EMS4 ~]# su - emsadmuser
[emsadmuser@EMS4 ~]$
[emsadmuser@EMS4 ~]$ /Tekelec/WebNMS/bin/inetService.sh restart
Redirecting to /bin/systemctl restart clear-reports.service
[emsadmuser@EMS4 ~]$
```

12. Click the **Folder** icon on the screen as shown in the figure in step 16.
13. In the selected path field, enter `/Tekelec/WebNMS/reportingStudio/` as displayed in the figure below:

Figure 10-44 Select the folder to add repository



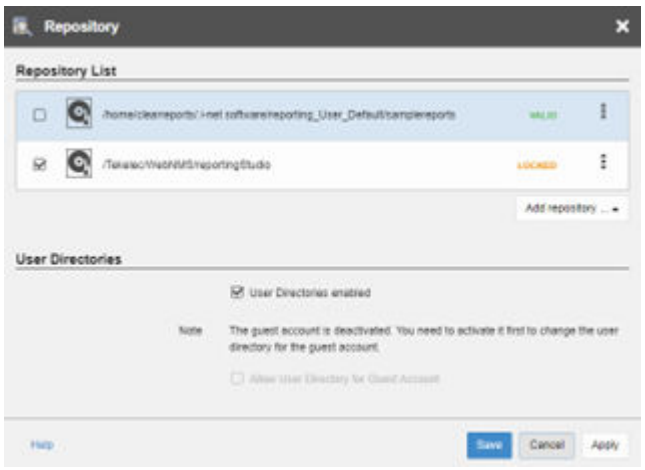
Click **OK**.

14. The following screen will appear. Click **OK**.

Figure 10-45 Add repository from file system

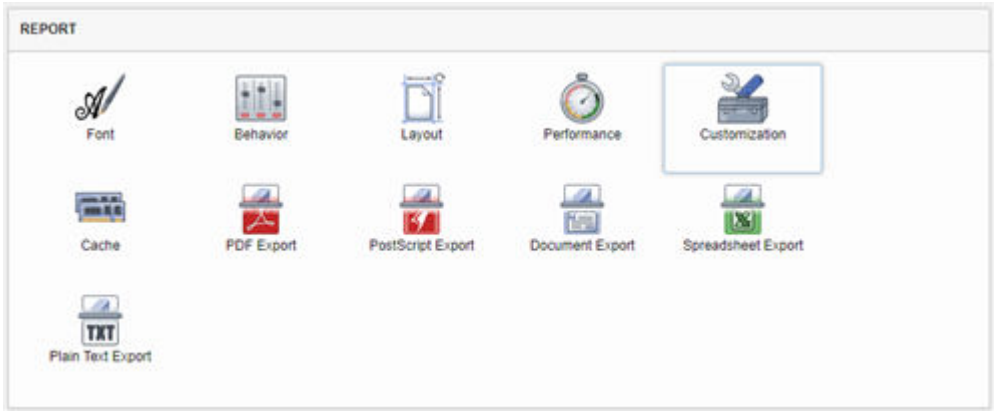
15. The Add Repository pop-up will appear. Click the checkbox beside the /Tekelec/WebNMS/reportingStudio option.
    a. Click **Apply**.
    b. Click **Save**.

Figure 10-46 Add repository



16. On the Advanced Configuration page, in the Report section, click the **Customization card**.

Figure 10-47 Report section

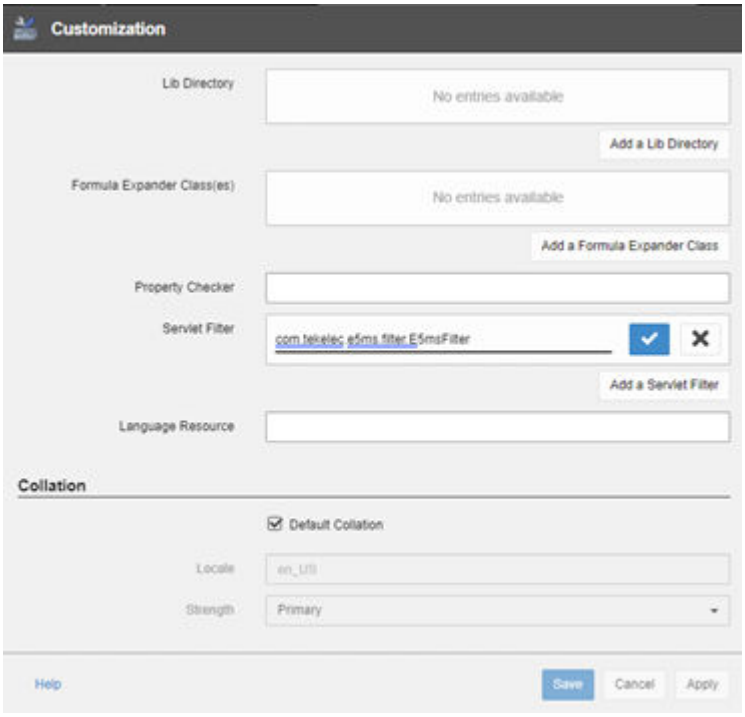


17. The following pop-up will appear. Click **Add a Servlet Filter**. In the Servlet field, enter the following:

`com.tekelec.e5ms.filter.E5msFilter`

Click **Check(✓)**.

Figure 10-48 Customization Pop-up

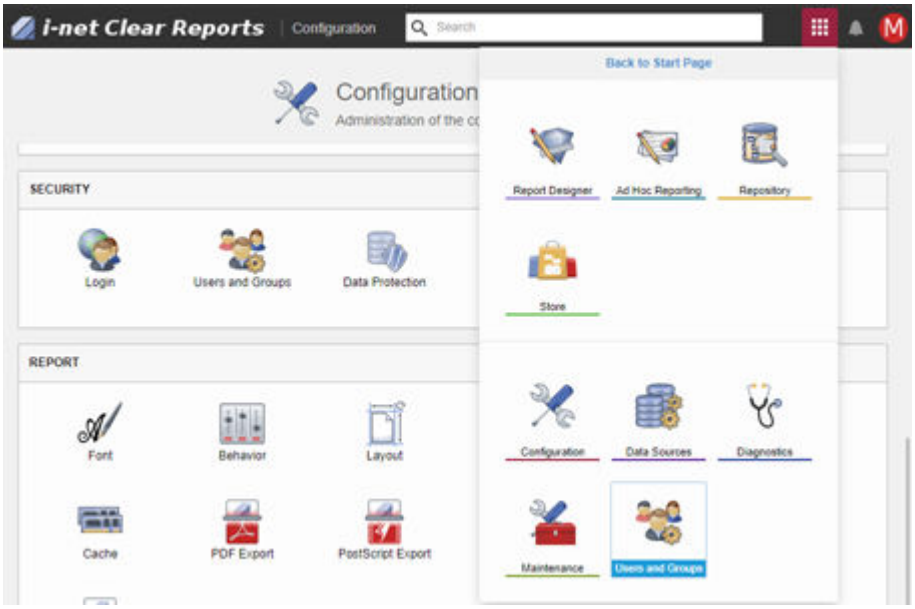


Click **Apply**.

Click **Save**.

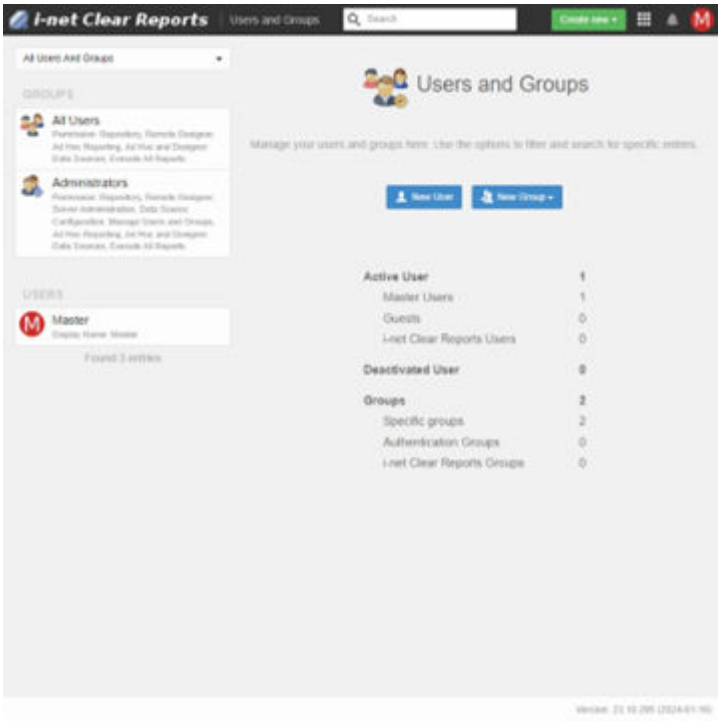
18. Click **Card Drawer** on the top right of the header and then click **Users and Groups** card as displayed in the figure below:

Figure 10-49 Clicking the Users and Groups Card



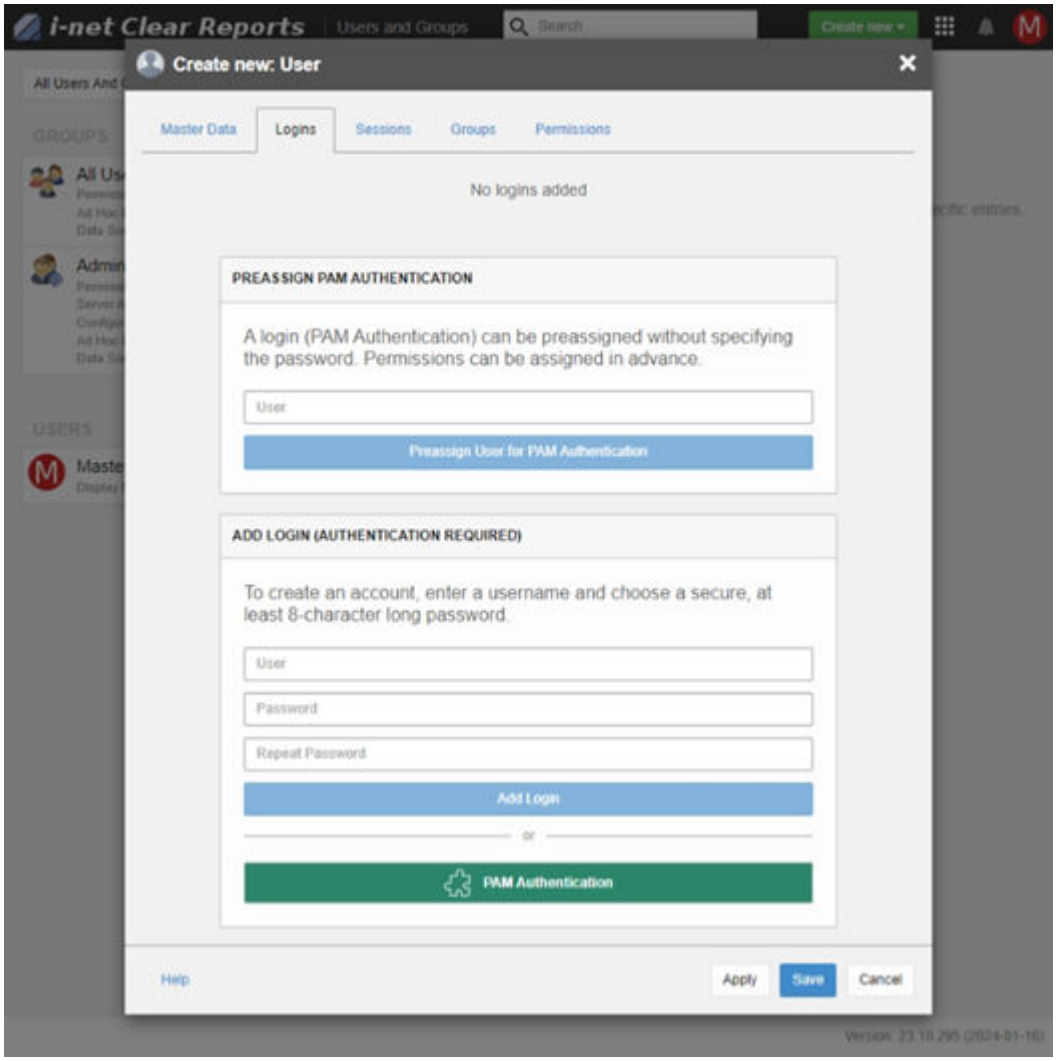
The following screen will appear.

Figure 10-50 Users and Groups



19. Click **New User** and navigate to the **Logins** tab.

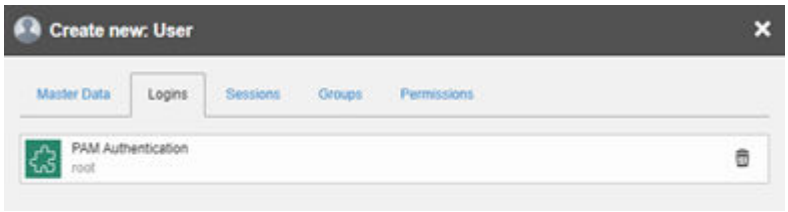
Figure 10-51 Creating New User



a. Enter **root** in the User field under Preassign PAM Authentication.

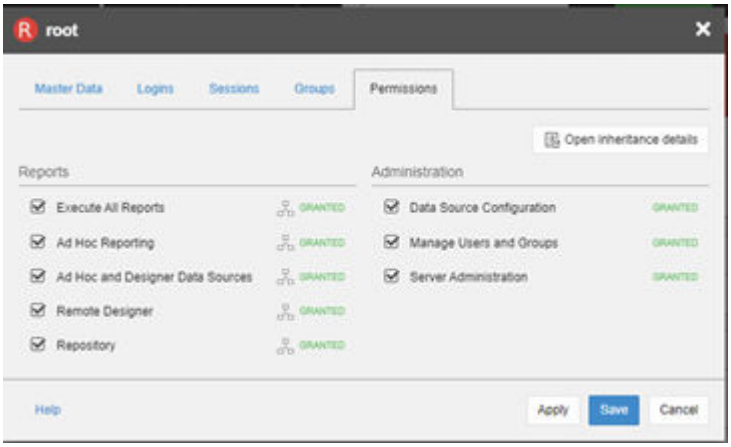
b. Click the **Preassign User for PAM Authentication** button.

Figure 10-52 PAM Authentication for Root Setup



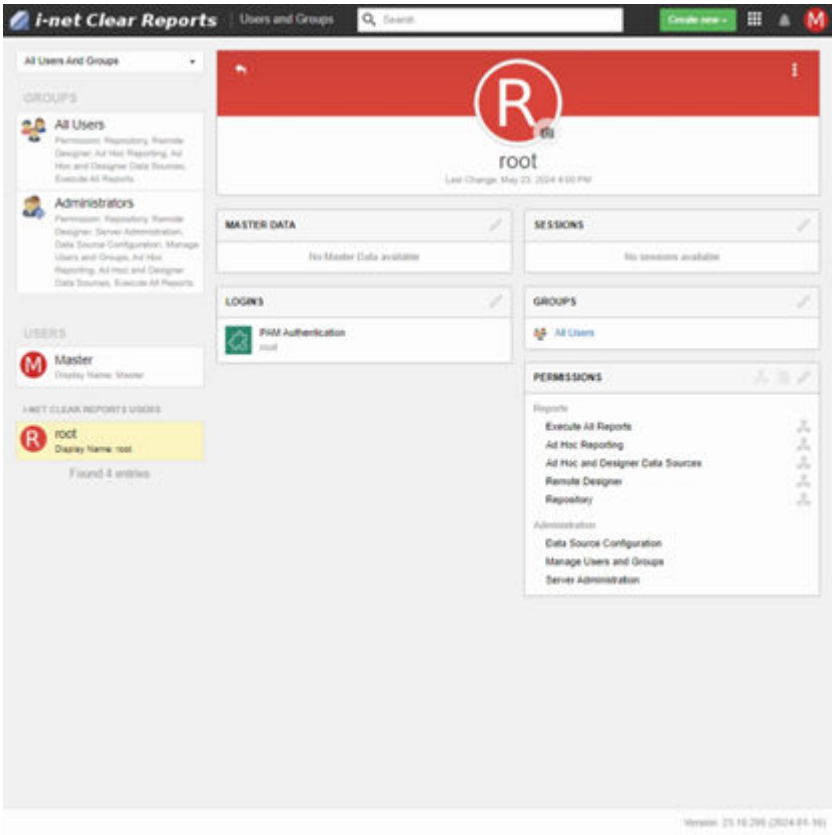
20. Click the **Permissions** tab and assign all the permissions as displayed in the figure below. Click **Apply** followed by **Save**.

Figure 10-53 Permissions tab



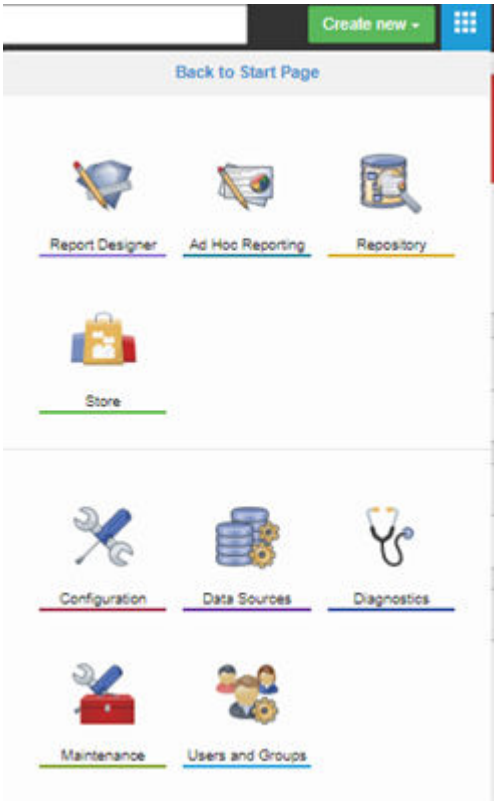
21. Verify the Permissions as follows:

Figure 10-54 Verifying the permissions



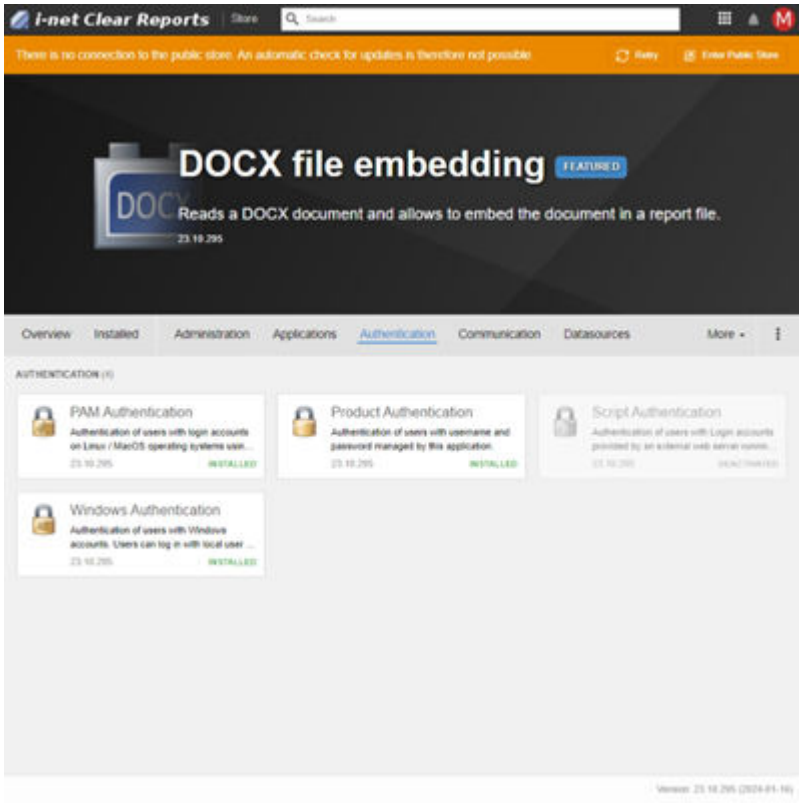
22. Click the **Cards Browser**. Select the **Store** Card.

Figure 10-55 Store Card



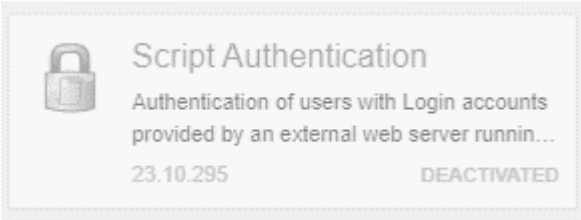
23. On selecting the Store Card, the following page will appear. Select the **Authentication** tab.

Figure 10-56 Authentication tab



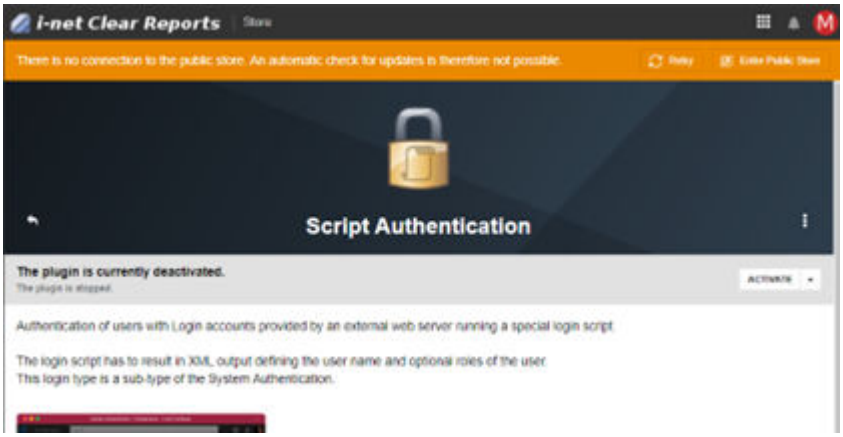
24. Click the grayed out **Script Authentication** Card.

Figure 10-57 Disable Script Authentication



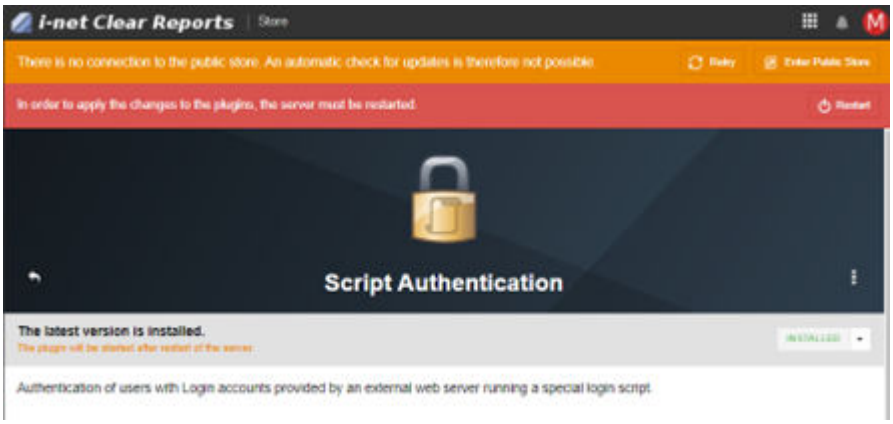
25. Click **Activate**.

Figure 10-58 Script Authentication Page



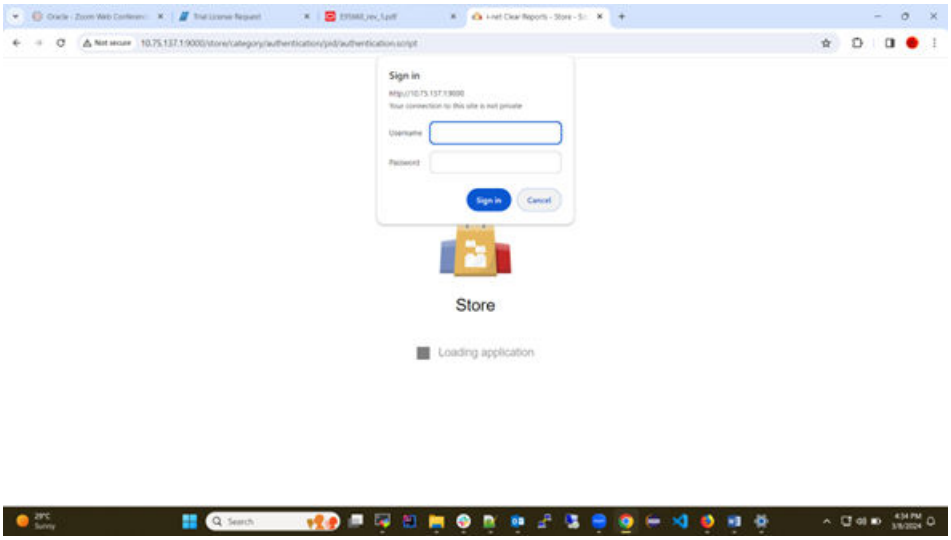
Once the script is authenticated, the following page will be updated to give the restart option as follows.

Figure 10-59 Restart option



26. If the browser asks to re-login as shown in the screenshot below, then close the browser tab and log in as master again.

Figure 10-60 Re-login

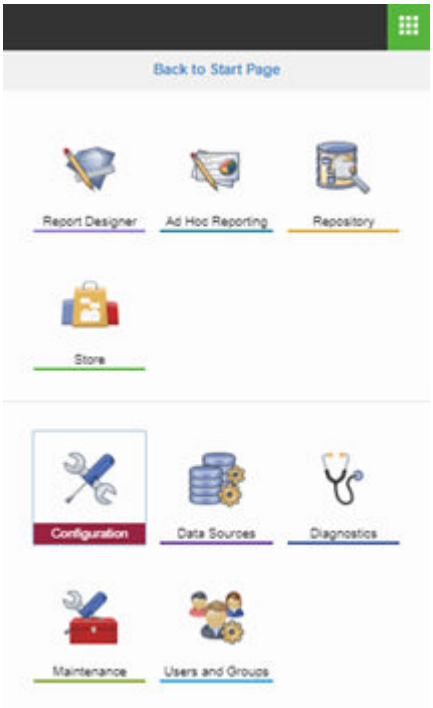


a. Type URL: `http://<IP address of the EMS Server>:9000/`

b. Log in as master with your master password.

27. Click **Card Browser** and click the **Configuration** card.

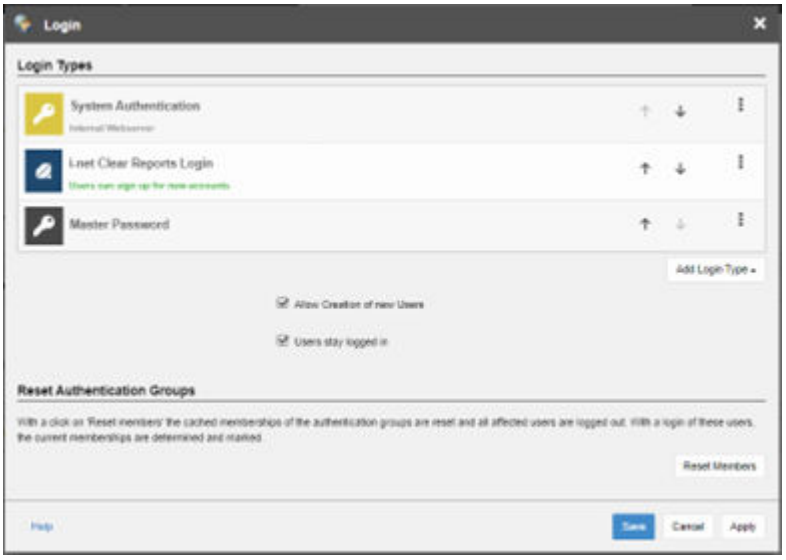
Figure 10-61 Condiguration Card



28. Under security, click **Login**.

The following pop-up screen will appear.

Figure 10-62 Login pop-up

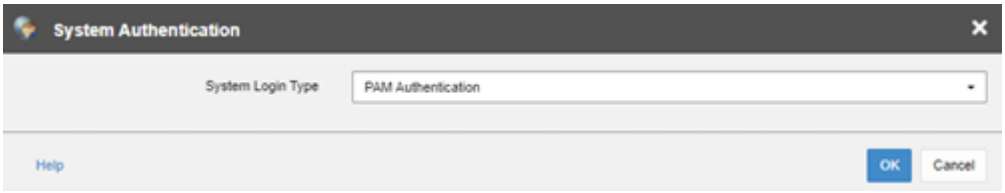


29. Click the **three dot** button beside System Authentication and click **Edit**.

Figure 10-63 Edit system authentication

The following screen will appear.

Figure 10-64 Authentication screen

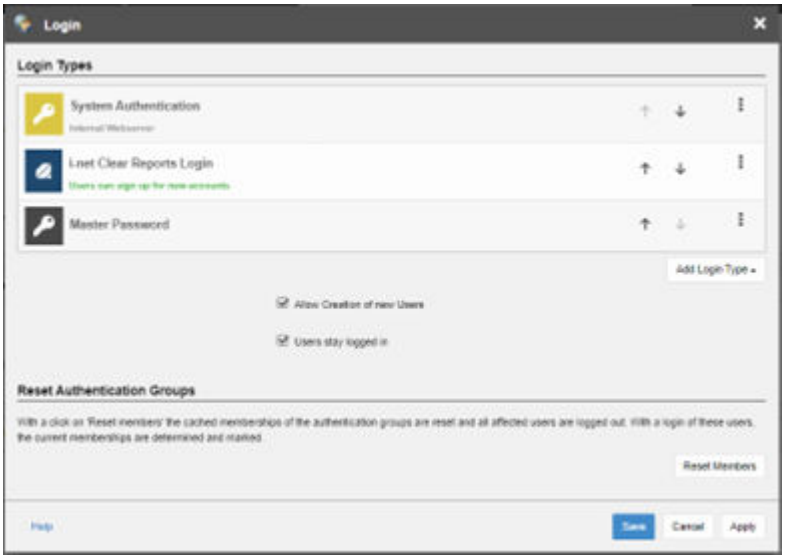


30. Click the **drop-down**, then the **Internal Webserver** option, and then click **OK**.

Figure 10-65 System authentication

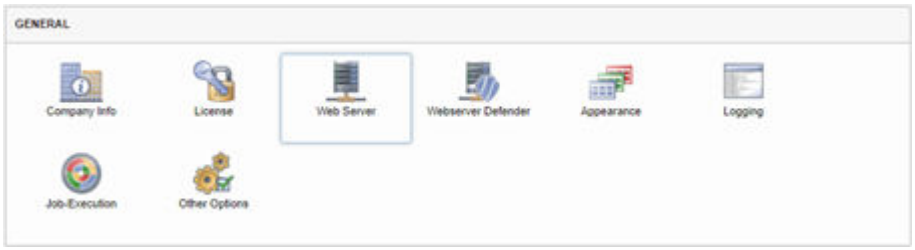
31. The following screen will appear. Click **Apply** and then **Save**.

Figure 10-66 Login pop-up



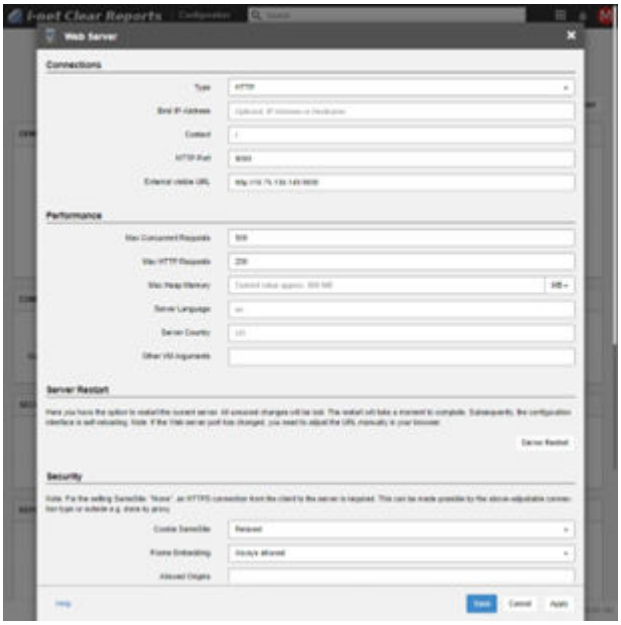
32. From the **Advanced Configuration** View, under the **General Section**, click the **Web Server Card**.

Figure 10-67 Webserver Card



The following pop-up screen will appear.

Figure 10-68 Web Server Pop-up

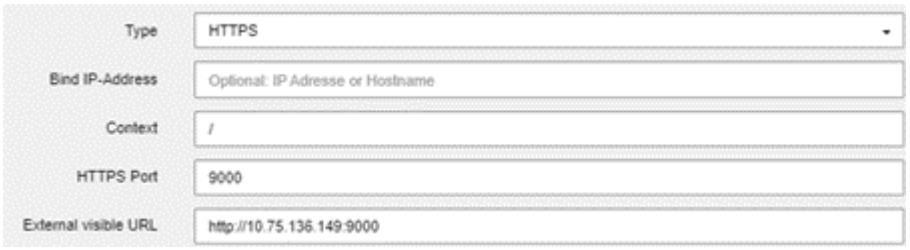


33. In the **Type** field, from the drop-down, select the **HTTPS** option.

Figure 10-69 Select HTTPS

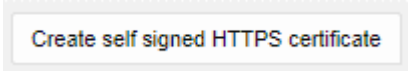
34. Update the PORT section as follows:

Figure 10-70 Updating the Web Server Pop-up



35. Click **Create self signed HTTPS certificate**.

Figure 10-71 Self Signed Certificate Button



36. Fill the certificate form as follows:

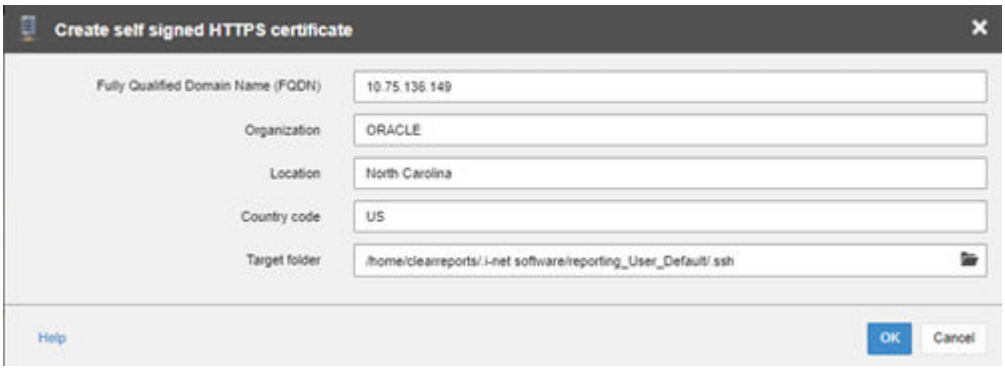
    Organization: <Use Organization Name>

Location: <use Organization location>

Country Code: <use Organization country>

FQDN: <use EMS server IP>

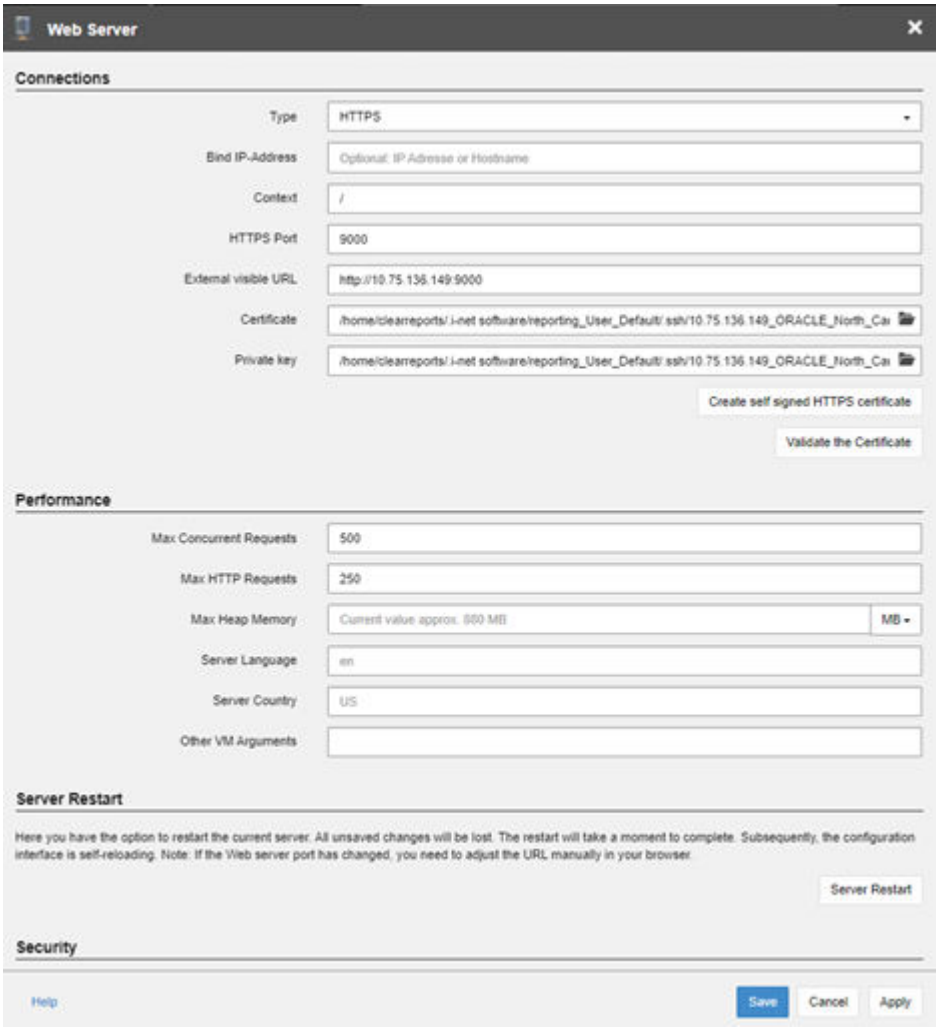
Figure 10-72 Self signed certificate form



Click **OK**.

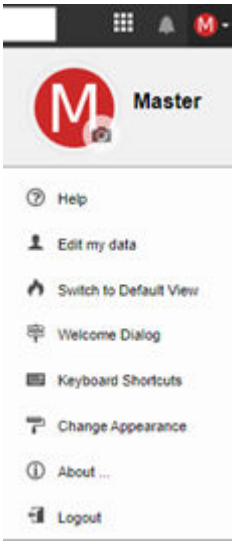
37. The **Web Server Form** will be as follows:

Figure 10-73 Filled up web server form



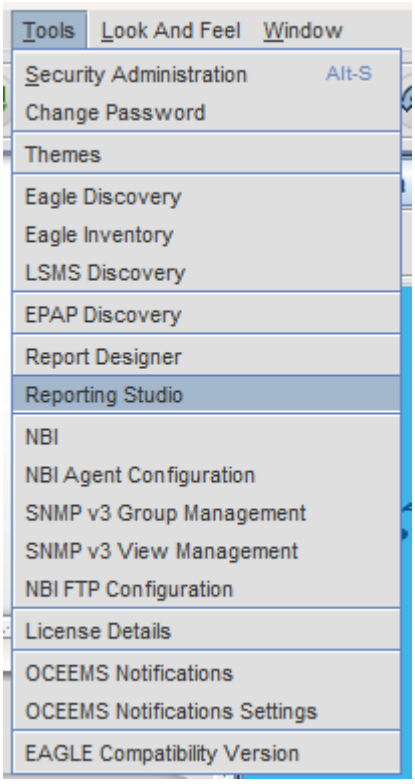
38. Click **Apply** and then **Restart Now**.
39. At ths point, the UI will freeze while loading.
40. Change the URL by adding https to it instead of http. The page will load.
41. Click **Save**.
42. Click the **User("M")** button and then **Logout** (Logout from Master).

Figure 10-74 Log out from Master



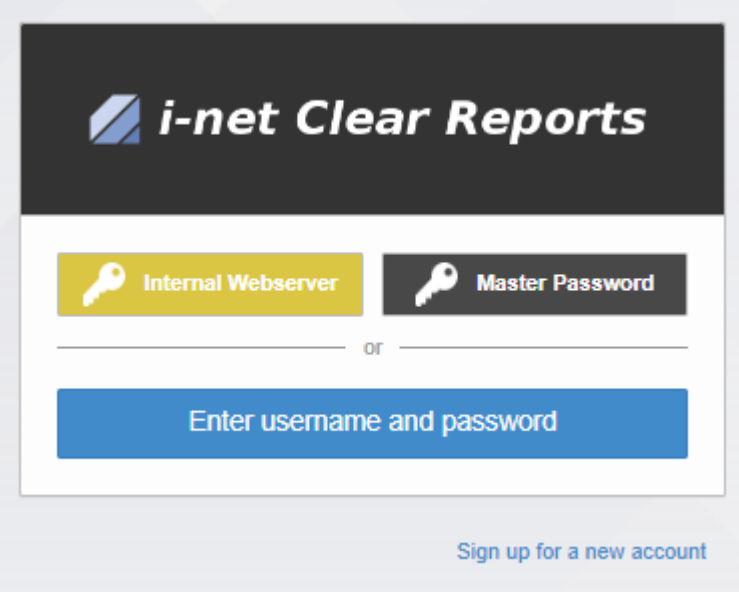
43. Open EMS GUI.
44. Launch Reporting Studio by cicking **Tools** and then **Reporting Studio**.

Figure 10-75 EMS GUI



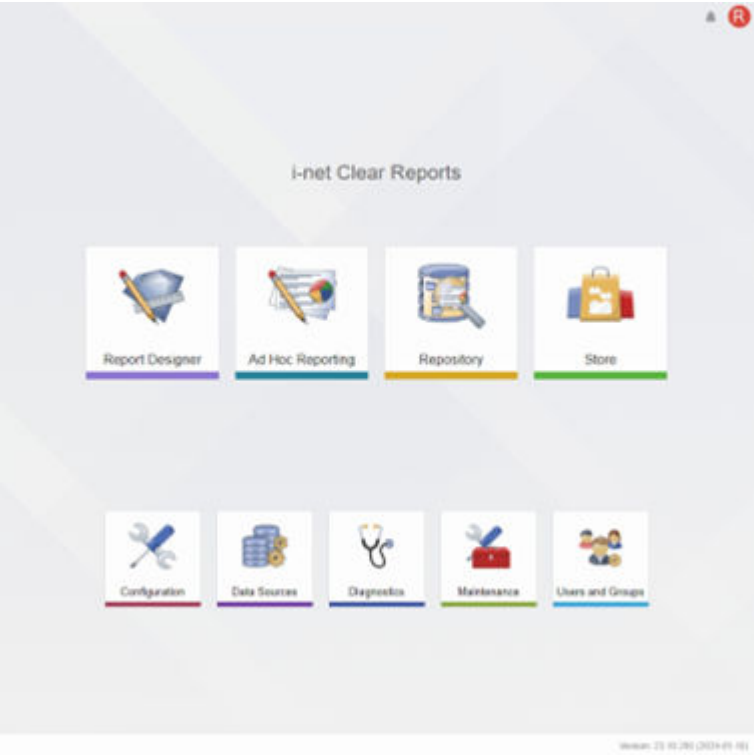
45. On selecting the Reporting Studio option, the following page will load in the browser. Click **Internal Webserver**.

Figure 10-76 Open Reporting Studio from EMS GUI



The following page will load.

Figure 10-77 Reporting Studio configured



46. Reporting Studio is now completely installed and configured.

Uninstalling i-net 23.x

Perform the following steps to uninstall i-net 23.x:

1. Run the following commands using the root user in the EMS Server CLI.

```
rm -rf /tmp/clear-reports-$currentInetUser.out
rpm -ev clear-reports-server
rm -rf /usr/share/i-net-clear-reports/
```

2. Remove the configuration if it is required. If the configurations are not removed, they will be restored on re-installing i-net Clear Reports 23.x. For removing the configuration, run the following commands with root user:

```
# rm -rf /home/clearreports/.java/.userPrefs/com/inet/report/config/cc/
Default/
# rm -rf /home/clearreports/.java/.userPrefs/com/inet/report/config/
datasource/e5msdb/
# rm -rf /home/clearreports/.i-net\ software/reporting_User_Default/
AllUsers/*
```

11

Configuration Management Interface

This chapter provides descriptions of the features and functions provided by the **OCEEMS** Configuration Management Interface (**CMI**).

Overview

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

The CMI module provides three main functions:

- Command execution on EAGLE(s) - The Send Command screen enables the users to execute single commands on desired EAGLE(s).
- Command script creation, management, and execution on EAGLE(s) - The following screens are provided to OCEEMS 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 scripts
  - 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)
- Command Class Management - To create and maintain custom command classes

Note

The CMI module is pre-populated with the command set from the EAGLE release with which the OCEEMS 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

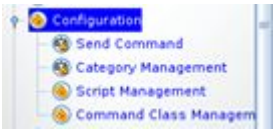
Functional Description

The assigned users can send commands and scripts to the EAGLE and get the 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.

The CMI module connects to EAGLE using the IPSM card(s) configured on the EAGLE. See the EAGLE Discovery Application chapter for the setup of the IP address from the OCEEMS to the EAGLE.

The Configuration Management Interface is accessed from the left pane of the OCEEMS GUI tree node, as shown in Figure 11-1.

Figure 11-1 CMI Tree Node

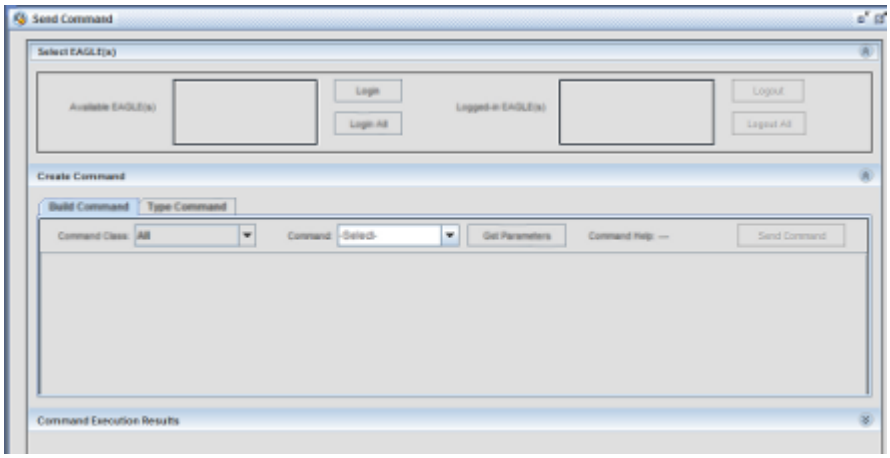


Send Command

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 Appendix A 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 Send Command Screen.

Figure 11-2 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).

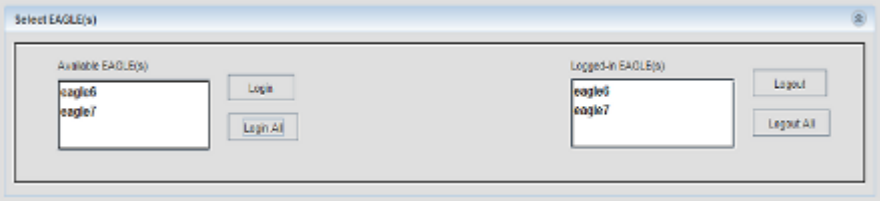
Select EAGLE(s) Pane

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 11-3 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 OCEEMS 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.

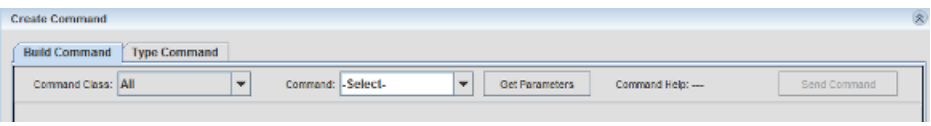
> **Note**
>
> The OCEEMS User remains logged in to these EAGLE system(s) until the OCEEMS User logs out.

Login will not be attempted on EAGLE(s) that the OCEEMS 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, as shown in Figure 11-4.

Figure 11-4 Create Command Pane

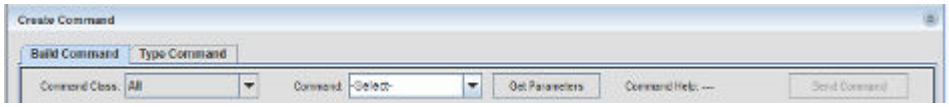


- The **Build Command** tab provides drop-down lists for Command Class and Commands to build a valid command to be sent to EAGLE systems.
  - The **Command Class** drop-down list is used to select a command class.
  - The **Command** drop-down list contains the commands associated with the command class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

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**.

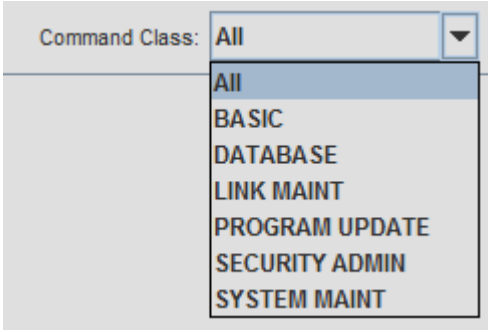
Figure 11-5 Build Command Tab



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

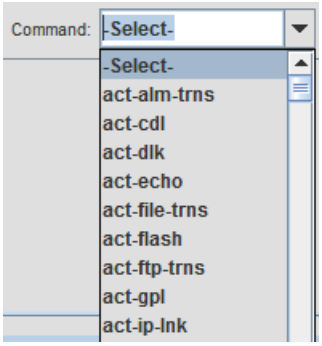
Figure 11-6 Command Class Menu



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

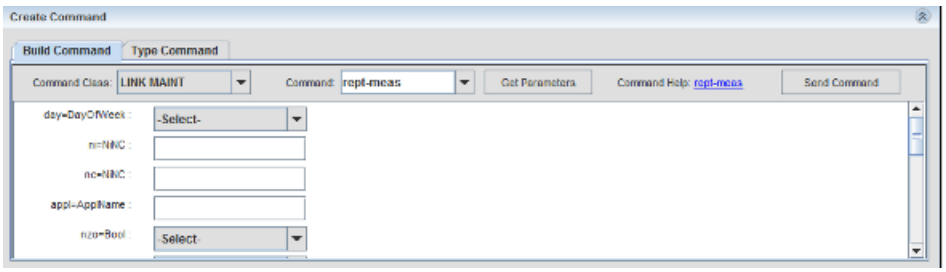
  The **Command** drop-down list has all the commands on which the user has access. The **All** corresponds to all the commands.

Figure 11-7 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 11-8 Get Parameters



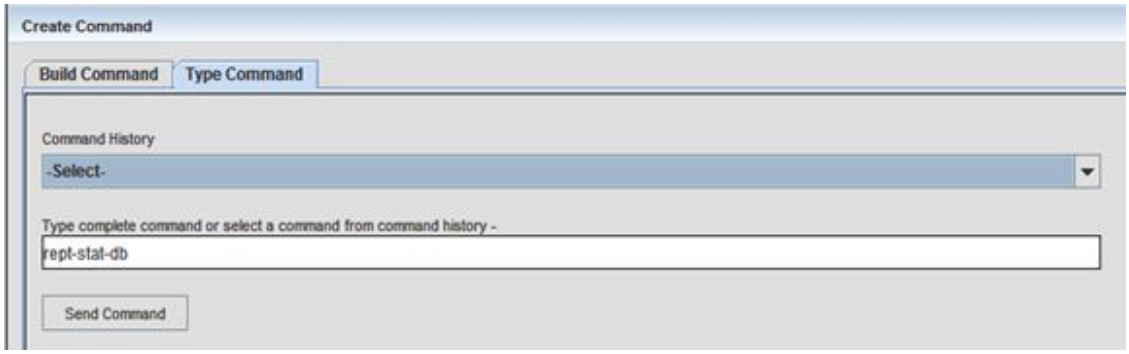
- If the command is one of the last n commands used in the current user session, then the previously used values for various parameters is automatically get populated.
- Reference message 9 in the CMI Informational / Error Messages List that displays if the user clicks on **Get Parameters** button while 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 in 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 11-9 Type Command Pane



> **Note**
>
> The user should not use pass command or any debug command from the **Send Command**, and then **Type Command** option. The pass through commands are to be used with caution under the direction of My Oracle Support.

A **Command History** drop-down menu is also available to display the most recent commands that a user previously sent to EAGLE via the Type Command pane. Command history is maintained on a per user basis and is persistent over OCEEMS client sessions. By default, the command history can contain up to 30 commands, and this value is configurable through the `commandHistorySize` parameter in the `/Tekelec/WebNMS/conf/tekelec/CmiParameters.conf` file. The OCEEMS administrator can update this value as required and restart OCEEMS to bring the new number of commands per user into effect. When a command is selected in the **Command History** drop-down menu, the command is added to the text field where it can be edited if desired.

A **Send Command** button is below the text field. This button is disabled when the text field is empty. Once a command is entered and the **Send Command** button is clicked, the command is checked for following cases:

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

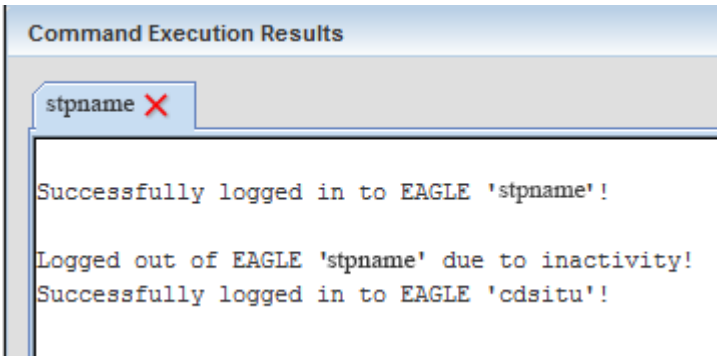
If the command string passes both the validations, the command is sent for execution to the EAGLE(s) selected by the user in the **Logged-in EAGLE(s)** list.

In the case that the command string does not pass either of the validations, the command is not sent for execution to the EAGLE(s) selected by user in the **Logged-in EAGLE(s)** list (see message 7 in CMI Informational / Error Messages List.

Command Execution Results Pane

This pane is used to display results of login, logout and other commands as shown in 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 11-10 Command Execution Results Pane



Viewing the Commands Sent to EAGLE Systems

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**).

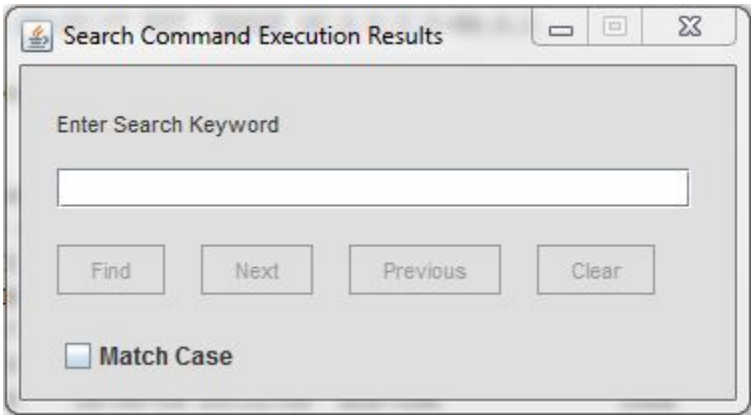
   The link **To view complete result, click here** file will not be visible after the **Clear Results** button is clicked.

> **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.

Searching Command Execution Results

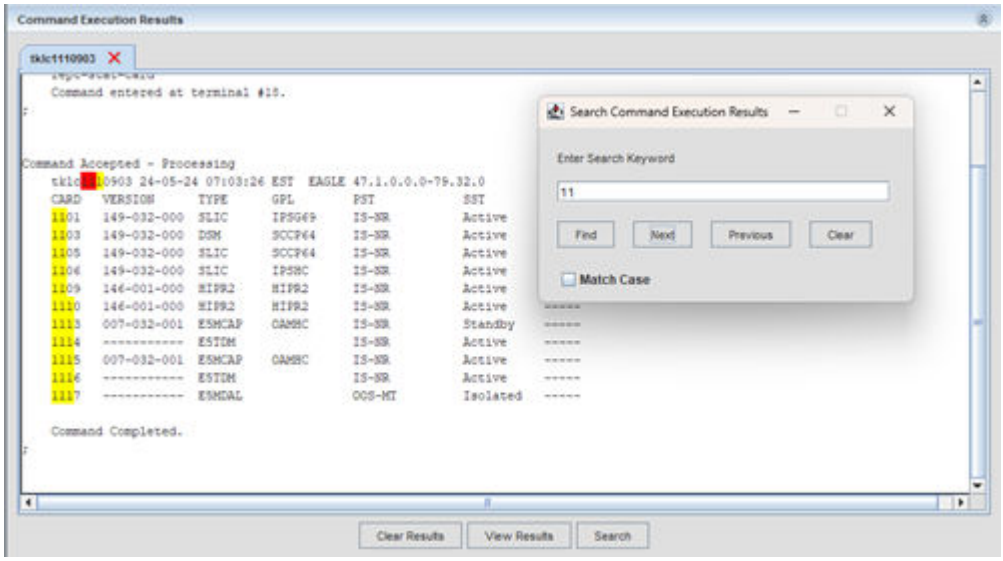
The **Search** button on the Send Command screen can be used to search the active STP tab in the Command Execution Results pane. Clicking the **Search** button brings up the search box:

Figure 11-11 Search Command Execution Results Box



Enter a search string and click **Find** to locate the string in the Command Execution Results, **Next** or **Previous** to go to the next or previous occurrence of the string, or **Clear** to clear the search box to its default state. Use **Match Case** for a case-sensitive search.

Figure 11-12 Send Command Search



Keyboard Shortcuts for Searching

The following shortcuts are provided to enable searching via the keyboard:

Ctrl + F
The **Ctrl + F** key combination can be used as an alternative to the **Search** button to bring up the search box.

Enter
The **Enter** key can be used as an alternative to the **Find** button to initiate a search.

-> (Right Arrow)
The **->** key can be used as an alternative to the **Next** button to proceed to the next match of the search keyword.

<- (Left Arrow)
The **<-** key can be used as an alternative to the **Previous** button to proceed to the previous match of the search keyword.

Ctrl + Q
The **Ctrl + Q** key combination can be used as an alternative to the **Clear** button to clear text typed into the search box (and any matches found if a search was done).

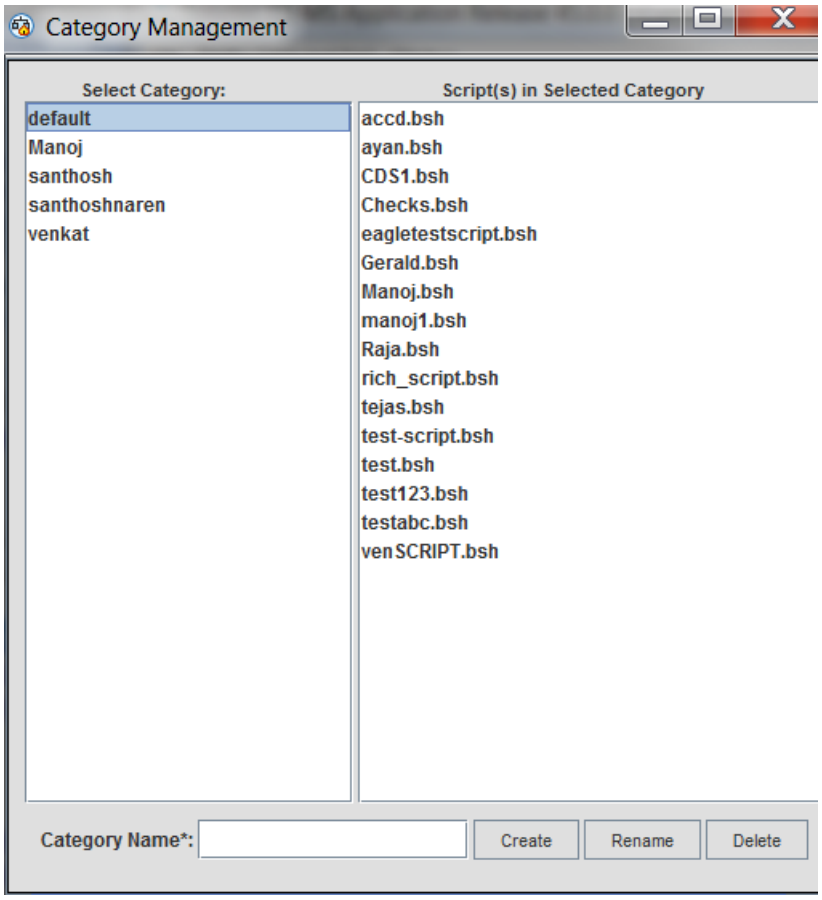
Tab as needed + space
To select the **Match Case** checkbox, repeatedly press the **Tab** key until **Match Case** is highlighted, and then press the **space** key to select the checkbox. The checkbox can be de-selected using similar steps.

Esc
The **Esc** key can be used as an alternative to the **X** (close) button on the search box to close the box.

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 OCEEMS under Configuration Management Interface. An example of this screen is shown in Category Management Screen.

Figure 11-13 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 OCEEMS 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.

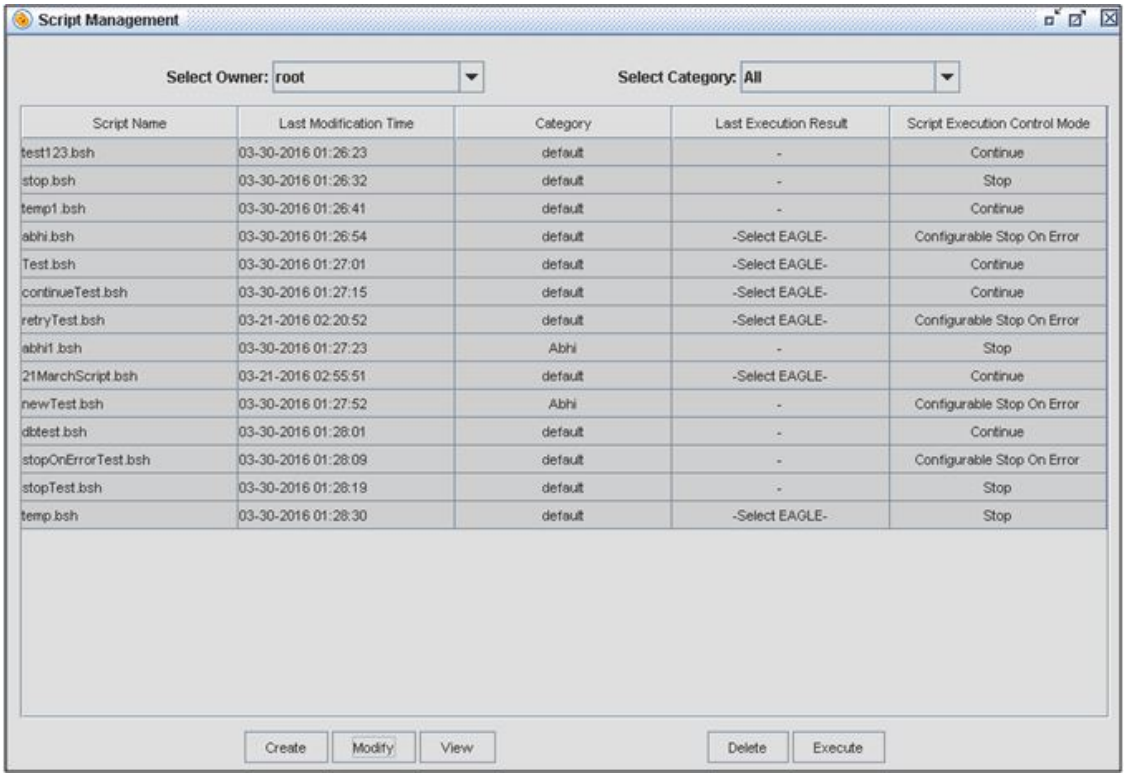
In case a category deletion fails reference message 28 and 29 in the CMI Informational / Error Message List.

In case a user is deleted from OCEEMS 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 OCEEMS GUI under Configuration.

Figure 11-14 Script Management Screen

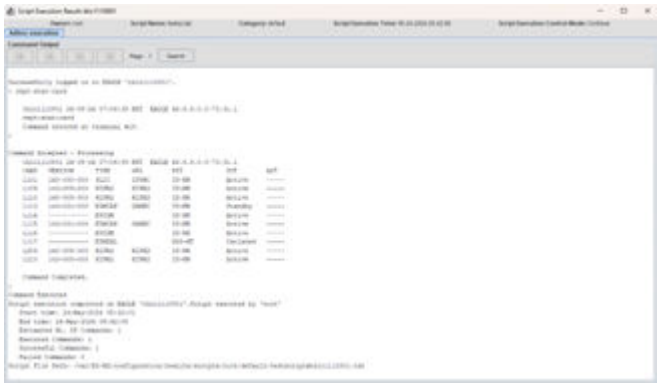


On top of the **Script Management**' screen, the **Select Owner** and **Select Category** drop-downs menus are provided. The **Select Owner** drop down allows the System Administrator to enable and disable a non-admin user. It lists all the OCEEMS users and the currently logged-in user's name. The **Select Category** drop down has the listing of all the categories for the user selected in the **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. The following columns are 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
- Script Execution Control Mode - Script Execution Control Mode for the script

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.

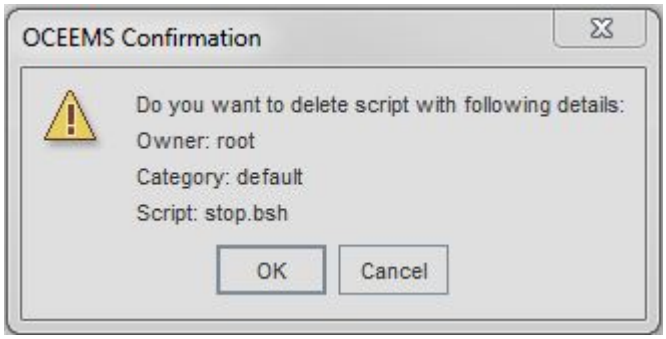
Figure 11-15 Script Execution Result screen



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 OCEEMS 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 OCEEMS 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 about deletion of the selected script.

Figure 11-16 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 OCEEMS admin.

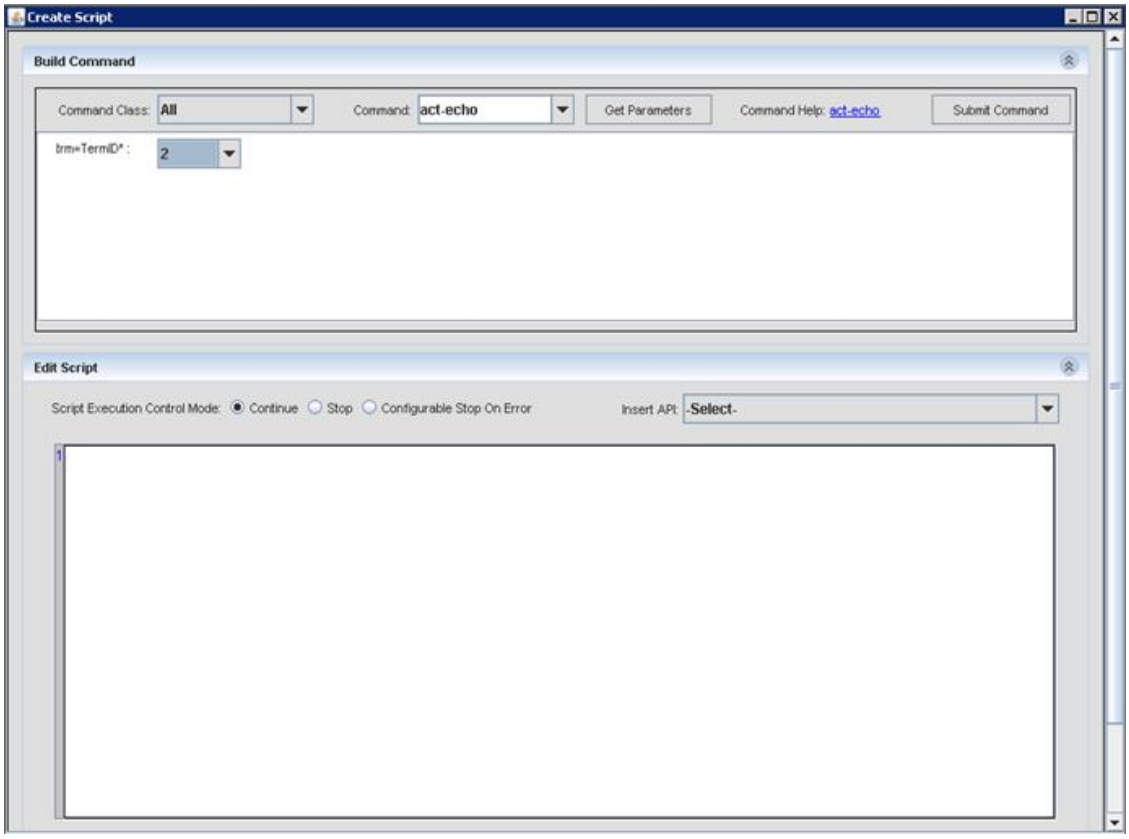
Create Script

The Create Script screen has three panes as follows:

- The Build Command pane enables the user to build a command to be included in the script.
- The Edit Script pane enables the user to manually edit the script.

- The Save Script Results pane (not pictured) displays the results of saving the script.

Figure 11-17 Create Script Screen



While creating command scripts, for command parameters with values that need to be specified in double quotes, you must use the backslash (\) character before each double quote to be able to save the script successfully. For example, to include the following command in a script:

```
chg-prefix:feature="GSM MAP":prefixnum=32:prefix=10
```

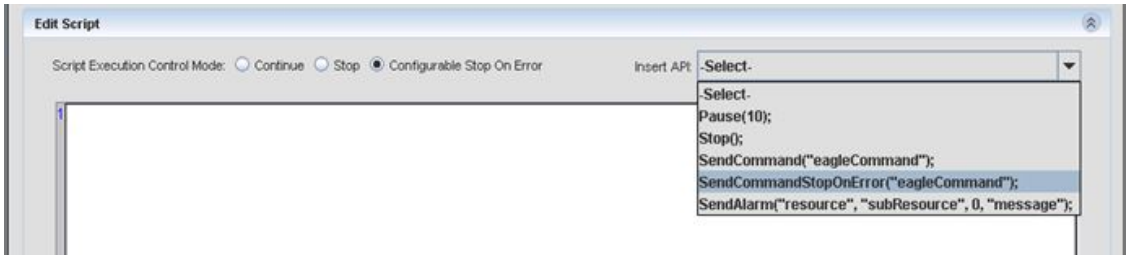
Specify the backslash (\) before each double quote in the feature parameter value as follows:

```
chg-prefix:feature=\"GSM MAP\":prefixnum=32:prefix=10
```

Edit Script Pane

This pane allows a user to edit a script manually.

Figure 11-18 Edit Script Pane

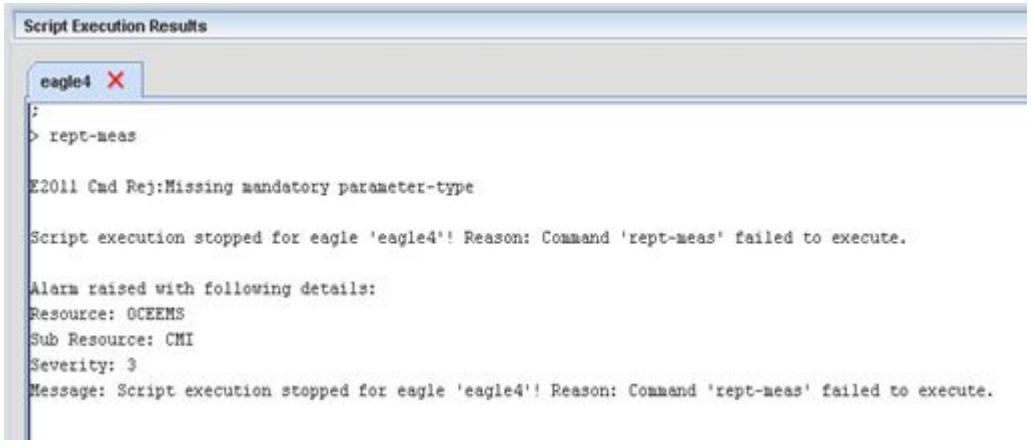


The **Script Execution Control Mode** radio buttons are available on the Create Script and Modify Script screens to control script behavior when a command fails on the EAGLE. The three possible behaviors are:

Continue
If the **Continue** mode is selected, script execution will continue irrespective of any command failures. All the commands in the script will be attempted for execution until the user manually stops script execution. This is the default mode when creating a script.

Stop
If the **Stop** mode is selected, script execution will stop at the first command failure, if the error code is not one of the errors listed for command retry. If the error code encountered is listed for command retry, the command is retried and the script will continue if the command succeeds or stop if it fails (after the defined number of retries or with an error not in the retry list). For more information, see Command Retry.
When script execution is interrupted because of a command failure in **Stop** mode, a log entry with an error code is made in the script results and an alarm is raised.

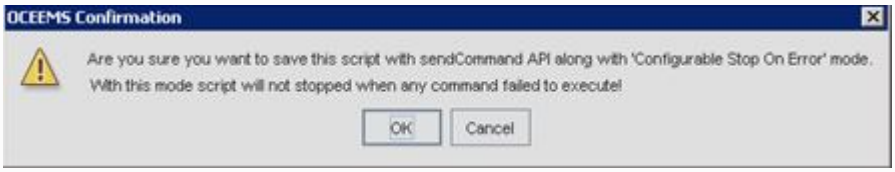
Figure 11-19 Log Entry for Stopped Script



Configurable Stop On Error
If the **Configurable Stop On Error** mode is selected, script execution can be controlled for command failures on a per command basis. A new API, **SendCommandStopOnError** must be used for the commands where script execution should be stopped on the command's failure.
When script execution is interrupted because of a command failure in **Configurable Stop On Error** mode, a log entry with an error code is made in the script results and an alarm is raised.

> **Note**
>
> Only the **SendCommandStopOnError** API should be used with the **Configurable Stop On Error** mode. Although the user has the option of using the **SendCommand** API, a script will not stop when a command in the **SendCommand** API fails. When attempting to save a script with the **SendCommand** API in **Configurable Stop On Error** mode, a warning message is issued.

Figure 11-20 Warning for SendCommand API in Configurable Stop On Error Mode



The drop down menu **Insert API** is provided above the free edit text area, which includes all the APIs defined in CMI Scripting Functions.

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.
   For some of the commands (for example, `chg-db`, `rept-stat-trbl`) that need long time to be run at Eagle, Pause() can be used so that command can be completed before stepping into further commands. Determine the Pause() interval based on the time needed for that command in that particular Eagle configuration.
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. **SendCommandStopOnError("eagleCommand")**: See **Script Execution Control Mode** above.
5. **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

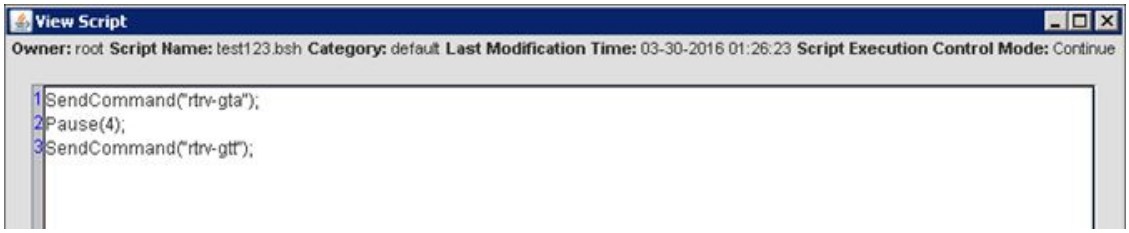
This screen is similar to the Create Script screen. When launched, it has the details of the script (script contents, name, and category) pre-populated on the page. The user can modify the script contents, name, and category, and then save.

If a user modifies the script content on the Modify Script screen and tries to close the window without saving the changes, a warning message is displayed about saving the script.

View Script

The View Script screen shows the contents of a script in a non-editable area.

Figure 11-21 View Script Screen

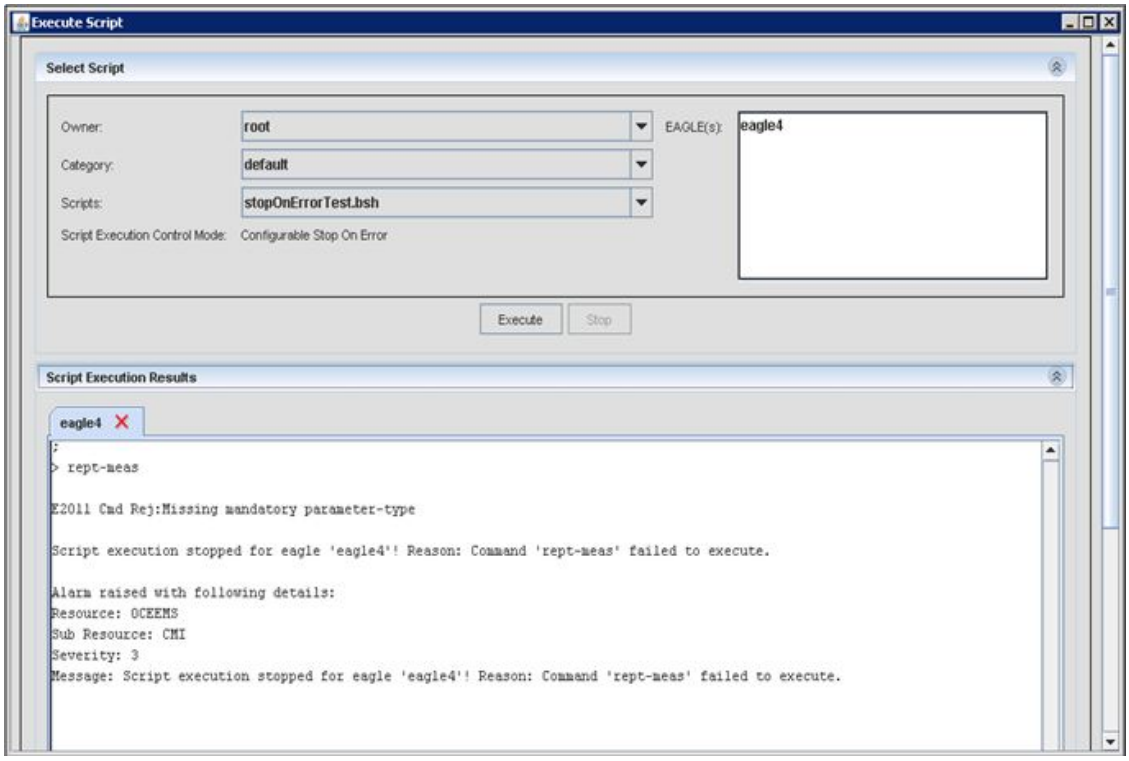


Execute Script

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

- Select Script pane - Enables the user to select a desired script and EAGLE(s) for execution.
- Script Execution Results pane - Displays the script execution results.

Figure 11-22 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 OCEEMS 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 the Owner drop down, then a category belonging to that user in the **Category** drop down, and then select the desired script to execute. A non-admin user can select their own scripts and execute them. The **Script Execution Control Mode** is also displayed.

Below the Select Script pane, the **Execute** and **Stop** buttons are 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. If there are one or more commands in the script to which 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, the 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 are displayed in that tab while the tab is open. Note that only the latest 5000 lines of results are shown in an EAGLE's tab. If there are more than 5000 lines, 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.

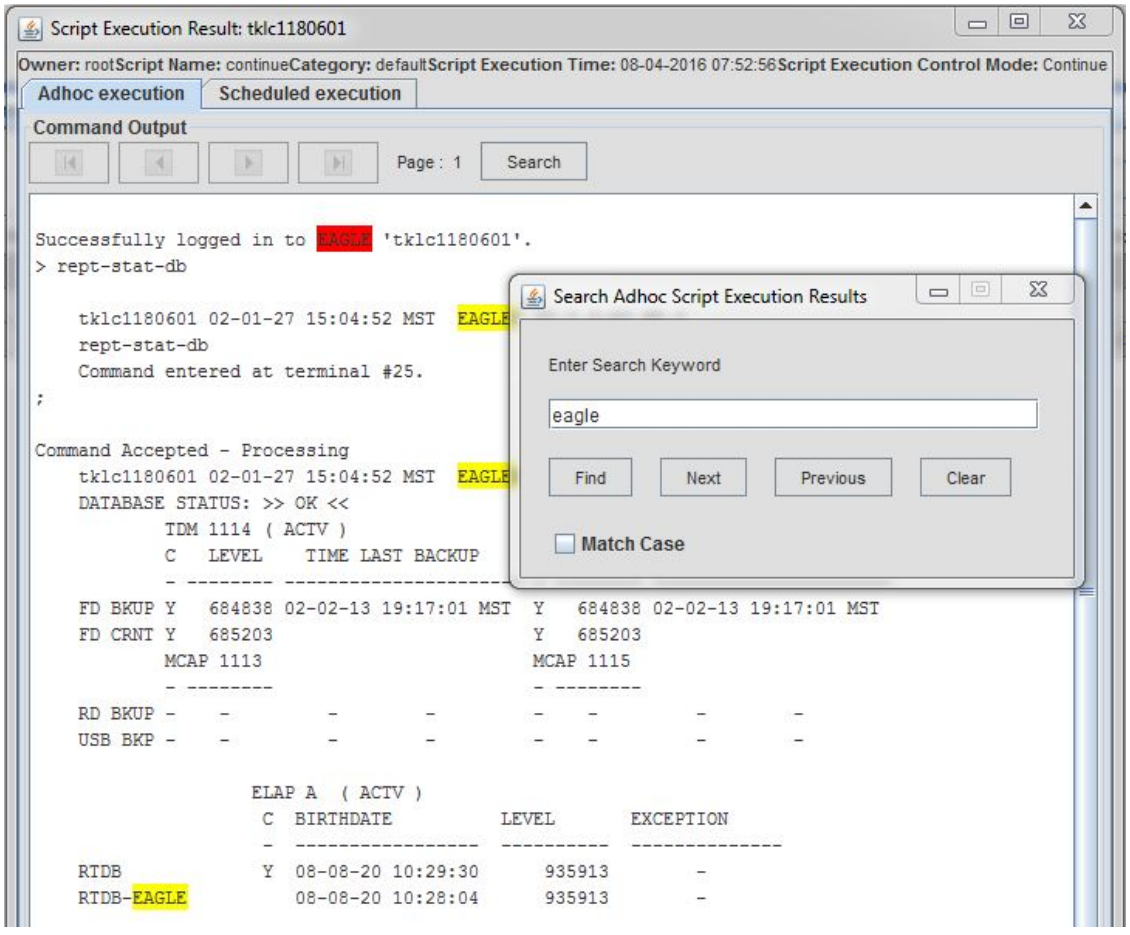
Searching Script Execution Results

A **Search** button is provided on the Adhoc execution and Scheduled execution tabs on the Script Execution Results pane.

Enter a search string and click **Find** to locate the string in the results, **Next** or **Previous** to go to the next or previous occurrence of the string, or **Clear** to clear the search box to its default state. Use **Match Case** for a case-sensitive search.

Keyboard shortcuts are also provided to enable searching via the keyboard. For information, see Keyboard Shortcuts for Searching.

Figure 11-23 Searching Script Execution Results



Script Execution Summary and Script File Path

OCEEMS provides a summary at the end of script execution that includes several counters. These counters provide information regarding the CMI script execution, and include the following:

```
Script executed by '<username>'
   Start time: <Date and time when script execution started>
   End time: < Date and time when script execution ended>
   Estimated No. Of Commands: <An estimated number of commands in the script>
   Executed Commands: <number of commands that were executed>
   Successful Commands: <number of commands that were successful>
   Failed Commands: <number of commands that failed>
   Global Error: <any error of global nature that failed the script, such as
login failure on EAGLE>
```

OCEEMS provides this summary on a per EAGLE node basis. For scheduled CMI scripts, the summary can be viewed by launching script execution results in the `Last Execution Result` column.

The path of the results file on a system is also appended to the results after script execution is complete. The path of the result file is in the following form:

```
/var/E5-MS/configuration/results/scripts/<script owner>/<script category>/
<script name>#<stp name>.txt
```

OCEEMS provides the summary and path for both ad hoc and scheduled script execution.

Figure 11-24 Summary of Script Execution and Script File Path

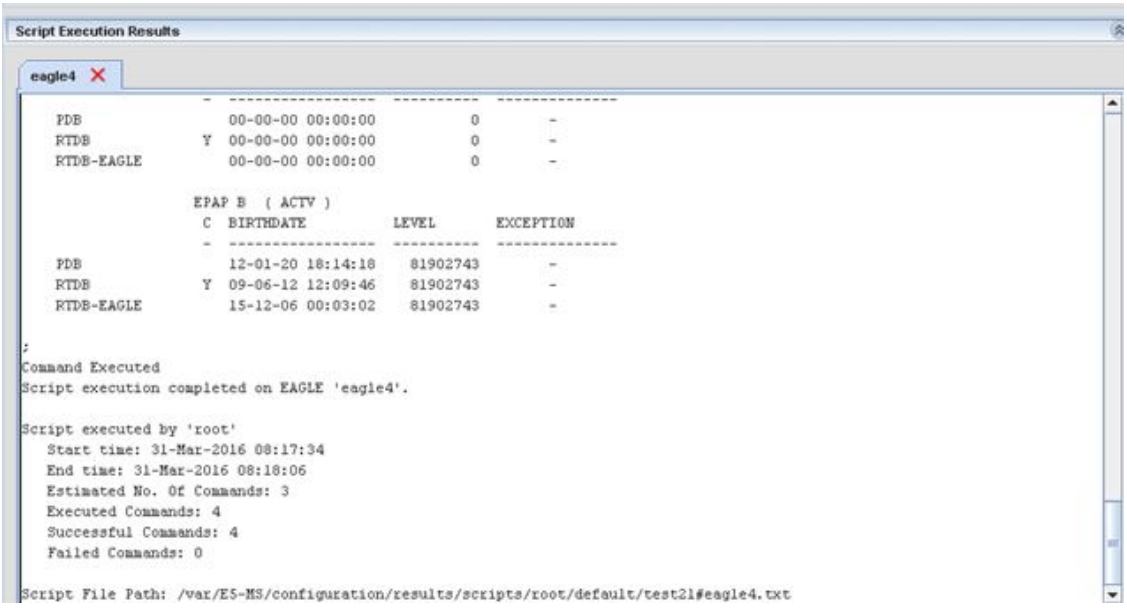
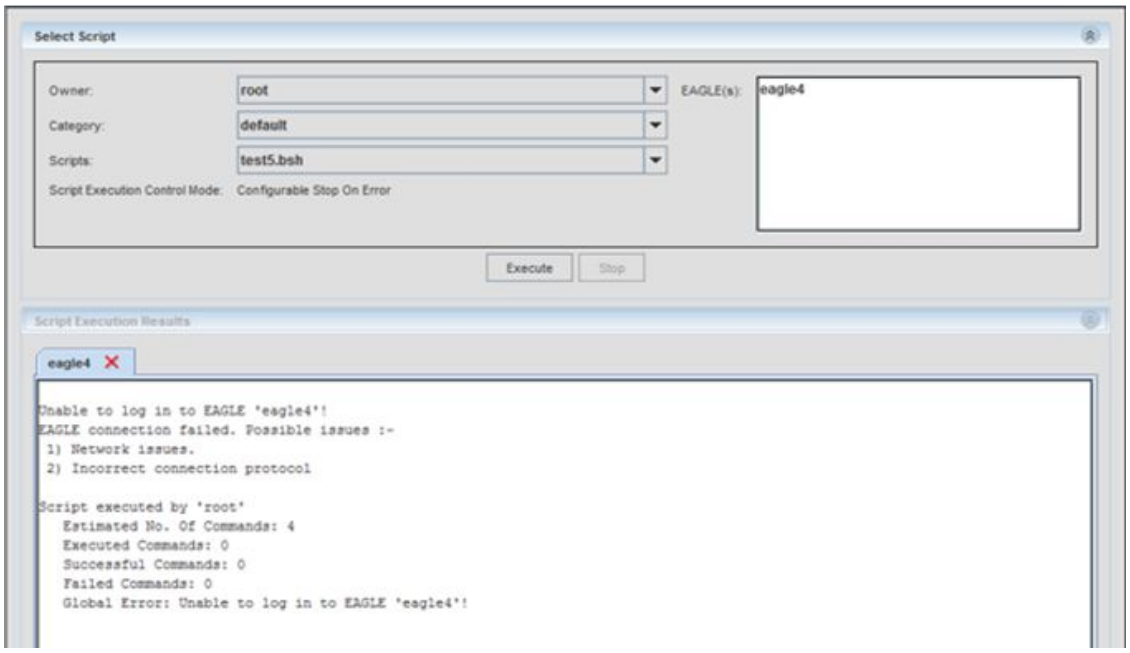


Figure 11-25 Summary of Script Execution with Global Error



Command Retry

The Command Retry mechanism is provided for command failure in CMI script execution. By default, OCEEMS automatically retries a command for execution when it fails with one of the following seven error codes: E2200, E2204, E2368, E2971, E3052, E4113, and E5277.

To enable the OCEEMS administrator to control the error codes to be used as the criteria for command retry, a comma-separated list of these error codes is available in the `eagleCommandErrorCodes` parameter in the `/Tekelec/WebNMS/conf/tekelec/CmiParameters.conf` file. The OCEEMS administrator can add/remove any error codes as required and restart OCEEMS to bring the new error codes into effect.

The number of times that a command is retried is also configurable, with the default value being three. When a command fails with one of the error codes given in the `eagleCommandErrorCodes` parameter, OCEEMS makes the designated number of retry attempts for the command. During any one of the retry attempts, if the command fails with an error code that is not available in the `eagleCommandErrorCodes` parameter, then no further retry attempts are made.

To enable the OCEEMS administrator to control the command retry number, the `commandRetryAttemptValue` parameter is available in the `/Tekelec/WebNMS/conf/tekelec/CmiParameters.conf` file. The OCEEMS administrator can update this value as required and restart OCEEMS to bring the new retry number into effect.

During script execution, if a command fails on the last retry attempt, the script will continue or stop depending upon the **Script Execution Control Mode**:

Table 11-1 Continue/Stop After Last Retry Attempt

Script Execution Control Mode	Continue or Stop Script?
Continue	Continue

Table 11-1 (Cont.) Continue/Stop After Last Retry Attempt

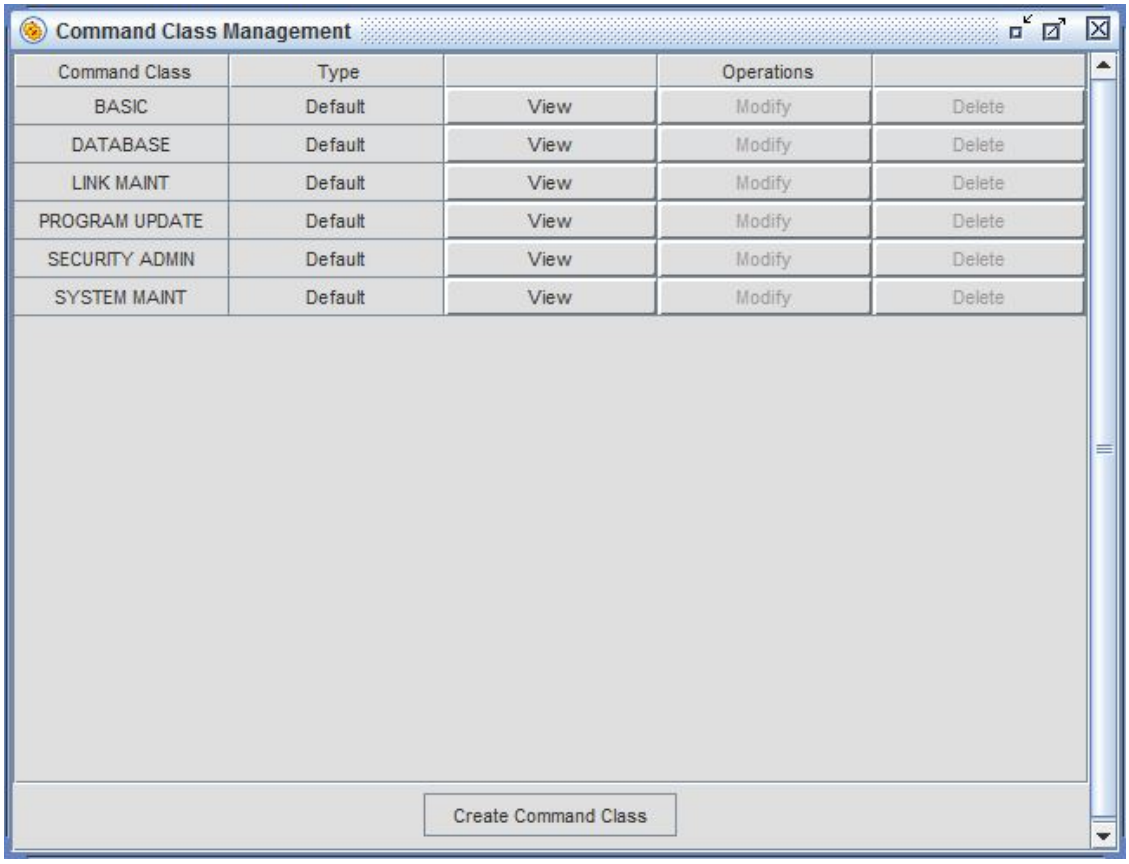
Script Execution Control Mode	Continue or Stop Script?
Stop	Stop
Configurable Stop On Error	Stop, as long as the command was sent using the **SendCommandStopOnError** API. If the command was sent using the **SendCommand** API, execution will continue. **Note** Only the **SendCommandStopOnError** API should be used with the **Configurable Stop On Error** mode.

For more information about **Script Execution Control Mode**, see Edit Script Pane.

Command Class Management

The Command Class Management screen can be used to create and maintain custom command classes. Click on **Configuration**, and then **Command Class Management** in the tree menu on the left side of the OCEEMS GUI to display the Command Class Management screen:

Figure 11-26 Command Class Management Screen

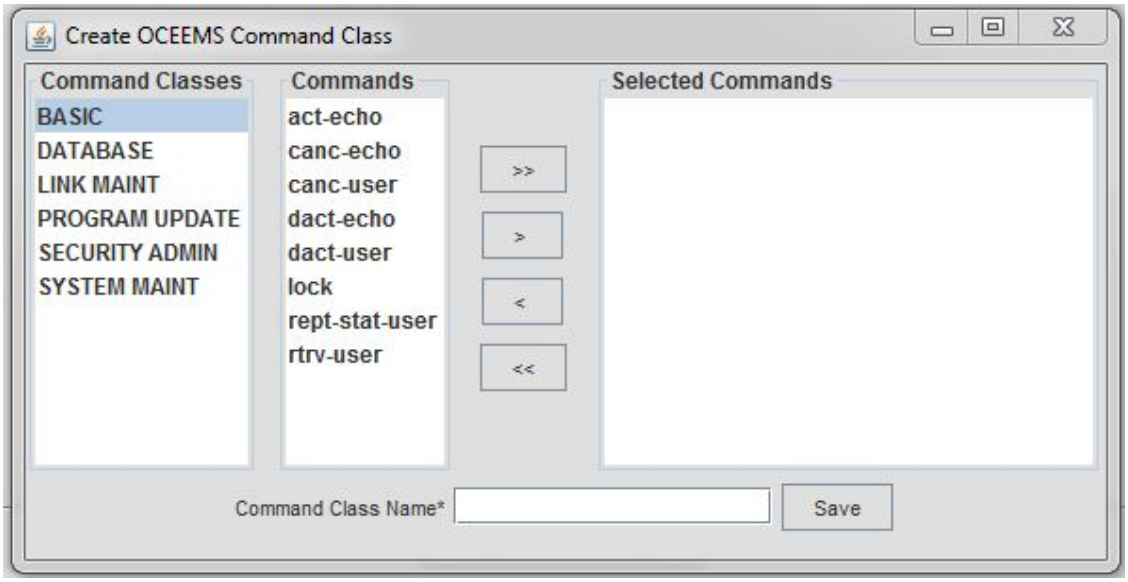


The Command Class Management screen includes all of the default command classes, which are used to create and maintain the custom command classes. The default command classes cannot be modified or deleted.

Creating a Custom Command Class

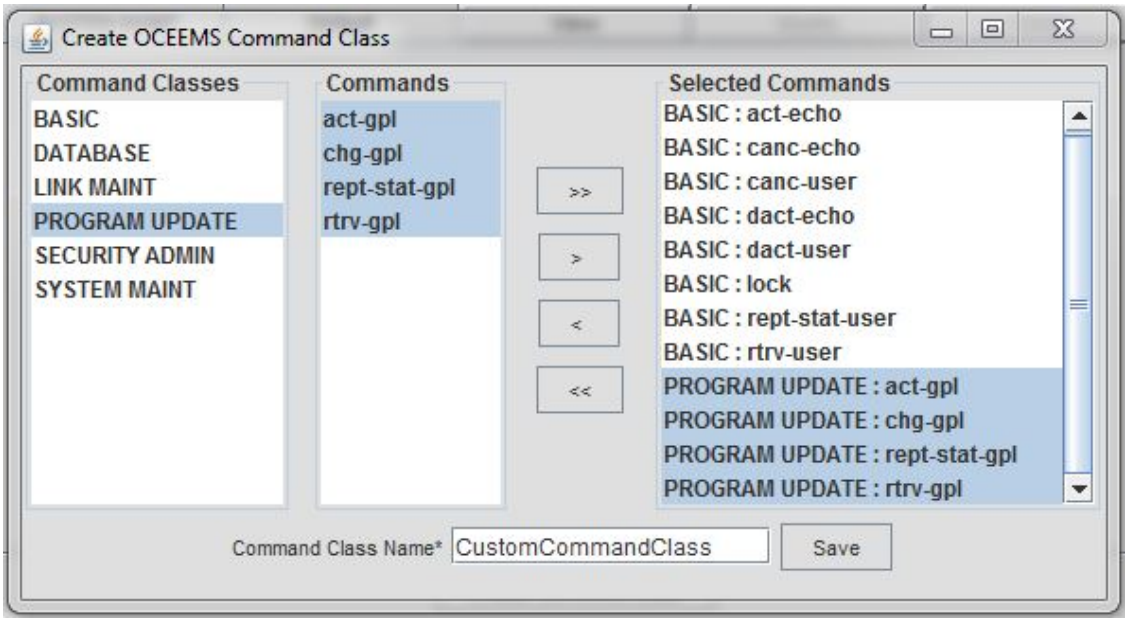
To create a custom command class, click on **Create Command Class** at the bottom of the Command Class Management screen. The Create OCEEMS Command Class screen is displayed:

Figure 11-27 Create OCEEMS Command Class Screen



Locate commands to be added to the custom command class by selecting a command class in the Command Classes pane on the left, selecting one or more commands from that command class from the Commands pane in the middle, and then using the arrow keys to move commands to the Selected Commands pane, as shown in Figure 11-28.

Figure 11-28 Selected Commands for Custom Command Class



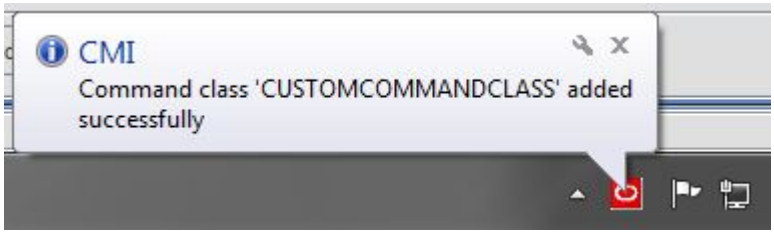
You can locate and select commands from multiple command classes to be included in the custom command class. In Figure 11-28, all commands from the BASIC and PROGRAM UPDATE command classes were selected.

Multiple commands from a command class can be selected by holding the **Ctrl** key. The arrow keys function as follows:

- **>>**
  Adds all commands that belong to the command class selected in the Command Classes pane to the Selected Commands pane.
- **>**
  Adds the commands selected in the Commands pane to the Selected Commands pane.
- **<**
  Removes the commands selected in the Selected Commands pane from the Selected Commands pane.
- **<<**
  Removes all commands from the Selected Commands pane.

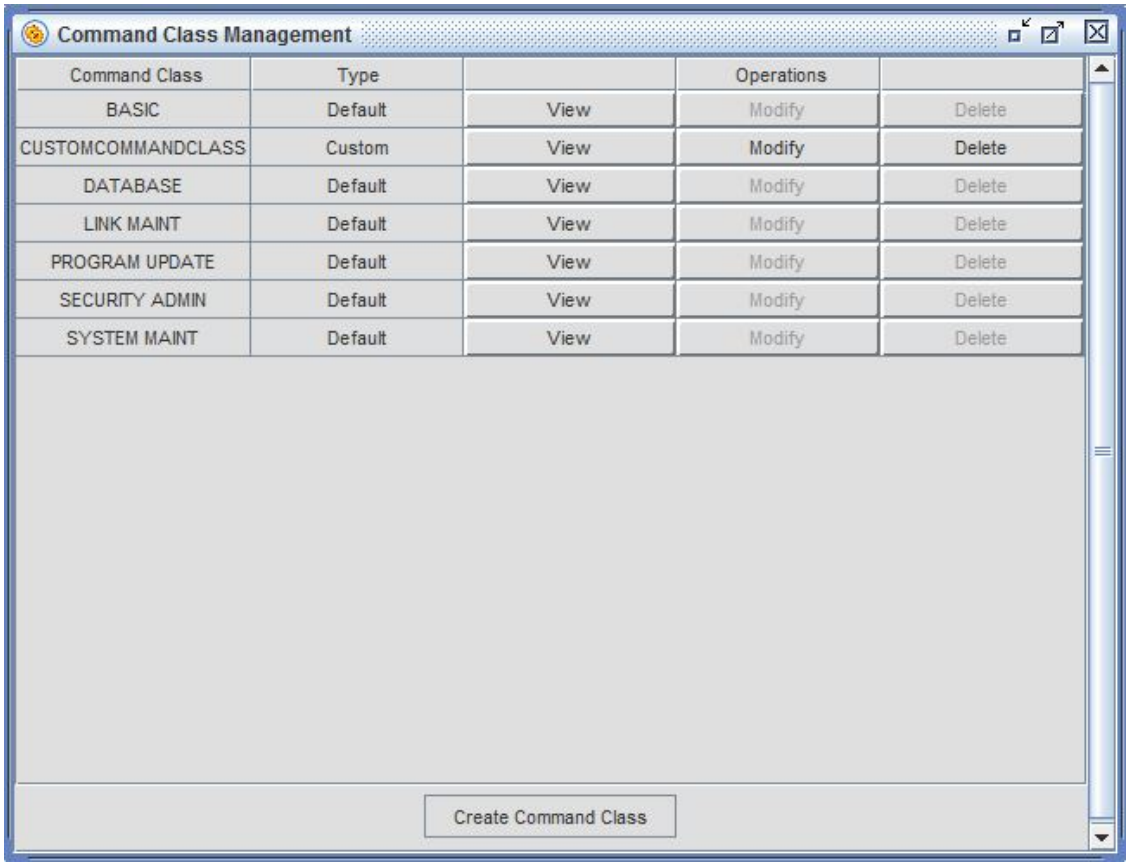
After moving the desired commands to the Selected Commands pane, enter the name for your custom command class (alphanumeric characters only; CustomCommandClass is used for this example) in the **Command Class Name** field and click **Save**. Your custom command class is created and a notification is displayed in the system tray, as shown in Figure 11-29.

Figure 11-29 Command Class Added Successfully



The Command Class Management screen will now include the custom command class, as shown in Figure 11-30.

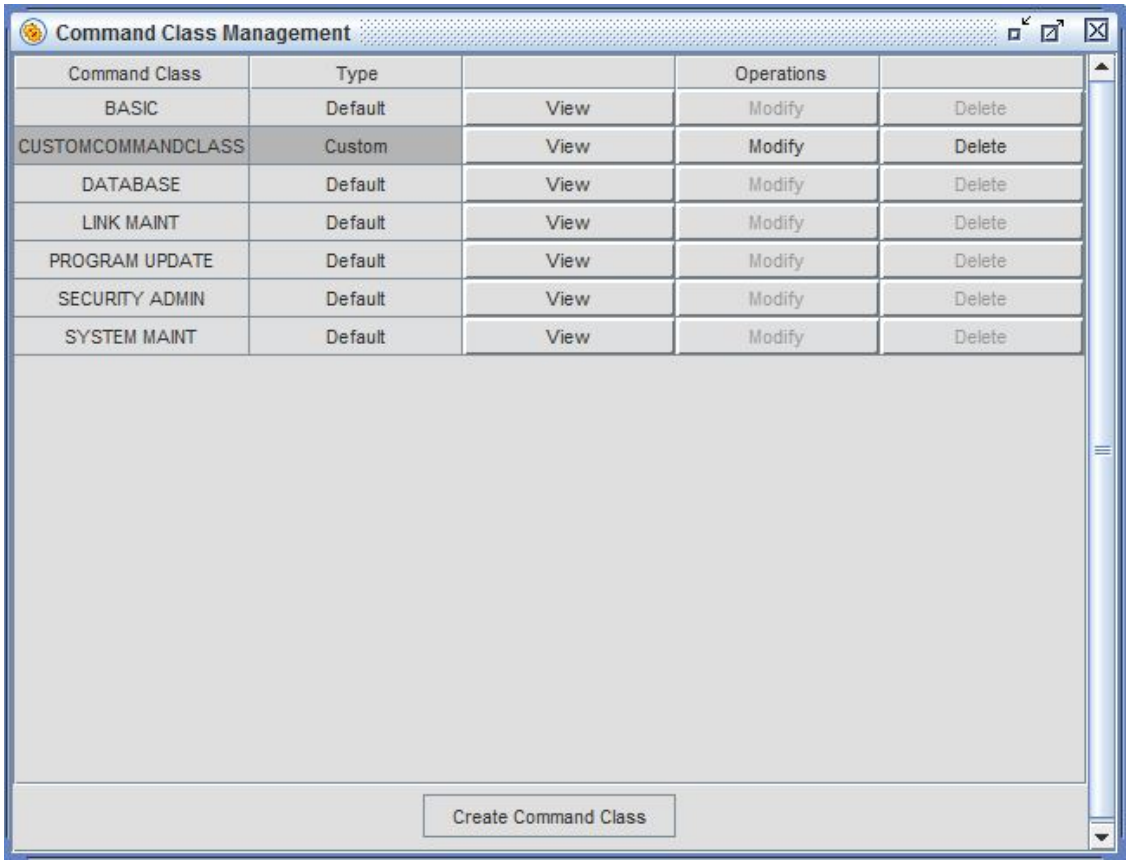
Figure 11-30 Command Class Management Screen with New Command Class



Viewing a Custom Command Class

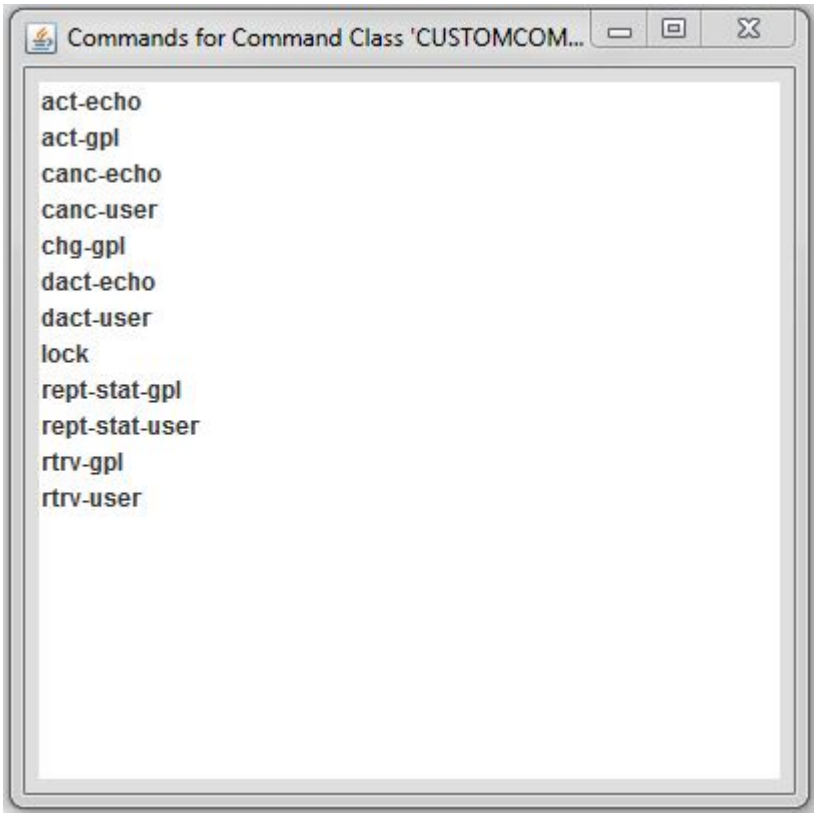
To view a custom command class, first click on it to select it as shown:

Figure 11-31 Viewing a Custom Command Class



Then click **View** to see the commands in the custom command class:

Figure 11-32 View of a Custom Command Class



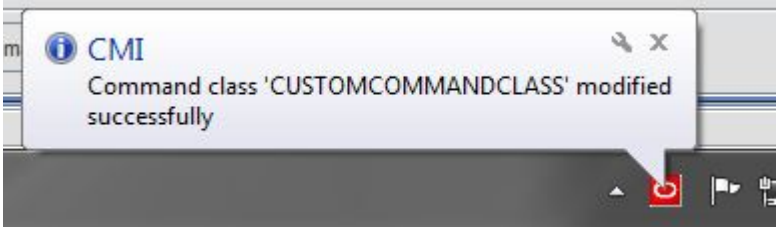
Modifying a Custom Command Class

To modify a custom command class:

1. Select it.
2. Use the arrow keys to add/remove commands, as described in Creating a Custom Command Class.
3. Click **Save**.

The contents of the command class are modified appropriately and a message is displayed in the system tray:

Figure 11-33 Command Class Modified Successfully

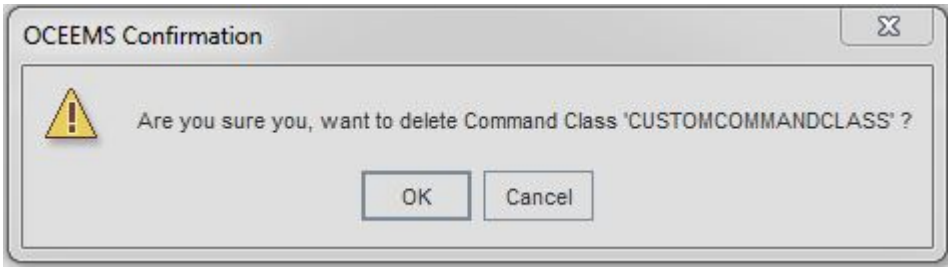


Deleting a Custom Command Class

To delete a custom command class:

1. Select it.
2. Click **Delete**.
3. Click **OK** in the confirmation box:

Figure 11-34 Confirm Command Class Deletion



The command class is removed from the command class list and a message is displayed in the system tray:

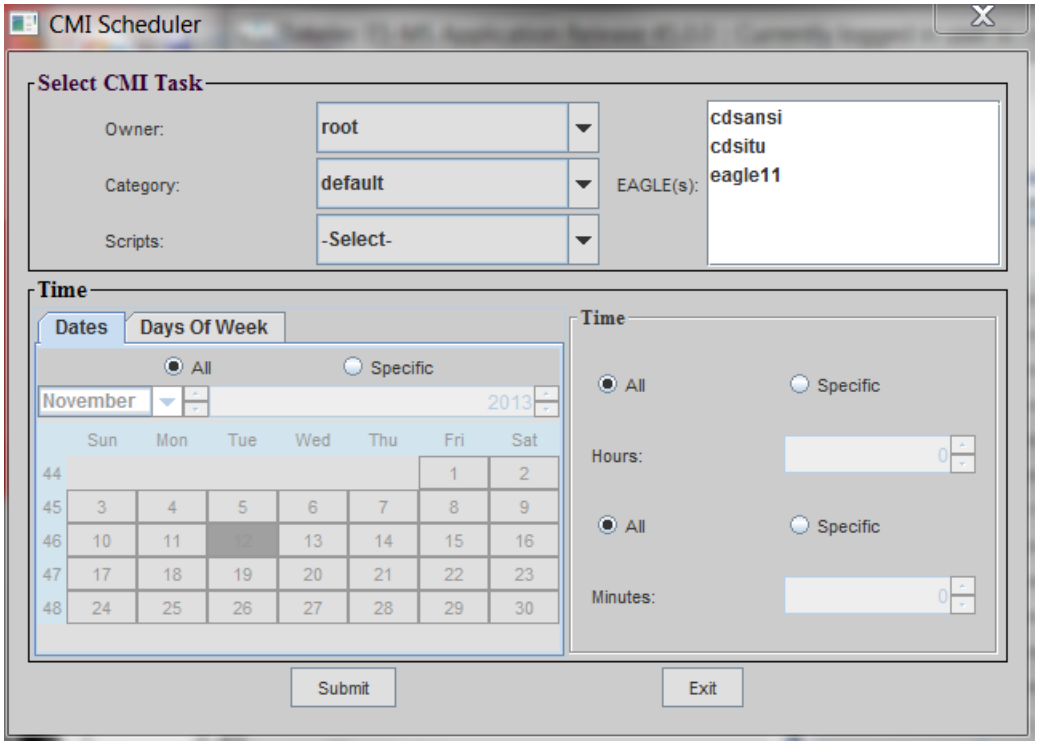
Figure 11-35 Command Class Deleted Successfully

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 users user group is provided the **Schedule CMI Script** operation by the OCEEMS 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 11-36 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 OCEEMS 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.

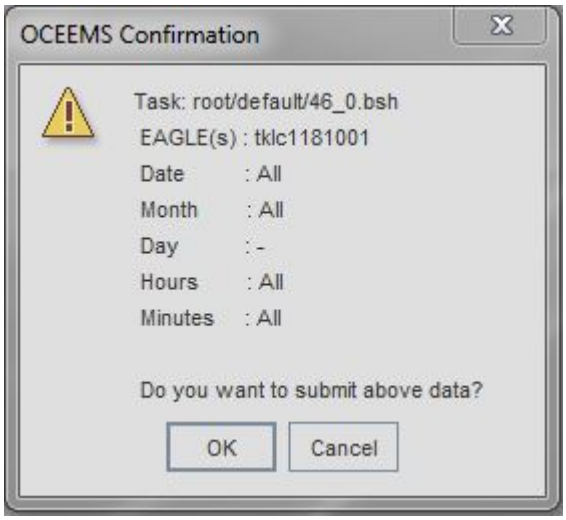
Time pane

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 11-37 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.
> - 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 OCEEMS server unstable.
>   - OCEEMS 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.

Failure during Login to Eagle

During daily schedule task executions, sometimes failure occurs during Eagle login. In such scenario, execute the `updateSchedule.sh` script manually to stagger the system generated scheduled scripts.

Do the following steps to use the `updateSchedule.sh` script to stagger activities for different Eagles:

1. Go to `/Tekelec/WebNMS/bin/` and update the `updateSchedule.sh` script parameter values as follows:

Parameter Name	Description	Values
BASETIME_UPDATE_GRAPHICS	The hour of the day when the `Update Graphic` script is to be executed.	**Default Value**: 0 Scheduled at 00:00 am
BASETIME_LUI_SCRIPT	The hour of the day when the `Lui polling` script is to be executed.	**Default Value**: 1 Scheduled at 01:00 am
BASETIME_INVENTORY_UPGRADE	The hour of the day when the `Update Inventory` script is to be executed.	**Default Value**: 2 Scheduled at 02:00 am
TIME_INTERVAL_UPDATE_GRAPHICS	Time (in minutes) by which `Update Graphic` script will be staggered.	**Default Value**: 2 Staggered by 2 minutes
TIME_INTERVAL_LUI_SCRIPTS	Time (in minutes) by which `Lui polling` script will be staggered.	**Default Value**: 2 Staggered by 2 minutes
TIME_INTERVAL_UPDATE_INVENTORY	Time (in minutes) by which `Update Inventory` script will be staggered.	**Default Value**: 3 Staggered by 3 minutes

   Set the appropriate values for these parameters.

   For example, if the `Update Graphic` script for the first eagle has to be scheduled at 02:00 am and all other needs to be staggered by 3 minutes each, then set BASETIME_UPDATE_GRAPHICS=2 and TIME_INTERVAL_UPDATE_GRAPHICS=3.

   Similarly, if the `Update Inventory` script for the first eagle has to be scheduled at 04:00 pm and all other needs to be staggered by 2 minutes each, then set BASETIME_UPDATE_GRAPHICS=16 and TIME_INTERVAL_UPDATE_GRAPHICS=2.

2. Execute the following script:

```
$ /Tekelec/WebNMS/bin/updateSchedule.sh
```

   > **Note**
   >
   > In case of addition of a new eagle, run this script again to schedule tasks for that eagle can be staggered accordingly.

3. After successful execution of the script, restart the OCEEMS server for the changes to take effect.

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.
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 OCEEMS administrator.
26.		Renaming of category '<category name>' failed! Category does not exist.
27.		Renaming of category '<category name>' failed! Please contact the OCEEMS administrator
28.		Deletion of category '<category name>' failed! Category does not exist.
29.		Deletion of category '<category name>' failed! Please contact the OCEEMS administrator.
30.		Deletion of category '<category name>' failed! One or more scripts with identical names already exist in category 'default'.

S. NO.	CMI Functionality	Error Message
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.
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!

12

Link Utilization Interface

This chapter provides information about the Link Utilization Interface (LUI). This interface is used for configuring capacity information in the OCEEMS 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 OCEEMS database, along with the data collected by the Measurements Module so the OCEEMS 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 the **Link Utilization** operation have access to Link Data, On Demand Polling, Threshold Configuration of LUI module, and the polling script entries on the **Schedule Management** screen. The LUI module automatically detects New EAGLE(s) added to OCEEMS and creates polling scripts for them.

When creating or modifying a usergroup, the admin can assign **Selected EAGLE(s)** and **Selected Command Classes** to the usergroup as follows:

- **Link Utilization** operation is selected, **Configuration** operation is not selected:
  The admin can assign **Selected EAGLE(s)** to the usergroup, and the mandatory command classes for the LUI module (that is, DATABASE and SYSTEM MAINT) will be automatically assigned to the usergroup. The admin will not be able to remove these mandatory command classes.
- **Configuration** operation is selected, **Link Utilization** operation is not selected:
  The admin can assign **Selected EAGLE(s)** and **Selected Command Classes** to the usergroup.
- Both the **Link Utilization** operation and the **Configuration** operation are selected:
  The admin can assign **Selected EAGLE(s)** to the usergroup. The mandatory command classes for the LUI module (that is, DATABASE and SYSTEM MAINT) will be automatically assigned to the usergroup and the admin will not be able to remove these mandatory command classes. The admin will, however, be able to assign/remove other command classes to the usergroup.
- Neither the **Link Utilization** operation or the **Configuration** operation are selected:
  No EAGLE(s) or command classes can be assigned to the usergroup.

Link Utilization GUI

Link Utilization is located in the OCEEMS applications tree node, as seen in Figure 12-10. There are three elements under Link Utilization as shown in Link Utilization Tree Node

Figure 12-1 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.

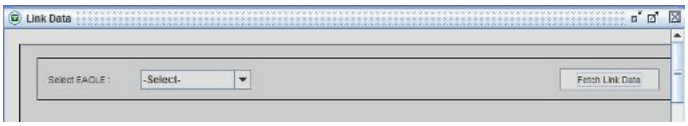
The procedure below will provide a user the steps to view information about each link supported by an EAGLE system.

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

   ```
   Link Data
   ```

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

   Figure 12-2 Link Data Screen

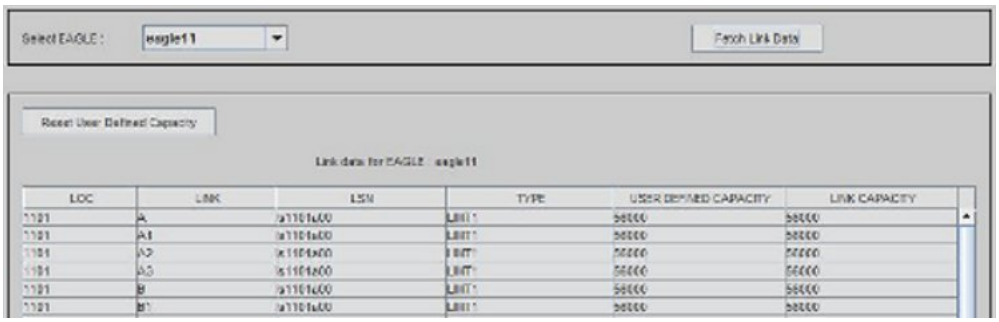
   The Link Data screen provides the following:

   - **Select** EAGLE to view the available link data: This field contains a drop-down list of the EAGLE systems to which the **OCEEMS** 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.

Figure 12-3 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.

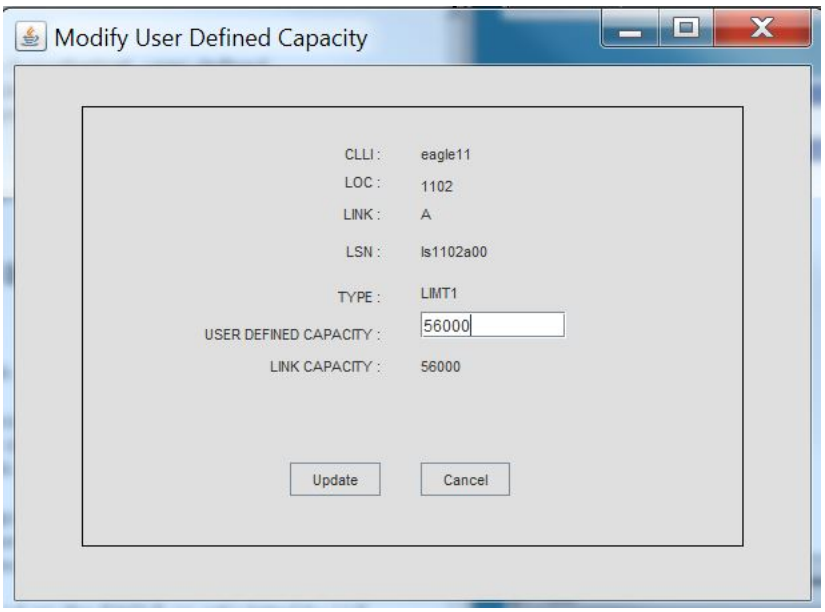
Modifying Link Capacity

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 OCEEMS is connected. This information is stored in the OCEEMS, not in the EAGLE system.

1. `Double click` on a row in table showing link data for an EAGLE. In the following example, you will see the Modify User Defined Capacity screen for the link data of the EAGLE11.

Figure 12-4 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 OCEEMS 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!`

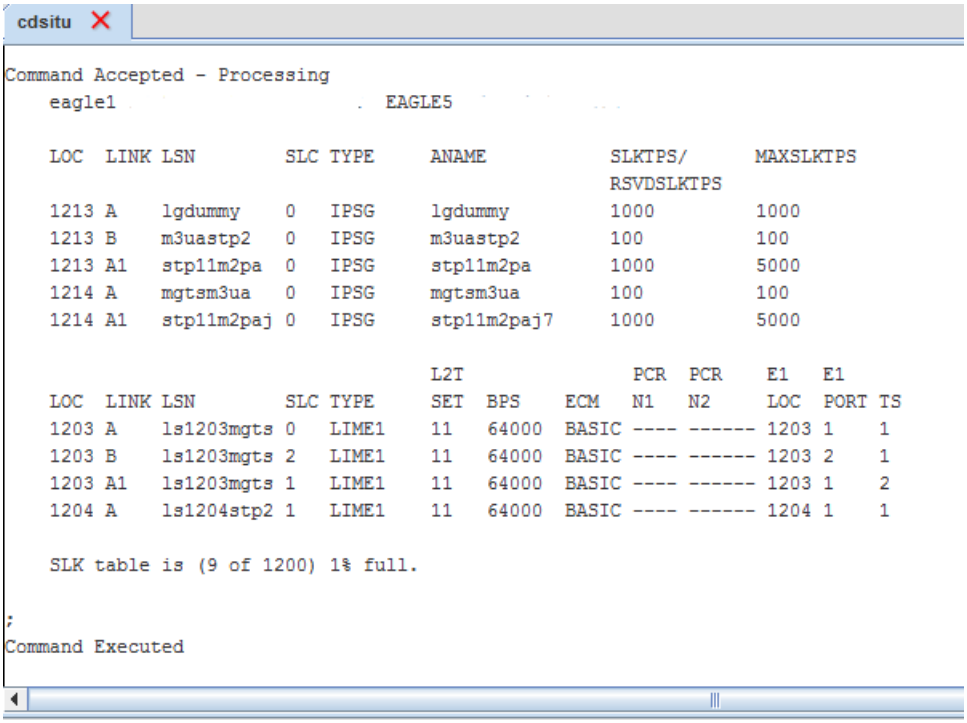
   Reset User Defined Capacity button: clicking the **Reset User Defined Capacity** button causes a confirmation dialog box to be displayed. Once the user clicks the **Ok** button, the link capacity values for BPS value for Non-IP links and SLKTPS value for IP links are populated under the **USER DEFINED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

Polling Scripts Creation

Every polling script shall consist of two EAGLE commands that run 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 RTRV-SLK Command Output.

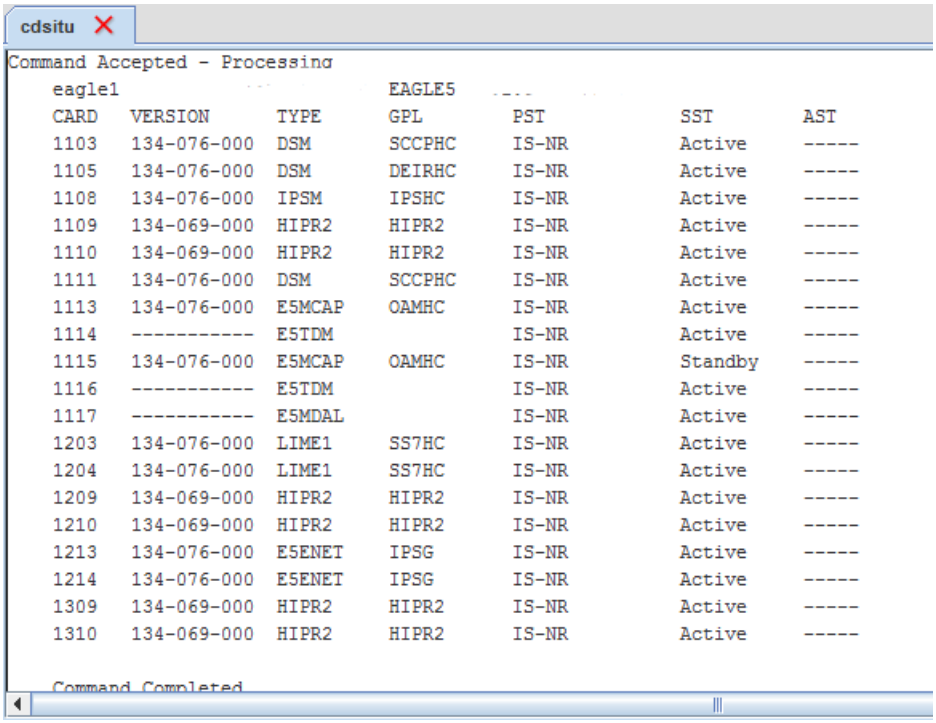
Figure 12-5 RTRV-SLK Command Output



- **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 OCEEMS. As shown in REPT-STAT-CARD Command Output

Figure 12-6 REPT-STAT-CARD 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.
```

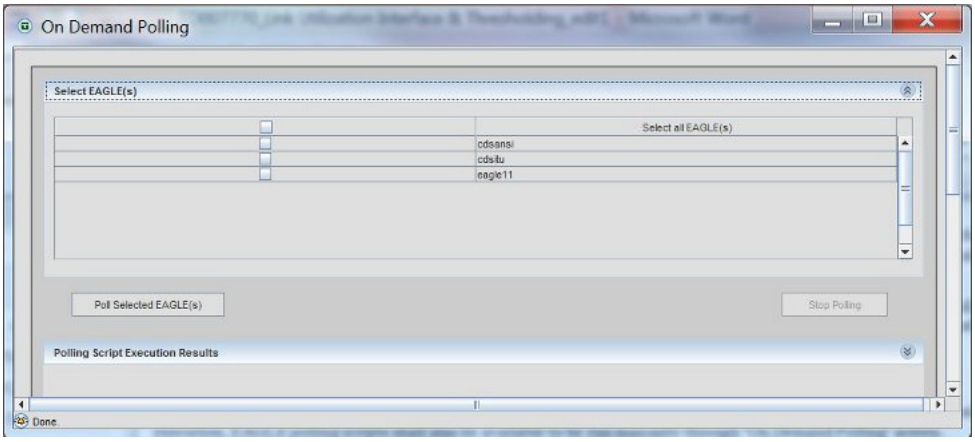
will be displayed on GUI.

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

1. Select **On Demand Polling** under the **Link Utilization** tree node in the main menu on the left side of the OCEEMS GUI page link as shown in On Demand Polling

   ```
   On Demand Polling
   ```

Figure 12-7 On Demand Polling



2. Click the check boxes from the **Select all EAGLE(s)** list which on-demand polling is being performed.

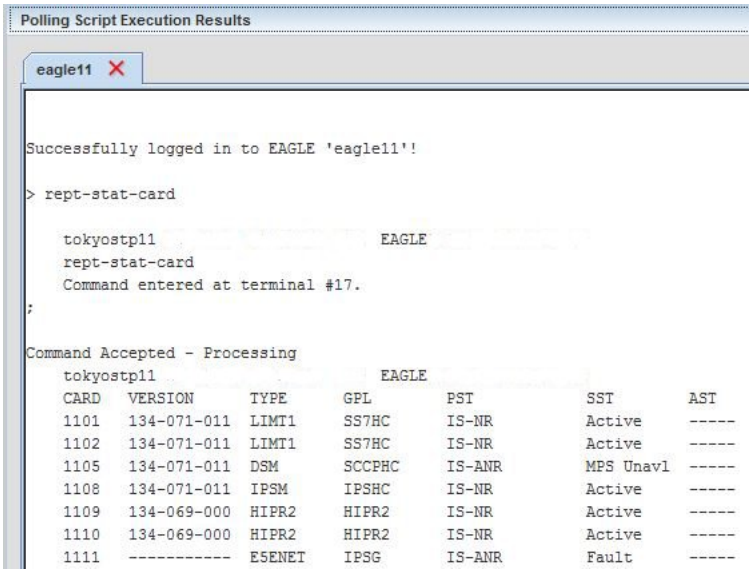
   A single, multiple, or all connected EAGLE systems may be selected.

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 12-8

Figure 12-8 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 OCEEMS.

Thresholding Configuration

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

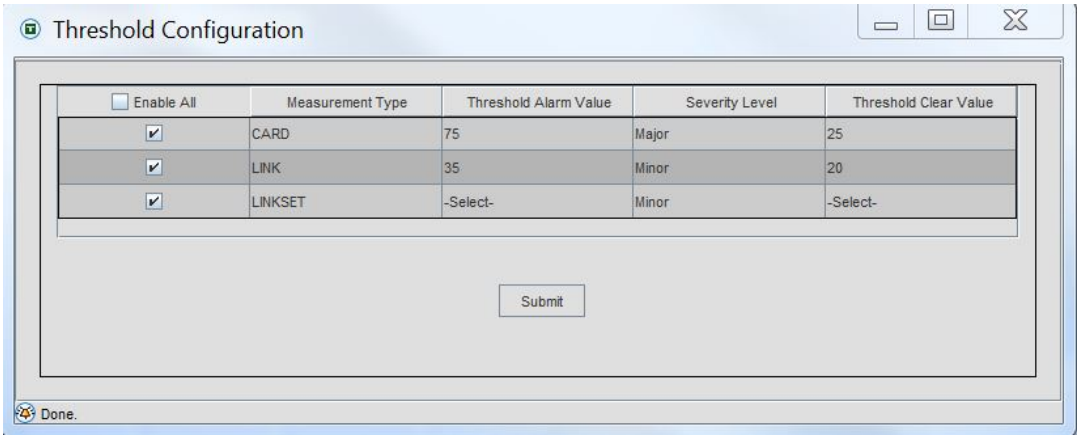
This procedure is used to sort the Threshold Alarm messages, Threshold Clear messages and Threshold Informational messages from the OCEEMS.

1. Select **Thresholding Configuration** under the **Link Utilization** tree node in the main menu on the left side of the OCEEMS GUI page link.

   `Thresholding Configuration`

   A screen will appear, as shown in Thresholding Configuration Screen.

Figure 12-9 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!`

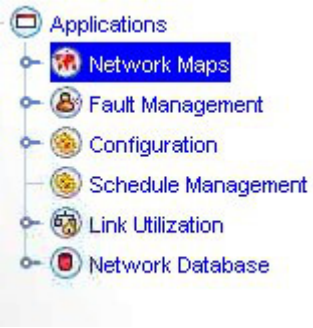
- The **Severity Level** drop down for a measurement type contains **Select**. Error message

  `The severity level for measurement type '<measurement type>' not selected!`

Schedule Management

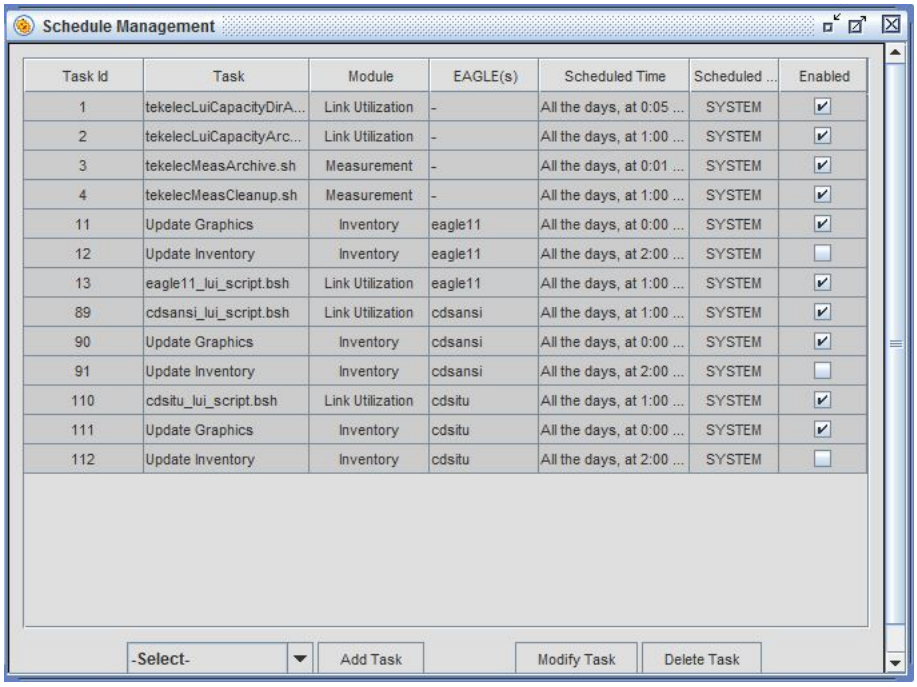
Schedule Management screen located in the tree node on the left side of the OCEEMS GUI, as shown in Figure 12-10, provides the same polling script and is scheduled to update graphics at 00:00 and update inventory at 2:00 am.

Figure 12-10 Schedule Management GUI



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.

Figure 12-11 Schedule Management



LUI Measurements Error and Informational Messages

The following error and informational messages are associated with the LUI Measurements feature.

Table 12-1 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!`

Table 12-1 (Cont.) LUI Measurements Error and Informational Messages

Scenario	Error or Information Message
In case **OCEEMS** 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 **OCEEMS** 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.`

13

Northbound Interface (NBI)

This chapter provides information about the **OCEEMS Northbound Interface**, which is a feature of the OCEEMS product that forwards alarms from EAGLE, EPAP, LSMS, and the OCEEMS to one or more client Network Management Systems.

Overview

The Northbound Interface (NBI) application is an optional feature of the OCEEMS that processes alarms received by the OCEEMS. The feature forwards events to Network Management Systems (NMS) in the form of SNMP traps.

OCEEMS supports the SNMP v3 security model for trap forwarding, as well as SNMP v2c. Alarms forwarded through the SNMP interfaces include:

- Alarms collected on the Southbound interfaces (EAGLE, EPAP, and LSMS alarms)
- OCEEMS alarms
- Alarms generated by features such as EAGLE EMS Measurements Based Threshold Alarms Tier 1.

The NBI is able to support trap forwarding to NMS(s) at a rate of 112 alarms per second. The rate has been derived for 14 mated pairs of EAGLEs (that is, 28 EAGLEs), with each sending alarms to OCEEMS at a rate of 4 alarms per second.

OCEEMS provides re-synchronization support in case an NMS becomes out of sync with OCEEMS.

OCEEMS includes an SFTP Northbound Interface to allow the "export" of the measurement reports collected from the different elements managed.

OCEEMS includes a MIB browser application that can be used as a proxy for an NMS to verify SNMP v3 features like trap forwarding and resynchronization. For information, see Using the OCEEMS MIB Browser as an NMS Proxy.

For more information about alarm processing for EAGLE, EPAP, and LSMS, including configuration examples, see:

- EAGLE Discovery Application
- OCEEMS Support of EPAP Alarms via SNMP Feed
- OCEEMS Support of LSMS Alarms via SNMP Feed

Further information about the configuration required on the EAGLE, EPAP, and LSMS to enable trap forwarding from OCEEMS can also be found in the documentation for each product:

- *E5-OAM SNMP Configuration* in *EAGLE Database Administration - Features User's Guide*
- *Configure EMS Server* and *Configure Alarm Feed* in *EPAP Administration Guide*
- *Configuring an SNMP Agent* in *LSMS Alarms and Maintenance Guide*

Implementing SNMP v3

After a fresh OCEEMS installation, OCEEMS supports only SNMP v3 by default. SNMP v3 trap forwarding is recommended because of the encryption and secured authentication mechanisms provided.

When upgrading OCEEMS from a release where SNMP v2c was enabled, both SNMP v2c and v3 modes are enabled by default so that SNMP v2c trap forwarding to existing NMS(s) will continue working after the upgrade. When ready, the **SNMP Agent Mode** setting on the NBI Agent Configuration screen can be changed to include only SNMP v3 mode. For more information about the **SNMP Agent Mode** setting, see SNMP Global Mode.

To configure SNMP v3 trap forwarding, follow these general steps:

1. Create SNMP v3 views.
   See SNMP v3 View Management.
2. Create one or more SNMP v3 groups that use the SNMP v3 views.
   See SNMP v3 Group Management.
3. Create SNMP v3 users associated with the SNMP v3 groups.
   See NBI Agent Configuration.
4. Configure the NBI agent for SNMP v3, with the SNMP v3 users that can be used for SNMP v3 communication between OCEEMS and the NMS(s).
   See NBI Agent Configuration.
5. Configure an NMS on OCEEMS, associating it to any one of the existing SNMP v3 users configured in step 4.
   See NMS Configuration.
6. On the NMS, discover the SNMP v3 user that was associated with the NMS in step 5.
   - For trap forwarding from OCEEMS to NMS:
     Discover the v3 user on the OCEEMS port provided in the `V3_USER_DISCOVERY_PORT_FOR_TRAPS` parameter in the `/Tekelec/WebNMS/conf/tekelec/server_conf.properties` file. This port must be opened bidirectionally on the OCEEMS firewall. The default value of the port is 1234, which is configurable (OCEEMS must be restarted if changed).
   - For alarm resynchronization:
     Discover the v3 user on port 8002.

   After successful discovery of the SNMP v3 user on the NMS, SNMP v3 trap forwarding will begin and the NMS can initiate alarm resynchronization with OCEEMS.

SNMP Global Mode

OCEEMS supports three SNMP global modes on the Northbound Interface. The SNMP global mode is controlled with the **SNMP Agent Mode** setting available on the NBI Agent Configuration screen. This screen is fully described in NBI Agent Configuration. A user having access to this screen can set/update the **SNMP Agent Mode** setting so that OCEEMS supports SNMP v3 only, SNMP v2c only, or both SNMP v3 and SNMP v2c.

By default, OCEEMS supports only SNMP v3 after a fresh OCEEMS installation. SNMP v3 trap forwarding is recommended because of the encryption and secured authentication mechanisms provided. Both SNMP v2c and SNMP v3 are supported after an upgrade from an OCEEMS release with SNMP v2c configured, so that SNMP v2c trap forwarding to existing

NMS(s) will continue working after the upgrade. When ready, the **SNMP Agent Mode** setting can be changed to include only SNMP v3 mode.

- **SNMP v2c**
  Selecting only the checkbox for this mode results in OCEEMS supporting only SNMP v2c on the Northbound Interface as follows:
  - OCEEMS will forward traps to only NMS(s) configured to support SNMP v2c.
  - OCEEMS will not forward traps to NMS(s) configured to support SNMP v3.
  - OCEEMS will allow addition of any new NMS that supports SNMP v2c, and will not allow addition of any new NMS that supports SNMP v3. Attempting to add an NMS that supports SNMP v3 or to modify an existing SNMP v2c-based NMS to SNMP v3 will result in the following error message:

    ```
    SNMP v3 based NMS cannot be added because SNMP v3 mode is not enabled!
    Try again after enabling SNMP v3 mode.
    ```

- **SNMP v3**
  Selecting only the checkbox for this mode results in OCEEMS supporting only SNMP v3 on the Northbound Interface as follows:
  - OCEEMS will forward traps to only NMS(s) configured to support SNMP v3.
  - OCEEMS will not forward traps to NMS(s) configured to support SNMP v2c.
  - OCEEMS will allow addition of any new NMS that supports SNMP v3, and will not allow addition of any new NMS that supports SNMP v2c. Attempting to add an NMS that supports SNMP v2c or to modify an existing SNMP v3-based NMS to SNMP v2c will result in the following error message:

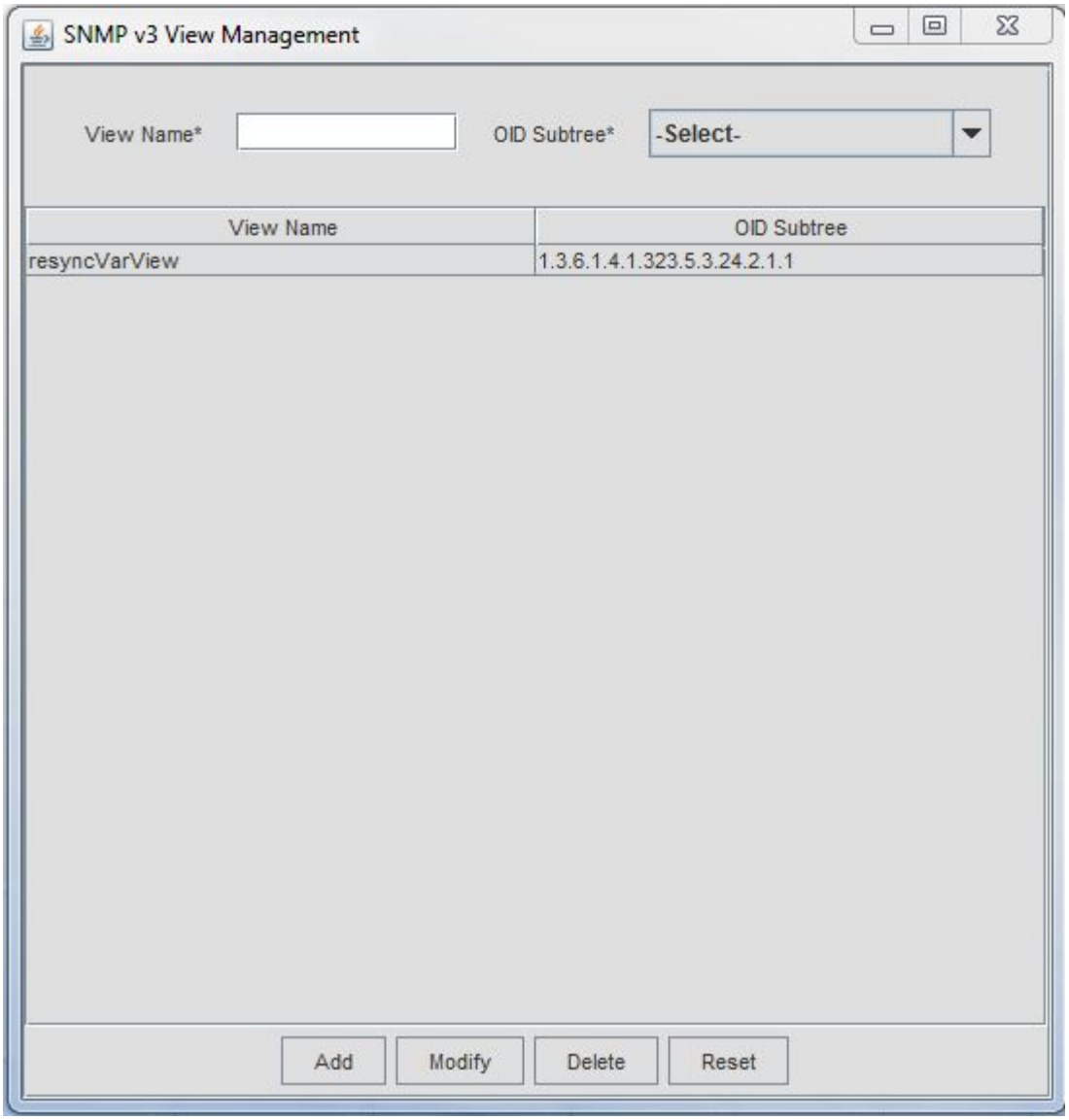
    ```
    SNMP v2c based NMS cannot be added because SNMP v2c mode is not enabled!
    Try again after enabling SNMP v2c mode.
    ```

- Both **SNMP v2c** and **SNMP v3**
  Selecting the checkbox for both **SNMP v2c** and **SNMP v3** results in OCEEMS supporting both SNMP v2c and SNMP v3 on the Northbound Interface as follows:
  - OCEEMS will forward traps to all NMS(s) configured to support SNMP v2c or SNMP v3.
  - OCEEMS will allow addition of any new NMS that supports SNMP v2c or SNMP v3.

SNMP v3 View Management

OCEEMS provides the SNMP v3 View Management screen (**Tools**, and then **SNMP v3 View Management**) for the addition, modification, and deletion of SNMP v3 views.

Figure 13-1 Sample SNMP v3 View Management Screen



Access to the **Tools**, and then **SNMP v3 View Management** menu item is provided to those OCEEMS users authorized for the **NBI Agent Configuration** operation. The menu item is not visible to unauthorized users.

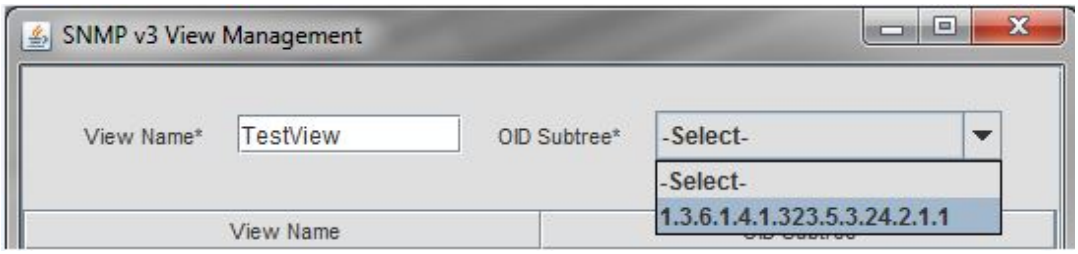
The **resyncVar** object with OID 1.3.6.1.4.1.323.5.3.24.2.1.1 is the only object available in the OCEEMS NBI MIB for read/write operations by a NMS. By default, OCEEMS provides a view named **resyncVarView** that is sufficient for controlling read/write access to the **resyncVar** object. The **resyncVarView** cannot be modified or deleted.

OCEEMS also provides the ability to create views with other desired names. View names must be unique (the check is case insensitive) and are 1 - 65 characters in length.

The following operations are available on the SNMP v3 View Management screen:

- **Add**
  To create a new view, provide a valid **View Name** and select **OID Subtree** 1.3.6.1.4.1.323.5.3.24.2.1.1, to which the view will have access:

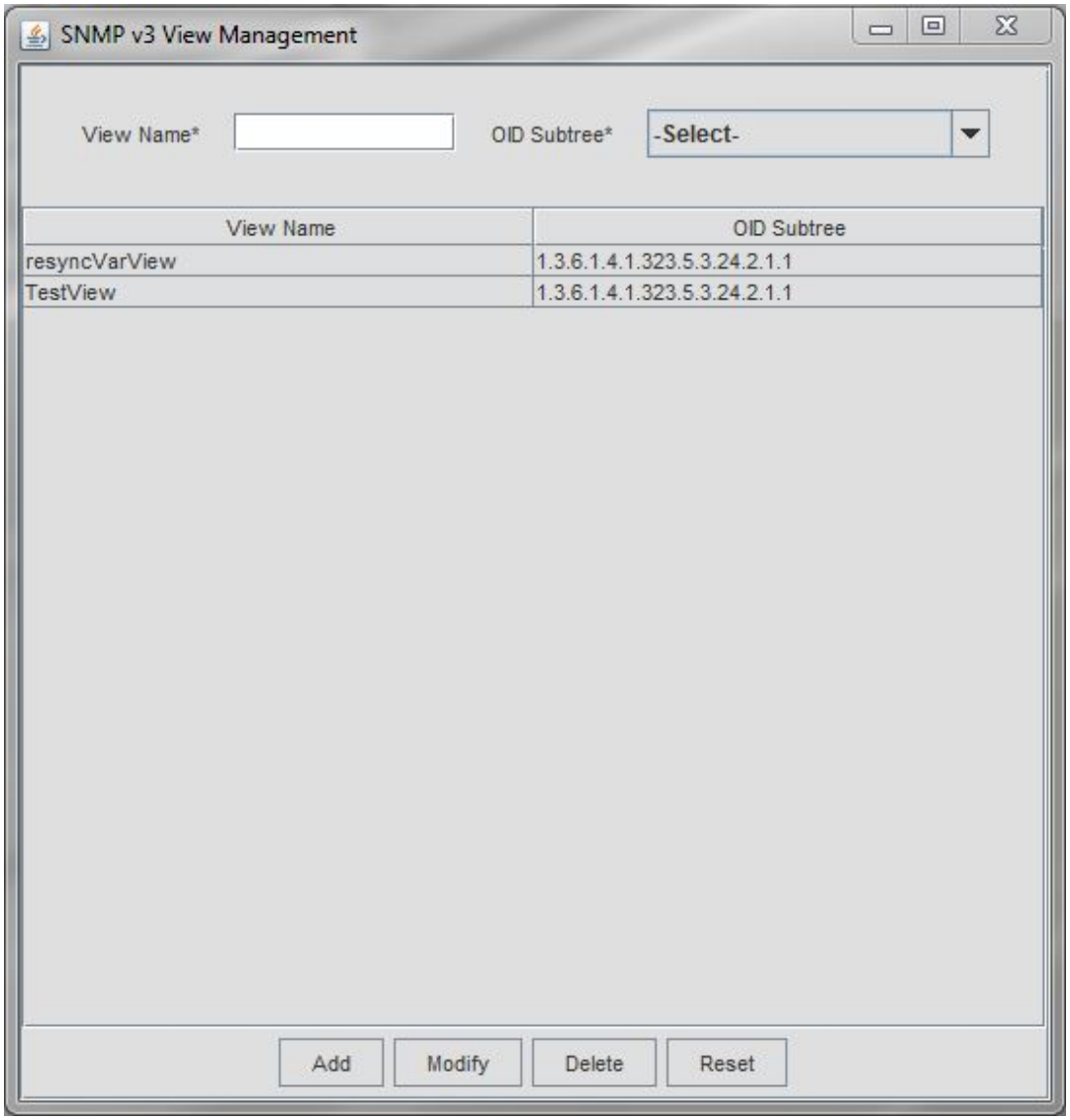
Figure 13-2 SNMP v3 View Management Screen - Adding a View



After adding the **View Name** and selecting the **OID Subtree**, click **Add** to create the new SNMP v3 view. A notification is provided in the system tray and the new view is added to the view list on the SNMP v3 View Management screen.

Figure 13-3 View Added Successfully Notification

Figure 13-4 SNMP v3 View Management Screen with Updated View List



- **Modify**
  To modify a view, select the view in the view list, which will populate the view details in the **View Name** and **OID Subtree** fields.

  Modify the **View Name** field appropriately, and click **Modify** to modify the view in the OCEEMS database and the view list on the screen.

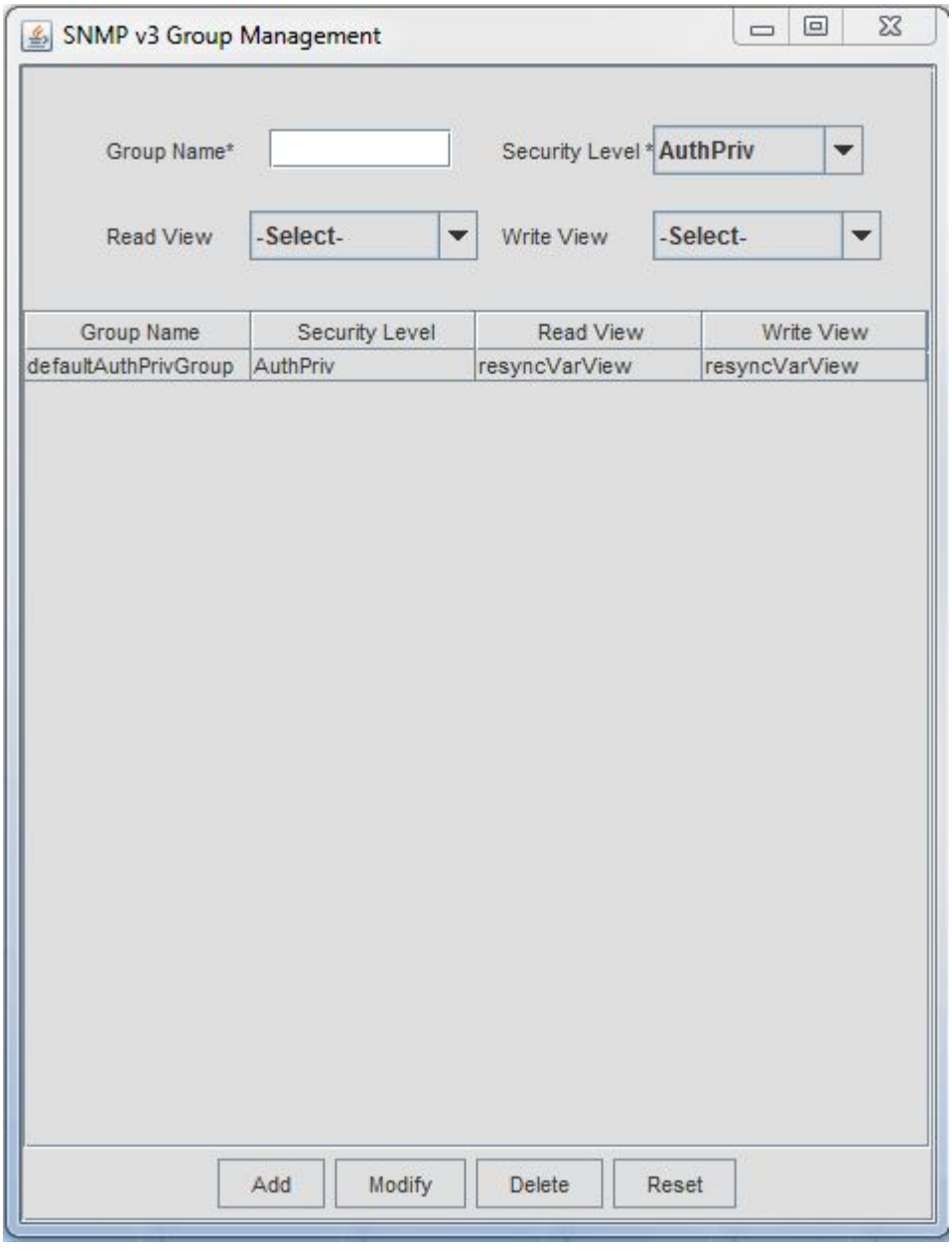
- **Delete**
  An existing SNMP v3 view can be deleted if it is not associated to any SNMP v3 group. Select the view from the view list and click **Delete**, followed by **Ok** in the confirmation box. Provided that the view is not associated with one or more SNMP v3 groups, the view will be deleted and removed from the view list.

- **Reset**
  Click **Reset** to reset the **View Name** and **OID Subtree** fields to their initial state (no value for **View Name** and **-Select-** for **OID Subtree**).

SNMP v3 Group Management

OCEEMS provides the SNMP v3 Group Management screen (**Tools**, and then **SNMP v3 Group Management**) for the addition, modification, and deletion of SNMP v3 groups.

Figure 13-5 Sample SNMP v3 Group Management Screen



Access to the **Tools**, and then **SNMP v3 Group Management** menu item is provided to those OCEEMS users authorized for the **NBI Agent Configuration** operation. The menu item is not visible to unauthorized users.

By default, an SNMP v3 group having security level **AuthPriv** is available for use on this screen. The default group can be modified or deleted if required.

Group names must be unique (the check is case insensitive) and are 1 - 35 characters in length.

The following operations are available on the SNMP v3 Group Management screen:

- **Add**
  To create a new SNMP v3 group, provide the following input:
  - Provide a **Group Name** and select the **Security Level** for the group. Security levels are shown in Table 13-1.

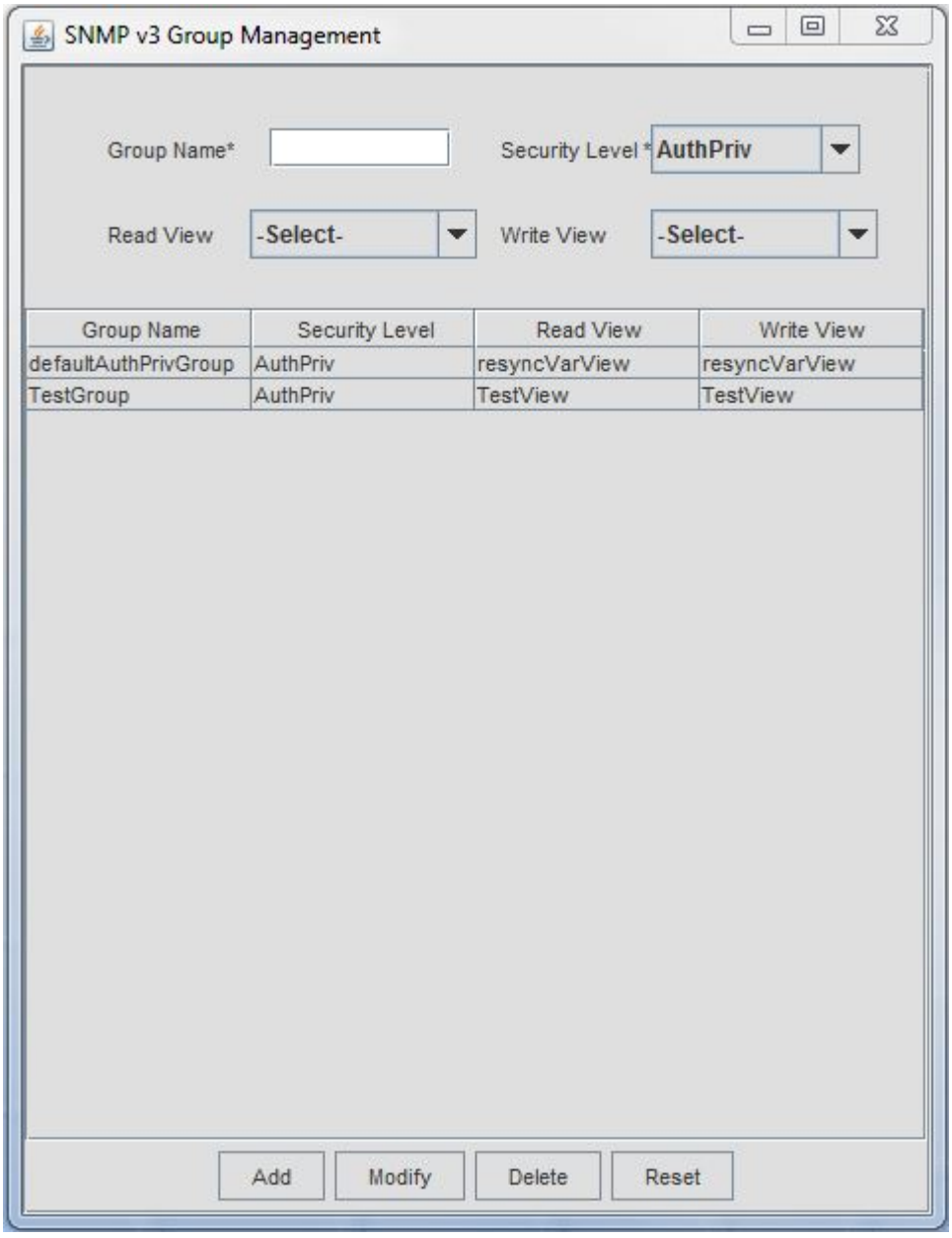
Table 13-1 SNMP v3 Security Levels

Level	Authentication	Encryption	Details
AuthPriv (Authentication and privacy)	Yes (SHA)	Yes (DES/AES)	Provides authentication and encryption based on the algorithms available in the Zoho WebNMS framework API
AuthNoPriv (Authentication, no privacy)	Yes (SHA)	No	Provides authentication based on the algorithms available in the Zoho WebNMS framework API
NoAuthNoPriv (No authentication, no privacy)	Username	No	Uses a username match for authentication

  - Optionally, associate a **Read View** and **Write View** to the group.
    - The **Read View** and **Write View** drop-down menus will include the views created on the SNMP v3 View Management screen.
    - If a **Read View** is not selected for a group, the group will have default read access to all OCEEMS NBI MIB objects.
    - If a **Write View** is not selected for a group, the group will not have write access to any of the OCEEMS NBI MIB objects.

  Click **Add** to add the new group to the OCEEMS database. The new group will also be added to the list on the SNMP v3 Group Management screen.

Figure 13-6 SNMP v3 Group Management Screen with Group List



- **Modify**
  To modify a group, select the group from the list on the screen, which populates the **Group Name**, **Security Level**, **Read View**, and **Write View** fields at the top of the screen with the values associated with the selected group.

  Modify the values as appropriate and click **Modify**, which modifies the group in the OCEEMS database as well as in the group list on the screen.

- **Delete**
  An existing SNMP v3 group can be deleted if it is not associated with any SNMP v3 users. Select the group from the groups list and click **Delete**, followed by **Ok** in the confirmation box. Provided that the group is not associated with one or more SNMP v3 users, the group will be deleted and removed from the group list.

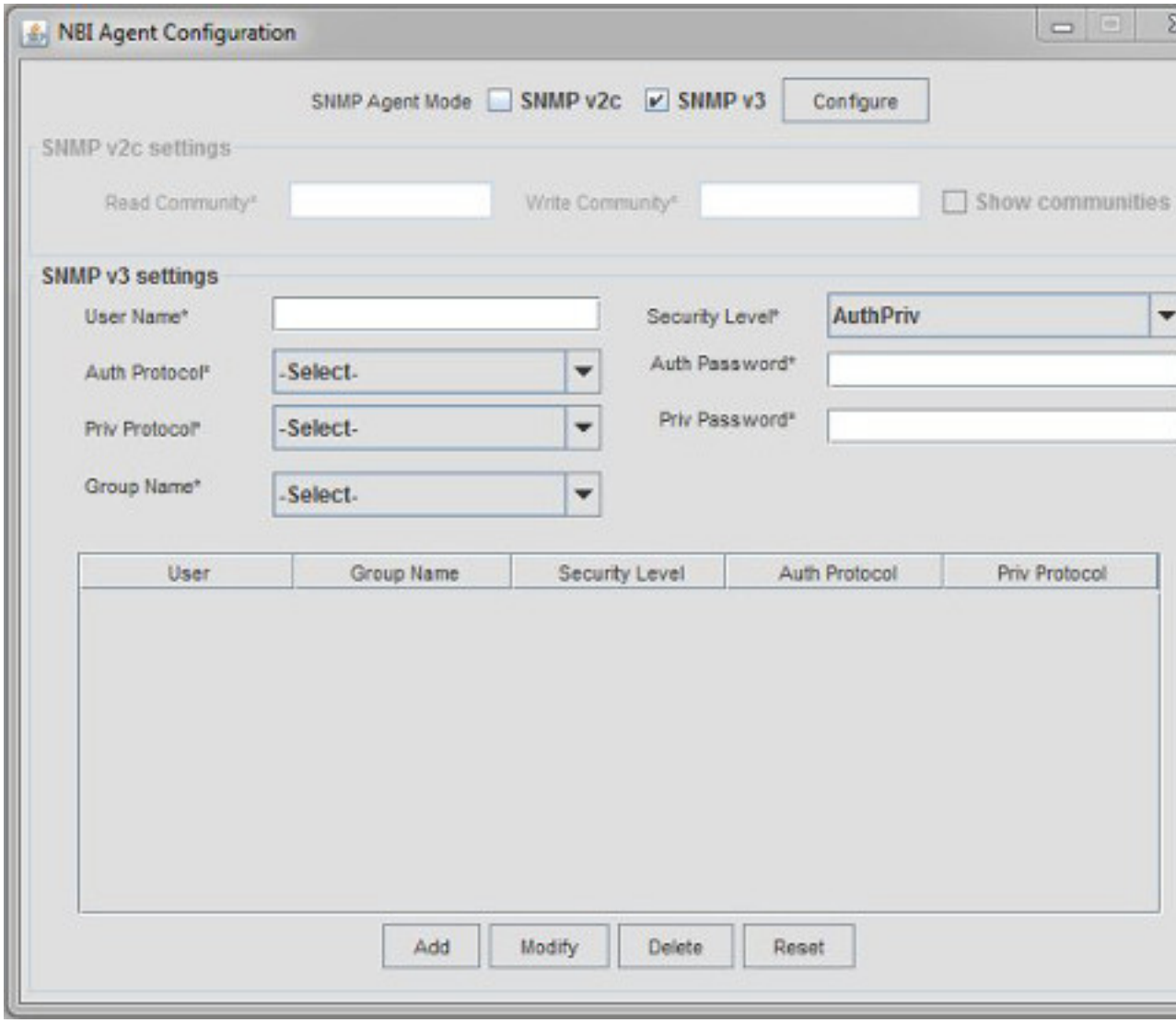
- **Reset**
  Click **Reset** to reset all fields to their initial state:

- No value in the **Group Name** field
- **AuthPriv** in the **Security Level** field
- **-Select-** in the **Read View** and **Write View** fields

NBI Agent Configuration

OCEEMS provides the NBI Agent Configuration screen (**Tools**, and then **NBI Agent Configuration**) for SNMP v2c and v3 agent configuration and SNMP v3 user management.

Figure 13-7 Sample NBI Agent Configuration Screen



Access to the **Tools**, and then **NBI Agent Configuration** menu option is available to those OCEEMS users authorized for the NBI Agent Configuration operation. The menu item is not visible to unauthorized users.

The NBI Agent Configuration screen includes the following three sections:

- **SNMP Agent Mode**
  The SNMP agent global mode can be selected by using the **SNMP Agent Mode** check boxes at the top of the NBI Agent Configuration screen. Either or both boxes can be checked. **SNMP v3** is recommended because of the encryption and secured authentication mechanisms provided.

  When a checkbox is selected, the corresponding **SNMP v2c settings** and **SNMP v3 settings** configuration sections become editable. After completing the appropriate configuration sections, you will click **Configure** to enable the selected mode(s) on OCEEMS.

  > **Note**
  >
  > A currently enabled SNMP mode can be disabled by un-checking its check box and clicking **Configure**. The mode's settings will still be available in the OCEEMS database (and on the screen) for future use.

  For more information about setting the **SNMP Agent Mode**, see SNMP Global Mode.

- **SNMP v2c settings**
  When the **SNMP v2c** checkbox is selected, the **Read Community** and **Write Community** fields must be specified. Empty community strings, or the use of the strings **public** and **private** (case insensitive) in the **Read Community** and **Write Community** fields, are not allowed.

  Use the **Show communities** checkbox to see the values entered.

  In an upgrade scenario, the community string fields are populated with the existing strings, which can be modified as needed prior to clicking **Configure**.

- **SNMP v3 settings**
  The **SNMP v3 settings** section is used to **Add**, **Modify**, or **Delete** SNMP v3 users. These operations and the **Reset** operation are described in the following subsections.

  If the **SNMP v3** mode is selected, at least one v3 user must exist.

  There can be any number of SNMP v3 users, with various security levels, and all existing users are listed in the **SNMP v3 settings** section. Clicking **Configure** will configure the OCEEMS SNMP agent to support v3 with all existing v3 users.

SNMP v3 Settings - Add

The **Add** operation is used to add a new SNMP v3 user to be used in SNMP v3 communication between OCEEMS and the NMS(s).

1. Specify the **User Name** to be added and select the **Security Level**.
   The **User Name** must be unique (the check is case insensitive) and 1 - 50 characters in length. The **Security Level** is one of the following:
   - **AuthPriv**
   - **AuthNoPriv**
   - **NoAuthNoPriv**

   For a description of the security levels, see SNMP v3 Group Management.
2. Select the **Group Name**.
   Selecting the **Security Level** automatically populates the **Group Name** drop-down menu with all the groups belonging to that security level.

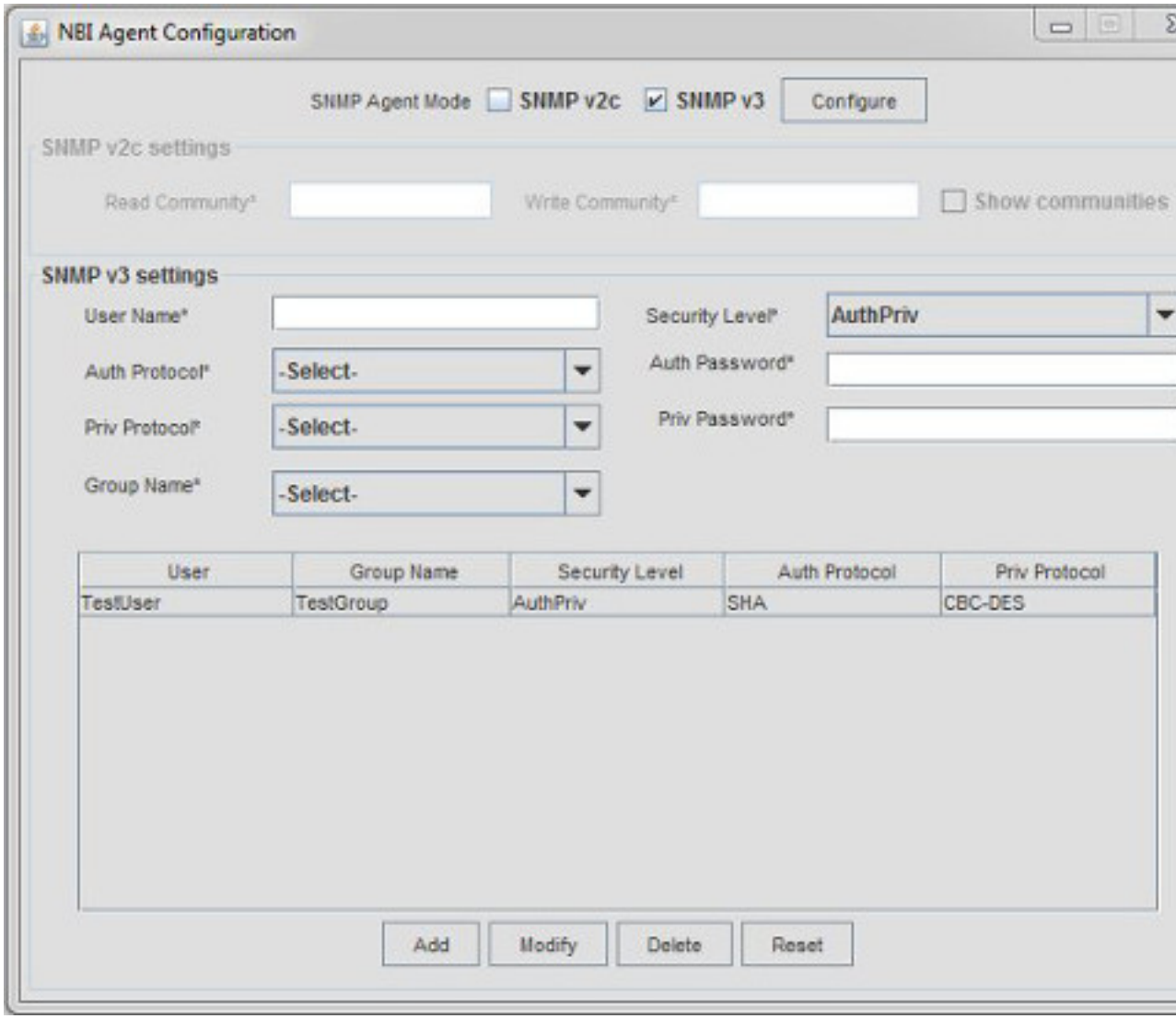
3. Select or specify the **Priv Protocol**, **Priv Password**, **Auth Protocol**, and **Auth Password** fields as required:
   - If the **Security Level** is **AuthPriv**, select the desired values for the **Auth Protocol** and **Priv Protocol** fields, and provide valid passwords in the **Auth Password** and **Priv Password** fields.
   - If the **Security Level** is **AuthNoPriv**, select the desired value for the **Auth Protocol** field and provide a valid password in the **Auth Password** field. The **Priv Protocol** and **Priv Password** fields are not required and are disabled for input.
   - If the **Security Level** is **NoAuthNoPriv**, the **Priv Protocol**, **Priv Password**, **Auth Protocol**, and **Auth Password** fields are not required and are disabled for input.

   The **Auth Protocol** and **Priv Protocol** drop-down menus are pre-populated with the following values:
   - **Auth Protocol** - **SHA**
   - **Priv Protocol** - **CBC-DES** or **CFB-AES-128**

   The **Auth Password** and **Priv Password** fields must be 8 - 255 characters in length. Valid characters include alphanumeric characters and the following special characters:

   @
   #
   $
   !
4. Click **Add** to add the new user to the OCEEMS database and to the list on the screen.

Figure 13-8 NBI Agent Configuration Screen with User List



SNMP v3 Settings - Modify

The **Modify** operation is used to modify an existing SNMP v3 user.

1. Select the user in the user list on the screen.
   Selecting the user populates the appropriate fields with the details for that user.
2. Modify the details as needed.
3. Click **Modify** to modify the user in the OCEEMS database and in the user list.

SNMP v3 Settings - Delete

The **Delete** operation is used to delete an existing SNMP v3 user, provided that the user is not associated with any SNMP v3 NMS.

1. Select the user in the user list.
2. Click **Delete**, and then **Ok** on the confirmation box.

Provided that the user is not associated with any SNMP v3 NMS, the user is deleted from the OCEEMS database and from the user list.

SNMP v3 Settings - Reset

Clicking **Reset** will reset the fields in the **SNMP v3 settings** section to their initial states:

- **User Name**, **Auth Password**, and **Priv Password** will contain no value.
- **Security Level** will contain **AuthPriv**.
- **Auth Protocol** will contain **SHA**.
- **Priv Protocol** will contain **CBC-DES**.
- **Group Name** will contain the first group (in alphabetical order) of all groups with the **AuthPriv** security level.

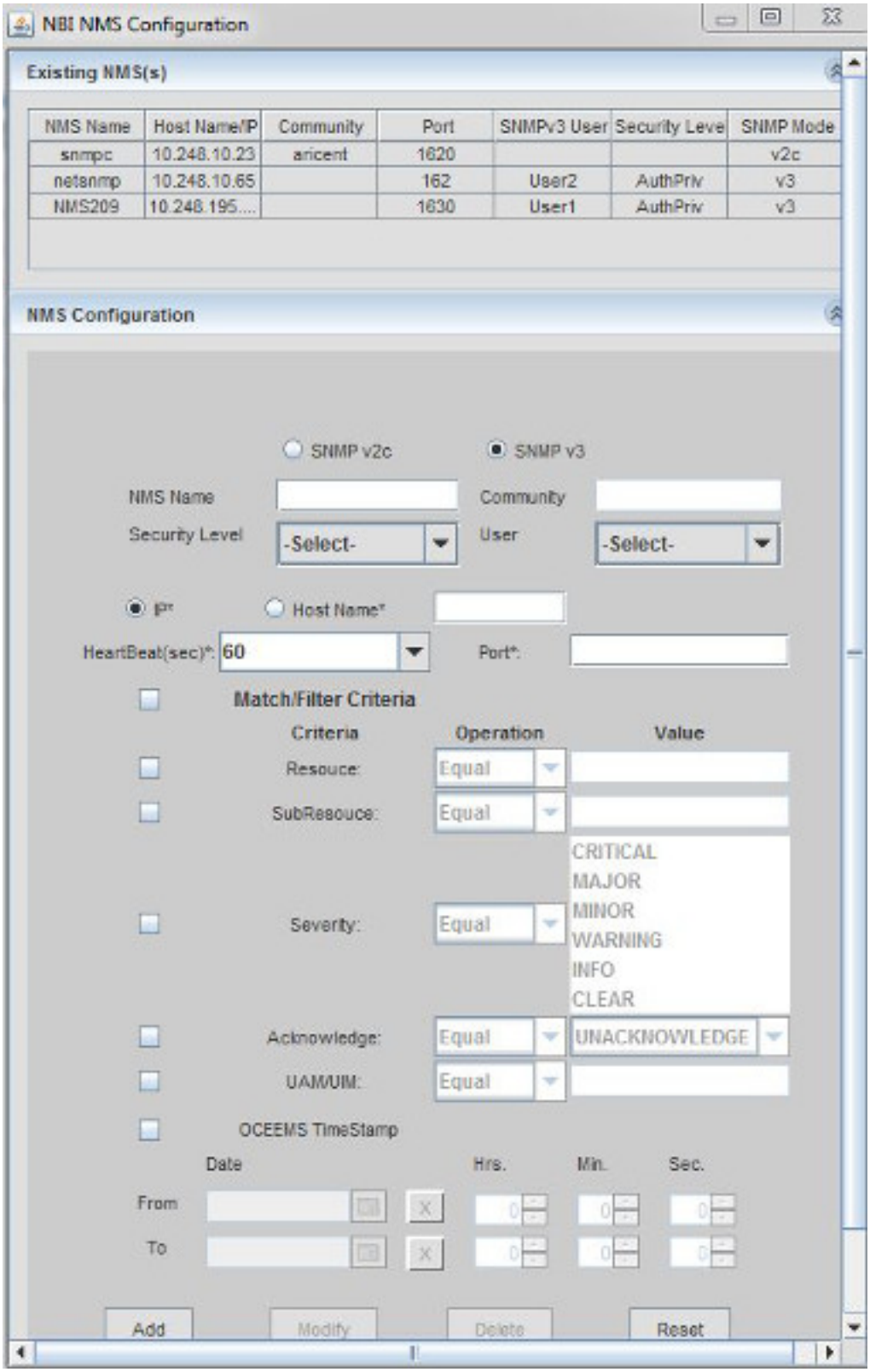
NMS Configuration

OCEEMS provides the NBI NMS Configuration screen (**Tools**, and then **NBI**) to configure an NMS along with matching/filtering patterns. These configurations are used by the NBI module to send autonomous/resync events received at OCEEMS to an NMS. Autonomous/resync events are filtered using matching/filtering patterns before they are sent to an NMS.

Access to the **Tools**, and then **NBI** menu item is provided to those OCEEMS users authorized for the **NBI NMS Configuration** operation. The menu item is not visible to unauthorized users.

The NBI NMS Configuration screen provides access to two collapsible panels, Existing NMS(s) and NMS Configuration. Each panel can be collapsed and expanded by clicking on its title bar.

Figure 13-9 Sample NBI NMS Configuration Screen



The Existing NMS(s) panel displays the configured NMS(s). Some columns are applicable for both SNMP modes (SNMP v2c and SNMP v3), and some columns are used only for SNMP v2c or only for SNMP v3.

The **SNMP v2c** and **SNMP v3** radio buttons at the top of the NMS Configuration panel are used to indicate the SNMP mode that the NMS being configured will use:

- **SNMP v2c**
  When **SNMP v2c** is selected, the **Community** field is required, and the **Security Level** and **User** drop-down menus are not used. For information about the **Community** field and other fields used for SNMP v2c, see NMS Configuration Data and Match/Filter Criteria Data.
- **SNMP v3**
  When **SNMP v3** is selected, selections on the **Security Level** and **User** drop-down menus are required, and the **Community** field is not used.
  - **Security Level**
    Security levels are **AuthPriv**, **AuthNoPriv**, and **NoAuthNoPriv**. Selecting a security level populates the **User** drop-down menu with all the existing SNMP v3 users that belong to a group at the selected security level.

    For more information about groups and security levels, see SNMP v3 Group Management. For more information about SNMP v3 users, see NBI Agent Configuration.
  - **User**
    Select the user to be associated with the NMS and used for communication (forwarding traps and resync requests) between OCEEMS and the NMS.

    > **Note**
    >
    > If any changes are made to the SNMP v3 user associated with an NMS on OCEEMS, the same changes must be made at the NMS end too, so that the v3 user configuration at NMS is in sync with OCEEMS.

  For information about the other fields used for SNMP v3, see NMS Configuration Data and Match/Filter Criteria Data.

The following operations are available from the NMS Configuration panel:

- **Add**
  After completing the NMS Configuration panel, click **Add** to add the new **NMS** to the OCEEMS database and to the Existing NMS(s) panel.
- **Modify**
  The **Modify** operation is used to modify an existing NMS:
  1. Select the NMS in the Existing NMS(s) panel.
     Selecting the NMS populates the NMS Configuration panel with the details for the selected NMS.
  2. Modify the details as needed.
  3. Click **Modify** to modify the NMS in the OCEEMS database and in the Existing NMS(s) panel.
- **Delete**
  The **Delete** operation is used to delete an existing NMS:
  1. Select the NMS in the Existing NMS(s) panel.

2. Click **Delete**, and then **Ok** in the confirmation box, to delete the NMS from the OCEEMS database and from the Existing NMS(s) panel.

- **Reset**
  Click **Reset** to set the fields in the NMS Configuration panel to their default values.

NMS Configuration Data

To add a NMS on the NMS Configuration panel, complete the appropriate fields:

SNMP v2c or SNMP v3
Depending upon the radio button selected, the SNMP mode that the NMS being configured will use.

NMS Name
A logical name for the NMS.

Community
SNMP community contained in SNMP v2c traps. The **Community** field is not used for SNMP v3.

Security Level
The SNMP v3 security level to be used; selecting a security level populates the **User** drop-down menu with all the existing SNMP v3 users that belong to a group at the selected security level. The **Security Level** field is not used for SNMP v2c.

User
The SNMP v3 user to be associated with the NMS and used for communication (forwarding traps and resync requests) between OCEEMS and the NMS. The **User** field is not used for SNMP v2c.

IP or Hostname
Depending upon the radio button selected, a unique IP address or hostname of the SNMP manager to receive traps.

Heartbeat
Number of seconds between heartbeat (i.e., system alive message) traps.

Port
Destination UDP port.

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)** panel.

NMS Configuration Element Rules

Element	Validation Rules
SNMP v2c or **SNMP v3** Radio Buttons	• Only one mode can be selected.
NMS Name Field	• Must be unique (the check is case insensitive). • Only alphanumeric characters, hyphen, and underscore are allowed.

Element	Validation Rules
	• It must have an alphabetic character as its first character. • Length is 5 to 20 characters.
Community Field	• String length cannot exceed 127 characters. • Blank string not allowed. • This field is not used for SNMP v3.
Security Level	• SNMP v3 security levels are AuthPriv, AuthNoPriv, and NoAuthNoPriv. • This field is not used for SNMP v2c.
User	• The **User** list is populated with SNMP v3 users that belong to a group having the selected security level. • This field is not used for SNMP v2c.
IP*	• Must be unique (no two NMS(s) can have the same IP address). • Blank is not allowed. • Valid IP address.
Host name*	• Must be unique (no two NMS(s) can have the same host name). • Composed of series of labels concatenated with dots. For example, "en.wikipedia.org". • Each label must be 1 - 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.
Heartbeat(sec)*	The user can either select a value from the drop-down menu or enter a value in the text box. The heartbeat drop-down menu will list the following entries- 60, 120, 300, 600, 900, 1800, 3600, 5400, and 7200. • Only numeric values between 5 and 7200 are allowed. • Blank is not allowed.
Port	• Only numeric values between 0 and 65535 are allowed.

Element	Validation Rules
	• Blank is not allowed.

Match/Filter Criteria Data

Match/Filter Criteria is disabled by default. A checkbox is provided to either enable all criteria at once or to individually enable required criteria. Enabling **Match/Filter Criteria** sets the **Operation** fields to **Equal** by default.

The following are optional search **Criteria** for alarms:

- **Resource**: Source of alarm.
- **Sub-resource**: Physical/logical component of source on which the alarm was actually raised.
- **Severity**: Severity level of alarm.
- **Acknowledge**: Determines whether the alarm is acknowledged at OCEEMS.
- **UAM/UIM**: UAM/UIM number of alarm received from EAGLE/EPAP/LSMS.
- **OCEEMS TimeStamp**: Determines the date and time range for alarms.

The **Operation** fields have the option of **Equal** or **Not Equal** values and use semicolons (;) to assist in the filtering. The asterisk (*) can be used in 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 (&&) operations are performed on all criteria configured, matching (i.e., **Operation** = **Equal**) and filtered (i.e., **Operation** = **Not Equal**).
- Logical OR (||) operations are performed between multiple values configured per criteria.
- Values other then those specified in match criteria (i.e., **Operation** = **Equal**) automatically become filtering criteria and vice versa.

Match/Filter Criteria Element Rules

Tip: When you hover the mouse over the fields for a rule, the following 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**	• Blank is not allowed. • Multiple resources can be separated via the semicolon (;) character. • Special characters underscore (_), hyphen (-), and asterisk (*) are allowed. For example, *XXXX, XXX*, and *XXX*.
SubResource	**Equal** or **Not Equal**	• Blank is not allowed.

Criteria	Operation	Value Rules
		• Multiple resources can be separated via the semicolon (;) character. • Special characters underscore (_), hyphen (-), and asterisk (*) are allowed. For example, *XXXX, XXX*, and *XXX*.
Severity	**Equal** or **Not Equal**	Severity levels: • **Critical** • **Major** • **Minor** • **Warning** • **Info** • **Clear** **Note** User can select multiple severities at a time, either matching or filtering criteria.
Acknowledge	**Equal** or **Not Equal**	Only applicable to resync events and not to autonomous events as **Acknowledge**/**Unacknowledge** is an OCEEMS operation. Autonomous event trap forwarding is not impacted when this criterion is configured.
UAM/UIM	**Equal** or **Not Equal**	• All UAM/UIM can be matched/filtered by specifying asterisk (*). • Multiple UAM/UIM can be specified, separated by a semicolon as follows: X;Y; A-B;Z • UAM/UIM range can be specified as A-B. • Asterisk can't be combined 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 when UAM/UIM range is specified.
OCEEMS TimeStamp	Not applicable	Specifies the date and time range for alarms.

Trap Forwarding

OCEEMS receives the following network element alarms/traps over southbound interfaces:

- EAGLE alarms/traps are received using TL1 or SNMPv2c

- EPAP alarms are received using SNMPv2c
- LSMS alarms are received using SNMPv1 or SNMPv3

The trap format (SNMPv2c/SNMPv3) used for forwarding over the Northbound Interface depends upon the global SNMP mode enabled and how the NMS(s) are configured:

- If SNMPv2c is enabled and one of more NMS(s) are configured in SNMPv2c, then all the alarms/traps are forwarded to those NMS(s) in SNMPv2c.
- If SNMPv3 is enabled and one of more NMS(s) are configured in SNMPv3, then all the alarms/traps are forwarded to those NMS(s) in SNMPv3.

For SNMP v3, an additional NMS user configuration/discovery (see note below) step is required because of enhanced security. After an NMS has been added and associated with a v3 user on the NMS configuration panel in OCEEMS, the same v3 user must be configured/discovered on the NMS as follows:

1. If configuration of the v3 user is needed at the NMS, configure the user with the user details (username, authentication protocol, authentication password, privacy protocol, privacy password) in OCEEMS and the engine ID value OCEEMSID (hex value: 4f4345454d534944).
2. If discovery of the v3 user is needed at the NMS, discover the v3 user on the port on OCEEMS provided in the `V3_USER_DISCOVERY_PORT_FOR_TRAPS` parameter in the `/Tekelec/WebNMS/conf/tekelec/server_conf.properties` file. This port must be opened bi-directionally on the OCEEMS firewall. The default value of this port is 1234, which is configurable (OCEEMS server must be restarted if changed).

> **Note**
>
> The requirement of v3 user discovery before trap forwarding has been observed only when using the OCEEMS MIB Browser as an NMS proxy. Testing with standard network monitoring tools like SNMPc and net-snmp has shown that v3 user discovery is not required, and configuring the v3 user with correct details (username, authentication protocol, authentication password, privacy protocol, privacy password) and the OCEEMS engine ID value OCEEMSID (hex value: 4f4345454d534944) is all that is needed for trap forwarding to work successfully.

After the v3 user has been successfully configured/discovered on the NMS, trap forwarding works as follows.

The SNMP traps forwarded to northbound NMS(s) are as per the OCEEMS MIB definition and have the following varbinds:

- alertTime - timestamp when OCEEMS system received the event for the managed sub-domain. This timestamp uses the ISO 8601 standard (http://www.w3.org/TR/NOTE-datetime), wherein:
  - Times are expressed in Coordinated Universal Time (UTC), with a T to indicate the beginning of the time element and a special UTC designator (Z) in the timestamp.
  - The format of the timestamp is *YYYY-MM-DD***T***hh*:*mm*:*ss***Z**. For example, 1985-04-12T23:20:50Z represents 20 minutes and 50 seconds after the 23rd hour of April 12th, 1985 in UTC.
- 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.
- alertSourceIp - the source IP address of the network element where the alarm/trap originated.

All the traps are forwarded to the NMS(s) on their respective listen ports as configured on the NMS Configuration panel.

Only those events that meet the matching/filtering criteria configured for an NMS on the NMS Configuration panel are forwarded to the NMS.

All internal events generated by OCEEMS are forwarded to the NMS(s). However, Status Update and EAGLE inventory discovery events (for example, discovery/addition of frame, shelf, card, etc.) are not forwarded to the NMS(s).

The OCEEMS sends heartbeat traps to an NMS periodically to indicate that the connection is still up. The periodicity of the heartbeat traps is as per the heartbeat value configured for an NMS on the NMS Configuration panel.

For SNMPv3, the trap PDU includes additional information related to the USM entry for an NMS.

In order to disable UserID in SNMP traps, complete the following procedure:

1. Open the `/Tekelec/WebNMS/conf/serverparameters.conf` file.
2. Find the `IS_USERNAME_ALLOWED_IN_ALARMS` parameter. By default, this parameter is set to **True**.
3. Set the `IS_USERNAME_ALLOWED_IN_ALARMS` parameter to **False** in order to disable UserID in NBI traps.
4. Save the file.
5. Restart the OCEEMS server using the `'service e5msService restart'` command.
6. The UserID in SNMP trap is disabled.

Resynchronization

If an NMS gets out of sync with OCEEMS, the NMS can send a SET request to OCEEMS for resynchronization. Alarm resynchronization between OCEEMS and an SNMP v3 based NMS is initiated in the same way as resynchronization between OCEEMS and an SNMP v2c based NMS, by setting the **resyncVar** variable in the OCEEMS NBI MIB to **1**. However, in the case of v3, the SET request should be made using the SNMP v3 user associated with the NMS on OCEEMS. Depending on whether the NMS requires discovery of the v3 user before sending any SET requests to OCEEMS, v3 user discovery might be needed (see the note below) before sending any SET request to OCEEMS:

1. If discovery of the v3 user is needed at the NMS before sending any GET/SET requests, discover the v3 user associated with the NMS on port 8002. After successful discovery of the user on the NMS, the NMS can send the SET request for **resyncVar** on port **8002** using the same v3 user.
2. If discovery of the v3 user is not needed at the NMS before sending any GET/SET requests, send the SET request for **resyncVar** on port **8002** using the v3 user associated with the NMS.

> **Note**
>
> The requirement of v3 user discovery for sending alarm resynchronization requests has been observed only when using the OCEEMS MIB Browser as an NMS proxy. Testing with standard network monitoring tools like SNMPc and net-snmp has shown that v3 user discovery is not required, and using the v3 user with correct details (username, authentication protocol, authentication password, privacy protocol, privacy password) is all that is needed for alarm resynchronization to work successfully.

When receiving an SNMP SET request, the OCEEMS triggers resynchronization as long as another SNMP SET request is not in progress at the NMS. In addition, for SNMPv3, the SET request is checked for validity (whether the SNMPv3 user that sent the request is valid and has permission to issue the request).

The port on which the OCEEMS NBI SNMP agent listens for SNMP GET/SET requests (port 8002) is not configurable. When resynchronization is triggered, the OCEEMS SNMP agent switches to resync mode for that NMS and the following steps are performed:

- Events are buffered in a queue and are not processed.
- Resync start trap is sent to the NMS.
- Active alarms are picked from the database that are less than or equal to the resync trigger time and are sent as resync traps, after the alarms are filtered using matching/filtering patterns.
- Resync stop trap is sent to the NMS.
- The mode is toggled from 'resync' to 'transition'. In transition mode, outstanding events are sent to the NMS.
- After all outstanding events are sent, the SNMP agent toggles the mode from 'transition' to 'normal'.

Functional Limitations

- A maximum of 10 Network Management Systems (NMSs) can be configured with NBI.

  > **Note**
  >
  > If the client tries to configure more than 10 NMSs, the following error message is displayed: `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 2 hours; that is, 2,000,000 events at an alarm rate of 180 events/second. Once a 2 million event threshold is met, there will be a loss of events.
- There is no check on a user adding the same NMS once using its IP address and once using its hostname; behavior of the OCEEMS SNMP NBI in such a case is unpredictable.

A

Decoupling OCEEMS from EAGLE

This appendix describes the Decoupling of OCEEMS from EAGLE.

Overview

The Decoupling of OCEEMS from EAGLE makes the OCEEMS independent of various EAGLE releases or versions. The OCEEMS will not be coupled with a single EAGLE release or version; it will be compatible with any particular EAGLE release 46.3 and later, but only one EAGLE release at a time.

The command Set in EAGLE typically differs from release to release. Any changes in the command set due to an EAGLE release upgrade will be reflected in OCEEMS without upgrading the OCEEMS Release.

Decoupling of the Command Manager Interface (CMI) from EAGLE

The OCEEMS user will be able to access the command set of any EAGLE release 46.3 and later, from OCEEMS, but only one EAGLE release at a time, during and after OCEEMS Release 47.0.0 installation.

Prerequisites for the Decoupling of the CMI from EAGLE

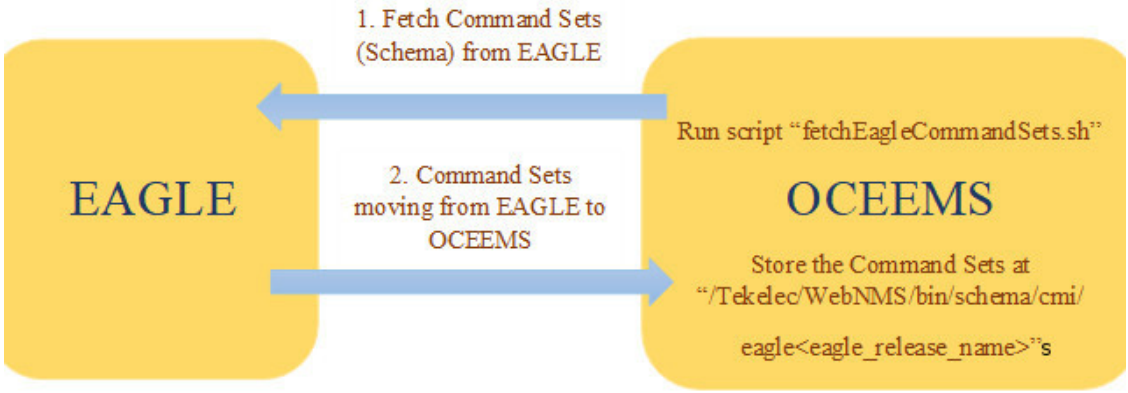
1. "PHP" must be installed on the OCEEMS server.
2. "DOM extension" must be installed on the OCEEMS server (`yum install php-xml`).
3. "wget" must be installed on the OCEEMS server (`yum install wget -y`).
4. PHP SSH2 extension must be installed on the OCEEMS server. The server should have internet access to install the required packages.
   Refer to Procedure to Install PHP Extension SSH2.
5. PHP-Posix package must be installed on the OCEEMS server (`yum install php-posix`).

After installation, OCEEMS 47.a.b will contain the schema (command set) of EAGLE 47.a.b by default. The default CMI schema will be present in `/Tekelec/WebNMS/bin/schema/cmi/eagle47.a.b`.

The CMI schema from other EAGLE releases will be present in `/Tekelec/WebNMS/ bin/schema/cmi/eagle<release_name>`. For example, the CMI schema of EAGLE release 47.x.y will be available in `/Tekelec/WebNMS/bin/schema/cmi/eagle47.x.y>`.

Fetching the Command Set from the EAGLE with a Specific EAGLE Release

Figure A-1 Fetch CMI Schema



Before installing the CMI schema (command set) of a specific EAGLE release, the CMI schema of that specific EAGLE release must be present in OCEEMS at `/Tekelec/WebNMS/bin/schema/cmi/eagle<eagle_release_name>`. If the respective CMI schema is not present in OCEEMS at the previously mentioned filepath, then `installE5MSSchema.sh` will not be able to install the CMI schema (command set) of that specific EAGLE release.

For that purpose, a new integrated script named `fetchEagleCommandSets.sh` has been introduced for OCEEMS 47.0 that will be available at `/Tekelec/WebNMS/bin/eagle`.

This script is able to fetch the CMI schema (command set) from EAGLE using both SSH and Telnet connection protocols.

Note

Before running the `fetchEagleCommandSets.sh` script:

Run the following command:

```
grep -oP "\"EAGLE\s+\K\w+" /Tekelec/WebNMS/bin/eagle/main.php
```

Check the release version from the output. If the major release matches the major release of the Eagle, skip this note, otherwise follow as below cases:

If the major release version fetched from the above command differs from the Eagle release major version for which data is being fetched, then run the following command:

For example:

Case 1:

If the output of the above command is 46 and the Eagle version is 47.xyz, then run the following command:

```
sed -i 's/EAGLE 46/EAGLE <Eagle Version>/g'
/Tekelec/WebNMS/bin/eagle/main.php
```

i.e.,

```
sed -i 's/EAGLE 46/EAGLE 47/g'
/Tekelec/WebNMS/bin/eagle/main.php
```

Case 2:

If the output of the above command is 47 and the Eagle version is 46.xyz, then run the following command:

```
sed -i 's/EAGLE 47/EAGLE <Eagle Version>/g'
/Tekelec/WebNMS/bin/eagle/main.php
```

i.e.,

```
sed -i 's/EAGLE 47/EAGLE 46/g'/Tekelec/WebNMS/bin/eagle/main.php
```

The following steps present the behavior of the `fetchEagleCommandSets.sh` script when Telnet and SSH connection protocols are used:

1. **Note**

   Using Telnet Connection:

   This script will take the following inputs from the OCEEMS user:

   a. Connection protocol to be used to fetch the command set (schema)

b. EAGLE IP, from which the command set (schema) is to be fetched

c. User name of the EAGLE

d. Password of the EAGLE

e. EAGLE terminal

The EAGLE Release will be dynamically fetched from EAGLE while fetching the Command Sets.

For example, refer the following figure. The figure contains the following inputs:

Connection protocol: telnet

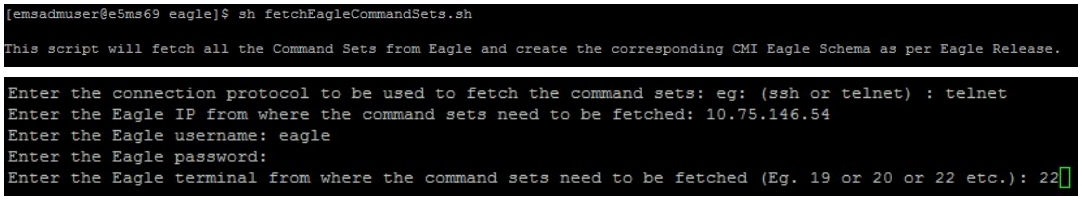
EAGLE IP: 10.75.146.54

EAGLE Username: eagle

EAGLE Password: <password>

EAGLE Terminal: 22

Figure A-2 `fetchEagleCommandSets.sh` Script



2. **Note**

   Using SSH Connection

This script will take the following inputs from the OCEEMS user:

a. Connection protocol to be used to fetch the command set (schema)

b. EAGLE IP, from which the command set (schema) is to be fetched

c. User name of the EAGLE

d. Password of the EAGLE

e. EAGLE terminal

f. Local server password where OCEEMS is installed (If logged in with root/non-root user, then corresponding password needs to be entered.)

The EAGLE Release will be dynamically fetched from EAGLE while fetching the Command Sets.

For example, refer to the following figure:

Connection protocol: ssh

EAGLE IP: 10.248.13.54

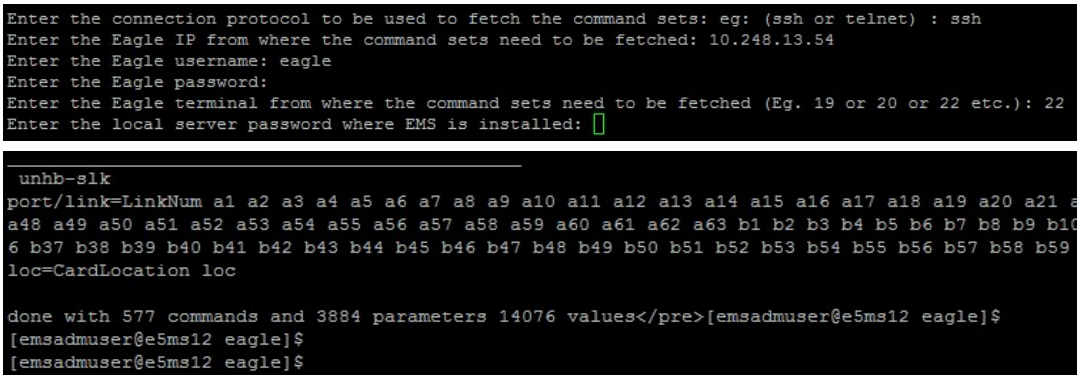
EAGLE Username: eagle

EAGLE Password: <password>

EAGLE Terminal: 22

EMS local server password: <server_password>

Figure A-3 Completion of the `fetchEagleCommandSets.sh` Script



The script will fetch the fresh command set (CMI schema) from the EAGLE entered in the previous figure with the specific EAGLE Release and will keep the same in OCEEMS at `/Tekelec/WebNMS/bin/schema/cmi/eagle<eagle_release_name>`.

In the following figure, the CMI schema for EAGLE Release 46.x.y is displayed, and the schema for EAGLE Release 47.0.0 is already present by default:

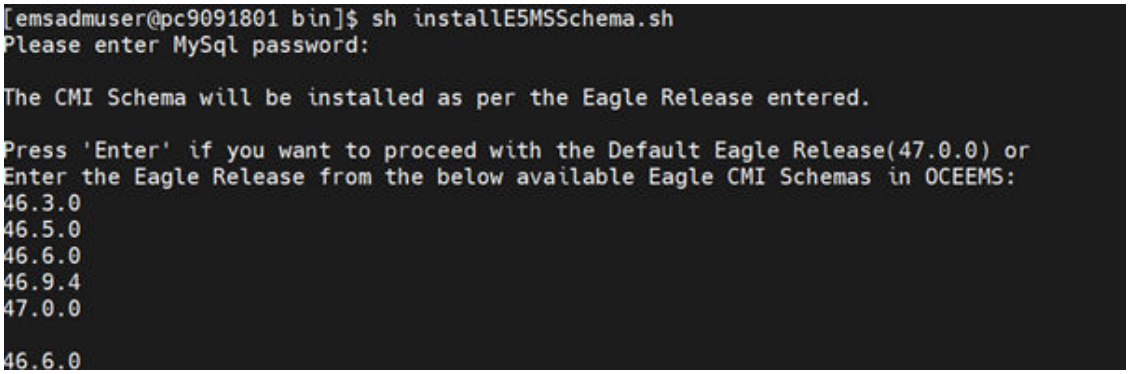
Figure A-4 EAGLE Release-specific CMI Schema

Installing the CMI Schema

While installing the schema during the installation of OCEEMS, the `installE5MSSchema.sh` script (present in `/Tekelec/WebNMS/bin`) provides two options:

1. Whether the OCEEMS user wants to proceed with the Default schema installation (schema of EAGLE 47.0.0)
2. Whether the OCEEMS user wants to install the schema from the available EAGLE CMI schemas in OCEEMS (fetched as per specific EAGLE Release)

Figure A-5 OCEEMS Schema Installation Options



Default Schema Installation

The script asks to press **Enter** to proceed with Default EAGLE Release, as in 47.a.b (example: 47.0.0). For default schema installation, the OCEEMS user must press **Enter** and the schema (commands sets) of the default compatible EAGLE 47.a.b will be installed automatically. Refer the following figure:

Figure A-6 Default Schema Installation

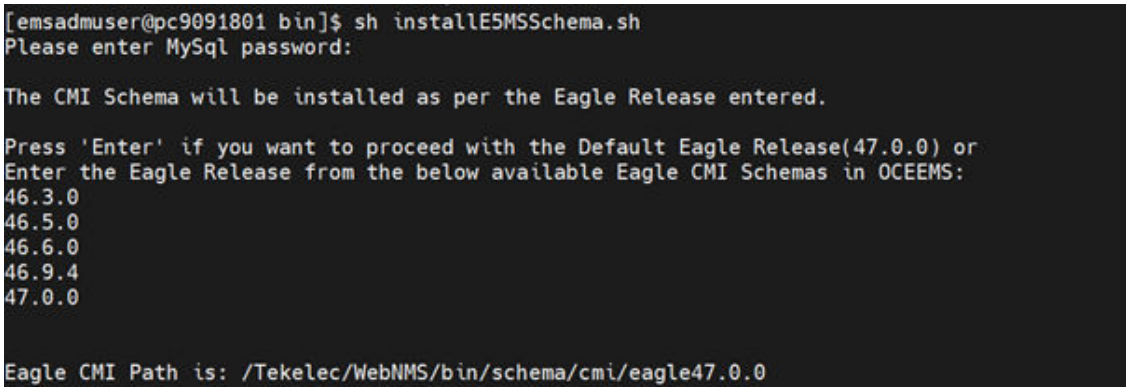
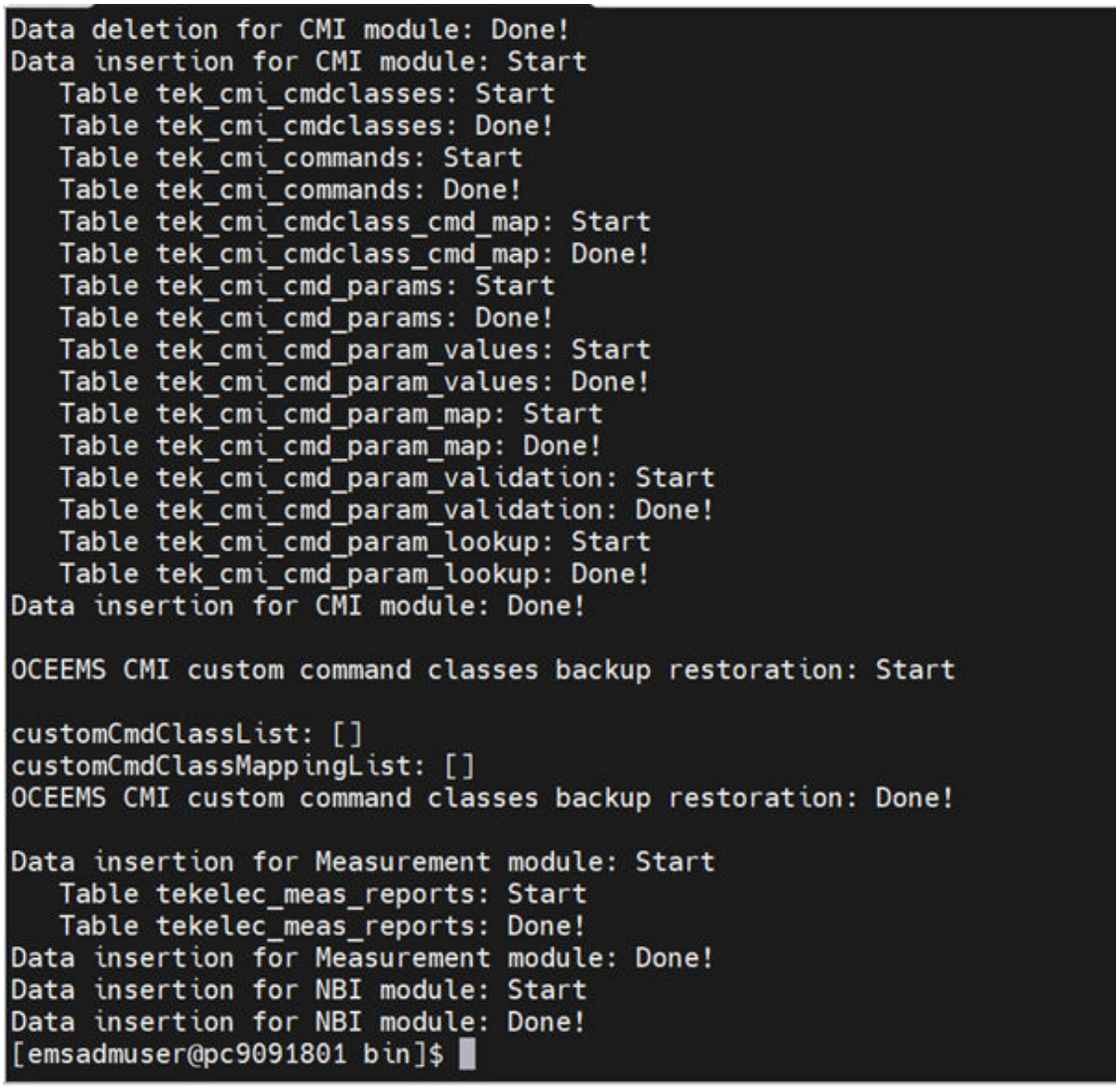


Figure A-7 Default Schema Installation Completion



Installing Schema from a Specific EAGLE Release

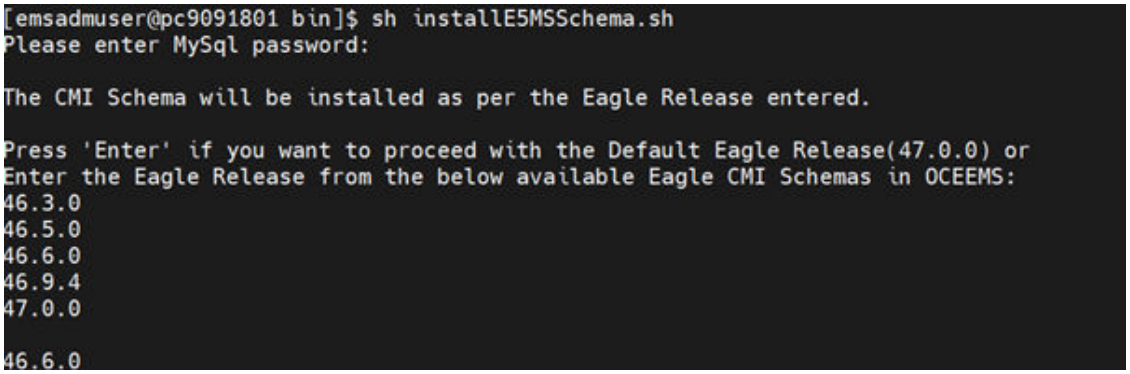
For installing schema from a specific EAGLE release, the respective schema must be present in OCEEMS at `/Tekelec/WebNMS/bin/schema/cmi/eagle<eagle_release_name>`. The OCEEMS user must run the `fetchEagleCommandSets.sh` script located at `/Tekelec/WebNMS/bin/eagle` in order to fetch the command set or schema from the specific EAGLE release.

The `fetchEagleCommandSets.sh` script will fetch and keep the schema or command set of the specific EAGLE release `/Tekelec/WebNMS/bin/schema/cmi / eagle<eagle_release_name>`.

Now the OCEEMS user must run the `installE5MSSchema.sh` script located at `/Tekelec/WebNMS/bin` to install the schema of that specific EAGLE release.

Refer to the following figure for an example of the schema of EAGLE Release 47.0.0 that has been installed:

Figure A-8 Installing Schema from a Specific EAGLE Release



Installing a CMI Schema After an OCEEMS Installation or When OCEEMS is Already Running

An additional option is to install a CMI Schema after an OCEEMS installation or when OCEEMS is already running. The CMI Schema can also be changed according to the EAGLE release after the OCEEMS client has been installed, as per the requirement of OCEEMS user. If the OCEEMS client is already installed and the user is currently using EAGLE 47.x.y, then the user can change the current EAGLE 47.x.y schema (command set) to the new EAGLE 47.x.y schema. The new EAGLE 46.x.y schema can be installed by running `installE5MSSchema.sh` script, provided the EAGLE 46.x.y schema is present at `/Tekelec/WebNMS/bin/schema/cmi/eagle47.x.y`. All the available schemas in the OCEEMS will be shown by the script.

If the EAGLE 46.x.y schema (command set) is not present at `/Tekelec/WebNMS/bin/schema/cmi/eagle46.x.y`, the OCEEMS user must run the `fetchEagleCommandSets.sh` script so that the required schema is fetched and available. After that, the user can install the new EAGLE 46.x.y schema.

Figure A-9 Changing the EAGLE Schema After Installation

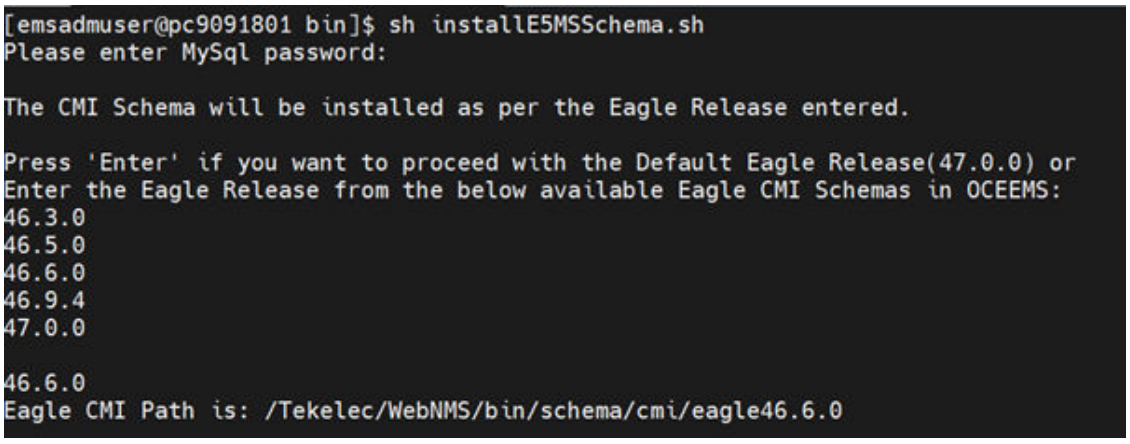
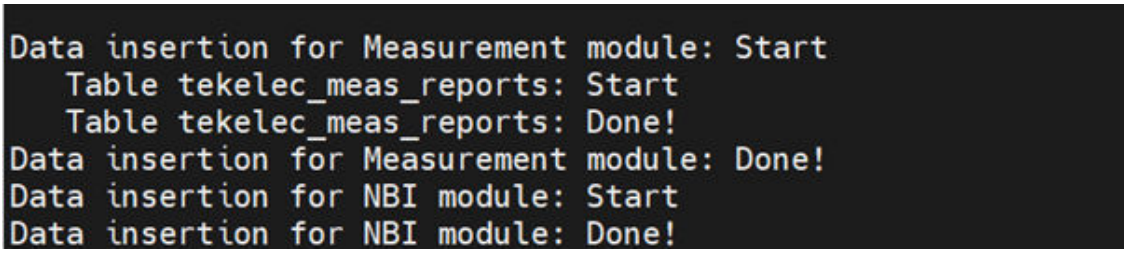


Figure A-10 Changing the Eagle Schema



Backup and Restoration of Custom Command Classes

The Custom Command Classes are the command classes that do not belong to EAGLE and are made by the OCEEMS user. When the OCEEMS user switches from one EAGLE release to another (changes the currently compatible EAGLE release with OCEEMS), the Custom Command Classes will be restored and all the commands under that command class will be visible after changing the EAGLE release at the OCEEMS CMI GUI. If the command is not present in the newly upgraded EAGLE release schema (command set), then that particular command will not be visible.

For example, if a command is present in the EAGLE 47.a.b schema (command set), but the same command is not present in the EAGLE 46.x.y schema (command set), then after upgrading or changing the EAGLE schema from 46.a.b to 46.x.y from OCEEMS, that command will not be available in the OCEEMS CMI GUI.

If all the commands belonging to a specific Custom Command Class are not present in new upgraded EAGLE release (46.x.y), then the Custom Command Class would not be available in the OCEEMS CMI GUI after changing the EAGLE Release schema (EAGLE 47.x.y to EAGLE 46.x.y).

The following figure shows the Custom Command Class "CUSTOM" and its command is restored after changing the current compatible EAGLE release from 47.x.y to 46.x.y:

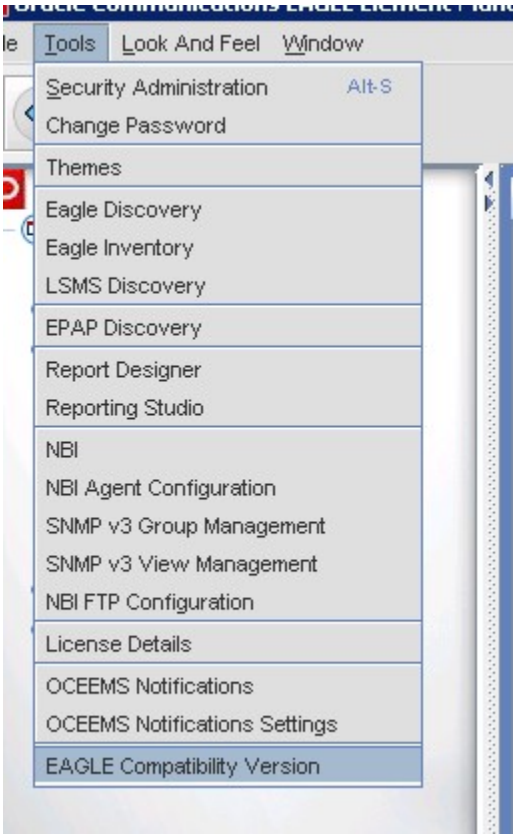
Figure A-11 Custom Command Class "CUSTOM" when the Current Compatible EAGLE Release is 47.x.y

Figure A-12 Custom Command Class "CUSTOM", Restored, when the Current Compatible EAGLE Release is 46.x.y

Current Compatible EAGLE Release with OCEEMS

The current compatible EAGLE release with OCEEMS can be accessed from the menu option **Tools**, and then **EAGLE Compatiblity Version**, as displayed in the following figure:

Figure A-13 EAGLE Compatibility Version Menu



The current compatible EAGLE release or version with the OCEEMS means that the OCEEMS is supporting the schema or command set of the displayed EAGLE release, with which it is currently compatible:

Figure A-14 Current EAGLE Compatibility Version

If the current compatible EAGLE Release is 47.a.b (for example, 47.0.0), then the OCEEMS is supporting the schema or command set of the EAGLE 47.0.0. The command set of EAGLE 47.0.0 is available in the OCEEMS CMI GUI.

The current compatible EAGLE release will change when the OCEEMS user changes the current EAGLE schema, as per the EAGLE release.

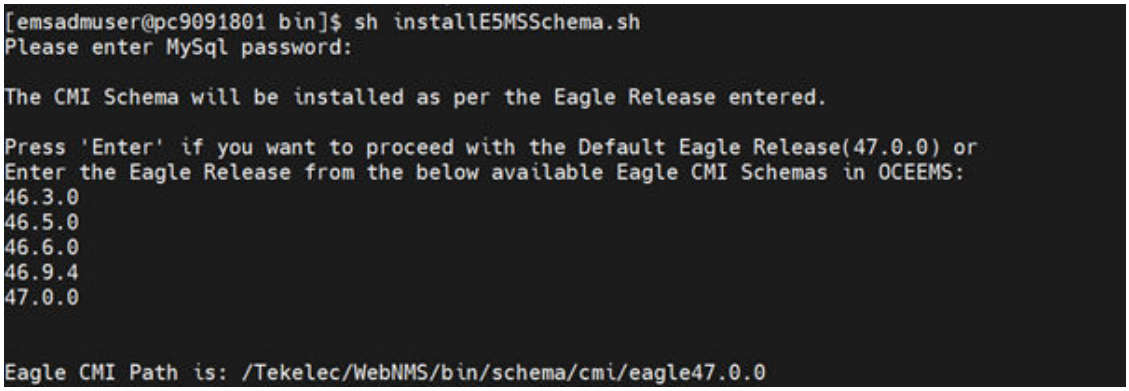
Moving Back to the Default EAGLE Release Schema from the OCEEMS

The OCEEMS user can move back to the default EAGLE Release Schema. If the user has upgraded the schema (command set) to a new EAGLE Release, by running the `installE5MSSchema.sh` script again, the user can move back or change the schema to the default EAGLE release.

For example, if the user has changed to the EAGLE 46.x.y (example, 46.7.0) schema from EAGLE 47.x.y schema (default), then the user can again install and change the schema to EAGLE 47.x.y (default).

The following figure illustrates the example of 47.x.y=47.0.0:

Figure A-15 Moving Back (installing) to the Default EAGLE Release Schema



Procedure to Decouple the CMI from EAGLE

Before starting this procedure, the OCEEMS must be installed on the target machine. The default CMI Schema of EAGLE Release 46.6.0 will be installed by default.

1. Log in to the target machine using root user if the OCEEMS is installed and running with root user, or log on using non-root user if the OCEEMS is installed and running with non-root user.

   Successful log on.

2. Move to the `/Tekelec/WebNMS /bin/eagle` directory by issuing the following command:

```
$ cd /Tekelec/WebNMS/bin/eagle
```

3. Execute the `/Tekelec/WebNMS/bin/eagle/ fetchEagleCommandSets.sh` script to fetch the command set or schema from an EAGLE with a specific EAGLE release.

```
$ sh fetchEagleCommandSets.sh

Output:
When Connection Protocol to be used is SSH:
This script will fetch all the Command Sets from Eagle and create the
corresponding CMI Eagle Schema as per Eagle Release.
```

Execute the script with root user if the OCEEMS is installed with root user, or execute the script with non-root user if the OCEEMS is installed with non-root user. The script will ask for Connection Protocol, EAGLE IP, EAGLE Username, EAGLE Password, EAGLE Terminal and Local Server password where EMS is installed as inputs.:

```
Enter the connection protocol to be used to fetch the command sets: eg:
(ssh or telnet) : ssh
Enter the Eagle IP from where the command sets need to be fetched:
10.248.13.52
Enter the Eagle username: eagle
Enter the Eagle password:
Enter the Eagle terminal from where the command sets need to be fetched
(Eg. 19 or 20 or 22 etc.): 19
Enter the local server password where EMS is installed:

Output: When Connection Protocol to be used is Telnet:
This script will fetch all the Command Sets from Eagle and create the
corresponding CMI Eagle Schema as per Eagle Release.

Enter the connection protocol to be used to fetch the command sets: eg:
(ssh or telnet) : telnet
Enter the Eagle IP from where the command sets need to be fetched:
10.248.13.52
Enter the Eagle username: eagle
Enter the Eagle password:
Enter the Eagle terminal from where the command sets need to be fetched
(Eg. 19 or 20 or 22 etc.): 19
```

Leave this step if the required schema is already present at `/Tekelec/WebNMS/bin/schema/cmi/eagle<specific_eagle_release>`:

```
Sending EAGLE command to connect....
. . . . . .
. . . . . .
. . . . . .
. . . . . .
a48 a49 a50 a51 a52 a53 a54 a55 a56 a57 a58 a59 a60 a61 a62 a63 b1 b2 b3
b4 b5 b6 b7 b8 b9 b10 b11 b12 b13 b14 b15 b16 b17 b18 b19 b20 b21 b22 b23
b24 b25 b26 b27 b28 b29 b30 b31 b32 b33 b34 b35 b36 b37 b38 b39 b40 b41
b42 b43 b44 b45 b46 b47 b48 b49 b50 b51 b52 b53 b54 b55 b56 b57 b58 b59
b60 b61 b62 b63
loc=CardLocation loc
```

```
done with 577 commands and 3884 parameters 14076 values
```

4. After the successful execution of the `fetchEagleCommandSets.sh` script, the fetched schema (command set) of that specific EAGLE release must be present at `/Tekelec/WebNMS/bin/schema/cmi/eagle<specific_eagle_release>`. Example:

   ```
   /Tekelec/WebNMS/bin/schema/cmi/eagle46.6.0
   ```

5. Move to the `/Tekelec/WebNMS /bin/` directory by issuing the following command:

   ```
   $ cd /Tekelec/WebNMS/bin
   ```

6. When the required schema of the specific EAGLE release is present at `/Tekelec/WebNMS/bin/schema/cmi/eagle<specific_eagle_release>`, then execute the `/Tekelec/WebNMS/bin/installE5MSSchema.sh` script to install the respective schema:

   ```
   sh installE5MSSchema.sh

   Output:
   Please enter MySql password:

   The CMI Schema will be installed as per the Eagle Release entered.
   ```

   Run the script with root user if the OCEEMS is installed with root user, or run the script with non-root user if the OCEEMS is installed with non-root user.

   Enter the release of EAGLE from the available CMI schemas in OCEEMS to install them. Select **Enter** if the schema of the Default EAGLE Release (47.0.0) has to be fetched:

   ```
   Press 'Enter' if you want to proceed with the Default Eagle Release(47.0.0)
         or
   Enter the Eagle Release from the below available Eagle CMI Schemas in
   OCEEMS:
   46.3.0
   46.5.0
   46.6.0
   46.9.4
   47.0.0
   46.6.0
   Eagle CMI Path is: /Tekelec/WebNMS/bin/schema/cmi/eagle46.6.0

   OCEEMS CMI custom command classes backup: Start

   customCmdClassList:[]
   customCmdClassMappingList: []

   OCEEMS CMI custom command classes backup: Done!
   customCmdExists:true

   Data deletion for Measurement module: Start
   Table tekelec_meas_reports: Start
   Table tekelec_meas_reports: Done!
   Data deletion for Measurement module: Done!
   Data deletion for NBI module: Start
   Data deletion for NBI module: Done!
   Data deletion for CMI module: Start
   ```

```
Table tek_cmi_cmd_param_lookup: Start
Table tek_cmi_cmd_param_lookup: Done!
Table tek_cmi_cmd_param_validation: Start
Table tek_cmi_cmd_param_validation: Done!
Table tek_cmi_cmd_param_map: Start
Table tek_cmi_cmd_param_map: Done!
Table tek_cmi_cmd_param_values: Start
Table tek_cmi_cmd_param_values: Done!
Table tek_cmi_cmd_params: Start
Table tek_cmi_cmd_params: Done!
Table tek_cmi_cmdclass_cmd_map: Start
Table tek_cmi_cmdclass_cmd_map: Done!
Table tek_cmi_commands: Start
Table tek_cmi_commands: Done!
Table tek_cmi_cmdclasses: Start
Table tek_cmi_cmdclasses: Done!
Data deletion for CMI module: Done!
Data insertion for CMI module: Start
Table tek_cmi_cmdclasses: Start
Table tek_cmi_cmdclasses: Done!
Table tek_cmi_commands: Start
Table tek_cmi_commands: Done!
Table tek_cmi_cmdclass_cmd_map: Start
Table tek_cmi_cmdclass_cmd_map: Done!
Table tek_cmi_cmd_params: Start
Table tek_cmi_cmd_params: Done!
Table tek_cmi_cmd_param_values: Start
Table tek_cmi_cmd_param_values: Done!
Table tek_cmi_cmd_param_map: Start
Table tek_cmi_cmd_param_map: Done!
Table tek_cmi_cmd_param_validation: Start
Table tek_cmi_cmd_param_validation: Done!
Table tek_cmi_cmd_param_lookup: Start
Table tek_cmi_cmd_param_lookup: Done!
Data insertion for CMI module: Done!

OCEEMS CMI custom command classes backup restoration: Start

customCmdClassList: []
customCmdClassMappingList: []
OCEEMS CMI custom command classes backup restoration: Done!

Data insertion for Measurement module: Start
Table tekelec_meas_reports: Start
Table tekelec_meas_reports: Done!
Data insertion for Measurement module: Done!
Data insertion for NBI module: Start
Data insertion for NBI module: Done!
```

7. After the successful completion of the `installE5MSSchema.sh` script, the schema of the specific EAGLE Release (here it is 46.6.0) must be installed:

   Launch the OCEEMS Client and select **Tools**, and then **EAGLE Compatibility Version** in the Menu bar.
   After changing and installing the schema of the current compatible EAGLE release to a specific EAGLE release, the current compatible EAGLE release will be visible in the OCEEMS from the menu: **Tools**, and then **EAGLE Compatibility Version**.

Example:

```
The OCEEMS is currently compatible with EAGLE Release 46.6.0
```

Procedure to Move Back to the Default EAGLE CMI Schema

If the current compatible EAGLE release and schema has already been changed to a new specific EAGLE release (for example, 46.7.0), then complete this procedure to move back to the default EAGLE 47.x.y (example, 47.0.0) schema.

1. Log on to the target machine using root user if the OCEEMS is installed and running with root user, or log on using non-root user if the OCEEMS is installed and running with non-root user.

   Successful log on.

2. Move to the `/Tekelec/WebNMS /bin/` directory by issuing the following command:

   ```
   $ cd /Tekelec/WebNMS/bin
   ```

3. Execute the `/Tekelec/WebNMS/ bin/installE5MSSchema.sh` script to install the default schema:

   ```
   sh installE5MSSchema.sh
   ```
   Execute the script with root user if the OCEEMS is installed with root user, or execute the script with non-root user if the OCEEMS is installed with non-root user.

   Select **Enter** for installing the default EAGLE 47.0.0 schema:

   ```
   Press 'Enter' if you want to proceed with the Default Eagle
   Release(47.0.0) or
   Enter the Eagle Release from the below available Eagle CMI Schemas in
   OCEEMS:
   46.3.0
   46.5.0
   46.6.0
   46.9.4

   Eagle CMI Path is: /Tekelec/WebNMS/bin/schema/cmi/eagle47.0.0

   OCEEMS CMI custom command classes backup: Start

   customCmdClassList:[11,'CUSTOM',1]

   customCmdClassMappingList: [11,rtrv-rtx]
   OCEEMS CMI custom command classes backup: Done!

   customCmdExists:true

   Data deletion for Measurement module: Start
      Table tekelec_meas_reports: Start
      Table tekelec_meas_reports: Done!
   Data deletion for Measurement module: Done!
   Data deletion for NBI module: Start
   Data deletion for NBI module: Done!
   Data deletion for CMI module: Start
      Table tek_cmi_cmd_param_lookup: Start
      Table tek_cmi_cmd_param_lookup: Done!
   ```

```
   Table tek_cmi_cmd_param_validation: Start
   Table tek_cmi_cmd_param_validation: Done!
   Table tek_cmi_cmd_param_map: Start
   Table tek_cmi_cmd_param_map: Done!
   Table tek_cmi_cmd_param_values: Start
   Table tek_cmi_cmd_param_values: Done!
   Table tek_cmi_cmd_params: Start
   Table tek_cmi_cmd_params: Done!
   Table tek_cmi_cmdclass_cmd_map: Start
   Table tek_cmi_cmdclass_cmd_map: Done!
   Table tek_cmi_commands: Start
   Table tek_cmi_commands: Done!
   Table tek_cmi_cmdclasses: Start
   Table tek_cmi_cmdclasses: Done!
Data deletion for CMI module: Done!
Data insertion for CMI module: Start
   Table tek_cmi_cmdclasses: Start
   Table tek_cmi_cmdclasses: Done!
   Table tek_cmi_commands: Start
   Table tek_cmi_commands: Done!
   Table tek_cmi_cmdclass_cmd_map: Start
   Table tek_cmi_cmdclass_cmd_map: Done!
   Table tek_cmi_cmd_params: Start
   Table tek_cmi_cmd_params: Done!
   Table tek_cmi_cmd_param_values: Start
   Table tek_cmi_cmd_param_values: Done!
   Table tek_cmi_cmd_param_map: Start
   Table tek_cmi_cmd_param_map: Done!
   Table tek_cmi_cmd_param_validation: Start
   Table tek_cmi_cmd_param_validation: Done!
   Table tek_cmi_cmd_param_lookup: Start
   Table tek_cmi_cmd_param_lookup: Done!
Data insertion for CMI module: Done!

OCEEMS CMI custom command classes backup restoration: Start

customCmdClassList: [11,'CUSTOM',1]
customCmdClassMappingList: [11,rtrv-rtx]
OCEEMS CMI custom command classes backup restoration: Done!

Data insertion for Measurement module: Start
   Table tekelec_meas_reports: Start
   Table tekelec_meas_reports: Done!
Data insertion for Measurement module: Done!
Data insertion for NBI module: Start
Data insertion for NBI module: Done!
```

4. After the successful completion of script "installE5MSSchema.sh", the schema of the default Eagle Release (here it is 47.0.0) must be installed.

   Launch the OCEEMS Client and select **Tools**, and then **EAGLE Compatibility Version** in the Menu bar.
   After changing and installing the schema of the default compatible EAGLE release, it will display the current compatible EAGLE version as "The OCEEMS is currently compatible with EAGLE Release <eagle_release>.

Example:

```
The OCEEMS is currently compatible with Eagle Release 47.0.0
```

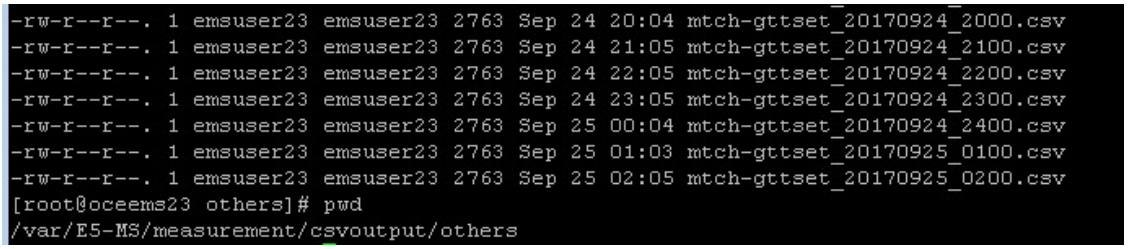
Decoupling of the Measurement Schema from EAGLE

From OCEEMS 46.6.0 and later, the user will be able to access the new measurement reports introduced in EAGLE 46.x.x from OCEEMS 46.x.x without upgrading OCEEMS from one version to another. A new `measurementSchema.sh` script is provided in OCEEMS 47.0.0. The script will be present in the `/Tekelec/WebNMS/bin` directory.

From OCEEMS 46.6 and later, if any new report is introduced in an upgraded EAGLE release (for example, 46.x.y), the current OCEEMS (for example, 47.0.0) will be able to parse the same report without upgrading OCEEMS to 46.x.y.

The generated report will move from path `/opt/E5-MS/measurement/csvinput/` to `/var/E5-MS/measurement/csvoutput/others`, as seen in the following figure:

Figure A-16 Not-parsed Report File Moved



This script (measurementSchema.sh) adds entries for new reports to the OCEEMS database. It requires 3 user inputs:

- Name of the new type of measurement report introduced in the new EAGLE Release
- Database(DB) Retention type (Hourly/Daily)
  - Hourly: DB retention days = 14
  - Daily: DB retention days = 30
- MySql password

This script makes an entry into the database table "tekelec_meas_reports".

As a result, when that new report (belonging to the new upgraded EAGLE release) is generated, it gets parsed and moved to path `/var/E5-MS/measurement/csvoutput/<eagle name>`.

Figure A-17 Output of the Measurement Script

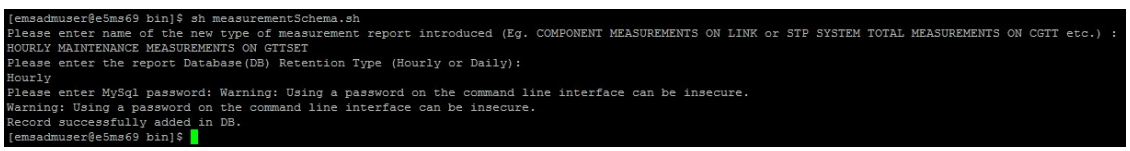


Figure A-18 Measurement Schema Name/Report Added to the DB

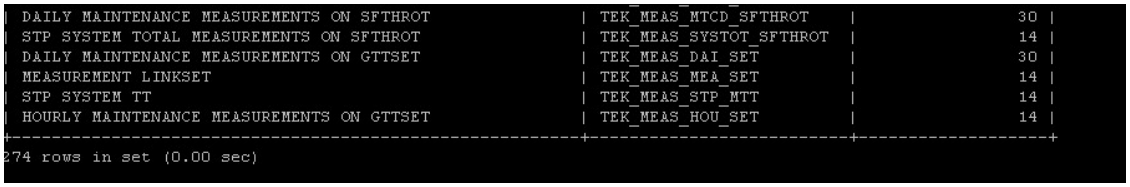
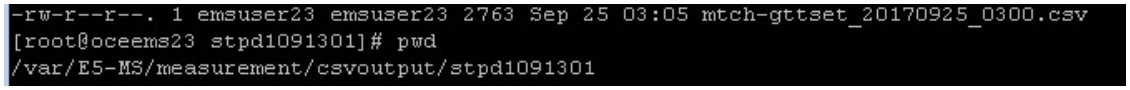


Figure A-19 Parsed Report Moved to the Directory with the EAGLE Name



Procedure to Decouple the Measurement Schema from EAGLE

Before completing this procedure, the OCEEMS must be installed on the target machine.

1. Log on to the target machine using root user if the OCEEMS is installed and running with root user, or log on using non-root user if the OCEEMS is installed and running with non-root user.

   Successful log on.

2. Check whether mysql is running on the target machine or not.

   ```
   $ ps -ef|grep mysql
   ```

3. Move to the `/Tekelec/WebNMS /bin/` directory by issuing the following command:

   $ cd /Tekelec/WebNMS/bin/

4. If mysql is already running on the machine, leave this step; otherwise, if mysql is not running, start mysql on the machine by running the `/Tekelec/WebNMS/bin/startMySQL.sh` script:

   ```
   $ sh startMySQL.sh
   ```

5. Move to the `/Tekelec/WebNMS /bin/` directory by issuing the following command

   $ cd /Tekelec/WebNMS/bin

6. Execute the `/Tekelec/WebNMS /bin/measurementSchema.sh` script to add a new measurement report:

   ```
   $ sh measurementSchema.sh
   ```
   Execute the script with root user if the OCEEMS is installed with root user, or execute the script with non-root user if the OCEEMS is installed with non-root user:

   ```
   Output:
   Please enter name of the new type of measurement report introduced (Eg.
   COMPONENT MEASUREMENTS ON LINK or STP SYSTEM TOTAL MEASUREMENTS ON CGTT
   etc.):
   HOURLY MAINTENANCE MEASUREMENTS ON GTTSET
   ```

The script will ask for three user inputs while running this command:

```
Please enter the report Database(DB) Retention Type (Hourly or Daily):
Hourly
Please enter MySql password:
Record successfully added in DB.
```

7. The newly introduced report in the new upgraded EAGLE release will be parsed successfully and moved to the `/var/E5-MS/measurement/csvoutput` folder with `<eagle_name>`.

   Example:

   ```
   /var/E5-MS/measurement/csvoutput/stpd1091031
   ```

(Optional) Enter the result of the procedure here.

Procedure to Add Help Files of a New Release to the OCEEMS

Before executing this procedure, make sure that the .zip file containing all the help files is copied on the OCEEMS machine. If a non-root user is configured to operate OCEEMS, then the .zip should be present at a location that is accessible to the non-root user.

1. Log in to the target machine using root user if the OCEEMS is installed and running with root user, or log on using non-root user if the OCEEMS is installed and running with non-root user.

   Successful log on.

2. Move to the `/Tekelec/WebNMS /bin/` directory by issuing the following command:

   ```
   $ cd /Tekelec/WebNMS/bin
   ```

3. Run the following command with non-root user:

   ```
   # sed -i -e 's/\r$//' addHelpFiles.sh
   ```

4. Execute the `addHelpFiles.sh` script to add help files:

   ```
   $ sh addHelpFiles.sh
   ```

   This script will ask for the path of the .zip file containing the help files, and the EAGLE release number for which the help files are added.

   ```
   Enter the Path of zip file containing the HTML help files:/tmp/
   OCEEMS_Commands_Release_46.5_rev_1.zip

   The path of zip file provided by you is: /tmp/
   OCEEMS_Commands_Release_46.5_rev_1.zip

   The supported EAGLE releases are displayed below.
   46.3.0
   46.5.0
   46.6.0
   Enter the EAGLE release of the Help files: 46.6.0

   Extracting Zip files...Archive:  /tmp/
   OCEEMS_Commands_Release_46.5_rev_1.zip
      creating: unzipHTML/concepts/
     inflating: unzipHTML/concepts/arrow_down.png
   ```

```
  inflating: unzipHTML/concepts/arrow_left.png
  inflating: unzipHTML/concepts/arrow_right.png
  inflating: unzipHTML/concepts/arrow_up.png
  inflating: unzipHTML/concepts/banner_background.png
.
.
.
  inflating: unzipHTML/tasks/t_your_password_has_expired.html
  inflating: unzipHTML/tasks/
t_your_user_id_and_password_were_not_accepted.html
  inflating: unzipHTML/tasks/t_your_user_id_is_already_being_used.html
  inflating: unzipHTML/tasks/t_you_must_change_your_password.html

File unzipped...
The Help files have been put into the required directory.
```

5. Go to the `/Tekelec/WebNMS/html/commandHelp` directory and check whether the directory for the new release is created or not.

```
$ cd /Tekelec/WebNMS/html/commandHelp

$ ls -ltr
```

Procedure to Install PHP Extension SSH2

1. Navigate to the following directory:

   ```
   cd /usr/local/src
   ```

   a. Download the following extension package:

      wget http://www.libssh2.org/snapshots/libssh2-1.6.1-20160109.tar.gz

   b. Untar/Unzip the extension package and enter the following in the directory:

      ```
      tar -zxvf libssh2-1.6.1-20160109.tar.gz
      cd libssh2-1.6.1-20160109
      ```

   c. Configure by providing a path to php-config:

      ```
      ./configure --with-php-config=/usr/local/bin/php-config
      ```

   d. Run its compilation and installation:

      ```
      make
      ```

      ```
      make install
      ```

2. Navigate to the following directory:

   ```
   cd /usr/local/src
   ```

   a. Download the extension package:

      wget http://pecl.php.net/get/ssh2-0.12.tgz

   b. Untar/Unzip the extension package and enter the following in the directory:

      ```
      tar -zxvf ssh2-0.12.tgz
      cd ssh2-0.12
      ```

   c. Run phpize:

```
phpize
```

d. Configure by providing a path to ssh2:

```
./configure --with-ssh2
```

e. Run its compilation and installation:

```
make
make install
```

3. Check if ssh2 extension is loaded by executing the following command:

```
php -m | grep ssh2
```

Expected output:

```
ssh2
```

B

OCEEMS System Administration

This appendix describes the GUI and text-based user interface that performs OCEEMS configuration and initialization.

Security Administration

The OCEEMS 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 OCEEMS 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 OCEEMS Workstation

The customer workstation serving as a client PC must meet certain criteria. For more information, see Hardware and Software Requirements.

Setting the Time Zone

If the time zone for OCEEMS 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).
2. Start the OCEEMS server by using the `service e5msService start` command.
3. Launch the OCEEMS client and perform resynchronization on a configured EAGLE.
4. Verify that the OCEEMS 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 OCEEMS server by using the `service e5msService stop` command.
7. Start the OCEEMS server by using the `service e5msService start` command.
8. Launch the OCEEMS client.

   Due to OCEEMS server restart, resynchronization is automatically triggered for the added EAGLE(s).
9. Validate that the OCEEMS timestamp on the Alarms GUI now reflects time zone *Y*.

Creating the OCEEMS SSL Certificate

To create the SSL certificate needed for HTTPS-based access for OCEEMS, 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@oceems8 bin]# cd /Tekelec/WebNMS/bin

[root@oceems8 bin]# sh E5MSCertificateCreationScript.sh

Welcome to OCEEMS SSL Certificate creation wizard!!!

Please provide OCEEMS 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. OCEEMS)-
(Must not be empty, permitted characters - alphanumeric, underscore, dot and
space): OCEEMS

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 OCEEMS root user's password (used for OCEEMS 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.
```

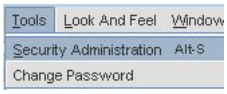
> **Note**
>
> The default OCEEMS root user password will be provided by the Support Team. For a fresh installation, that password should be supplied when asked in the script. For an upgrade scenario where the root user password has been changed by the customer, the updated password should be supplied when asked in the script.

Security Administration Screen

The OCEEMS security module is centered on providing excessive security to OCEEMS. 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 OCEEMS, they can access the Security Administration application by selecting the **Security Administration** option under the **Tools** menu on the OCEEMS client menu bar (or pressing**ALT+S** on the OCEEMS client window), as shown in Figure B-1.

Figure B-1 System Administration Tree Node



The Security Administration GUI will display, as shown in Figure B-2.

Figure B-2 Security Administration Screen

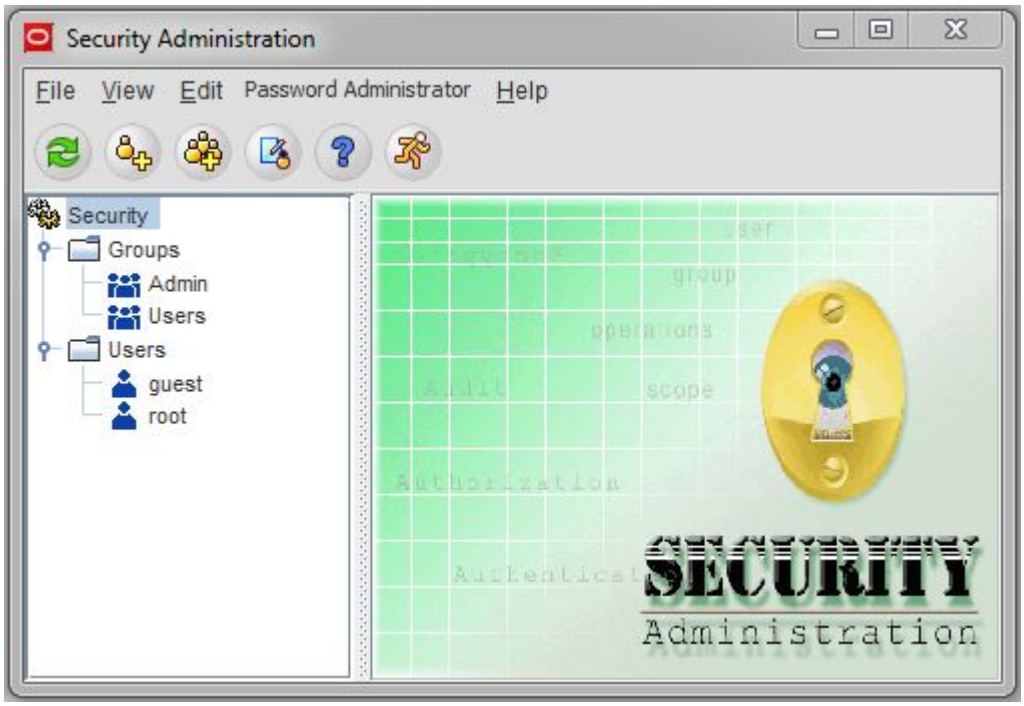
This page is accessed by the System Administrator to set Usergroup and User access permissions.

Management of Usergroups and Users

The Security Administration GUI provides the System Administrator with the ability to manage OCEEMS security. The OCEEMS administrator creates new usergroups or new users to control different security levels of the OCEEMS, by associating operations to usergroups. Once the user has logged in to the OCEEMS client, all the operations available to the user are based on the usergroup to which the user belongs. The OCEEMS administrator can configure various rules and constraints required to support password management in the OCEEMS through the Security Administration GUI. The following sections provide detailed descriptions of the OCEEMS 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 B-3 Security Administration Screen with Groups and Users



The System Administrator is responsible for adding and removing usergroups to and from the OCEEMS. A usergroup **Admin** will always exist in the OCEEMS, 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.

> **Note**
>
> While creating a usergroup under the security module, the EAGLE permissions are not applicable to the Alarms and Maps GUI. If the permission of Alarms and Maps is given to a particular usergroup, the users of that group are able to access Alarms and Map details of all the devices. The permission of the EAGLEs is only applicable to the CMI and Link Utilization module. The EAGLE selection option will be available only when a user selects any of these two modules.

Create a Usergroup

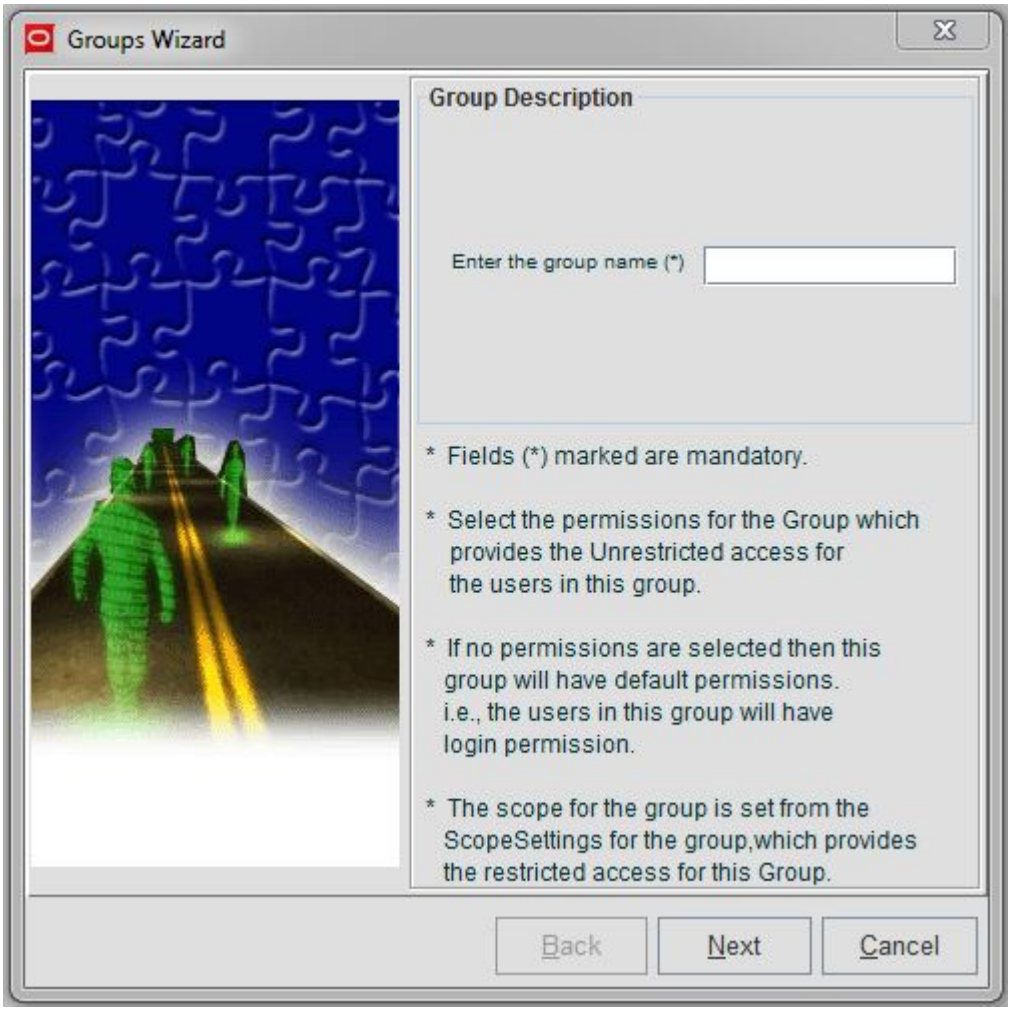
Only the **OCEEMS System Administrator**s can create **Usergroups**.

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 B-4 appears.

Figure B-4 Groups Wizard screen



2. Enter the name of the new **Usergroup** to be created in the **Enter the group name (*)** field.

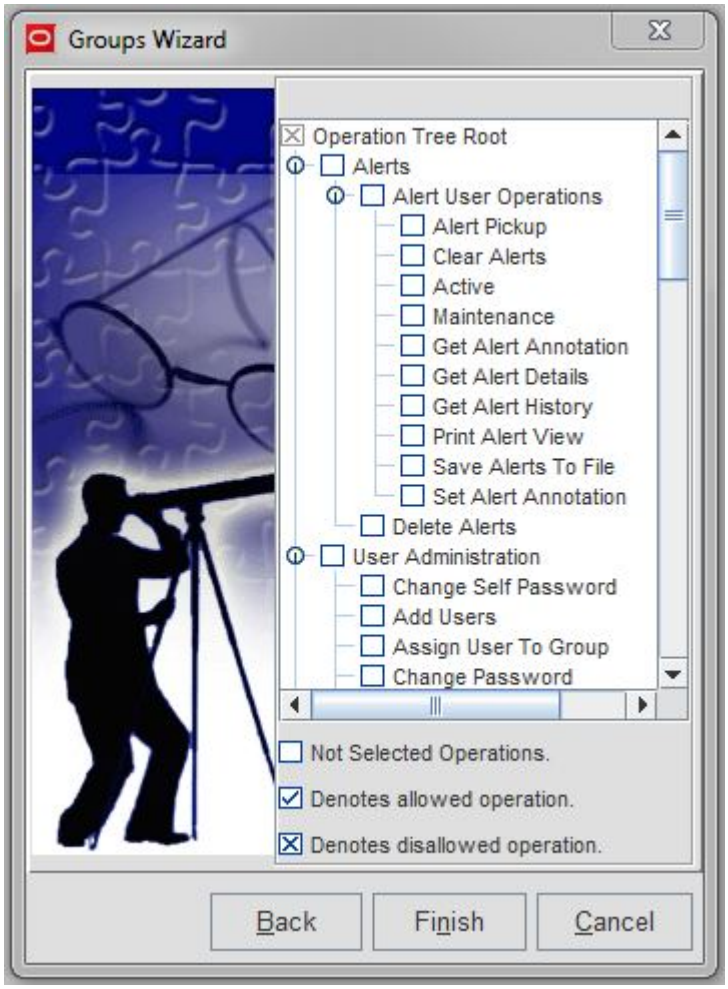
   The new **Usergroup** name must be unique within the OCEEMS. Existing Usergroup names are listed in the left pane under **Groups**. The new Usergroup name must meet the following constraints:

   - 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 B-5 is displayed.

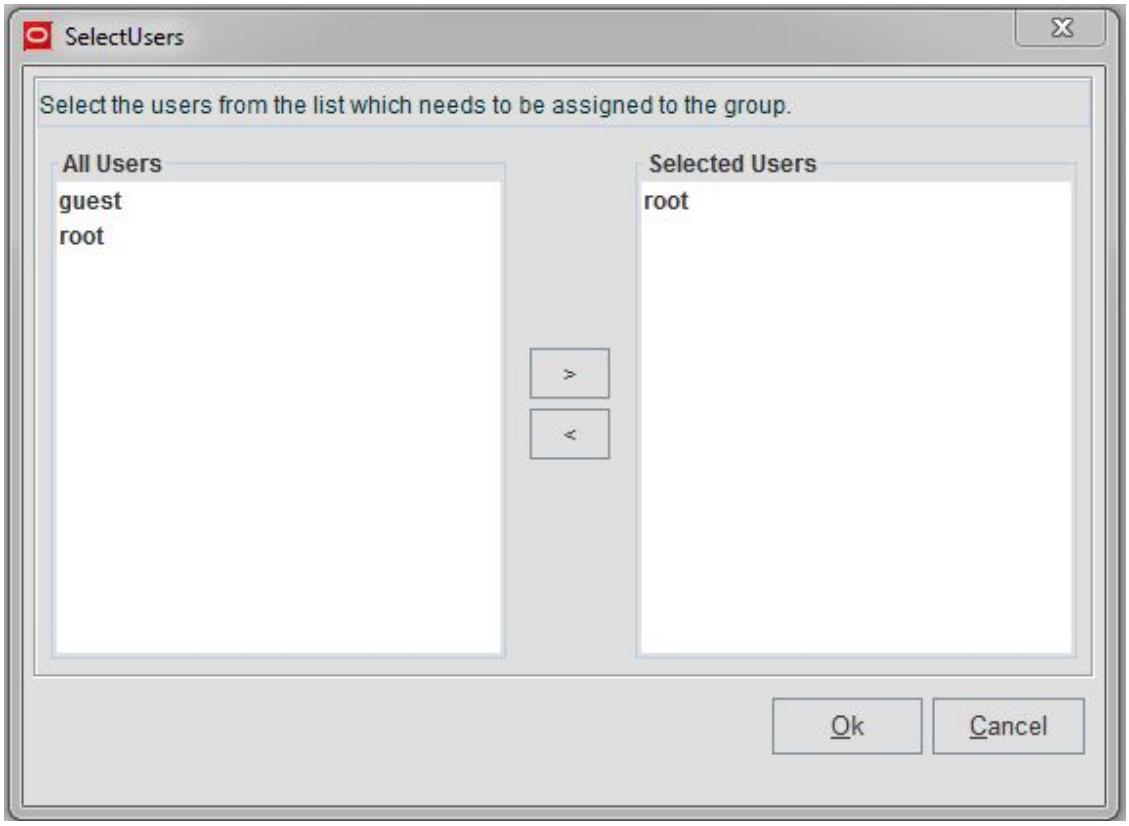
Figure B-5 Usergroup Attributes



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 B-6 Select Users



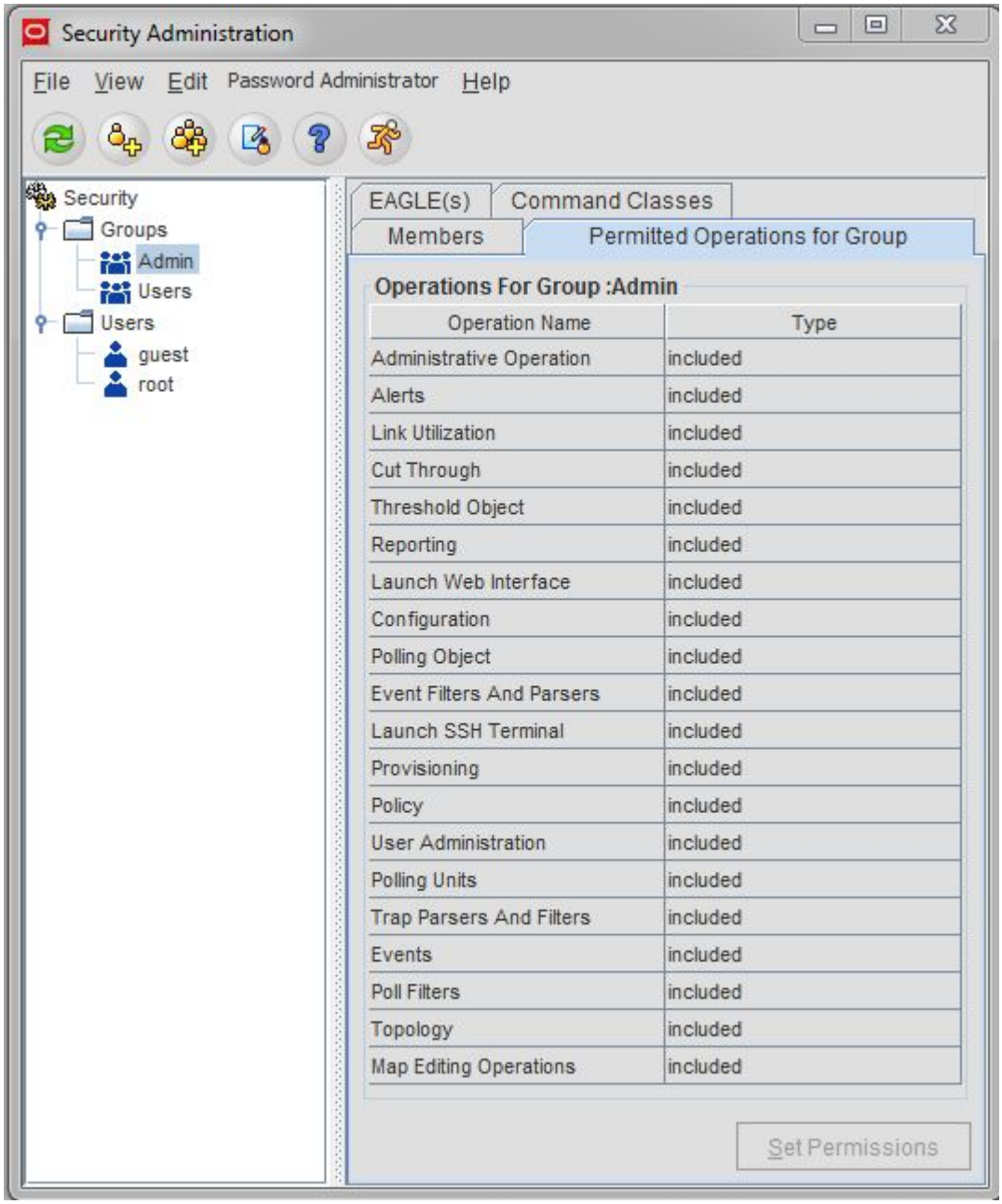
As shown in Figure B-6, all users are listed on the left side of the screen. The users assigned to the usergroup are listed on the right side of the screen. There are arrows in the middle to move users to the right or the left panes.

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 B-7.

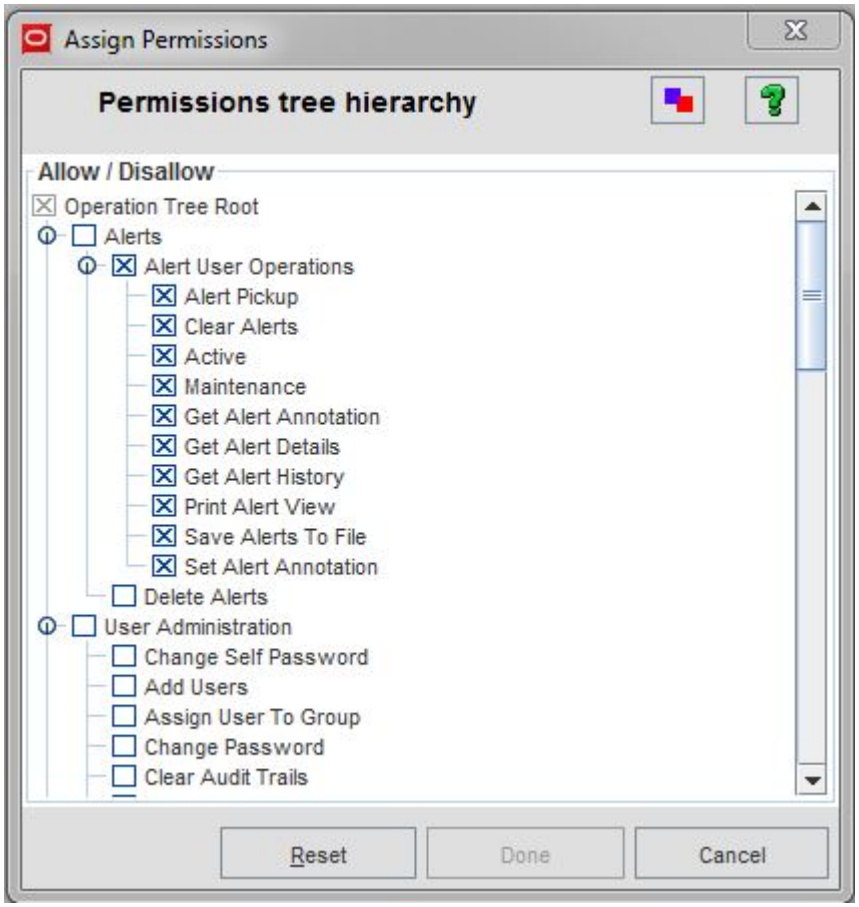
Figure B-7 Permitted Operations for Group



All OCEEMS 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 B-8.

Figure B-8 Assign Permissions Screen



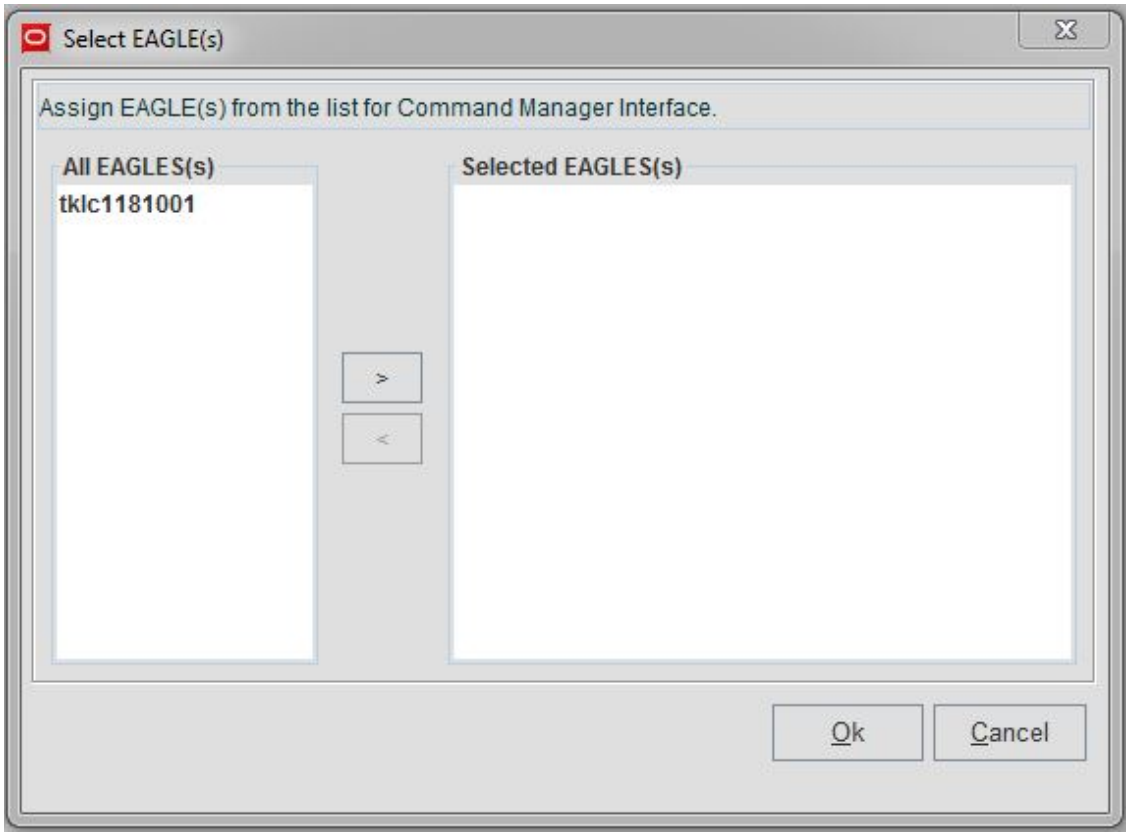
The Permissions tree hierarchy is logically arranged in a tree structure with parent and child operations under the Operation Tree Root. There are operations within the tree that are parent/child nodes, parent/child/child nodes, and operations without child nodes.

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 OCEEMS 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 B-9.

Figure B-9 Select EAGLE(s)



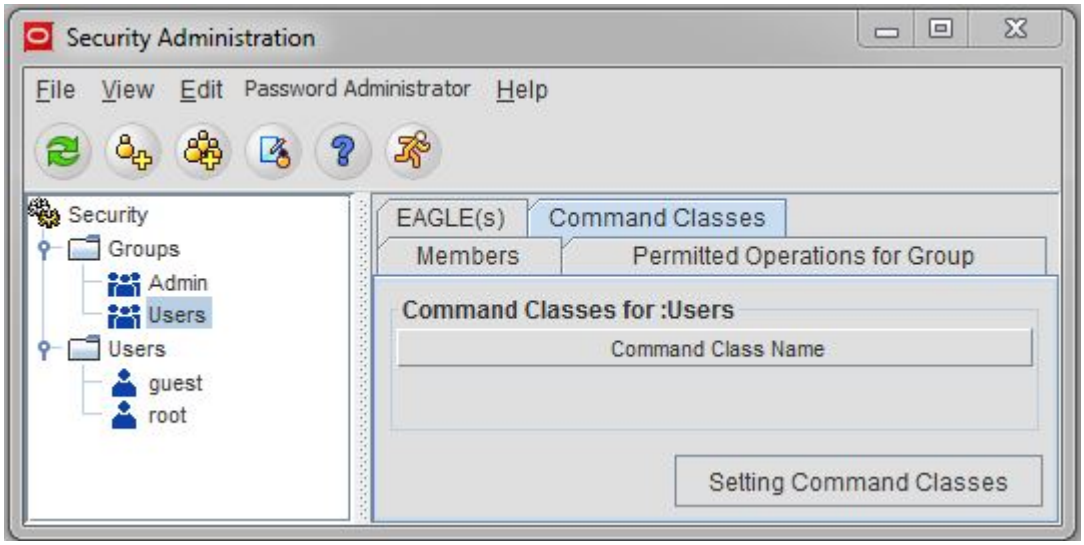
All EAGLEs within the client's network are listed on the left side of the screen. The EAGLEs assigned to the usergroup are listed on the right side of the screen. There are arrows in the middle to move an EAGLE to the right or the left panes.

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 B-10.

Figure B-10 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 OCEEMS 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 OCEEMS 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 OCEEMS user has access to the OCEEMS only if the user is associated with an OCEEMS usergroup. When the user belongs to the OCEEMS Administrator usergroup, they can perform all the OCEEMS operations. If the user does not belong to the OCEEMS 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

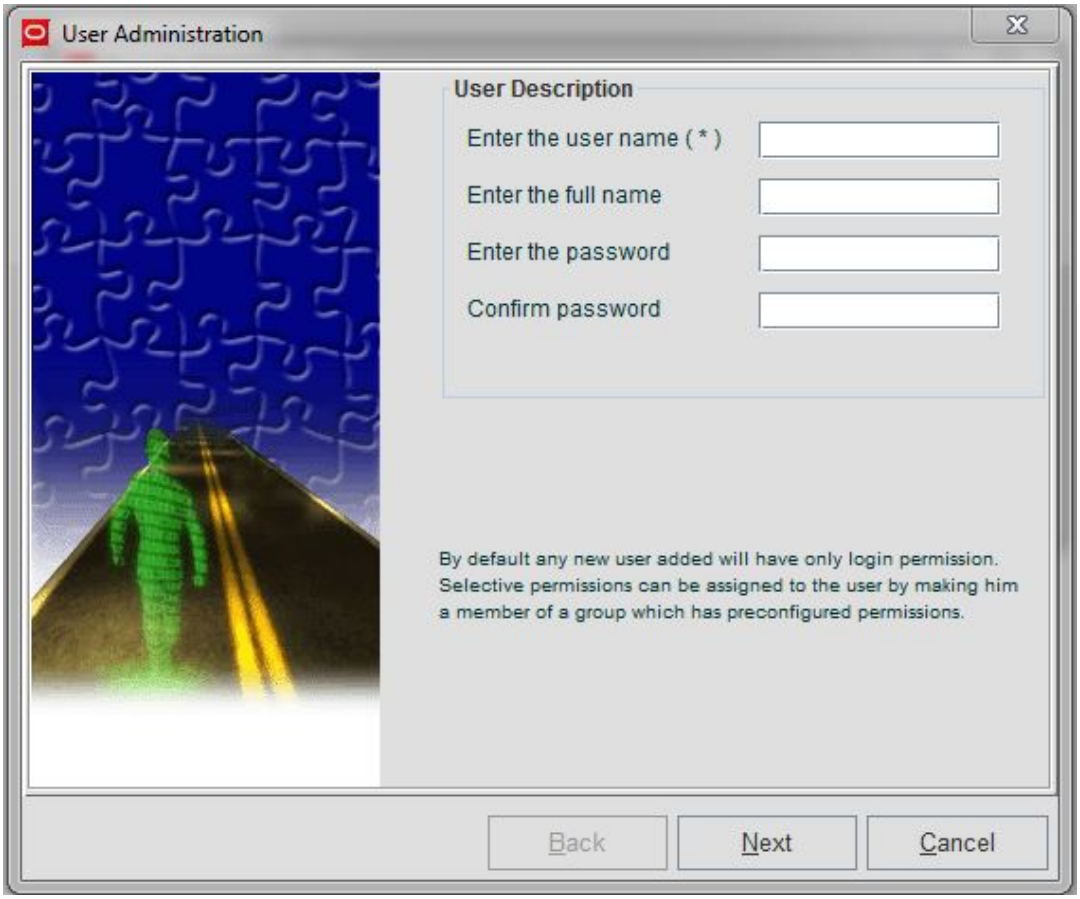
Only **OCEEMS System Administrator**s can add new **users**.

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 B-11 is displayed.

Figure B-11 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 OCEEMS. The **user** name must be unique within the OCEEMS. 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.

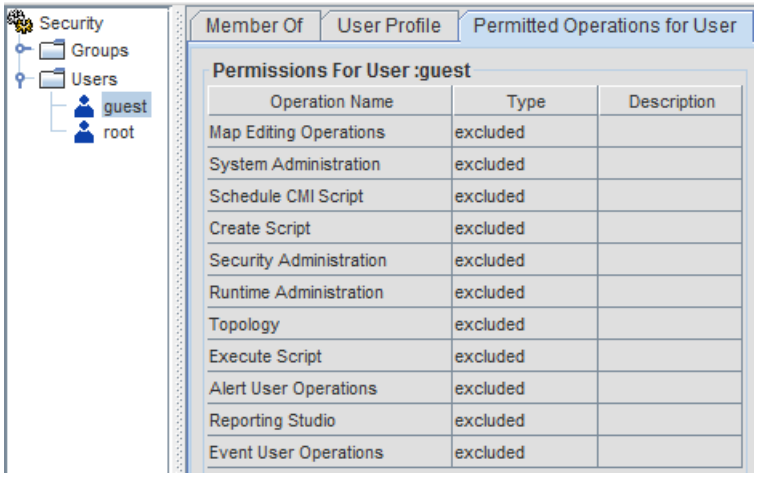
4. Create a password for the new user. All the password constraints configured by the administrator are applicable to the password being set for a new user. Only a password

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 B-12.

Figure B-12 Permitted Operations for User

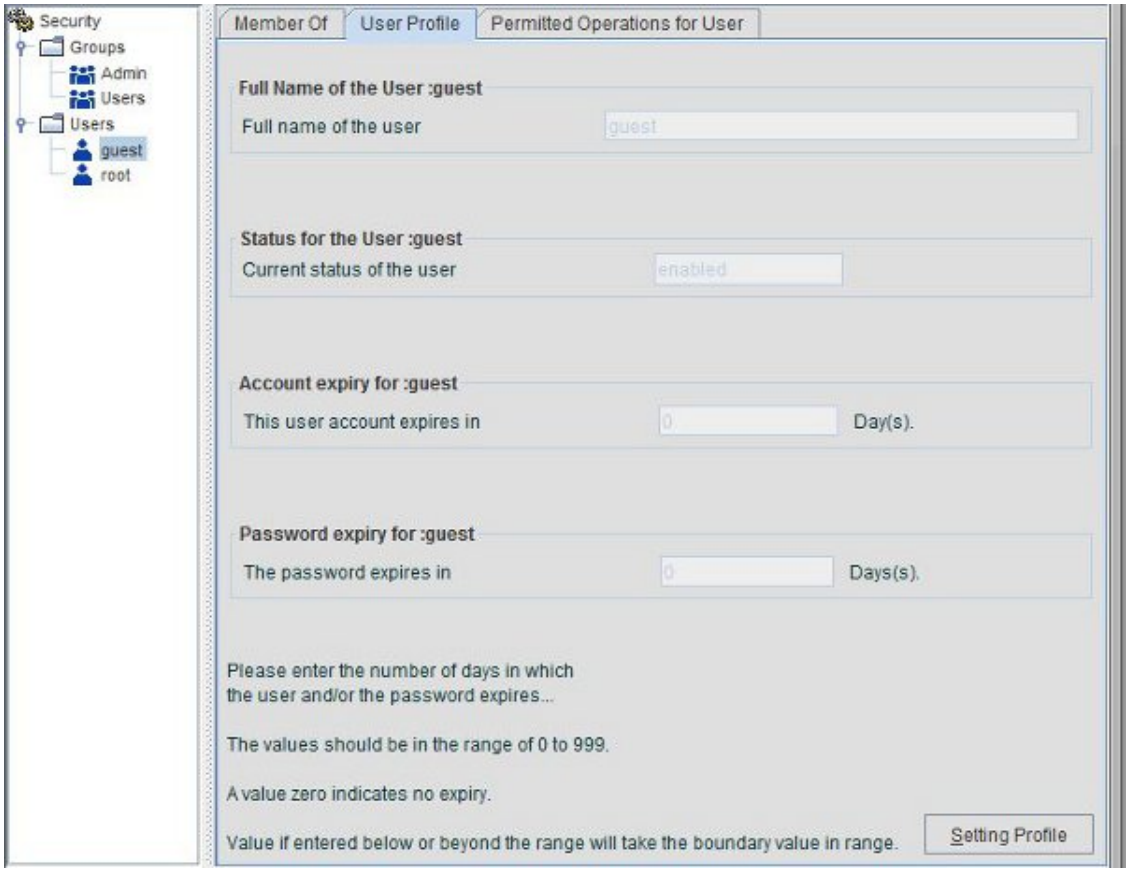


All OCEEMS operations are listed under Operation Name. The operations assigned to the user are listed as included and the operations discarded are excluded. Operation assignment to a user cannot be modified, since the operations of a user are set under usergroup operations.

Modify User Profile

This procedure describes how a System Administrator modifies a user profile.

Figure B-13 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 OCEEMS. By default, a user account and password never expire.

LDAP Client on OCEEMS

The LDAP Client on OCEEMS feature implements the Lightweight Directory Access Protocol (LDAP) client interface on the OCEEMS system to allow centralized user management and authentication. The LDAP protocol allows the authenticated clients to access the LDAP database and use the information to in turn authenticate users based on the information retrieved from the LDAP servers.

Figure B-14 Sample Call Flow for LDAP Authentication

OCEEMS supports the following modes of User Authentication:

1. OCEEMS Local Authentication: In this mode, the LDAP interface is not used and all information about the user is locally stored, including encrypted passwords.
2. LDAP authentication: In this mode, the LDAP interface is used for authentication. In case the LDAP server is unreachable, authentication will not be allowed.

See *Security Guide* for more information.

Configuring LDAP Client on EMS 47.0

Perform the following steps to configure LDAP Client on EMS 47.0.

1. Add the LDAP server details at the end of this file as shown in the following example: Open the file `vim /etc/hosts` and add `10.75.137.0 ldap.oceems.com` at the end.
2. Run the following command to install the prerequisites packages:

   ```
   yum install -y openldap-clients nss-pam-ldapd
   ```

   > **Note**
   >
   > Check “/etc/sssd” folder is created or not.

   If “/etc/sssd” folder is available, then continue. Else, run the following command:

   ```
   yum install sssd*
   ```

3. Stop and disable firewall in the client machine.

```
systemctl stop firewalld


systemctl disable firewalld


cd /etc/openldap/


makdir “cacerts”
```

4. Copy certificates and key from LDAP server to the client machine.

```
root@<Ldapserver IP>:/etc/openldap/certs/*.pem cacerts/
```

For example:

```
scp root@10.75.137.0:/etc/openldap/certs/*.pem cacerts/
ldapkey.pem  100% 1704 1.0MB/s 00:00
ldap.pem 100% 1407 1.0MB/s 00:00
```

> **Note**
>
> Verify certificate and key is copied to the client machine by running the following command:
>
> ```
> # ll  cacerts/
> Total 8
> -rw-r--r--. 1 root root 1704 Jul  5 03:38 ldapkey.pem
> -rw-------. 1 root root 1407 Jul  5 03:38 ldap.pem
> ```

5. Move to openldap folder.

```
cd /etc/openldap
```

6. Check the content.

```
drwxr-xr-x. 2 root root   6 Jul  2 19:07 certs
-rw-r--r--. 1 root root 900 Jul  2 19:07 ldap.conf
drwxr-xr-x. 2 root root 26 Jul  5 02:58 schema
```

7. Edit `ldap.conf` folder and the the Ldap server details at end of the file.

```
vim ldap.conf
```

Add the following:

```
TLS_CACERTDIR /etc/openldap/cacerts
TLS_CACERT   /etc/openldap/cacerts/ldap.pem
```

```
URI ldap://ldap.oceems.com
BASE dc=oceems, dc=com
```

8. Save and exit the file.
9. Run the following command:

   ```
   echo "TLS_REQCERT allow" >> /etc/openldap/ldap.conf
   ```

10. Edit the file "`/etc/nslcd.conf`" and add the following lines at the end of this files.

    ```
    vim /etc/nslcd.conf
    ```

    Update the following:

    ```
    uri ldap://127.0.0.1/ -> uri ldap://ldap.oceems.com
    base dc=example, dc=com - > base dc=oceems, dc=com
    ```

11. Save and exit the file.
12. Run the following command:

    ```
    echo "tls_reqcert allow" >> /etc/nslcd.conf
    ```

13. Navigate to the folder "`/etc/sssd/`"

> **Note**
>
> - This step is followed if the following file does not exist.
> - Check the content of the file that matches the below data.

```
cd /etc/sssd
```

a. Make the file `sssd.conf`:

   ```
   touch sssd.conf
   ```

b. Add the following line:

   ```
   [sssd]
   config_file_version = 2
   services = nss, pam, autofs
   domains = default

   [nss]
   homedir_substring = /home

   [pam]

   [domain/default]
   id_provider = ldap
   autofs_provider = ldap
   ```

```
auth_provider = ldap
chpass_provider = ldap
ldap_uri = ldap://ldap.oceems.com
ldap_search_base = dc=oceems,dc=com
ldap_id_use_start_tls = True
ldap_tls_cacertdir = /etc/openldap/cacerts
cache_credentials = True
ldap_tls_reqcert = allow
[autofs]
```

> **Note**
>
> i. Check ldapserver details as per available LDAP server.
>
> ii. Check ldapserver details as per available LDAP server.

14. Change the permissions on the `/etc/sssd/sssd.conf` file:

    ```
    chmod 600 /etc/sssd/sssd.conf
    ```

15. Update the configurations by running the following command:

    ```
    authconfig --enableldaptls --update
    ```

16. Navigate to `/etc/authselect/` and run the following command:

    ```
    cd /etc/authselect/
    ```

    a. Edit the file as shown below.

    ```
    vim user-nsswitch.conf
    ```

    b. Update the following lines:

    ```
    passwd:  files sss system   -> ldap files sss systemd
    shadow:   files sss.           -> ldap files sss
    group:    files sss system     -> ldap files sss systemd
    ```

17. Run the following command to apply the changes:

    ```
    authselect apply-changes
    ```

    For example:

    ```
    #authselect apply-changes
    ```
    Changes were successfully applied.

> **Note**
>
> a. Check if `nsswitch.conf` is updated after running the above command:
>
> b. Open the file and go to end of the file to check and change the the following line:
> `shadow: ldap files sss`

18. Run the following two commands:

    a. `service nslcd restart`

    b. `service sssd restart`

    Logs:

```
[root@EMS4 authselect] # service nslcd restart
Redirecting to /bin/systemctl restart nslcd.service
[root@EMS4 authselect] #
[root@EMS4 authselect]# service sssd restart
Redirecting to /bin/systemctl restart sssd.service
[root@EMS4 authselect] #
```

19. Confirm LDAP is configured correctly by running command:
    Confirmation 1:

```
Id <ldapserver username>
```

    Logs:

```
[root@EMS4 authselect] # id ldapuser1
uid=1001(ldapuser1) gid=1001(ldapuser1) groups=1001(ldapuser1)
[root@EMS4 authselect] #
```

> **Note**
>
> Bold output indicates that the LDAP server is configured successfully.

    Confirmation 2:

    Log in to the VM machine using LDAP username and password.

Password Management

OCEEMS security is centered on providing excessive security to OCEEMS. The OCEEMS 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. OCEEMS 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 OCEEMS 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 OCEEMS Administrator).
4. Password should not contain associated username.

The OCEEMS 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 OCEEMS 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 OCEEMS 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 OCEEMS 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 OCEEMS 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, OCEEMS manages two time period values:

- **Password expiry**
  The number of days (0 - 999) until a user password expires. This value is set separately by the OCEEMS Administrator for each OCEEMS user. Configuring a value of 0 disables the **Password expiry** for a user. The **Password expiry** can also be disabled by selecting the **Password never expires** option when a user profile is created/modified by the OCEEMS Administrator.
- **Password expiry notification period**
  The number of days (0 - 30) prior to expiration of the **Password expiry**, from which the OCEEMS starts notifying the user about their upcoming password expiration. This value is set once by the OCEEMS Administrator and applies to all users. Configuring a value of 0 disables the function.

If the days remaining in the **Password expiry** for a user is less than or equal to the **Password expiry notification period**, then warning messages are displayed after the user successfully logs in, indicating the number of days left before password expiration. Upon expiration of the **Password expiry**, 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 OCEEMS, 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 OCEEMS Administrator also configures a **User account expiry**. The **User account expiry** is the number of days (0 - 999) until the user's account expires and is set separately for each OCEEMS user. Configuring a value of 0 disables the **User account expiry** for a user. The **User account expiry** can also be disabled by selecting the **Account never expires** option when a user profile is created/modified by the OCEEMS Administrator. Upon expiration of the **User account expiry**, the user's account status is updated in the database to show the account has expired, and the user cannot log in to OCEEMS.

The OCEEMS Administrator can configure the number of previously used passwords (0 - 12) that a user cannot reuse as a new password by setting the **Number of old passwords that cannot be reused** option. This setting applies to all users. By default, the **Number of old passwords that cannot be reused** option is disabled (a value of 0 is used). Up to 12 most recently used passwords for every user can be encrypted and stored in the database. When a user password is modified, the encrypted password string is compared with the previously encrypted user password strings for that user, and if the new string matches any of the stored strings, the new password is rejected and an error message is displayed.

The OCEEMS Administrator can configure a **Minimum change interval for password** (0 - 30 days) for OCEEMS users. This setting applies to all users, and specifies that an OCEEMS 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. A user can contact the OCEEMS Administrator if they need to change their password more than once during this period. The default is 0 days, which disables the function.

User Status Icons

OCEEMS provides the Administrator status icon of the user in the User Tree in security Administration window.

Icon	Description
	User account is enabled.

Icon	Description
	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 OCEEMS System Administrator responsible for all the Usergroups and User access levels. The System Administrator will have access to all management operations.

System Administrator Login

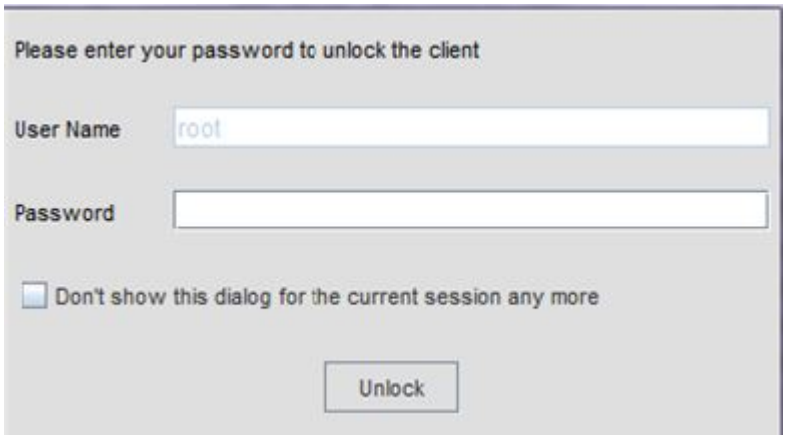
Once the OCEEMS is launched, the System Administrator is prompted at the E5-MS Authentication Screen to login. They will use **root** as the User ID and the password provided by the Support Team.

When an OCEEMS user logs in to OCEEMS for the first time after the user has been created by the administrator, the OCEEMS user is required to change their password to continue their login to OCEEMS. Once their password has been successfully modified, the user can then continue their login to OCEEMS.

An OCEEMS Administrator can configure the maximum permissible number of wrong login attempts that can be made by an OCEEMS 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 OCEEMS 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 OCEEMS, and an attempt to do so results in an error message on the GUI. An OCEEMS Administrator can disable the enforcement of this rule for all OCEEMS 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 OCEEMS 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 OCEEMS. Once logged-in, the user can continue their OCEEMS session.

Figure B-15 Lock Screen



An OCEEMS 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 OCEEMS session. The lockout time is less than the termination time, but if the administrator configures a termination time less than the lockout time, than the lockout functionality will not be in effect, and only the termination time is used.

An OCEEMS Administrator can disable the login rights of another OCEEMS user (except OCEEMS Administrators) through the GUI interface. An OCEEMS Administrator can disable a user while modifying the user's profile through the Security administrator window. When a user is disabled by an OCEEMS 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 OCEEMS because the login rights of that user are disabled. An attempt to do so results in an error message on the GUI. When an OCEEMS Administrator disables a user who is already logged in, the user is logged out of OCEEMS and prompted with a corresponding message. Also, an OCEEMS 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 OCEEMS 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.

Figure B-16 Password Composition

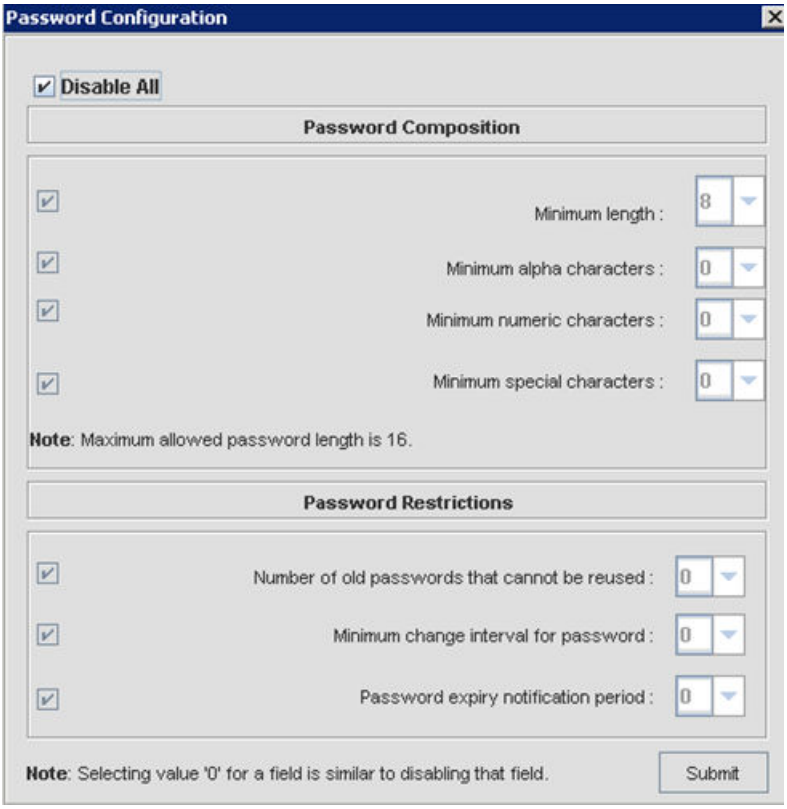
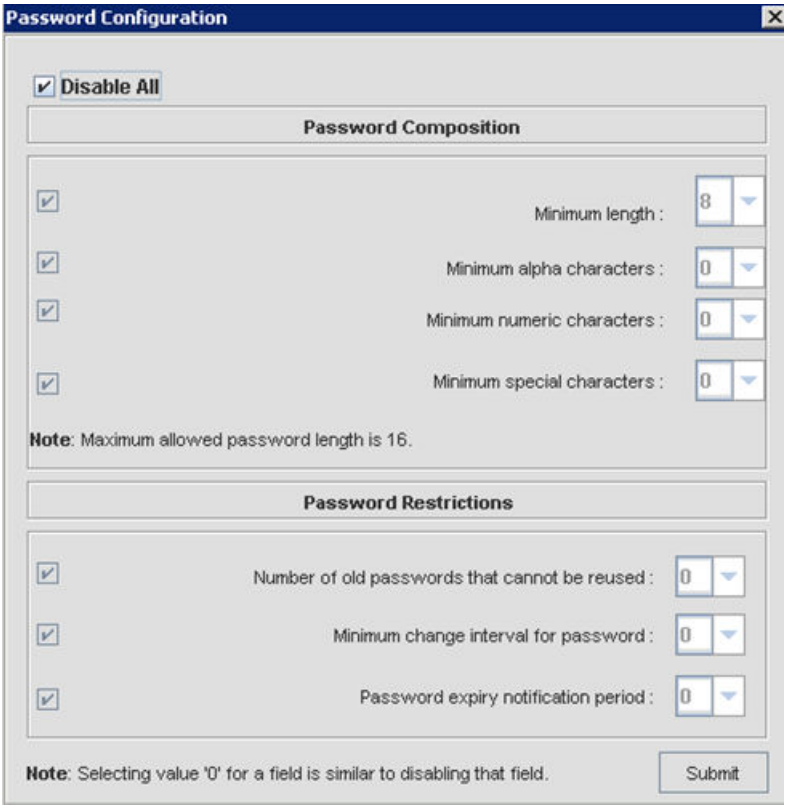


Figure B-17 Password Restrictions



Password Composition Section

In the 'Password Composition' section, an OCEEMS 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 OCEEMS 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 OCEEMS 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 OCEEMS 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 OCEEMS 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 OCEEMS Administrator.
2. When the minimum length constraint is disabled by an OCEEMS Administrator and the total count of minimum required alpha, numeric, and special characters exceeds the maximum allowed password length (16).

Updating the System User and Password for OCEEMS

This procedure describes how to change the system user and its password for OCEEMS. Execute the `/Tekelec/WebNMS/bin/E5MSConfigurationScript.sh` script:

```
[emsadmuser@pc9091801 bin]$ sh E5MSConfigurationScript.sh
Please enter OCEEMS home path (Absolute path till 'WebNMS' directory): /
Tekelec/WebNMS
Press 1 To update current system username and password in OCEEMS
2 To update current mysql root user's password in OCEEMS
3 To ExitYour Choice (1, 2 or 3): 1
Enter Username (e.g. emsadmuser): emsadmuser
Enter Password:Do you want to proceed with the entered username and password?
(y/n): y
Username and Password updated successfully in OCEEMS.
```

> **Note**
>
> If the OCEEMS server is already running when this procedure is applied, a restart of OCEEMS is required for the change to be effective. Use the following command to restart OCEEMS:
>
> ```
> service e5msService restart
> ```

MySQL Root User Password Change for Standalone Server

This procedure describes how to change the MySQL root user's password for a standalone server.

1. Shut down the OCEEMS 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:

   a. Log in to MySQL as the root user with its current password:

   ```
   -bash-4.2# ./mysql -uroot -p
   Enter password:
   Welcome to the MySQL monitor. Commands end with ; or \g.
   Your MySQL connection id is 10125
   Server version: 8.0.3-rc-log MySQL Community Server (GPL)

   Copyright (c) 2000, 2017, 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.

   Type 'help;' or '\h' for help. Type '\c' to clear the current input
   statement.
   ```

   b. Set mysql as the database:

   ```
   mysql> use mysql;
   ```

   c. Set the new password for the root user and flush:

   ```
   mysql> SET PASSWORD FOR 'root'@'localhost' = PASSWORD('<Your
   password>');
   Query OK, 0 rows affected (0.00 sec)
   mysql> FLUSH PRIVILEGES;
   Query OK, 0 rows affected (0.00 sec)
   ```

   d. 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@oceems-12 bin]# sh stopMySQL.sh
   Enter Password:
   STOPPING server from pid file /Tekelec/WebNMS/mysql/data/oceems-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 OCEEMS:

```
# sh E5MSConfigurationScript.sh
Please enter OCEEMS home path.(Absolute path till WebNMS directory)
/Tekelec/WebNMS/
Press 1 To update current system username and password in OCEEMS
2 To update current mysql root user's password in OCEEMS
3 To Exit
Your Choice (1, 2 or 3): 2
Enter new password for MySQL root user: *****
Do you want to proceed with the entered password? (y/n) y
MySQL Password updated successfully.
```

6. Start the OCEEMS server:

```
service e5msService start
```

MySQL Root User 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:
   a. Log in to MySQL as the root user using its current password:

```
-bash-4.2# ./mysql -uroot -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 10125
Server version: 8.0.3-rc-log MySQL Community Server (GPL)

Copyright (c) 2000, 2017, 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.

Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.
```

   b. `STOP SLAVE;`
   c. `RESET SLAVE;`
   d. `QUIT`
2. Shut down the standby server and then the primary server by using the following command:

```
# service e5msService stop
Stopping OCEEMS server...
```

```
MySQL not stopped for failover
Done.
```

3. On each server, follow steps 3 to 5 in MySQL Root User 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 after Fresh Installation 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
   ```

Account Recovery

The OCEEMS 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 OCEEMS administrator, or when the password has expired. An OCEEMS 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 OCEEMS administrator is able to log in to OCEEMS because of password expiration or account locking, contact () for password recovery.a password recovery mechanism is provided by Oracle Support to recover the OCEEMS Administrator 'root' account.

C

OCEEMS Backup and Restore

This appendix describes the configuration and execution of backup and restore for the OCEEMS.

Overview

OCEEMS is used to manage and monitor EAGLE, EPAP, and LSMS nodes in the network. OCEEMS 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. OCEEMS 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 (for example emsadmuser) involved in the installation and configuration of OCEEMS will manage the setup of 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 OCEEMS system to the previous configured state.

Restore uses a previously generated backup, bring the OCEEMS system back to a state when the backup was generated.

System Requirement

Backup shall approximately require space equivalent to 100 MB + size of OCEEMS database dump file. The size of OCEEMS database dump file shall depend upon the size of OCEEMS database. OCEEMS database size shall be variable depending upon the number of EAGLEs being managed i.e. database size shall grow on the basis of deployed OCEEMS configuration (Small, Medium, or Large).

Backup in OCEEMS

Backup of the OCEEMS 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 OCEEMS can be restored to a state close to the disaster point.

By default, automatic (scheduled) backup of OCEEMS 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 OCEEMS state. As part of backup following OCEEMS 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**
>
> It is suggested not to modify the content of files or directories to be backedup to ensure that the upgrade process does not get impacted.

Automatic Backup

Configuration for Automatic Backup

The default configuration for automatic backup in OCEEMS is given in /Tekelec/WebNMS/conf/BackUp.conf file. It is shown below:

```
<BACKUP
className="jdbc.MysqldumpBackup"
HOUR="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:

```
HOUR="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 OCEEMS home (`/Tekelec/WebNMS`). This is to ensure that the backup is not deleted in case of un-installation of OCEEMS RPM.

Default Backup Destination

By default, the OCEEMS 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 OCEEMS will be taken
BACKUP_DESTINATION /var/backup
```

Manual Backup

A system user (for example, emsadmuser) with privileges to run `/Tekelec/WebNMS/bin/backup/BackupDB.sh` script will have the ability to take manual backup of OCEEMS. The location where the backup will be generated can also be controlled by the user.

Manual backup on the default location

Manual backup of OCEEMS for the default backup location /var/backup can be taken using the command given below:

```
[emsadmuser@EMS1 ~] 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.

```
[emsadmuser@EMS1 ~]  sh /Tekelec/WebNMS/bin/backup/BackupDB.sh -d <Backup
location>
```

For example:

```
[emsadmuser@EMS1 ~] sh /Tekelec/WebNMS/bin/backup/BackupDB.sh -d  /var/
manual_backup
```

The above command will generate a backup at location /var/tklc/backup.

The directory where a manual backup would take place will have write permissions to the `emsadm` group as the system user (for example `emsadmuser`) who will take the backup belongs to the `emsadmgroup`. For example, to make `/var/manual_backup` as the directory to create a manual backup, run the following commands:

```
#mkdir /var/manual_backup
#chown root:emsadm /var/manual_backup
#chmod 770 /var/manual_backup
Check the permission.
# ls -l /var
drwxrwx---.  2 root emsadm    6 Aug 24 10:51 manual_backup
```

> **Note**
>
> While making the directory for a manual backup at a desired location, choose a partition where enough space is available to create the manual 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 OCEEMS 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.

OCEEMS 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	<BACKUP className="jdbc.MysqldumpBackup" DAILY="true" />
Weekly	<BACKUP className="jdbc.MysqldumpBackup" WEEKLY="true" />
Hour and Day_of_the_Week	This parameter deals with two values - HOUR and DAY. The value for HOUR can be specified in comma separated form. The value can be any number from 1 to 24 (representing 24 hours). 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. For example, if backup is needed on Monday and Wednesday, it can be specified as shown below: **Example:** <BACKUP className="jdbc.MysqldumpBackup" HOUR="3,7" DAY_OF_THE_WEEK="MON,WED" />
Hour and Day_of_the_Month	HOUR has to be specified as a list. For example, 2,5,22. It must be between 1 and 24. DAY_OF_THE_MONTH has to be given as a range (starting from 1 to a maximum of 31). The value of "*" is ALL. **Example:** To perform backup at HOUR 3,7 and DAY_OF_THE_MONTH 10-20 - <BACKUP className="jdbc.MysqldumpBackup" HOUR="3,7" DAY_OF_THE_MONTH="10-20" />

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 extenal 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 OCEEMS 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 OCEEMS database. OCEEMS database size shall be variable depending upon the number of EAGLEs being managed i.e. the deployed OCEEMS 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	OCEEMS Backup	Backup is in progress
Backup completes successfully	SYSTEM	Backup Service	<time>	SUCCESS	OCEEMS Backup	Backup is completed
Backup creation fails	SYSTEM	Backup Service	<time>	FAILURE	OCEEMS Backup	Backup creation failed
Backup creation fails because of non-availability of space on backup location	SYSTEM	Backup Service	<time>	FAILURE	OCEEMS 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	OCEEMS 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

```
[emsadmuser@EMS1 ~] sh /Tekelec/WebNMS/bin/backup/BackupDB.sh -d /var/
manual_backup


Please wait! Backup of OCEEMS is in progress...-


OCEEMS database backup file "OCEEMS_Database_BackUp.sql"
successfully created.


Backup of directories successfully created.


OCEEMS Backup is completed.
```

Output while Restoring from a Backup

```
[emsadmuser@EMS1 ~] sh RestoreDB.sh /var/backup/
OCEEMS_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 OCEEMS database from the dump
file: /var/backup/OCEEMS_Database_BackUp.sql


OCEEMS database restoration in progress...

Successfully restored OCEEMS database.

The following files will be restored now to OCEEMS:

/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/tl1browsermenu.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/tl1browsermenu.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/scr1.bsh
/Tekelec/WebNMS//Tekelec/WebNMS/commandManagerScripts/usr4/cat1
/Tekelec/WebNMS/commandManagerScripts/usr4/cat1/scr1.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

OCEEMS successfully restored.
```

Restore in OCEEMS

How to Restore from Existing Backup

A system user (For Example emsadmuser) with privileges to run `/Tekelec/WebNMS/bin/backup/RestoreDB.sh` script will have the ability to restore OCEEMS system to a previous state by using the backup generated earlier. Before restoring the contents, OCEEMS server must be shut down. This is because the restore script deletes the database tables and re\u0002creates them using the database backup file.

> **Note**
>
> If backup is taken on EMS 46.6.x and restored on EMS 47.0, then the following must be considered:
>
> Steps 13-15 must be followed from EMS Install/Upgrade Guide 47.0, Section 4.0 - UPGRADE PROCEDURE (STANDALONE/FAILOVER SERVER).

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:

```
[emsadmuser@EMS1 ~]  sh /Tekelec/WebNMS/bin/backup/RestoreDB.sh
<absolute path of database backup file>
```

Note that the path of database backup file provided while running the restore script must also have the other configuration files backed up by OCEEMS. The default location of backup automatically has all the content backed up by OCEEMS as shown below.

- /var/backup/Classes
- /var/backup/commandManagerScripts
- /var/backup/conf
- /var/backup/defaultconf
- /var/backup/html
- /var/backup/linkUtilizationScripts

- /var/backup/reportingStudio
- /var/backup/users
- /var/backup/E5MS_Database_BackUp.sql

In case, user wishes to provide a location of the backup file that is different from the default location, s/he must first verify that the location has all the contents mentioned above. In case the non-default location does not have all the contents, then the user should first copy the contents from the default location to the non-default location and then proceed with restoration.

For example, for restoring from default backup following command can be issued:

```
[emsadmuser@EMS1 ~]  sh /Tekelec/WebNMS/bin/backup/RestoreDB.sh
/var/backup/E5MS_Database_BackUp.sql
```

Sample output of restore script 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.

- Database Tables

  ```
  <RESTORE="ALL"
                DYNAMIC TABLES="true"
                SKIP_INDEX="TRUE">
  </RESTORE>
  ```

  The above statement means restoring all the database tables present in the database backup file.

- Configuration

The significance of the entries in the above configuration in the TablesToRestore.conf file is explained below: 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/securitydbData.xml,conf/
clientp
arameters.conf,classes/hbnlib/hibernate.cfg.xml,classes/hbnlib/secondary/
hibernate
.cfg.xml,conf/transportProvider.conf,conf/trapport.conf,conf/
NmsProcessesBE.conf,c
onf/serverparameters.conf,conf/SmartUpdateManager.xml,html/
NMSSocketPort.html">
</FILES_TO_RESTORE>
```

The above statement means restoring all the files listed in ‘FILE_NAMES’ tag and all the directories listed in ‘DIR_NAMES’ tag respectively.

Time taken in Restore

The time taken by restore process shall depend upon the size of OCEEMS backup. The size of backup will in turn depend upon the size of OCEEMS database backup file. Restoration will approximately take few minutes (for example, 10 to 15 minutes for small database) or more depending upon the size of backup.

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 C-1 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 OCEEMS backup.
/Tekelec/WebNMS/bin/backup/ResotreDB.sh	Script to be used to restore the OCEEMS from a previously generated backup.
/Tekelec/Web NMS/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.

D

OCEEMS Failover

This appendix describes the failover for the OCEEMS.

Overview

In OCEEMS, 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 OCEEMS 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 OCEEMS server databases before implementing failover. Refer to How to Set Up Failover after Fresh Installation 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 OCEEMS 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 OCEEMS.

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, OCEEMS 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 <password>
```

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

.

Failover Alarms

Failover alarms are raised for client switchover and when database replication is not working.

Client Switchover Alarm

When client switchover from the primary server to the standby server occurs, a minor alarm is raised. Subsequent client switchover occurrences increase the count and modify the existing switchover alarm. When the switchover alarm is raised, the following alarm details are displayed:

Element	Description
Category	Failover
Severity	Minor
Resource	OCEEMS
Entity	OCEEMS_Client_Switchover
Message	OCEEMS client switchover complete. New primary server is <Primary / Standby IP Address>
OCEEMS Timestamp	For example, May 27,2015 02:48:10

This alarm must be manually cleared. The following details are displayed in the event GUI for the clear event:

Element	Description
Category	Failover
Severity	Clear
Resource	OCEEMS
Entity	OCEEMS_Client_Switchover
Message	Alarm cleared by OCEEMS user <username>.
OCEEMS Timestamp	For example, May 27,2015 02:48:10

Database Replication Broken Alarm

When database replication is broken between the servers, a major alarm is raised. If the alarm is not cleared, subsequent replication status checks (scan interval is 20 seconds) do not raise an alarm or increase the alarm count, so that multiple events will not fill the network events GUI and database table. Following are the replication alarm details shown on the alarm GUI:

Element	Description
Category	Failover
Severity	Major
Resource	OCEEMS
Entity	OCEEMS_Database_Replication

Element	Description
Message	OCEEMS database replication is broken
OCEEMS Timestamp	For example, May 27,2015 02:48:10

The database replication alarm is cleared automatically when replication is reestablished between the servers. The following details are displayed in the event GUI for the clear event:

Element	Description
Category	Failover
Severity	Clear
Resource	OCEEMS
Entity	OCEEMS_Database_Replication
Message	OCEEMS database replication is broken
OCEEMS Timestamp	For example, May 27,2015 02:48:10

Files and Location in FAILOVER

The following files are used for failover process.

Directory/File	Description
/Tekelec/WebNMS/bin/startnms.sh	The script file is used to start OCEEMS server. For failover, the value of a property - Djava.awt.headless is modified from - Djava.awt.headless=**false** to - Djava.awt.headless=**true**. This change has already been done in the file and no manual changes are required while creating failover setup. For more details, visit: http://www.oracle.com/technetwork/articles/javase/headless-136834.html
/Tekelec/WebNMS/bin/startMySql.sh	The script file is used to pass arguments to the MySQL server that are necessary to implement database replication. 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 after Fresh Installation.
/Tekelec/WebNMS/conf/ serverparameters.conf	A property **DB_REPLICATION** with value **true** has been added to this file to enable database replication for OCEEMS. No manual changes are required for this file during the failover setup procedure.

Directory/File	Description

/Tekelec/WebNMS/conf/Failover.xml	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.
	The OCEEMS configuration files/directories which are to be backed up are also specified in this file as follows:
	
	`<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>`

Note

Any changes made in the Failover.xml file would be effective only after server restart.

Directory/File	Description
/Tekelec/WebNMS/classes/hbnlib/ hibernate.cfg.xml	The following c3p0 entries have been un-commented: **<property name="hibernate.c3p0.acquireRetryAttempts">2</property>** **<property name="hibernate.c3p0.acquireRetryDelay">3000</property>** **<property name="hibernate.c3p0.breakAfterAcquireFailure">false</property>** 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 after Fresh Installation. **<property name="connection.url">jdbc:mysql://*localhost* /WebNmsDB?dumpQueriesOnException=true&jdbcCompliantTruncation=false</property>**
/Tekelec/WebNMS/classes/hbnlib/ secondary/ hibernate.cfg.xml	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.
/Tekelec/WebNMS/jre/lib/security/ java.policy	The following entries have been appended to the file: **permission java.awt.AWTPermission "*";** **permission java.security.SecurityPermission "createAccessControlContext";** **permission java.net.SocketPermission "*:1024-65535","connect,accept,resolve,listen";** For details go to: http://docs.oracle.com/javase/1.5.0/docs/guide/security/permissions.html
/var/E5-MS/failover/logs/failover.txt	Failover-related log for client switchover and database replication broken alarms.

Failover Setup

To set up failover between the primary and standby servers, database replication is a must. To enable DB replication, one needs to set up various global parameters. Also, changes need to be done in OCEEMS for establishing failover between the primary and standby servers.

How to Set Up Failover after Fresh Installation

For setting up failover after a fresh installation, 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:

- Login credentials of the non-root system user for OCEEMS on both the primary and standby servers.
- MySQL root user's password for both the primary and standby servers.

- 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.
- MySQL replication user name and its password on the primary server. In the following procedure, these values are called **<primary replication user>** and **<primary replication user password>** respectively.
- MySQL replication user name and its password on the standby server. In the following procedure, these values are called **<standby replication user>** and **<standby replication user password>** respectively.

1. Log into the primary OCEEMS server using the non-root system user for OCEEMS.
2. Update the `hibernate.cfg.xml` file in the `/Tekelec/WebNMS/classes/hbnlib` directory and replace the **localhost** value in the following statement with the hostname of the primary server:

   ```
   <property name="connection.url">jdbc:mysql://localhost/WebNmsDB?dump
   QueriesOnException=true&jdbcCompliantTruncation=false
   </property>

   For example:

   <property name="connection.url">jdbc:mysql://e5ms1/WebNmsDB?dump
   QueriesOnException=true&jdbcCompliantTruncation=false
   </property>
   ```

3. Move to directory `/Tekelec/WebNMS/bin`:

   ```
   $ cd /Tekelec/WebNMS/bin
   ```

4. 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**.
5. 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
   ```

6. Move to the `/Tekelec/WebNMS/mysql/bin` directory:

   ```
   $ cd /Tekelec/WebNMS/mysql/bin
   ```

7. 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.

   ```
   -bash-4.2# ./mysql -uroot -p
   Enter password:
   Welcome to the MySQL monitor. Commands end with ; or \g.
   Your MySQL connection id is 10125
   Server version: 8.0.3-rc-log MySQL Community Server (GPL)
   ```

```
Copyright (c) 2000, 2017, 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.

Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.
```

8. Log into the standby OCEEMS server using the non-root system user for OCEEMS.
9. Update the `hibernate.cfg.xml` file in the `/Tekelec/WebNMS/classes/hbnlib` directory and replace the **localhost** value in the following statement with the hostname of the standby server:

```
<property name="connection.url">jdbc:mysql://localhost/WebNmsDB?dump
QueriesOnException=true&jdbcCompliantTruncation=false
</property>

For example:

<property name="connection.url">jdbc:mysql://e5ms2/WebNmsDB?dump
QueriesOnException=true&jdbcCompliantTruncation=false
</property>
```

10. Move to directory `/Tekelec/WebNMS/bin`:

```
$ cd /Tekelec/WebNMS/bin
```

11. 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.
12. 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
```

13. Move to the `/Tekelec/WebNMS/mysql/bin` directory:

```
$ cd /Tekelec/WebNMS/mysql/bin
```

14. 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.

```
-bash-4.2# ./mysql -uroot -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 10125
Server version: 8.0.3-rc-log MySQL Community Server (GPL)
```

```
Copyright (c) 2000, 2017, 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.

Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.
```

15. On the MySQL session opened in step 7 on the primary server, execute the following five MySQL commands.

> **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;
```

16. On the MySQL session opened in step 14 on the standby server, execute the following five MySQL commands.

> **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;
```

17. 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.000002 |      973 | 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>**.

18. 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>**.

19. 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;
```

20. 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;
```

21. 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 follwing is displayed -
*************************** 1. row ***************************
               Slave_IO_State: Waiting for master to send event
                  Master_Host: e5ms1
                  Master_User: primary
                  Master_Port: 3306
                Connect_Retry: 60
              Master_Log_File: log-bin.000002
          Read_Master_Log_Pos: 120
               Relay_Log_File: relay-bin.000002
                Relay_Log_Pos: 149415
        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: 149254
              Relay_Log_Space: 229712
              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: 770
Master_SSL_Verify_Server_Cert: No
                Last_IO_Errno: 0
                Last_IO_Error:
               Last_SQL_Errno: 0
               Last_SQL_Error:
  Replicate_Ignore_Server_Ids:
             Master_Server_Id: 1
                  Master_UUID: 836db629-e017-11e3-b81f-00151a6e0499
             Master_Info_File: /Tekelec/WebNMS/mysql/data/master.info
                    SQL_Delay: 0
          SQL_Remaining_Delay: NULL
      Slave_SQL_Running_State: creating table
           Master_Retry_Count: 86400
                  Master_Bind:
```

```
      Last_IO_Error_Timestamp:
     Last_SQL_Error_Timestamp:
               Master_SSL_Crl:
           Master_SSL_Crlpath:
           Retrieved_Gtid_Set:
            Executed_Gtid_Set:
                Auto_Position: 0
1 row in set (0.00 sec)
```

22. 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 follwing is displayed -
*************************** 1. row ***************************
               Slave_IO_State: Waiting for master to send event
                  Master_Host: e5ms2
                  Master_User: secondary
                  Master_Port: 3306
                Connect_Retry: 60
              Master_Log_File: log-bin.000002
          Read_Master_Log_Pos: 120
               Relay_Log_File: relay-bin.000002
                Relay_Log_Pos: 149415
        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: 149254
              Relay_Log_Space: 229712
              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: 770
Master_SSL_Verify_Server_Cert: No
                Last_IO_Errno: 0
                Last_IO_Error:
               Last_SQL_Errno: 0
```

```
               Last_SQL_Error:
  Replicate_Ignore_Server_Ids:
             Master_Server_Id: 1
                  Master_UUID: 836db629-e017-11e3-b81f-00151a6e0499
             Master_Info_File:
/Tekelec/WebNMS/mysql/data/master.info
                    SQL_Delay: 0
          SQL_Remaining_Delay: NULL
      Slave_SQL_Running_State: creating table
           Master_Retry_Count: 86400
                  Master_Bind:
      Last_IO_Error_Timestamp:
     Last_SQL_Error_Timestamp:
               Master_SSL_Crl:
           Master_SSL_Crlpath:
           Retrieved_Gtid_Set:
            Executed_Gtid_Set:
                Auto_Position: 0
1 row in set (0.00 sec)
```

23. On the primary server, log in to the OCEEMS database and create a DUMMY table. After creation, verify that it has been created successfully by using the `SHOW TABLES` command.

```
-bash-4.2# ./mysql -uroot -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 10125
Server version: 8.0.3-rc-log MySQL Community Server (GPL)

Copyright (c) 2000, 2017, 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.

Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.

mysql> USE WebNmsDB;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> CREATE TABLE DUMMY(dummy_column VARCHAR(100));
Query OK, 0 rows affected (0.21 sec)

mysql> SHOW TABLES;
```

24. On the standby server, log in to the OCEEMS database and verify that the DUMMY table is present by using the `SHOW TABLES` command.

```
-bash-4.2# ./mysql -uroot -p
Enter password:
```

```
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 10125
Server version: 8.0.3-rc-log MySQL Community Server (GPL)

Copyright (c) 2000, 2017, 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.

Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.

mysql> USE WebNmsDB;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> SHOW TABLES;
```

25. On the standby server, delete the DUMMY table from the OCEEMS database by using the `DROP TABLE` command.

```
mysql> DROP TABLE DUMMY;
Query OK, 0 rows affected (0.05 sec)
```

26. On the primary server, verify that the DUMMY table no longer exists in the OCEEMS database by using the `SHOW TABLES` command.

```
mysql> SHOW TABLES;
```

> **Note**
>
> For client switchover to function, the entries for primary and standby servers must be done in the client machines' `hosts` file. On a Windows machine, the `hosts` file is in the `C:\Windows\System32\drivers\etc` folder. The following two lines should be added in the `hosts` file:

```
<PRIMARY SERVER IP> <PRIMARY SERVER HOSTNAME>
<STANDBY SERVER IP> <STANDBY SERVER HOSTNAME>

For example:

10.248.10.25 e5ms1
10.248.10.21 e5ms2
```

How to Set Up Failover after Upgrade

Before proceeding with setting up of failover after upgrading OCEEMS, the following details should be known:

- Login credentials of the non-root system user for OCEEMS on both the primary and standby servers.
- MySQL root user's password for both the primary and standby servers.
- 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.
- MySQL replication user name and its password on the primary server. In the following procedure, these values are called **<primary replication user>** and **<primary replication user password>** respectively.
- MySQL replication user name and its password on the standby server. In the following procedure, these values are called **<standby replication user>** and **<standby replication user password>** respectively.

> **Note**
>
> Before proceeding with setting up of failover, e5msService must be stopped on both the primary and standby servers.

1. Log into the primary OCEEMS server using the non-root system user for OCEEMS.
2. Move to directory `/Tekelec/WebNMS/bin`:

   ```
   $ cd /Tekelec/WebNMS/bin
   ```

3. 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**.
4. Start MySQL by invoking the `startMySQL.sh` script:

   ```
   $ sh startMySQL.sh
   ```

5. Move to the `/Tekelec/WebNMS/mysql/bin` directory:

   ```
   $ cd /Tekelec/WebNMS/mysql/bin
   ```

6. 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.

   ```
   -bash-4.2# ./mysql -uroot -p
   Enter password:
   Welcome to the MySQL monitor. Commands end with ; or \g.
   Your MySQL connection id is 10125
   Server version: 8.0.3-rc-log MySQL Community Server (GPL)

   Copyright (c) 2000, 2017, 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.
   ```

```
Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.
```

7. Log in to the standby OCEEMS server using the non-root system user for OCEEMS.
8. Move to directory `/Tekelec/WebNMS/bin`:

   ```
   $ cd /Tekelec/WebNMS/bin
   ```

9. 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.
10. Start the MySQL server by invoking the `startMySQL.sh` script:

    ```
    $ sh startMySQL.sh
    ```

11. Move to the `/Tekelec/WebNMS/mysql/bin` directory:

    ```
    $ cd /Tekelec/WebNMS/mysql/bin
    ```

12. To ensure that both databases are in sync before failover setup, take a backup of the database and configuration files on the primary server and restore them on the standby server:
    a. On both the primary and standby servers, create a temporary backup directory for storing backups by using the following command on each server:

       ```
       $ mkdir /tmp/backup
       ```

       > **Note**
       >
       > If the `/tmp/backup` directory is already present on the system, make sure the non-root system user has write permission to it.

    b. On the primary server, run the `/Tekelec/WebNMS/bin/backup/BackupDB.sh` script and create a backup in the temporary backup location `/tmp/backup`:

       ```
       $ cd /Tekelec/WebNMS/bin/backup
       $ sh BackupDB.sh -d /tmp/backup/
       ```

    c. On the primary server, run the following commands to tar the contents of the `/tmp/backup` directory:

       ```
       $ cd /tmp/backup
       $ tar cvf /tmp/primarybackup.tar *
       ```

    d. On the primary server, run the following commands to transfer the tar file created above to the standby server:

       ```
       $ scp /tmp/primarybackup.tar non-root@<ip of secondary server>:/tmp
       ```

e. On the standby server, run the following commands to restore the contents of the tar file transferred from the primary server:

```
$ cd /tmp/backup
$ tar xvf /tmp/primarybackup.tar
$ cd /Tekelec/WebNMS/bin/backup/
./RestoreDB.sh /tmp/backup/E5MS_Database_BackUp.sql
```

13. On the standby server, update the `/Tekelec/WebNMS/classes/hbnlib/hibernate.cfg.xml` file to point the JDBC connection to the hostname of the standby server. Update the following statements:

```
<property name="connection.url">jdbc:mysql://<hostname of standby server>/
WebNmsDB?dumpQueriesOnException=true&amp;jdbcCompliantTruncation=false</
property>
```

This needs to be done because the hibernate.cfg.xml file on the standby server gets overwritten by the one from the primary server when restoring the database and configurations files in the prior step, and this needs to be corrected.

14. Move to the `/Tekelec/WebNMS/bin` directory and start MySQL by executing the `startMySQL.sh` script. After MySQL is started, move to the `/Tekelec/WebNMS/mysql/bin` directory and connect to the MySQL client. Provide the password for the MySQL root user when prompted.

```
$ cd /Tekelec/WebNMS/bin

$ sh startMySQL.sh

$ cd /Tekelec/WebNMS/mysql/bin

-bash-4.2# ./mysql -uroot -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 10125
Server version: 8.0.3-rc-log MySQL Community Server (GPL)

Copyright (c) 2000, 2017, 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.

Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.
```

15. On the primary server, check whether replication slave privilege for the primary replication user is present for the standby host by executing the following query:

```
show grants for '<primary replication user>'@'<standby server hostname>';
```

16. If output similar to the following is observed, it means replication privileges were provided to a user (primary replication user) logging from the standby host. In this case, execute the next step.

```
+-----------------------------------------------------------------------------
-------------------+
| Grants for <primary replication user>@<standby server hostname>|
+-----------------------------------------------------------------------------
-------------------+
| GRANT REPLICATION SLAVE ON *.* TO <primary replication user>@<standby
server hostname> IDENTIFIED BY PASSWORD 'Some encrypted password' |
+-----------------------------------------------------------------------------
-------------------+
1 row in set (0.00 sec)
```

Else, if output similar to the error log is shown, it means that replication privileges were not given to the primary replication user from the standby host during the earlier failover setup. In this case, skip the next step.

```
ERROR 1141 (42000): There is no such grant defined for user <primary
replication user> on host '<standby server hostname>'
```

17. Remove any privileges for all hosts by executing the following command at the MySQL prompt:

```
REVOKE REPLICATION SLAVE ON *.* FROM '<primary replication user>'@'%';
```

18. Execute the following two MySQL commands.

```
GRANT REPLICATION SLAVE ON *.* TO ‘<primary replication user>’@’<standby
server hostname>’ IDENTIFIED BY ‘<primary replication user password>’;

FLUSH PRIVILEGES;
```

19. On the standby server, check whether replication slave privilege for the standby replication user is present for the primary host by executing the following query:

```
show grants for '<standby replication user>'@'<primary server hostname>';
```

20. If output similar to the following is observed, it means replication privileges were provided to a user (standby replication user) logging from the primary host. In this case, execute the next step.

```
+-----------------------------------------------------------------------------
-------------------+
| Grants for <standby replication user>@<primary server hostname>|
+-----------------------------------------------------------------------------
-------------------+
| GRANT REPLICATION SLAVE ON *.* TO <standby replication user>@<primary
server hostname> IDENTIFIED BY PASSWORD 'Some encrypted password' |
+-----------------------------------------------------------------------------
-------------------+
1 row in set (0.00 sec)
```

Else, if output similar to the error log is shown, it means that replication privileges were not given to the standby replication user from the primary host during the earlier failover setup. In this case, skip the next step.

```
ERROR 1141 (42000): There is no such grant defined for user <standby
replication user> on host '<primary server hostname>'
```

21. Remove any privileges for all hosts by executing the following command at the MySQL prompt:

```
REVOKE REPLICATION SLAVE ON *.* FROM '<standby replication user>'@'%';
```

22. Execute the following two MySQL commands.

```
GRANT REPLICATION SLAVE ON *.* TO '<standby replication user>'@'<primary
server hostname>' IDENTIFIED BY '<standby replication user password>';

FLUSH PRIVILEGES;
```

23. 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.000002 |      973 | 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>**.

24. 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>**.

25. Execute the following three MySQL commands on the primary server. In the command, use the values for **<StandbyLogPosition>** and **<StandbyLogFile>** noted previously in this procedure.

```
STOP SLAVE;

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;
```

26. Execute the following three MySQL commands on the standby server. In the command, replace the values for **<PrimaryLogPosition>** and **<PrimaryLogFile>** noted previously in this procedure.

```
STOP SLAVE;

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;
```

27. 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 follwing is displayed -
*************************** 1. row ***************************
               Slave_IO_State: Waiting for master to send event
                  Master_Host: e5ms1
                  Master_User: primary
                  Master_Port: 3306
                Connect_Retry: 60
              Master_Log_File: log-bin.000002
          Read_Master_Log_Pos: 120
               Relay_Log_File: relay-bin.000002
                Relay_Log_Pos: 149415
        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: 149254
              Relay_Log_Space: 229712
              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: 770
Master_SSL_Verify_Server_Cert: No
                Last_IO_Errno: 0
                Last_IO_Error:
               Last_SQL_Errno: 0
               Last_SQL_Error:
  Replicate_Ignore_Server_Ids:
             Master_Server_Id: 1
                  Master_UUID: 836db629-e017-11e3-b81f-00151a6e0499
             Master_Info_File: /Tekelec/WebNMS/mysql/data/master.info
                    SQL_Delay: 0
          SQL_Remaining_Delay: NULL
      Slave_SQL_Running_State: creating table
           Master_Retry_Count: 86400
                  Master_Bind:
      Last_IO_Error_Timestamp:
     Last_SQL_Error_Timestamp:
               Master_SSL_Crl:
           Master_SSL_Crlpath:
           Retrieved_Gtid_Set:
            Executed_Gtid_Set:
                Auto_Position: 0
1 row in set (0.00 sec)
```

28. 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 STAUS \G;

Output similar to the follwing is displayed -
*************************** 1. row ***************************
               Slave_IO_State: Waiting for master to send event
                  Master_Host: e5ms12
                  Master_User: secondary
                  Master_Port: 3306
                Connect_Retry: 60
              Master_Log_File: log-bin.000002
          Read_Master_Log_Pos: 120
               Relay_Log_File: relay-bin.000002
                Relay_Log_Pos: 149415
        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: 149254
```

```
                  Relay_Log_Space: 229712
                  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: 770
Master_SSL_Verify_Server_Cert: No
                  Last_IO_Errno: 0
                  Last_IO_Error:
                 Last_SQL_Errno: 0
                 Last_SQL_Error:
  Replicate_Ignore_Server_Ids:
              Master_Server_Id: 1
                   Master_UUID: 836db629-e017-11e3-b81f-00151a6e0499
              Master_Info_File: /Tekelec/WebNMS/mysql/data/master.info
                     SQL_Delay: 0
           SQL_Remaining_Delay: NULL
       Slave_SQL_Running_State: creating table
            Master_Retry_Count: 86400
                   Master_Bind:
       Last_IO_Error_Timestamp:
      Last_SQL_Error_Timestamp:
                Master_SSL_Crl:
            Master_SSL_Crlpath:
            Retrieved_Gtid_Set:
             Executed_Gtid_Set:
                 Auto_Position: 0
1 row in set (0.00 sec)
```

29. On the primary server, log in to the OCEEMS database and create a DUMMY table. After creation, verify that it has been created successfully by using the `SHOW TABLES` command.

```
-bash-4.2# ./mysql -uroot -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 10125
Server version: 8.0.3-rc-log MySQL Community Server (GPL)

Copyright (c) 2000, 2017, 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.

Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.

mysql> USE WebNmsDB;
Reading table information for completion of table and column names
```

```
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> CREATE TABLE DUMMY(dummy_column VARCHAR(100));
Query OK, 0 rows affected (0.21 sec)

mysql> SHOW TABLES;
```

30. On the standby server, log in to the OCEEMS database and verify that the DUMMY table is present by using the SHOW TABLES command.

```
-bash-4.2# ./mysql -uroot -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 10125
Server version: 8.0.3-rc-log MySQL Community Server (GPL)

Copyright (c) 2000, 2017, 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.

Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.

mysql> USE WebNmsDB;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> SHOW TABLES;
```

31. On the standby server, delete the DUMMY table from the OCEEMS database by using the DROP TABLE command.

```
mysql> DROP TABLE DUMMY;
Query OK, 0 rows affected (0.05 sec)
```

32. On the primary server, verify that the DUMMY table no longer exists in the OCEEMS database by using the SHOW TABLES command.

```
mysql> SHOW TABLES;
```

> **Note**
>
> For client switchover to function, the entries for primary and standby servers must be done in the client machines' `hosts` file. On a Windows machine, the `hosts` file is in the `C:\Windows\System32\drivers\etc` folder. The following two lines should be added in the `hosts` file:

```
<PRIMARY SERVER IP> <PRIMARY SERVER HOSTNAME>
<STANDBY SERVER IP> <STANDBY SERVER HOSTNAME>

For example:

10.248.10.25 e5ms8
10.248.10.21 e5ms9
```

Synchronizing Databases

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.

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 OCEEMS 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
LASTCOUNT	bigint(20)		Value incremented after every HEART_BEAT_INTERVAL

Field Name	Type	Constraints	Description
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 OCEEMS 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 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

Table Name	Purpose
CORBANode	The discovered CORBA object is mapped to the CORBANode. The properties are given in the corbaseed.file in <Web NMS Home>/conf directory. 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.
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 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.

Table Name	Purpose
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.
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.

Table Name	Purpose
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.
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	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 tl1seed.file in<Web NMS Home>/conf directory, 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 fromtl1seed.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.
TL1Node	The discovered TL1 object is mapped to the TL1 Node. The properties are given in the tl1seed.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

Table Name	Purpose
ViewPropertiesTable	The ViewPropertiesTable maps a view name to the properties of objects
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

OCEEMS 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.
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 OCEEMS tasks, and related attributes, scheduled by OCEEMS 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 OCEEMS is enabled via a valid OCEEMS 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 OCEEMS 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 OCEEMS 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 OCEEMS 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, OCEEMS allows n+1 retries. As per WebNMS this behavior is by design. Also, OCEEMS will try indefinitely to connect to the failed primary server, if the value is set to '0' or less.

E

EPAP Support Messages

This appendix lists the error and informational messages for OCEEMS support of EPAP.

Error/Informational Messages for EPAP Support

The error and informational messages for OCEEMS support of EPAP are listed in Table E-1. 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 E-1 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/' '> IPv6 address provided is invalid! Valid IPv6 address format is 'xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx'.
8	EPAP <A/B/' '> IP address is blank!
9	EPAP <A/B/' '> port number is blank!
10	EPAP <A/B/' '> port number can contain only numeric value between 0 and 65535!
11	EPAP <A/B/' '> login name can contain only alphanumeric characters, hyphen and underscore!
12	EPAP <A/B/' '> login name can contain a minimum of 5 and a maximum of 20 characters!
13	EPAP <A/B/' '> login name must have an alphabet as its first character!
14	EPAP <A/B/' '> login password string is blank!

Table E-1 (Cont.) Error/Informational Messages for EPAP Support

15	EPAP <A/B/' '> login password string length cannot exceed 20 characters!
16	EPAP <A/B/' '> description field length cannot exceed 200 characters!
17	EPAP addition request has been sent to server. Please wait for status.
18	EPAP '<EPAP A IP>' discovery failed! Reason: <REASON>. Please resolve the issue and retry.
19	EPAP modification request has been sent to server. Please wait for status.
20	EPAP '<EPAP A IP >' modified by user '<USER NAME>'.
21	EPAP '<EPAP A IP >' added by user '<USER NAME>'.
22	EPAP '<EPAP A IP>' modification failed! Reason: <REASON>. Please resolve the issue and retry.
23	Both EPAP A and EPAP B status cannot be 'Active' simultaneously!
24	EPAP deletion request has been sent to server. Please wait for status.
25	EPAP '<EPAP A IP>' deleted by user '<USER NAME>'.
26	EPAP '<EPAP A IP>' deletion failed! Reason: <REASON>. Please resolve the issue and retry.
27	Provisioning, SNMP/SSH and Web IP address cannot be same in 'PDB Only' EPAP!
28	EPAP A and EPAP B IP address cannot be same in 'PROV' and 'Non PROV' EPAP!
29	Please fill up all mandatory fields before proceeding!
30	Alarm resynchronization initiated for EPAP: <EPAP name> by user: <USER NAME>!
31	Alarm resynchronization completed for EPAP: <EPAP NAME> initiated by user: <USER NAME>!
32	Alarm resynchronization failed for EPAP: <EPAP NAME> initiated by user: <USER NAME>! Reason: <REASON> Please resolve the issue and try again.
33	OCEEMS cannot connect to EPAP: <EPAP NAME> for receiving alarms! Please check the connection.
34	Invalid selection for 'PDB Only' EPAP type!
35	EPAP added to OCEEMS.
36	Received 'resyncRequiredTrap' from EPAP for alarm resynchronization.
37	Regaining connection.
38	Warm start of OCEEMS server.
39	Automatic alarm resynchronization completed for EPAP <EPAP NAME>.
40	Automatic alarm resynchronization failed for EPAP! Reason: <REASON> Please resolve the issue and try again.

Table E-1 (Cont.) Error/Informational Messages for EPAP Support

41	Automatic alarm resynchronization failed for EPAP: <EPAP NAME>! Reason: <REASON> Please resolve the issue and try again.
42	Buffer overflows during southbound resynchronization for EPAP: <EPAP NAME>! This could result in loss of alarms.
43	EPAP '<EPAP A IP>' modification failed! Reason: No field was changed during modification operation. Please resolve the issue and retry.
44	EPAP <A/B/' '> write community string is blank!
45	EPAP <A/B/' '> write community string length cannot exceed 20 characters!
46	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'.
47	EPAP <SNMP/SSH or Provisioning or Web> IP address is blank!

F

Fault Management GUI Custom Views

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.

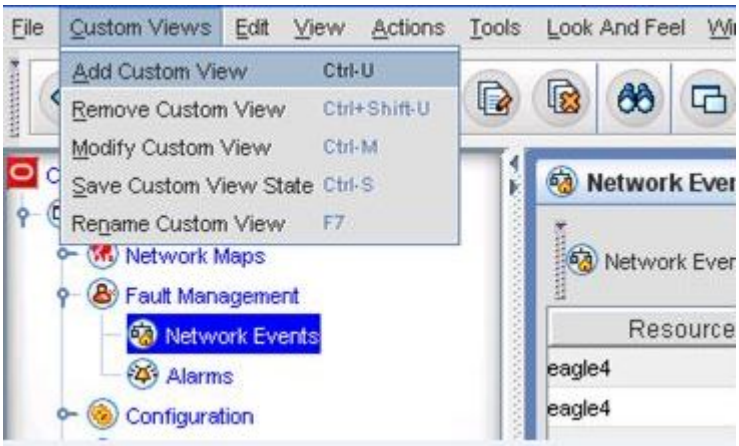
Adding a New Custom View

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.

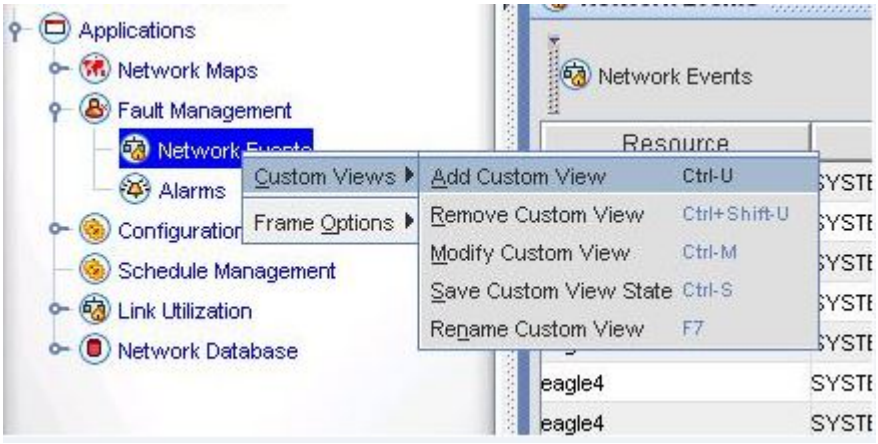
2. Use either of the following two methods to create a custom view:
   - From the **Custom Views** menu in the top menu bar, choose **Add Custom View** as shown in Figure F-1.

Figure F-1 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**, and then **Add Custom View** as shown in Figure F-2.

Figure F-2 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 F-3. 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 F-4.

Figure F-3 Specify Event Filter Criteria

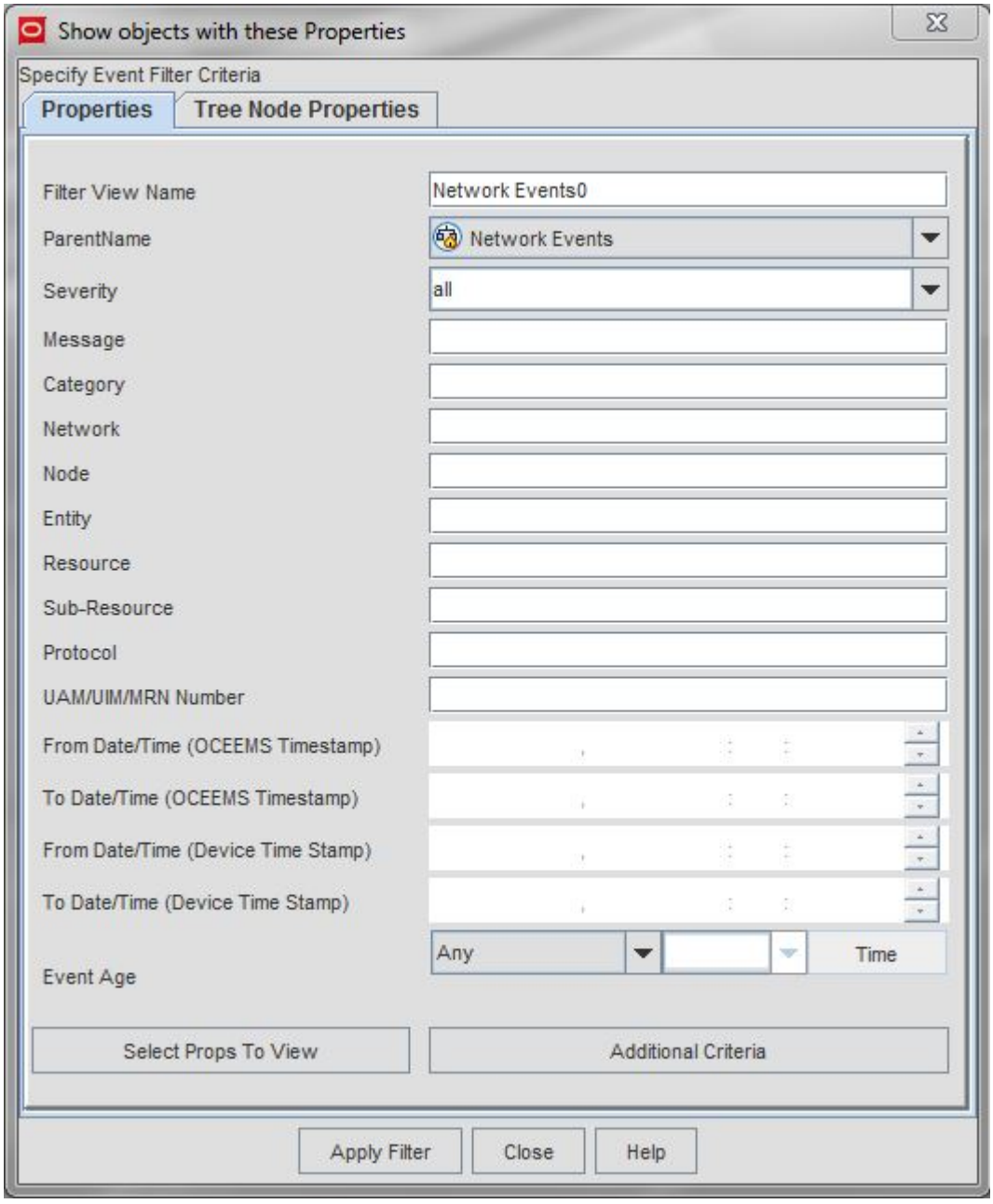
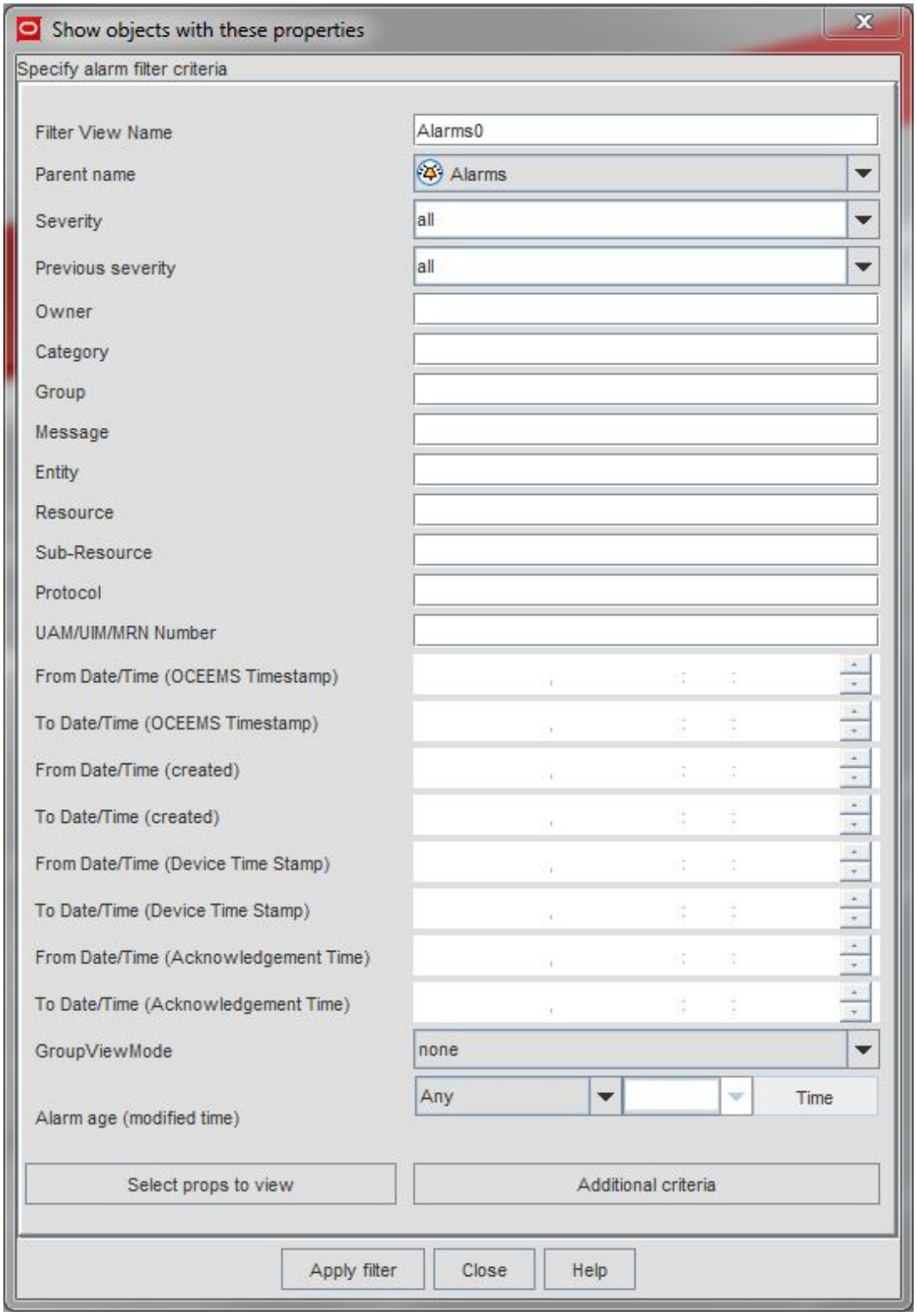


Figure F-4 Specify Alarm Filter Criteria



3. Specify the custom view name in the **Filter View Name** field, and the match criteria to be used to filter the data.

   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.

> **Note**
>
> The **Additional criteria** button near the bottom of the screen is no longer needed to add properties to the filtering criteria; all properties available for filtering are now available in the Show objects with these Properties dialog box.

4. 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.

5. 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 F-5 and Figure F-6).

Figure F-5 Custom View for Network Events

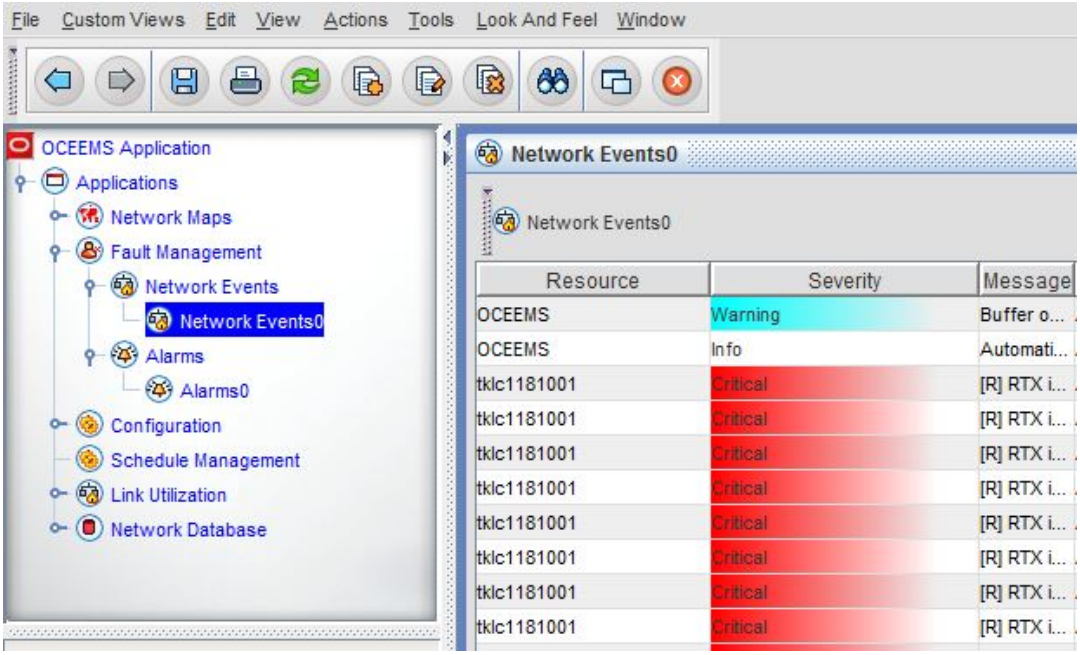
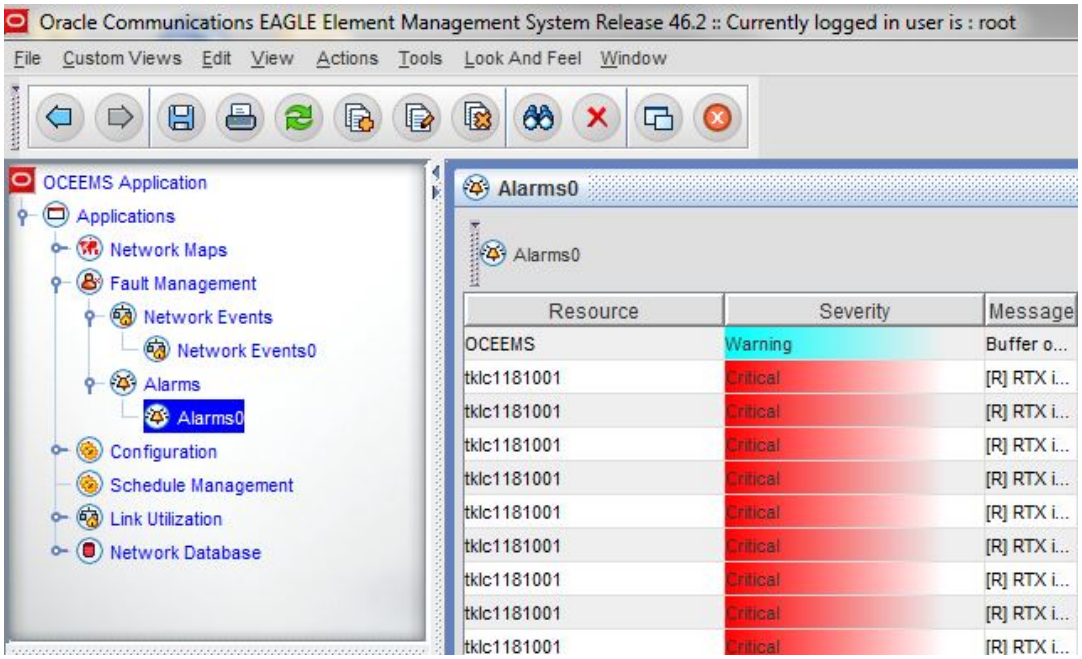


Figure F-6 Custom View for Alarms



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.

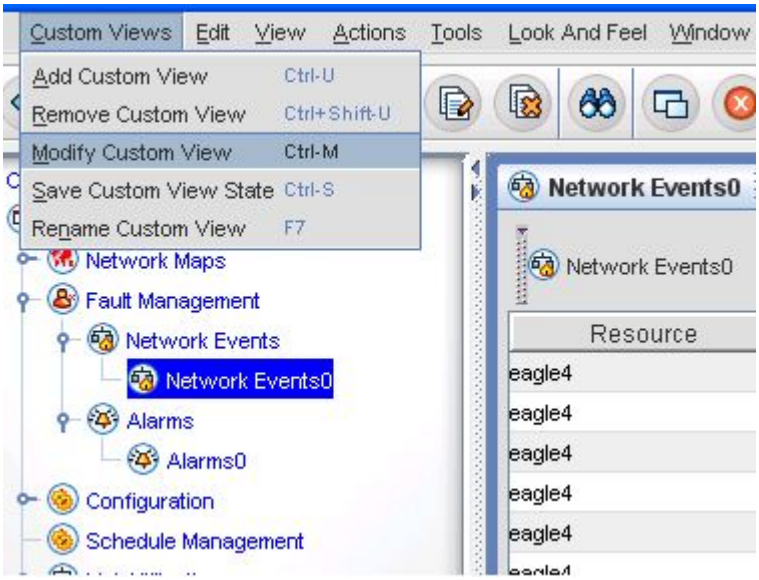
Modifying a Custom View

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.

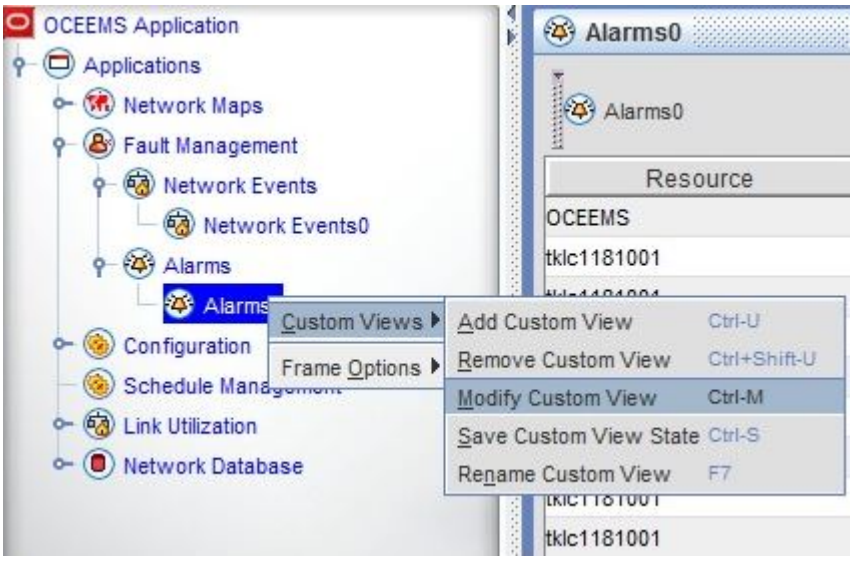
2. Perform either of the following two procedures to modify the custom view:
   - From the **Custom Views** menu in the top menu bar, choose **Modify Custom View** as shown in Figure F-7.

Figure F-7 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**, and then **Modify Custom View** as shown in Figure F-8.

Figure F-8 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.

3. Follow steps 3 to 5 in Adding a New Custom View to modify the custom view as required.

Saving a Custom View

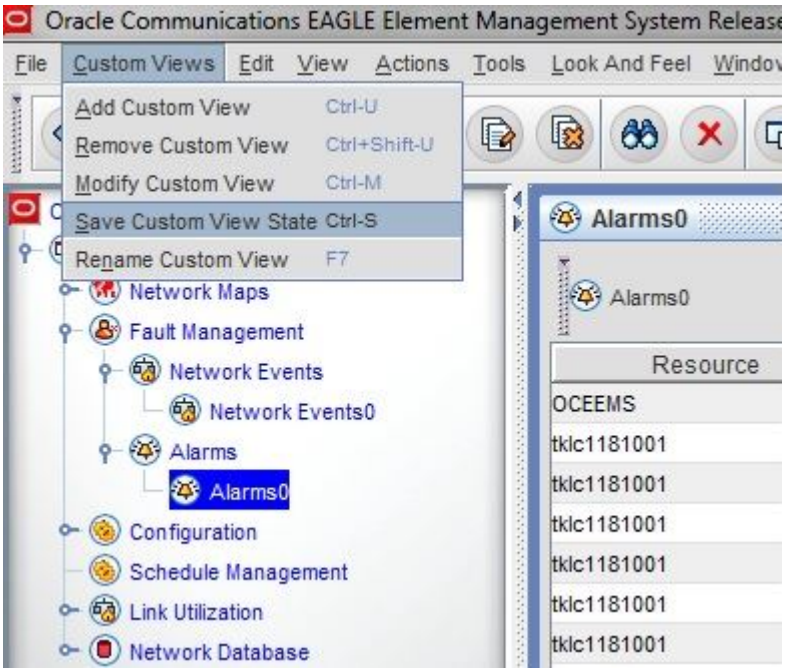
This procedure describes how to save the current state of the custom view, such as the order of the columns, the sorted alarms, and the first and the last viewed alarms.
To save an existing custom view, perform the following steps:

1. Click on the custom view node under Network Events/Alarms node in the left navigation pane.

2. Perform either of the following two procedures to save the custom view:

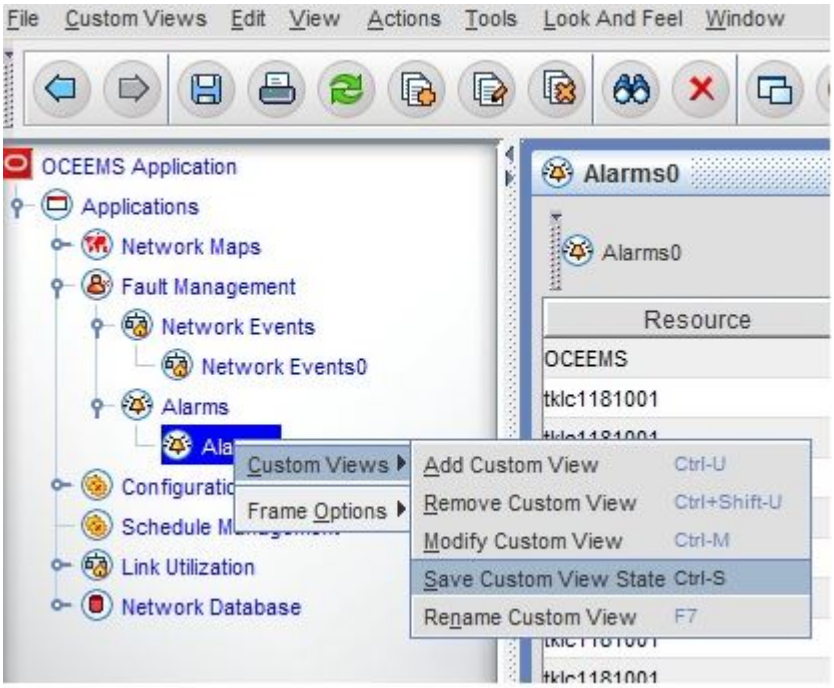
   - From the **Custom Views** menu in the top menu bar, choose **Save Custom View State** as shown in Figure F-9.

Figure F-9 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**, and then **Save Custom View State** as shown in Figure F-10.

Figure F-10 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 F-11.

Figure F-11 Custom View Saved Successfully

Deleting a Custom View

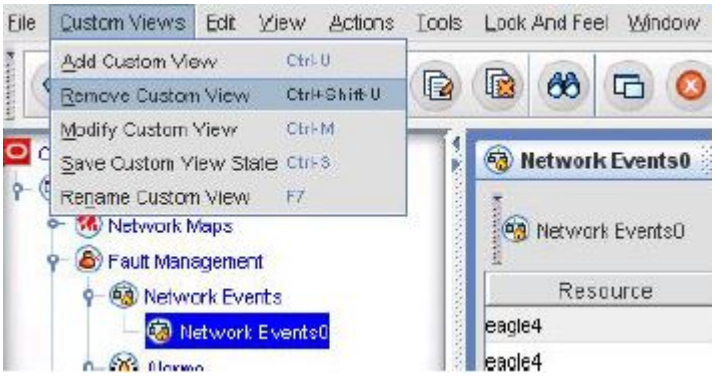
This procedure describes how to delete an existing custom view.
Perform the following steps to delete a custom view:

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:

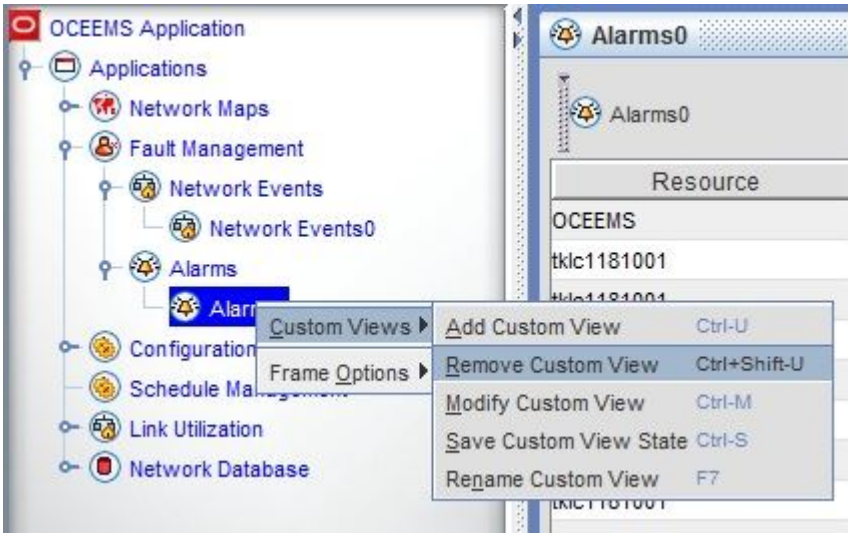
   - From the **Custom Views** menu in the top menu bar, choose **Remove Custom View** as shown in Figure F-12.

Figure F-12 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**, and then **Remove Custom View** as shown in Figure F-13.

Figure F-13 Deleting a Custom View By Using Left Navigation Pane



3. Click **Yes** in the confirmation box to delete the custom view.

   Note:

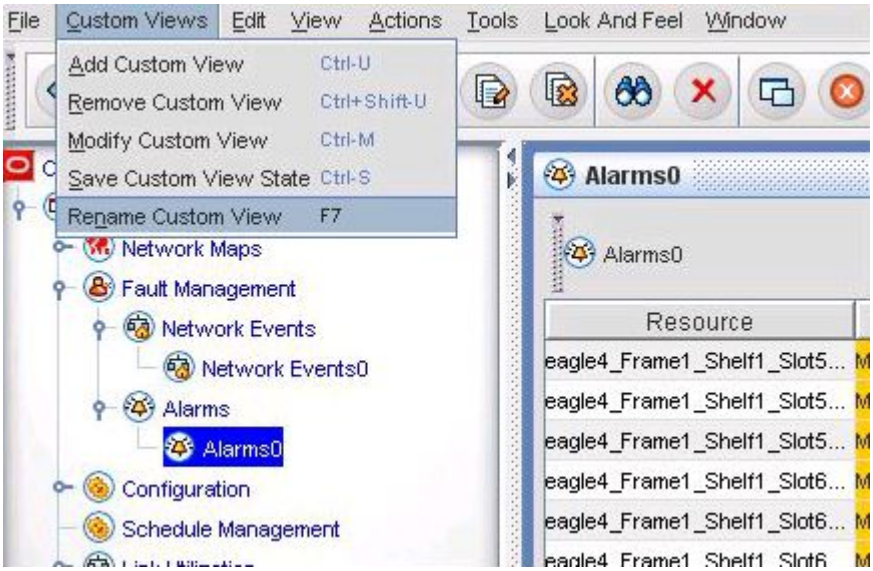
   Deleting a parent custom view also deletes any child custom views added under the parent view (as described in Adding a New Custom View).

Renaming a Custom View

This procedure describes how to rename an existing custom view.
Perform the following steps to rename a custom view:

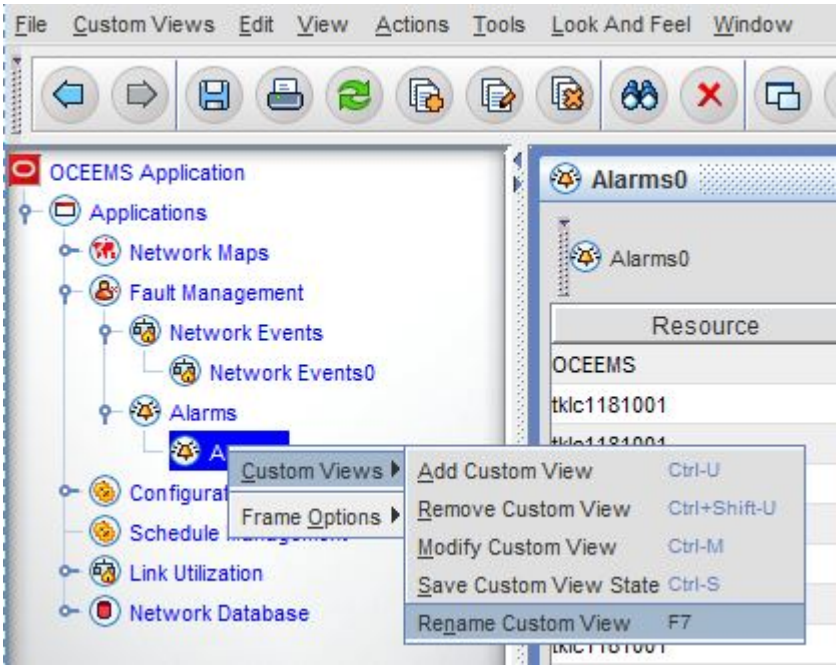
1. Click on the custom view node under the Network Events or Alarms node in the left navigation pane.
2. Perform either of the following two procedures to rename the custom view:
   - From the **Custom Views** menu in the top menu bar, choose **Rename Custom View** as shown in Figure F-14.

Figure F-14 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**, and then **Rename Custom View** as shown in Figure F-15.

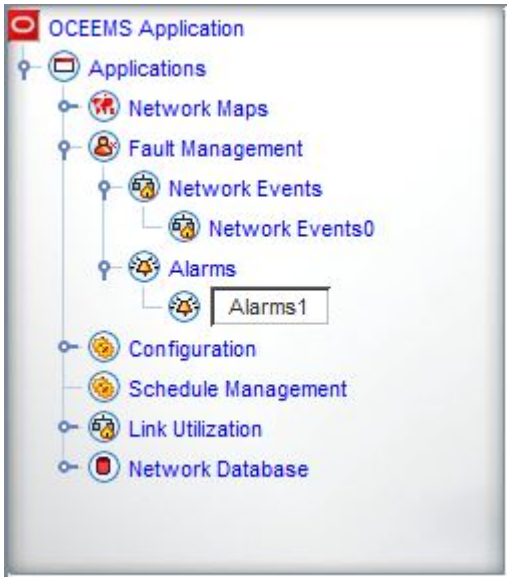
Figure F-15 Rename a Custom View By Using Left Navigation Pane



3. Type the new name for custom view as shown in Figure F-16, and press **Enter**.

   Note: To retain the existing name and not proceed with renaming, press the **Esc** key.

Figure F-16 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 F-3 and Figure F-4, click the **Select Props To View** button.

   The **Select Table Columns** dialog box is displayed, as shown in Figure F-17 and Figure F-18. The selected fields are the columns that can be seen in the resulting custom view.

Figure F-17 Selecting Table Columns for Network Events

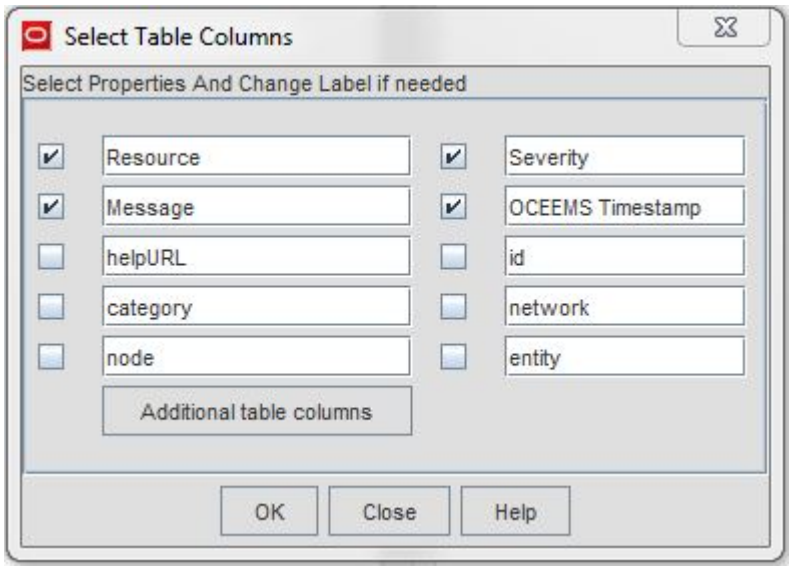
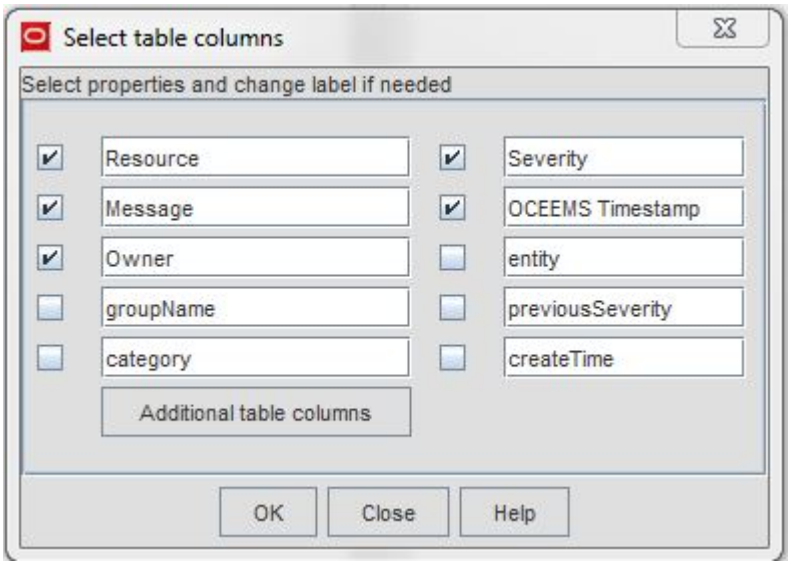


Figure F-18 Selecting Table Columns for Alarms



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 F-17 and Figure F-18.

   The **User defined table columns** dialog box is displayed, as shown in Figure F-19 and Figure F-20.

Figure F-19 Specifying Additional Table Columns for Network Events

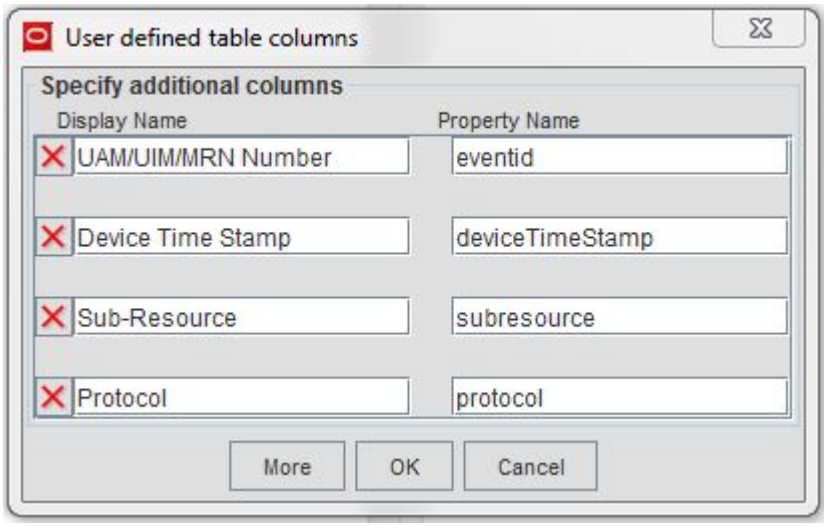
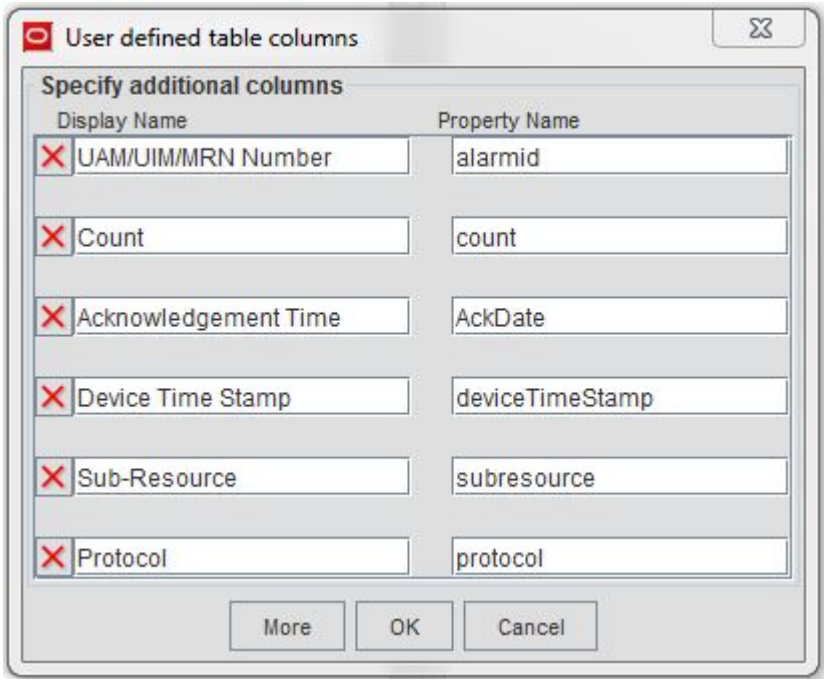


Figure F-20 Specifying Additional Table Columns for Alarms



4. Enter the display name and corresponding property name in the **Display Name** and **Property Name** fields exactly as shown in Figure F-19 and Figure F-20.
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 (OCEEMS 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 (OCEEMS 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	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 OCEEMS system. By default, the value specified is Any, whereby events of all ages are displayed. Other options are minutes, hours, days, today, and yesterday. **Example:** 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.

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	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 severity on which alarms are to be filtered in the custom view. **Tip:** For multiple severities, type the severity values separated by a comma (for example: Major, Minor).

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 is 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 to the non-root user configured for OCEEMS, then only the alarms owned by that user 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 ***Node Clear.***, 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 (OCEEMS 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 (OCEEMS 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	From the drop-down box, choose the mode used to group the alarms in the custom view. **max** Alarms of maximum severity are grouped and displayed at the beginning of the list. **latest** The newest alarms are grouped and displayed at the beginning of the list. **none** The alarms are not grouped.
21.	Alarm Age (modified time)	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 OCEEMS system. By default, the value specified is Any, whereby alarms of all ages are displayed. Other options are minutes, hours, days, today, and yesterday. **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.

Tips and Tricks for Using Custom Views

Following are some tips to effectively use custom views:

- OCEEMS 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 as a wildcard to match zero or more characters.
	Examples:
	– To view all objects with names that start with **test**, specify:
	`test*`
	– To view all objects that end with **com**, specify:
	`*com`

! (exclamation mark)	An exclamation mark filters the search using the NOT operator.
	Examples:
	– To view all objects with names that do not start with **test**, specify:
	`!test*`
	– To view all alarms except alarms with *Critical* and *Major* severity, specify:
	`!war*, !cle*`
	or
	`!warning, !clear`

, (comma)	A comma filters the search using the OR operator; it 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)	Two ampersands are used to combine two or more conditions in the same criteria. **Example:** If all the objects with names that do not start with **ven** but do end with **com** are required, specify: `!ven*&&*com`
<between> "value1" and "value2"	This notation is used to retrieve objects with numeric values within a specific range. **Example:** To retrieve object names with a poll interval value ranging from **300** to **305**, specify: `<between> 300 and 305` 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.

G

Using the OCEEMS MIB Browser as an NMS Proxy

The MIB browser application bundled with OCEEMS can be used as a proxy for an NMS to verify SNMP v3 features like trap forwarding and resynchronization.

Procedure to Use the OCEEMS MIB Browser as an NMS Proxy

Before you begin, verify that OCEEMS is running in SNMP v3 mode and verify the NMS configuration, so the MIB browser can be set up to discover the appropriate user at the SNMP v3 agent running at the target host (OCEEMS).

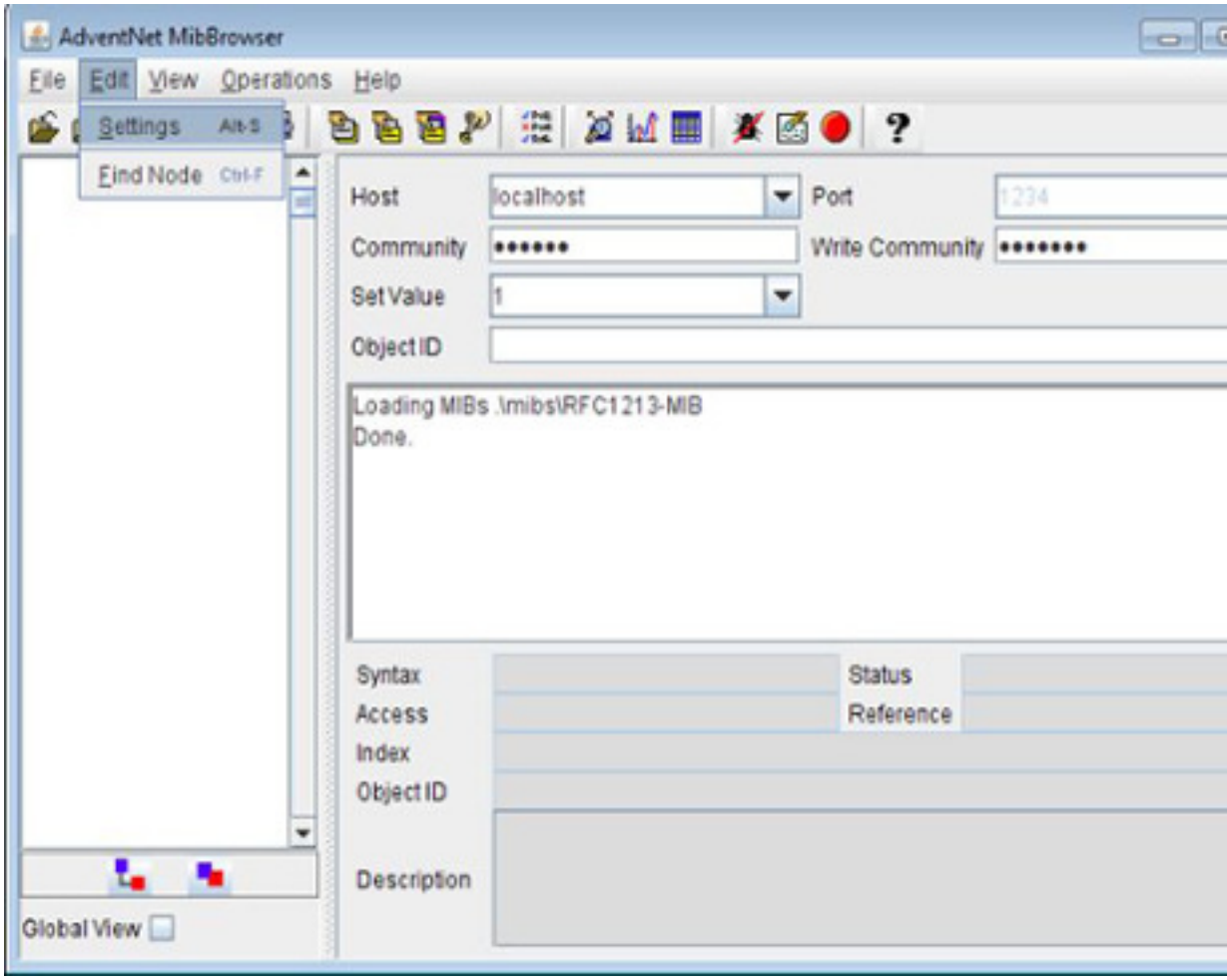
To receive SNMP v3 traps in the MIB browser from OCEEMS, follow these steps:

1. Launch the MIB browser by running the MibBrowser script (`OCEEMS_HOME\bin\browsers\MibBrowser.sh`).

   The AdventNet MibBrowser screen will be displayed.

2. On the AdventNet MibBrowser screen, select **Edit**, and then **Settings** as shown:

Figure G-1 AdventNet MibBrowser Screen

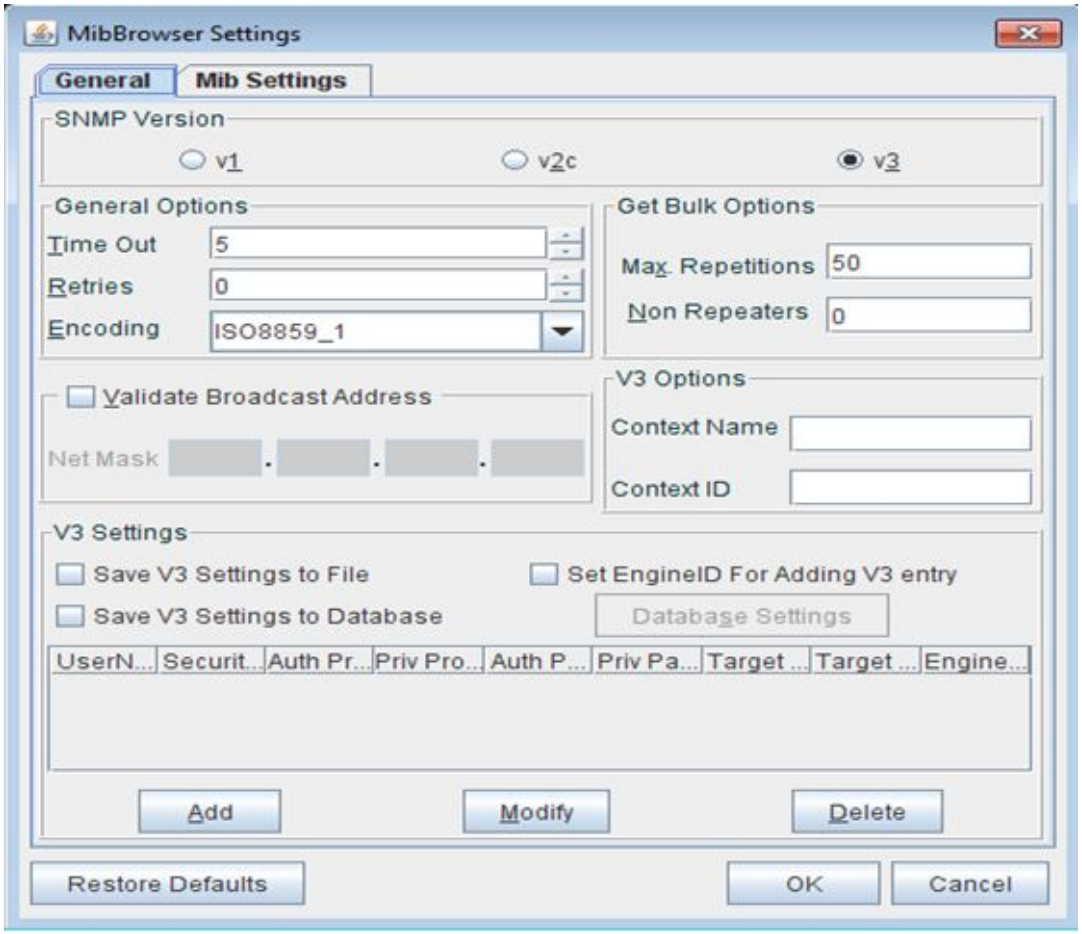


The MibBrowser Settings window will be displayed.

3. Select the **v3** radio button.

   The configuration settings for SNMP v3 will appear under the General tab as shown:

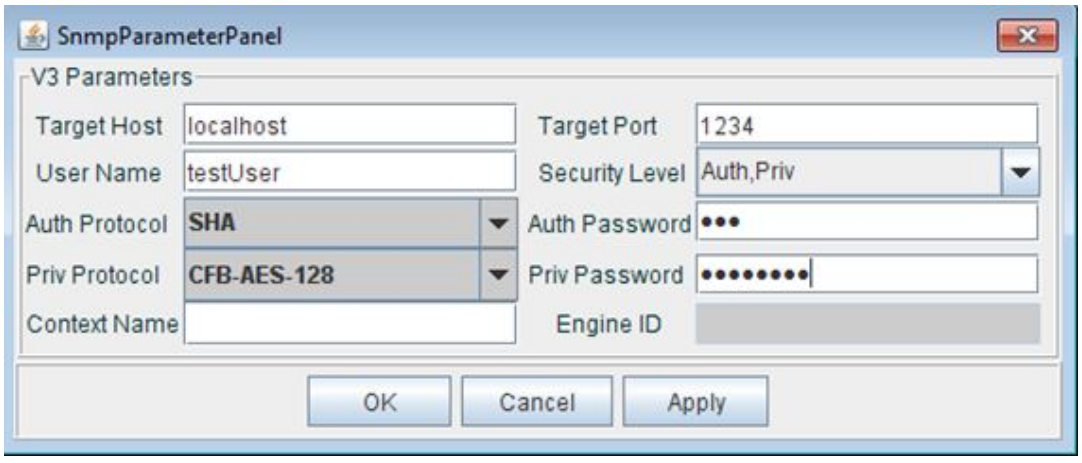
Figure G-2 MIB Browser Settings for v3



4. Click **Add** to add SNMP v3 parameters.

   The SnmpParameterPanel will be displayed. As shown, this panel enables the addition of SNMP v3 parameters like target host (OCEEMS) IP address, target port, and the SNMP v3 user to be used in SNMP v3-based communication between OCEEMS and the MIB browser.

Figure G-3 SNMP Parameter Panel



5. Populate the SnmpParameterPanel fields as follows:

   Target Host
   IP address of the OCEEMS server

   Target Port
   Port on the OCEEMS server where it listens for incoming SET requests from the NMS

   User Name
   SNMP v3 user associated with the NMS in OCEEMS; the user here must be the same user with which the NMS is configured on OCEEMS. This way the authentication/privacy protocols and passwords are known to both the sender and the receiver.

   Security Level
   The **Security Level** assigned to the SNMP v3 user associated with the NMS in OCEEMS

   Auth Protocol
   The **Auth Protocol** assigned to the SNMP v3 user associated with the NMS in OCEEMS

   Auth Password
   The **Auth Password** assigned to the SNMP v3 user associated with the NMS in OCEEMS

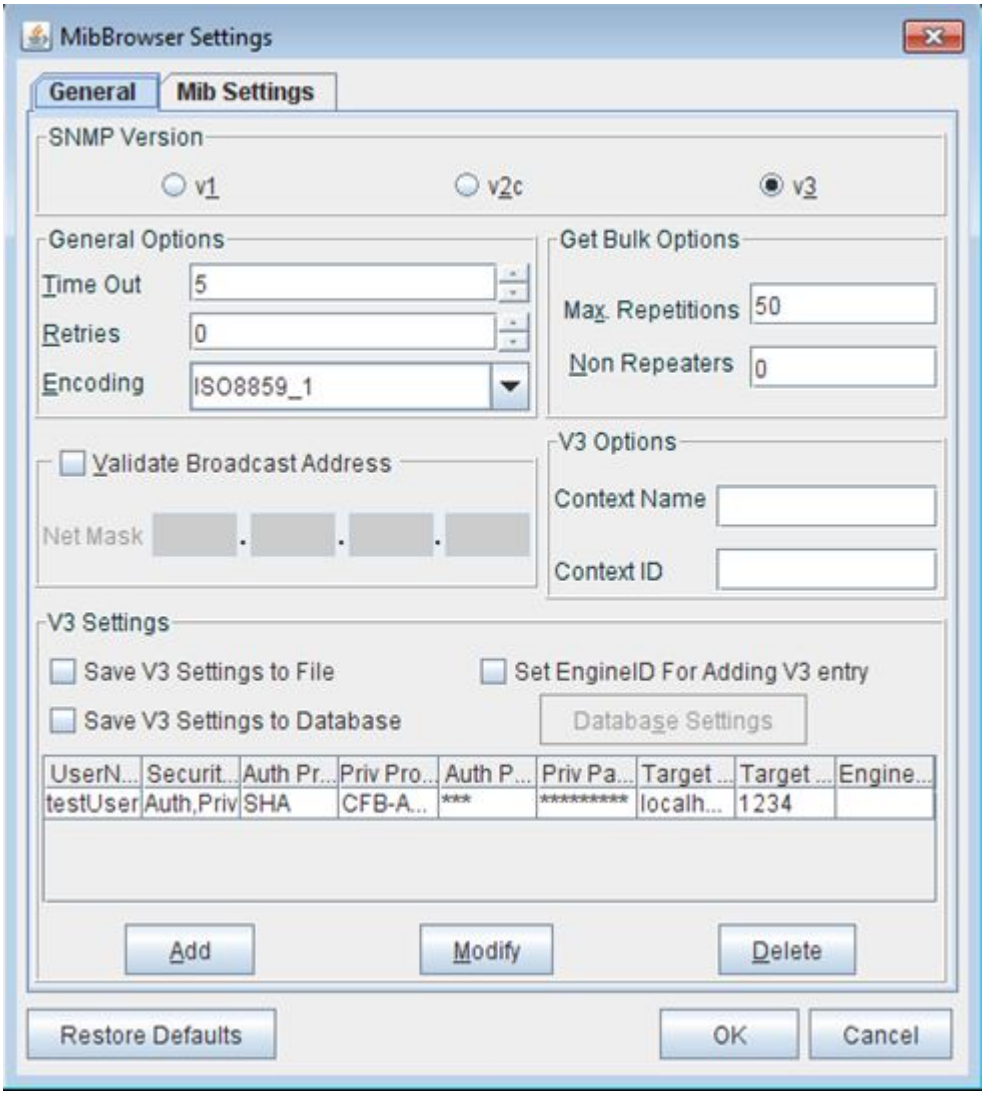
   Priv Protocol
   The **Priv Protocol** assigned to the SNMP v3 user associated with the NMS in OCEEMS

   Priv Password
   The **Priv Password** assigned to the SNMP v3 user associated with the NMS in OCEEMS

6. Click **Apply** and then **OK**.

   If the user discovery with the given values is successful, the v3 parameters are saved in the MIB browser as shown below:

Figure G-4 MIB Browser Settings with Saved User

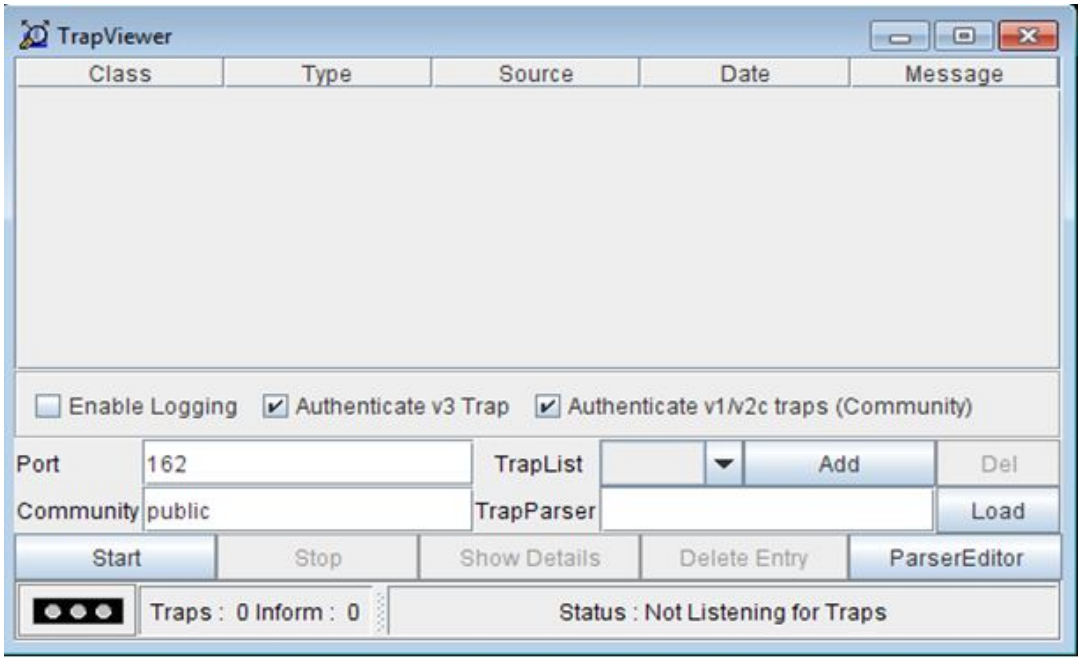


7. Select the saved entry and click **OK**.
8. Back on the AdventNet MibBrowser screen, select **View**, and then **Trap Viewer** as shown:

Figure G-5 Starting the Trap Viewer

The TrapViewer screen will be displayed:

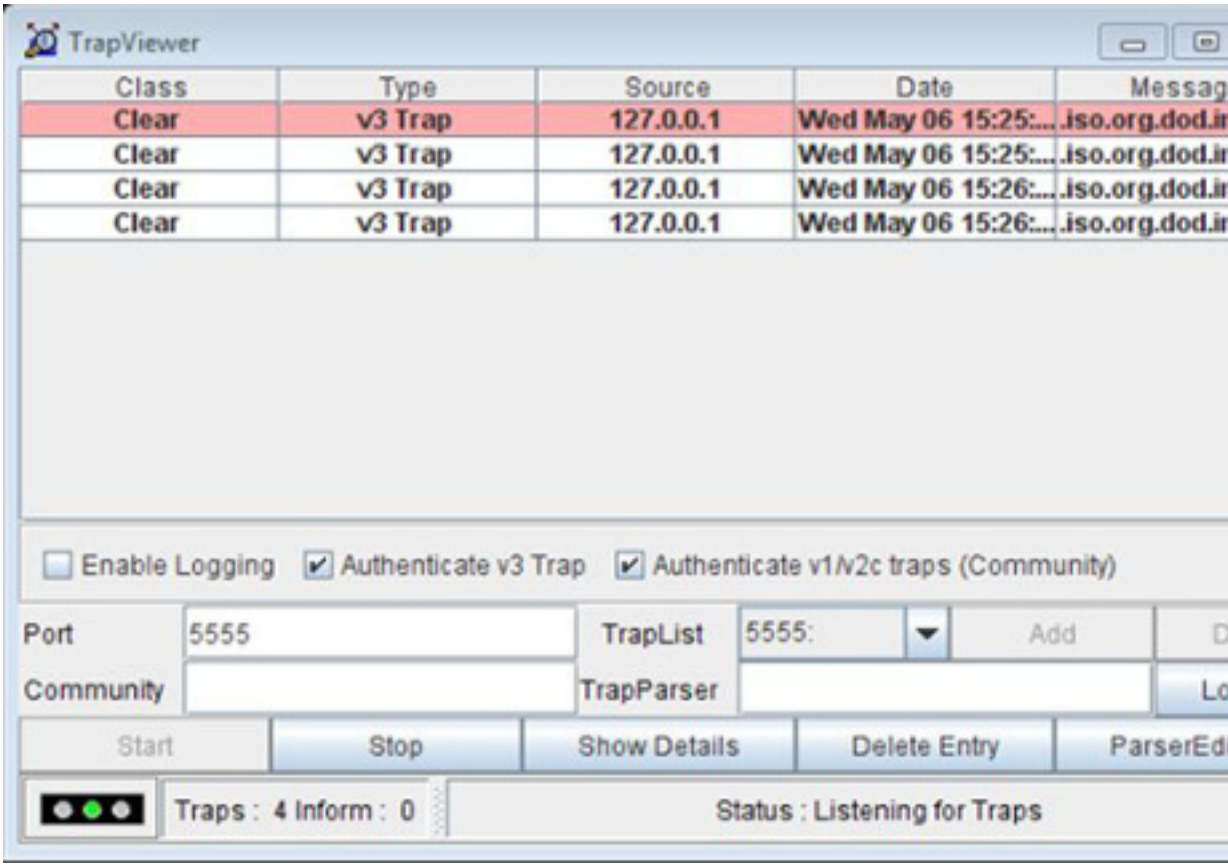
Figure G-6 Trap Viewer Screen



9. Change the **Port** field to the port where SNMP v3 traps are expected from OCEEMS and then click **Start**.

   Traps will be received in the trap viewer as shown:

Figure G-7 Trap Viewer Screen



H

Measurement Report Configuration on EAGLE

This appendix provides the EAGLE commands needed for measurement report configuration.

EAGLE Commands for Measurement Report Configuration

First, you need to enable the E5-OAM Integrated Measurements feature.

Commands to Enable the E5-OAM Integrated Measurements feature

1. Log into EAGLE via Telnet or SSH.
2. Add an OCEEMS entry as the FTP server:
   `ent-ftp-serv:ipaddr=<IP address of OCEEMS server>:app=meas:prio=1:path="/opt/E5-MS/measurement/csvinput":login=<non-root system user for OCEEMS>`

   When prompted for the password, provide the password of the non-root system user configured for OCEEMS.

   For example:

```
ent-ftp-serv:ipaddr=10.250.54.19:app=meas:prio=1:path="/opt/E5-MS/measurement/csvinput":login=oceemsuser

stpb9070401 16-08-08 01:31:27 EST  EAGLE5 46.2.0-67.10.0
ent-ftp-serv:ipaddr=10.250.54.19:app=meas:prio=1:path="/opt/E5-MS/measurement/csvinput":login=oceemsuser
    Command entered at terminal #17.
;
 Enter Password :
    stpb9070401 16-08-08 01:31:32 EST  EAGLE5 46.2.0-67.10.0
    FTP SERV table is (3  of 10)  30% full
Command Accepted - Processing
    ENT-FTP-SERV: MASP A - COMPLTD
;
Command Executed
```

3. Check your entry by using the `rtrv-ftp-serv` command.

```
rtrv-ftp-serv
    stpb9070401 16-08-08 01:32:19 EST  EAGLE5 46.2.0-67.10.0
    rtrv-ftp-serv
    Command entered at terminal #17.
;
Command Accepted - Processing
    stpb9070401 16-08-08 01:32:19 EST  EAGLE5 46.2.0-67.10.0
    APP       IPADDR           LOGIN            SECU  PRIO  PATH
    --------  ---------------  ---------------  ----  ----  ----
    dist      192.168.56.10    pv105            OFF   1     /export/home/mgtsusers/pv1
    db        192.168.55.71    nest             OFF   1     /tmp/tmpk3ugl6
    meas      10.250.54.19     oceemsuser       OFF   1     /opt/E5-MS/measurement/csv
    FTP SERV table is (3  of 10)  30% full
;
Command Executed
```

4. Enable and turn on the OAM IP Security feature:

```
ENBLE-CTRL-FEAT:partnum=893400001
    stpb9070401 16-08-08 01:34:22 EST  EAGLE5 46.2.0-67.10.0
    ENABLE-CTRL-FEAT:partnum=893400001
    Command entered at terminal #17.
```

```
;
Command Accepted - Processing
    stpb9070401 16-08-08 01:34:22 EST  EAGLE5 46.2.0-67.10.0
    ENABLE-CTRL-FEAT: MASP A - COMPLTD
;
Command Executed


CHG-CTRL-FEAT:partnum=893400001:status=On
stpb9070401 16-08-08 01:34:47 EST  EAGLE5 46.2.0-67.10.0
    CHG-CTRL-FEAT:partnum=893400001:status=On
    Command entered at terminal #17.
;
    stpb9070401 16-08-08 01:34:47 EST  EAGLE5 46.2.0-67.10.0
    CHG-CTRL-FEAT: MASP A - Command Aborted
;
Command Executed
```

5. Change the FTP server to be secure:
   `chg-ftp-serv:security=on:ipaddr=<IP address of OCEEMS server>:app=meas`

   For example:

   ```
   chg-ftp-serv:security=on:ipaddr=10.250.54.19:app=meas
   ```

6. Turn on the E5-OAM Integrated Measurements feature.

   ```
   chg-measopts:oamhcmeas=on
   ```

7. Get Integrated Measurements status, such as card location and state.

   ```
   rept-stat-meas
   ```

8. Send test files to the FTP server.

   ```
   pass:cmd="ftptest -a meas":loc=1113

   pass:cmd="ftptest -a meas":loc=1115
   ```

9. Check the status of the measurement options.

   ```
   rtrv-measopts
      stpb9070401 16-08-08 01:35:14 EST  EAGLE5 46.2.0-67.10.0
       rtrv-measopts
       Command entered at terminal #17.
   ;
   Command Accepted - Processing
       stpb9070401 16-08-08 01:35:14 EST  EAGLE5 46.2.0-67.10.0
       PLATFORMENABLE   = off
       COLLECT15MIN     = off
       CLLIBASEDNAME    = off
       OAMHCMEAS        = on
       UNCHLINKLABEL    = off
       ----------------------
       SYSTOTSTP        = on
   ```

```
    SYSTOTTT          = on
    SYSTOTSTPLAN      = on
    SYSTOTIDPR        = on
    SYSTOTSIP         = on
    COMPLINK          = on
    COMPLNKSET        = on
    COMPSCTPASOC      = on
    COMPSCTPCARD      = on
    COMPUA            = on
    GTWYSTP           = on
    GTWYLNKSET        = on
    GTWYORIGNI        = on
    GTWYORIGNINC      = on
    GTWYLSORIGNI      = on
    GTWYLSDESTNI      = on
    GTWYLSONISMT      = on
    NMSTP             = on
    NMLINK            = on
    NMLNKSET          = on
    AVLLINK           = on
    AVLSTPLAN         = on
    AVLDLINK          = on
;
Command Executed
```

10. Activate the automatic generation and FTP transfer of all scheduled measurements reports.

    ```
    chg-measopts:all=on
    ```

11. Verify the collect parameter is on and the scheduled measurement reports.

    ```
    rtrv-meas-sched
    ```

12. Turn on required parameters. For example:

    ```
    chg-meas:complink=on
    ```

    (Similarly, turn on other required parameters with the `chg-meas` command)

Commands to Enable the Measurements Platform

Similarly, use the following commands to enable the Measurements Platform.

1. `ent-ftp-serv:ipaddr=<IP address of OCEEMS server>:app=meas:prio=1:path="/opt/E5-MS/measurement/csvinput":login=<non-root system user for OCEEMS>`
   When prompted for the password, provide the password of the non-root system user configured for OCEEMS.
2. `chg-ftp-serv:security=on:ipaddr=<IP address of OCEEMS server>:app=meas`
3. `chg-feat:measplat=on`
4. `chg-measopts:platformenable=on`

5. `rept-stat-meas`
6. `pass:cmd="ftptest -a meas":loc=<location of mcpm card received in step 5>`
7. `rtrv-measopts`
8. `chg-measopts:all=on`
9. `rtrv-meas-sched` (to verify whether the collect parameter is on or not)
10. `chg-meas:comp link=on` (Similarly, turn on other required parameters with the `chg-meas` command)

PDF Download Error from Reporting Studio: Network Error/Internet Connection Error

Description: When downloading PDF report on chromium-based browsers, this issue is encountered as when downloading it mentions Network issue or Internet Connectivity Issue.

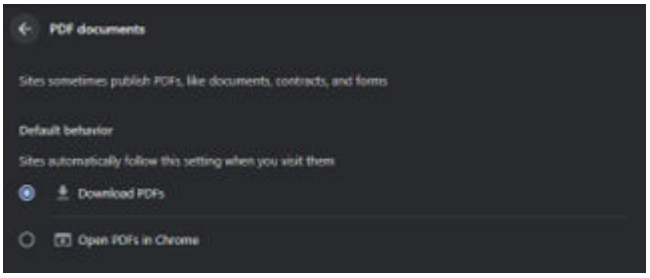
Procedure:

1. In case there is `.pdf` report download error.

Figure I-1 Download error

2. Change the Browser PDF Settings as follows:
   a. Chrome: PDF Chrome setting (Privacy and Security/Site Settings/PDF Documents) from Open PDFs in Chrome to Download PDF Documents.

Figure I-2 PDF settings in Chrome

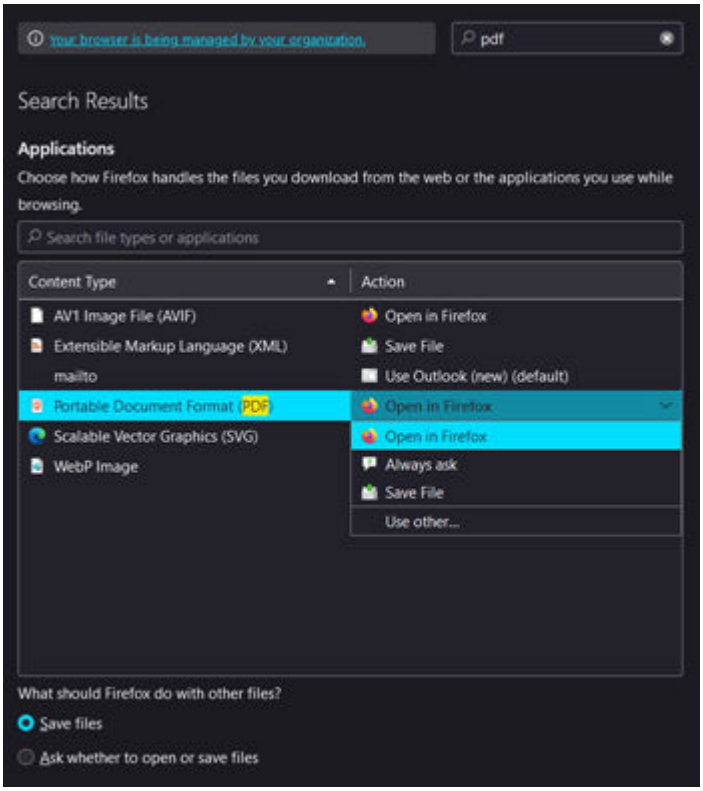


   b. Edge: Go to **Settings**, then **Cookies and site permissions**, then **Site permissions**, then **PDF documents**, and then enable “Always download PDF files”.

Figure I-3 Enable “Always download PDF files”

   c. Mozilla Firefox: Go to **Settings**, search for PDF, and then from the drop-down beside PDF documents, select **Save File**.

Figure I-4 PDF settings on Mozilla Firefox



J

Truncated field shown in Reporting Studio Reports

Description: Sometimes in the Measurement Reports generated by Reporting Studio, some of the fields (for example, LSN) gets truncated.

For example, the LSN name is `nsdmobor1`. Somewhere it is shown as `nsdmo`, while in some places as `nsdmobor`. It needs to display the actual name consistently.

Procedure:

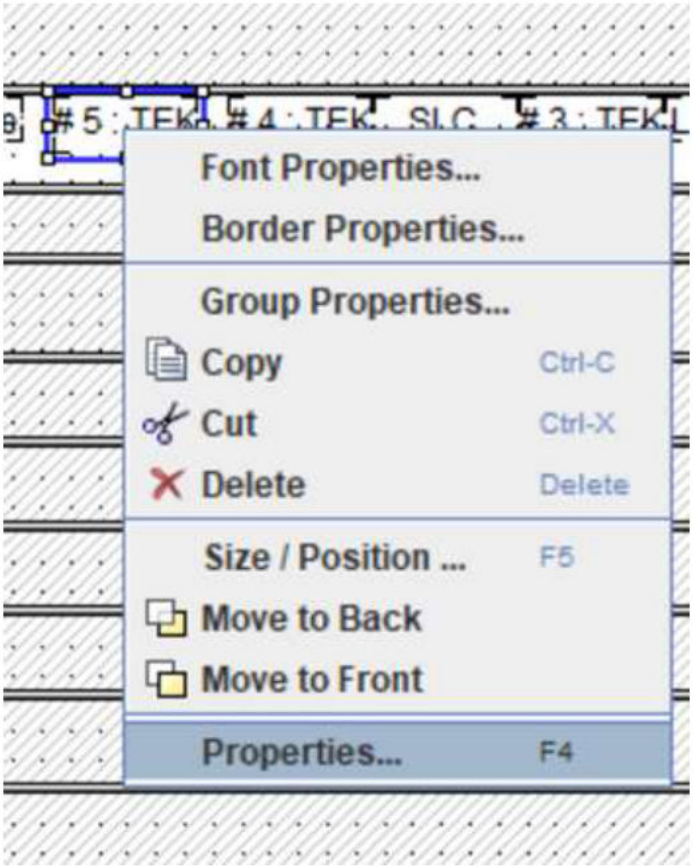
For the above issue, we need to enable the “Can Grow” property for the database field that is getting truncated in the report to get the complete data.

Verify that in the DB, the CLLI is not getting truncated.

You can enable the “Can Grow” property in the I-net designer tool by the following steps:

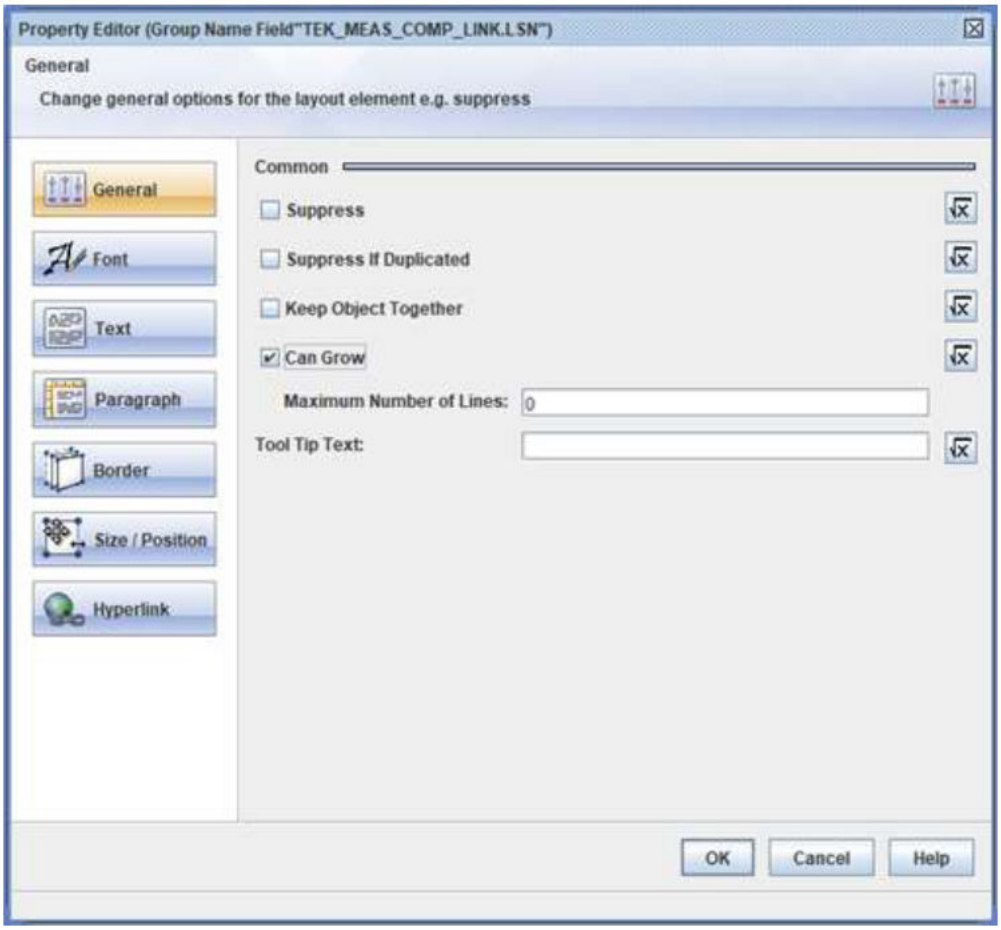
1. Right click the field and click **Properties...**.

Figure J-1 Properties



2. Enable the **Can Grow** property.
3. Click **Ok**.

Figure J-2 Enable the Can Grow Property



K

Prune Binary Log Procedure

Description: Run the following procedure to automate the pruning of MySQL Binary Logs. Binary Logs are used to sync the two EMS servers in case of dual setup. The Binary Logs accumulate over time which takes significant storage space. This procedure creates a nightly cron job that prunes the binary logs timely and frees up the storage space.

Procedure:

> **Note**
>
> Both the admin user names for e5ms1 and e5ms2 should be the same. This process must be done after completely setting up the dual EMS setup.

Consider two setups, e5ms1 (10.75.137.1) and e5ms2 (10.75.137.0), in a dual setup and run the following commands using the root user.

1. Run the following command on servers e5ms1 and e5ms2.

   ```
   #vim /etc/hosts
   ```

   a. On server e5ms1, add the following content:
   ```
   10.75.137.1 e5ms1 localhost

   10.75.137.0 e5ms2 mate
   ```

   b. On server e5ms2, add the following content:
   ```
   10.75.137.0 e5ms2 localhost

   10.75.137.1 e5ms1 mate
   ```

2. Generate SSH key pair. If you haven't already generated an SSH key pair, you can do so using the

   ```
   ssh-keygen
   ```

   command. Make sure to not set a passphrase for simplicity. Perform this step on both the servers.
   The above command will provide a default name.

3. Copy public key to remote host: Copy the public key to the remote host's `~/.ssh/<keyname>` file. This allows you to authenticate the remote host using the corresponding private key.

   ```
   ssh-copy-id -i ~/.ssh/id_rsa.pub <remote user>@<remote host ip>
   ```

   For example, when running from 10.75.137.1, the command will be:

   ```
   ssh-copy-id -i ~/.ssh/id_rsa.pub root@10.75.137.1
   ```

4. On both the EMS servers, run the following command:

   ```
   [root@EMS2 ~]# vim /etc/ssh/sshd_config
   ```

   Uncomment the ```PubkeyAuthentication yes``` line.

   If it is uncommented, then do not alter it.

5. Create `pruner.bin` and `rmt_pruner.bin` files.

   ```
   [root@EMS2 bin]# cd /Tekelec/WebNMS/bin
   [root@EMS2 bin]# ./prePrune
   Enter the local_mysql_password: ********
   Enter the remote_mysql_password: ********
   Encrypted passwords saved to pruner.bin and rmt_pruner.bin
   ```

6. In case the admin user name in the EMS is something other than the default user name (that is emsadmuser), then run the following command:

   ```
   # sed -i 's/emsadmuser/<admin_username>/g' /Tekelec/WebNMS/bin/
   pruneBinaryLogs.sh
   ```

   > **Note**
   >
   > If the admin username is emsadmuser, then do not run the above command.

7. Add the following line to the cron jobs list on both sides using the following command: `#crontab -e`

   Add the following line and save the cron file.

   ```
   15 04 * * * sudo /Tekelec/WebNMS/bin/pruneBinaryLogs.sh > /
   pathOfOutputFile 2>&1
   ```

   For example:

   ```
   15 04 * * * sudo /Tekelec/WebNMS/bin/pruneBinaryLogs.sh > /pathOfOutputFile
   2>&1
   ```

   This will ensure that the cron job runs properly.

8. Run the following command to manually prune the binary logs:

   ```
   sudo /Tekelec/WebNMS/bin/pruneBinaryLogs.sh > /pathOfOutputFile 2>&1
   ```

   This will ensure that the cron job runs properly.

L

How to use savelogs in EMS

Description: In E5-MS, there are two kinds of logs, application logs and framework logs. The application logs are stored as per the module at `/var/E5-MS/<module_name>/` and framework logs are stored at `/Tekelec/WebNMS/logs`. These logs play an important role in debugging, hence a script `savelogs.sh` is written at `/Tekelec/WebNMS/bin` to save these logs. All the applications logs will be stored at `/tmp/savelogs/ems` and the framework logs will be stored at `/tmp/savelogs/framework`. Both the EMS and framework directories are tarred to form a zip file in the format `savelogs_ddmmmyyyy.tar.gz` at `/tmp/savelogs`. Additionally, some important conf files are also being backed by this script at `/tmp/savelogs/confFiles`.

Procedure:

This script helps you to save logs of required modules and required number of log files of each module and framework. The following are the different commands that `savelogs.sh` script provides to save the logs as per requirement.

1. Run the following command to see the module numbers and their usage.

> **Note**
>
> Here, each number represents a module (channel, configuration,...). `-m` signifies the input for modules and `-n` signifies the latest n number of logfiles. `-a`represents all the logs and modules.

```
#sh savelogs.sh
```

Usage:

```
sh savelogs.sh -m[<module1,module2,..] -n[<count>]
```

-m signifies signifies the module number[s] whose logs are to be saved.

-n signifies the latest number of logfile[s] to be saved of each module and framework.

> **Note**
>
> - Multiple modules can be input as comma seperated module numbers (as explained in the following example).
> - The framework logs are saved by default.
> - If the `/tmp/savelogs` folder already exists, remove the savelogs folder and then run the savelogs utility.

For example:

```
sh savelogs.sh (To see the usage)
sh savelogs.sh -h (To see the usage)
```

```
sh savelogs.sh -m 1,2 -n 5 (To save latest 5 logfiles of module 1 and 2
and framework)
sh savelogs.sh -a (To save all logfiles of all modules and framework)
sh savelogs.sh -a -n 2 (To save latest 2 logfiles of all modules and
framework)
Below table lists down the module numbers (to be input in savelogs
command) corresponding to each module of EMS
--------------------------------
Module Number | Module Name
--------------------------------
1             | channel
2             | configuration
3             | discovery
4             | failover
5             | fault
6             | inventory
7             | license
8             | licensing
9             | linkUtilization
10            | maps
11            | measurement
12            | nbi
13            | reporting
14            | scheduler
15            | security
16            | userOperations
17            | utils
--------------------------------
```

The logs will be saved in the format `savelogs_ddmmmyyyy.tar.gz` file at `/tmp/savelogs/savelogs_ddmmmyyyy.tar.gz`.

2. Run the following command to save log files of all modules and framework logs.

```
# savelogs.sh -a
```

Warning: Make sure /tmp folder doesn't have a folder named savelogs already. If present, remove it manually before proceeding further.

Do you want to continue[y/n]?

n

rm -rf /tmp/savelogs

savelogs.sh -a

Warning: Make sure /tmp folder doesn't have a folder named savelogs already. If present, remove it manually before proceeding further.

Do you want to continue[y/n]?

y

tar: savelogs: file changed as we read it

```
#ls -lrt /tmp/savelogs/

total 224
drwxr-xr-x. 2 root root     50 May  1 09:56 ems
```

```
drwxr-xr-x. 2 root root   4096 May  1 09:56 framework
drwxr-xr-x. 3 root root     21 May  1 09:56 confFiles
-rw-r--r--. 1 root root 243182 May  1 09:56 savelogs_01May2024.tar.gz
```

3. Run the following command to save latest “n” log files of all modules and framework logs.

   ```
   # savelogs.sh -a -n 2
   ```

   For example, here n=2

   Warning: Make sure /tmp folder doesn't have a folder named savelogs already. If present, remove it manually before proceeding further.

   Do you want to continue[y/n]?

   y

   tar: savelogs: file changed as we read it

   ```
   # ls -lrt /tmp/savelogs

   total 244
   drwxr-xr-x. 2 root root     50 May  1 09:56 ems
   drwxr-xr-x. 2 root root   4096 May  1 09:56 framework
   drwxr-xr-x. 3 root root     21 May  1 09:56 confFiles
   -rw-r--r--. 1 root root 243182 May  1 09:56 savelogs_01May2024.tar.gz
   ```

4. Run the following command to save the latest “n” log files of required modules and framework logs. For example here the modules be channel,configuration and n=3

   ```
   # savelogs.sh -m 1,2 -n 3
   ```

   Warning: Make sure /tmp folder doesn't have a folder named savelogs already.If present, remove it manually before proceeding further.

   Do you want to continue[y/n]?

   y

   tar: savelogs: file changed as we read it.

   ```
   # ls -lrt /tmp/savelogs/ems

   total 8

   -rw-r--r--. 1 root root 914 May 1 09:56 channel.txt

   -rw-r--r--. 1 root root 3471 May 1 09:56 configuration.txt
   ```

> **Note**
>
> The choice to the warning of the script depends on your `/tmp` folder. If the savelogs directory is already present at `/tmp`, remove it first and run the script again.

M

SSH Server CBC Mode Ciphers Enabled

Description: After running a vulnerability scan, you get the following results:

SSH Server CBC Mode Ciphers Enabled

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plain text message from the ciphertext. Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Plugin Output: The following client-to-server Cipher Block Chaining (CBC) algorithms are supported:

- 3des-cbc
- aes128-cbc
- aes192-cbc
- aes256-cbc
- blowfish-cbc
- cast128-cb

The following server-to-client Cipher Block Chaining (CBC) algorithms:

- 3des-cbc
- aes128-cbc
- aes192-cbc
- aes256-cbc
- blowfish-cbc
- cast128-cbc

Procedure:

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

For this vulnerability scan result, modify the configuration of SSHD to fix the issue:

1. Open sshd_config in /etc/ssh directory.
2. Remove the CBC ciphers under Ciphers to use “Ciphers aes256-ctr,aes192-ctr,aes128-ctr” only.

Figure M-1 Remove the CBC Ciphers

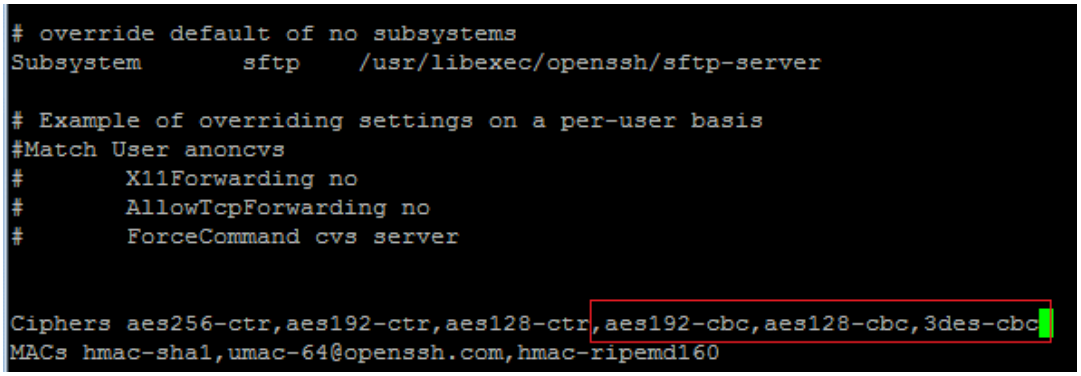
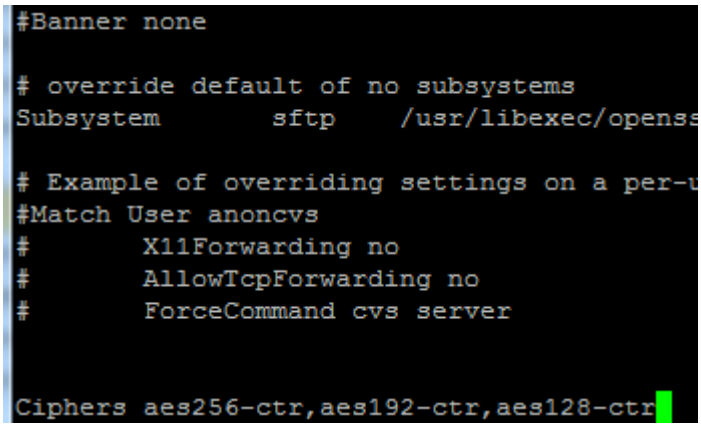


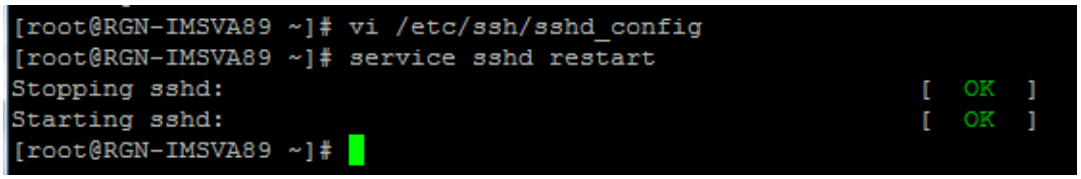
Figure M-2 Use Ciphers aes256-ctr,aes192-ctr,aes128-ctr only



3. Save and exit.
4. Restart sshd service using the following command:

```
[root@imsva~#] service sshd restart
```

Figure M-3 Restart sshd service



N

Null is passed for a clisession is observed in the inventory logs

Null is passed for a clisession is observed in the inventory logs.

1. Log in as emsadmuser.
2. cd /Tekelec/WebNMS/bin/
3. Run `E5MSConfigurationScript.sh`.
4. Restart EMS services.

O

rsyslog configuration for transfer of system log files to remote server

Oracle Linux includes the rsyslog utility, which can be configured to transfer system log files from a Linux machine, such as an EMS server, to a remote machine. This appendix provides detailed instructions on the necessary configurations for the EMS server to ensure the proper functioning of the rsyslog utility.

1. Before starting the configuration first make sure that rsyslog is installed using the following commands on CLI:

```
[root@EMS1 log]# rpm -qa | grep rsyslog
rsyslog-8.24.0-52.el7.x86_64
root@EMS1 log]# rsyslogd -v
rsyslogd 8.24.0-52.el7, compiled with:
       PLATFORM:    x86_64-redhat-linux-gnu
       PLATFORM (lsb_release -d):
       FEATURE_REGEXP: Yes
       GSSAPI Kerberos 5 support: Yes
       FEATURE_DEBUG (debug build, slow code): No
       32bit Atomic operations supported: Yes
       64bit Atomic operations supported: Yes
       memory allocator: system default
       Runtime Instrumentation (slow code): No
       uuid support: Yes
       Number of Bits in RainerScript integers: 64
```

   See http://www.rsyslog.com for more information.

```
[root@EMS1 log]#
```

2. If rsyslog is not installed in the system do that by the following:

```
[root@EMS1 log]# yum install rsyslog
         (Preferably use the following version : yum install
rsyslog-8.24.0-52.el7.x86_64 )
```

3. You have to install rsyslog on both the systems from which you are sending the logs (client) and to which you are sending the logs (server).
4. On the client side:

a. Run the following commands on the CLI:

```
[root@EMS1 log]# systemctl start rsyslog.service
root@EMS1 log]# systemctl enable rsyslog.service
root@EMS1 log]# systemctl status rsyslog.service


rsyslog.service - System Logging Service
Loaded: loaded /usr/lib/systemd/system/rsyslog.service; enabled; vendor
preset: enabled)
Active: active(running) since Mon 2024-02-05 05:59:20 EST; 16s ago
Docs: man:rsyslogd(8)
    http://www.rsyslog.com/doc/
Main PID: 29071 (rsyslogd)
  CGroup: /system.slice/rsyslog.service
     └─29071 /usr/sbin/rsyslogd -n


Feb 05 05:59:20 EMS1 systemd[1]: Starting System Logging Service...
Feb 05 05:59:20 EMS1 rsyslogd[29071]: [origin software="rsyslogd"
swVersion="8.24.0-52....artFeb 05
    05:59:20 EMS1 systemd[1]: Started System Logging Service.
Hint: Some lines were ellipsized, use -l to show in full.
```

b. `[root@EMS1 log]#`

Edit the configuration file using the following commands:

- `vim /etc/rsyslog.conf`
- Add the following code: (make sure to replace the with the ip of the server side)

```
# rsyslog configuration file

# For more information see /usr/share/doc/rsyslog-*/
rsyslog_conf.html
# If you experience problems, see http://www.rsyslog.com/doc/
troubleshoot.html

#### MODULES ####

# The imjournal module bellow is now used as a message source
instead of imuxsock.
$ModLoad imuxsock # provides support for local system logging (e.g.
via logger command)
$ModLoad imjournal # provides access to the systemd journal
$ModLoad imklog # reads kernel messages (the same are read from
journald)
#$ModLoad immark  # provides --MARK-- message capability

# Provides UDP syslog reception
#$ModLoad imudp
#$UDPServerRun 514

# Provides TCP syslog reception
```

```
#$ModLoad imtcp
#$InputTCPServerRun 514
$ModLoad imfile
$InputFileName /var/log/messages
$InputFileTag message-file-tag
$InputFileStateFile message-statefile
$InputFileFacility local8
$InputRunFileMonitor

$ModLoad imfile
$InputFileName /var/log/secure
$InputFileTag secure-file-tag
$InputFileStateFile secure-statefile
$InputFileFacility local9
$InputRunFileMonitor

$ModLoad imfile
$InputFileName /Tekelec/WebNMS/logs/stdout.txt
$InputFileTag stdout-file-tag
$InputFileStateFile stdout-statefile
$InputFileFacility local10
$InputRunFileMonitor

$ModLoad imfile
$InputFileName /var/log/audit/audit.log
$InputFileTag audit-file-tag
$InputFileStateFile audit-statefile
$InputFileFacility local11
$InputRunFileMonitor

#### GLOBAL DIRECTIVES ####

# Where to place auxiliary files
$WorkDirectory /var/lib/rsyslog

# Use default timestamp format
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

# File syncing capability is disabled by default. This feature is
usually not required,
# not useful and an extreme performance hit
#$ActionFileEnableSync on

# Include all config files in /etc/rsyslog.d/
$IncludeConfig /etc/rsyslog.d/*.conf

# Turn off message reception via local log socket;
# local messages are retrieved through imjournal now.
$OmitLocalLogging on

# File to store the position in the journal
$IMJournalStateFile imjournal.state

#### RULES ####

# Log all kernel messages to the console.
```

```
# Logging much else clutters up the screen.
#kern.*                                                 /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none                /var/log/
messages

# The authpriv file has restricted access.
authpriv.*                                              /var/log/
secure

# Log all the mail messages in one place.
mail.*                                                  -/var/log/
maillog

# Log cron stuff
cron.*                                                  /var/log/
cron

# Everybody gets emergency messages
*.emerg                                                 :omusrmsg:*

# Save news errors of level crit and higher in a special file.
uucp,news.crit                                          /var/log/
spooler

# Save boot messages also to boot.log
local7.*                                                /var/log/
boot.log

# ### begin forwarding rule ###
# The statement between the begin ... end define a SINGLE forwarding
# rule. They belong together, do NOT split them. If you create
multiple
# forwarding rules, duplicate the whole block!
# Remote Logging (we use TCP for reliable delivery)
#
# An on-disk queue is created for this action. If the remote host is
# down, messages are spooled to disk and sent when it is up again.
#$ActionQueueFileName fwdRule1 # unique name prefix for spool files
#$ActionQueueMaxDiskSpace 1g   # 1gb space limit (use as much as
possible)
#$ActionQueueSaveOnShutdown on # save messages to disk on shutdown
#$ActionQueueType LinkedList   # run asynchronously
#$ActionResumeRetryCount -1    # infinite retries if host is down
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
*.*  @@<server_ip>:514
local8.* @@<server_ip>:514
local9.* @@<server_ip>:514
local10.* @@<server_ip>:514
local11.* @@<server_ip>:514
# ### end of the forwarding rule ###
```

If you want to add more files to log you can add them using the following steps:

i. Add the following set of commands:

```
$ModLoad imfile
        $InputFileName   <path to the file>
        $InputFileTag    <file tag name>
        $InputFileStateFile   <statefile name>
        $InputFileFacility   ---------here x follows up the number
after the previous set
        $InputRunFileMonitor
```

ii. Add the forwarding rule at the bottom of the script as follows:
`localx.* @@:514`

iii. Run the following commands on the CLI to make sure that SELinux doesn't create denial issues and the files have proper labels:

```
semanage fcontext -a -t var_log_t '/Tekelec'
    restorecon '/Tekelec'
    semanage fcontext -a -t var_log_t '/Tekelec/WebNMS'
    restorecon '/Tekelec/WebNMS'
    semanage fcontext -a -t var_log_t '/Tekelec/WebNMS/logs'
    restorecon '/Tekelec/WebNMS/logs'
    semanage fcontext -a -t var_log_t '/Tekelec/WebNMS/logs/
stdout.txt'
    restorecon '/Tekelec/WebNMS/logs/stdout.txt'
    semanage fcontext -a -t var_log_t '/var/log/audit'
    restorecon '/var/log/audit'
    semanage fcontext -a -t var_log_t '/var/log/audit/audit.log'
    restorecon '/var/log/audit/audit.log'
```

iv. Run the following commands on the CLI:

```
[root@EMS1 log]# systemctl restart rsyslog.service
        [root@EMS1 log]# systemctl enable rsyslog.service
```

5. On the server side:

a. Run the following commands on the CLI:

```
[root@EMS2 EMS1]# systemctl start rsyslog.service
[root@EMS2 EMS1]# systemctl enable rsyslog.service  [root@EMS2 EMS1]#
systemctl status rsyslog.service



rsyslog.service - System Logging Service
Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled;
vendor preset: enabled)
Active: active (running) since Mon 2024-02-05 06:03:38 EST; 14s ago
  Docs: man:rsyslogd(8)
      http://www.rsyslog.com/doc/
Main PID: 22130 (rsyslogd)
 CGroup: /system.slice/rsyslog.service
    └─22130 /usr/sbin/rsyslogd -n

Feb 05 06:03:38 EMS2 systemd[1]: Starting System Logging Service...
```

```
Feb 05 06:03:38 EMS2 systemd[1]: Started System Logging Service.
[root@EMS2 EMS1]#
```

b. Edit the configuration file using the command

```
vim /etc/rsyslog.conf
```

and add the following code:

```
# rsyslog configuration file

# For more information see /usr/share/doc/rsyslog-*/rsyslog_conf.html
# If you experience problems, see http://www.rsyslog.com/doc/
troubleshoot.html

#### MODULES ####

# The imjournal module bellow is now used as a message source instead
of imuxsock.
$ModLoad imuxsock # provides support for local system logging (e.g. via
logger command)
$ModLoad imjournal # provides access to the systemd journal
#$ModLoad imklog # reads kernel messages (the same are read from
journald)
#$ModLoad immark  # provides --MARK-- message capability

# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514

# Provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 514

$template MsgFormat, "%msg%\n"

$template FileFormat,"/var/log/%HOSTNAME%/secure"
:msg, contains, "secure-file-tag"
{
*.* -?FileFormat;MsgFormat
&~
}

$template AuditFormat,"/var/log/%HOSTNAME%/Var_Log_Audit.log"
:msg, contains, "audit-file-tag"
{
*.* -?AuditFormat;MsgFormat
&~
}

$template MsgFileFormat,"/var/log/%HOSTNAME%/messages"
:msg, contains, "message-file-tag"
{
*.* -?MsgFileFormat;MsgFormat
&~
```

```
}

$template StdoutFileFormat,"/var/log/%HOSTNAME%/Stdout.txt"
:msg, contains, "stdout-file-tag"
{
*.* -?StdoutFileFormat;MsgFormat
&~
}

$template RemoteLogs,"/var/log/%HOSTNAME%/%PROGRAMNAME%.log"
*.* ?RemoteLogs
&~

#### GLOBAL DIRECTIVES ####

# Where to place auxiliary files
$WorkDirectory /var/lib/rsyslog

# Use default timestamp format
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

# File syncing capability is disabled by default. This feature is
usually not required,
# not useful and an extreme performance hit
#$ActionFileEnableSync on

# Include all config files in /etc/rsyslog.d/
$IncludeConfig /etc/rsyslog.d/*.conf

# Turn off message reception via local log socket;
# local messages are retrieved through imjournal now.
$OmitLocalLogging on

# File to store the position in the journal
$IMJournalStateFile imjournal.state

#### RULES ####

# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                                 /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none                /var/log/
messages

# The authpriv file has restricted access.
authpriv.*                                              /var/log/secure

# Log all the mail messages in one place.
mail.*                                                  -/var/log/
maillog

# Log cron stuff
cron.*                                                  /var/log/cron
```

```
# Everybody gets emergency messages
*.emerg                                                 :omusrmsg:*

# Save news errors of level crit and higher in a special file.
uucp,news.crit                                          /var/log/spooler

# Save boot messages also to boot.log
local7.*                                                /var/log/
boot.log

local4.*        /var/log/ldap.log

# ### begin forwarding rule ###
# The statement between the begin ... end define a SINGLE forwarding
# rule. They belong together, do NOT split them. If you create multiple
# forwarding rules, duplicate the whole block!
# Remote Logging (we use TCP for reliable delivery)
#
# An on-disk queue is created for this action. If the remote host is
# down, messages are spooled to disk and sent when it is up again.
#$ActionQueueFileName fwdRule1 # unique name prefix for spool files
#$ActionQueueMaxDiskSpace 1g   # 1gb space limit (use as much as
possible)
#$ActionQueueSaveOnShutdown on # save messages to disk on shutdown
#$ActionQueueType LinkedList   # run asynchronously
#$ActionResumeRetryCount -1    # infinite retries if host is down
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
#*.* @@remote-host:514
# ### end of the forwarding rule ###
```

6. Make sure that Firewall Setups are done on both the server and the client side using the following commands on the CLI:

```
$ firewall-cmd --permanent --add-port=514/udp
$ firewall-cmd --permanent --add-port=514/tcp
$ firewall-cmd –reload
```

7. Run the following commands on the CLI:

```
[root@EMS2 EMS1]# systemctl restart rsyslog.service
[root@EMS2 EMS1]# systemctl enable rsyslog.service
```

8. The logs from the system will be added to the `%Client_HOSTNAME%` folder that will be on the `path /var/log/` on the server side. For example, in this case, we have the logs in the location

```
[root@EMS2 EMS1]# pwd
/var/log/EMS1
```

Note

- Any change made to the `.conf` files on any side requires to restart and enable the rsyslog service on that particular side.
- Preferably use the following version of rsyslog:

```
[root@EMS1 log]# rsyslogd -v
rsyslogd 8.24.0-52.el7, compiled with:
    PLATFORM: x86_64-redhat-linux-gnu
    PLATFORM (lsb_release -d):
    FEATURE_REGEXP: Yes
    GSSAPI Kerberos 5 support: Yes
    FEATURE_DEBUG (debug build, slow code): No
    32bit Atomic operations supported: Yes
    64bit Atomic operations supported: Yes
    memory allocator:          system default
    Runtime Instrumentation (slow code): No
    uuid support: Yes
    Number of Bits in RainerScript integers: 64
```

For more information, see http://www.rsyslog.com.

P

Transport Exception while launching Application(.jnlp)

Transport Exception Error is observed when jnlp is launched and application is not able to connect to the server.

Solution:

1. Navigate to `<Installation Path of JAVA/JDK>\security` and update `java.security`. If the path is not known, then search for the file in the jdk installation directory file. Remove the parameter TLSv1, TLSV1.1:
   Before:

   ```
   # Example:
   # jdk.tls.disabledAlgorithms=MD5, SSLv3, DSA, RSA keySize < 2048
   jdk.tls.disabledAlgorithms=SSLv3, TLSv1, TLSv1.1, RC4, DES, MD5withRSA, \
   # DH keySize < 1024, EC keySize < 224, 3DES_EDE_CBC, anon, NULL, \
   # include jdk.disabled.namedCurves
   ```

   After:

   ```
   # Example:
   # jdk.tls.disabledAlgorithms=MD5, SSLv3, DSA, RSA keySize < 2048
   jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5withRSA, \
   DH keySize < 1024, EC keySize < 224, 3DES_EDE_CBC, anon, NULL, \
   include jdk.disabled.namedCurves\
   ```

2. Clean the cache in the user directory. For example, .cache.

> **Note**
>
> These steps need to be performed in the client machine (where the GUI will open).