System Release 7.17
ASTRO ® 25
INTEGRATED VOICE AND DATA

Unified Event Manager

NOVEMBER 2016

MN003370A01-A

Copyrights

The Motorola Solutions products described in this document may include copyrighted Motorola Solutions computer programs. Laws in the United States and other countries preserve for Motorola Solutions certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola Solutions computer programs contained in the Motorola Solutions products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola Solutions.

Furthermore, the purchase of Motorola Solutions products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola Solutions, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a particular system, or may be dependent upon the characteristics of a particular mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola Solutions contact for further information.

Trademarks

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

European Union (EU) Waste of Electrical and Electronic Equipment (WEEE) directive

The European Union's WEEE directive requires that products sold into EU countries must have the crossed out trash bin label on the product (or the package in some cases).

As defined by the WEEE directive, this cross-out trash bin label means that customers and end-users in EU countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end-users in EU countries should contact their local equipment supplier representative or service centre for information about the waste collection system in their country.

This page intentionally left blank.

Contact Us

Motorola Solutions Support Center

The Solutions Support Center (SSC) is the primary Motorola Solutions support contact. Call:

- Before any software reload.
- To confirm troubleshooting results and analysis before removing and replacing a Field Replaceable Unit (FRU) and Field Replaceable Entity (FRE) to repair the system.

For...	Phone
United States Calls	**800-221-7144**
International Calls	**302-444-9800**

North America Parts Organization

For assistance in ordering replacement parts or identifying a part number, contact the Motorola Solutions Parts organization. Your first response when troubleshooting your system is to call the Motorola Solutions SSC.

For...	Phone
Phone Orders	**800-422-4210** (US and Canada Orders) For help identifying an item or part number, select choice 3 from the menu.
	302-444-9842 (International Orders) Includes help for identifying an item or part number and for translation as needed.
Fax Orders	**800-622-6210** (US and Canada Orders)

Comments

Send questions and comments regarding user documentation to documentation@motorolasolutions.com.

Provide the following information when reporting a documentation error:

- The document title and part number
- The page number with the error
- A description of the error

We welcome your feedback on this and other Motorola Solutions manuals. To take a short, confidential survey on Motorola Solutions Customer Documentation, go to docsurvey.motorolasolutions.com or scan the following QR code with your mobile device to access the survey.

This page intentionally left blank.

Document History

Version	Description	Date
MN003370A01-A	Original release of the *Unified Event Manager* manual	November 2016

This page intentionally left blank.

Contents

This page intentionally left blank.

List of Figures

List of Tables

List of Processes

This page intentionally left blank.

List of Procedures

This page intentionally left blank.

About Unified Event Manager

This manual provides an introduction to Unified Event Manager (UEM). Included is a comprehensive introduction, tools used for troubleshooting, and system-level troubleshooting.

This manual covers the use of UEM, the application that provides reliable fault management services for devices in the ASTRO® 25 IV&D radio system. It includes a comprehensive introduction, description of operation and troubleshooting.

What Is Covered In This Manual?

This manual contains the following chapters:

- UEM Description on page 37, provides a functional description of Unified Event Manager (UEM).
- UEM Installation on page 79, contains installation requirements for UEM.
- UEM Configuration on page 81, contains configuration procedures necessary to make UEM operational.
- UEM Optimization on page 121, contains procedures for optimizing UEM hardware and software components.
- UEM Operation on page 123, contains procedures for operating UEM.
- UEM Maintenance on page 245, contains periodic maintenance procedures for UEM.
- UEM Troubleshooting on page 255, contains troubleshooting procedures and information.
- Digital Notification on page 275, contains information about the Digital Notification feature.
- Terminal Session Software Installation on page 289, provides installation procedures for software that you can use to launch terminal sessions for the network elements managed on UEM through SDM3000 SCADA.

Helpful Background Information

Motorola Solutions offers various courses designed to assist in learning about the system. For information, go to http://www.motorolasolutions.com/training to view the current course offerings and technology paths.

Related Information

For associated information about the radio system, see the following documents:

Related Information	Purpose
Standards and Guidelines for Communication Sites	Provides standards and guidelines that should be followed when setting up a Motorola Solutions communications site. Also known as the R56 manual. This manual may be purchased on CD 9880384V83, by calling the North America Parts Organization at 800-422-4210 (or the international number: 302-444-9842).
System Overview and Documentation	Provides an overview of the ASTRO® 25 new system features, documentation set, technical illustrations, and system-level dis-

Table continued…

Related Information	Purpose
	aster recovery that support the ASTRO® 25 radio communication system.
Dynamic System Resilience Feature Guide	Provides information necessary to understand, operate, maintain, and troubleshoot the Dynamic System Resilience (DSR) feature that adds a geographically separate backup zone core to an existing zone core to protect against catastrophic zone core failures.
Edge Availability with Wireline Console Feature Guide for Trunking Subsystems	Provides an overview of the Edge Availability with Wireline Console feature which supports the Trunking subsystem (Tsub) architecture in M core ASTRO® 25 systems. It also includes setup and management instructions for the Tsub. The Tsub provides dispatch and mobility services within a local area when normal system-wide area communication is not possible.
License Manager	Provides information about the use of licenses to gain access to features and functions in ASTRO® 25 systems, including the installation of the License Manager in the system and instructions on using the web-based License Manager user interface to load, view, and manage licenses in the system.
MOSCAD Network Fault Management Feature Guide	Provides information required to install, configure, manage, and use the MOSCAD® Network Fault Management (NFM), an optional ASTRO® 25 systems solution that provides tools to configure, monitor, and control auxiliary system devices, such as tower lights or power and environmental equipment, in communication sites.
Private Network Management Client	Describes how to install, configure, and manage the Private Network Management (PNM) client, a PC workstation which system administrators and technicians use for a variety of system-related tasks, such as viewing equipment operational status, monitoring network utilization and performance, or viewing alarms generated by system equipment.
Private Network Management Servers	Provides information on the installation, configuration, and management of the Private Network Management (PNM) servers, namely, Air Traffic Router (ATR), User Configuration Server (UCS), Unified Event Manager (UEM), Zone Database Server (ZDS), System Statistical Server (SSS), and Zone Statistical Server (ZSS).
SNMPv3	Provides information relating to the implementation and management of the SNMPv3 protocol in ASTRO® 25 systems.
UEM/GMC Transition Setup Guide	Provides an introduction to a transition from Unified Event Manager (UEM) and MOSCAD Network Fault Management (NFM) software to a centralized and integrated management solution.
Virtual Management Server Hardware	Provides information for implementing, maintaining, and replacing common Hewlett-Packard hardware for servers in ASTRO® 25 systems.
Virtual Management Server Software	Provides procedures for implementing and managing VMware ESXi-based virtual server hosts on the common Hewlett-Packard hardware platform in ASTRO® 25 systems.

Chapter 1

UEM Description

Unified Event Manager (UEM) is an application that provides reliable fault management services for the ASTRO® 25 system.

The main functions of UEM are:

- Device discovery
- Fault management
- Supervision
- Synchronization

Licensing of Unified Event Manager

In the ASTRO® 25 system, you need to purchase a license or licenses to get access to selected applications, features, and services. UEM is a licensed application. This means that to use UEM, you need to purchase one or more licenses. There are two kinds of licenses:

- session licenses
- feature licenses

Sessions Licensed in Unified Event Manager

Session licenses are used to manage a number of application client sessions. For UEM, you can buy several licenses for a group of users. When a user starts a UEM session, a license from a pool of your session licenses is used. For L and M core system configuration, depending on the licenses, you can simultaneously manage 16 UEM client sessions, including 2 dedicated sessions for the **sscadmin** user. For K core system configuration, depending on the licenses, you can simultaneously manage 5 UEM client sessions. For more information, see the *License Manager* manual.

Features Licensed in Unified Event Manager

Apart from session licenses that enable you to manage a number of UEM client sessions, there are also feature licenses that manage your use of system features, capabilities, and services. You need a license to enable and use licensed features. In UEM, the following services are licensed:

- e-mail notifications
- North Bound Interface (NBI)
- system maps
- geographical maps
- site views
- network element views
- microwave user interface

This means that to use these services, you need to purchase the appropriate feature licenses. For more information, see the *License Manager* manual.

1.1
IP-Managed Devices

An IP-managed device is any device that does not support any protocol-based management interface. Therefore, these devices have limited fault management capabilities in UEM. These devices are discovered as generic nodes, and are supervised using Internet Control Message Protocol (ICMP) requests. UEM still manages and reports communication link status of these devices.

1.2
Protocols Supported by UEM

Devices that are managed by Unified Event Manager (UEM) support various protocols.

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is a set of protocols used for managing complex networks. It is an application layer protocol that facilitates the exchange of management information between network devices. It is also a part of the Transmission Simple Network Management Protocol (SNMP) is a set of protocols used for managing complex networks. It is an application layer protocol that facilitates the exchange of management information between network devices. It is also a part of the Transmission Control Protocol/Internet Protocol (TCP/IP) suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

SNMPv3 prevents the following threats:

Modification of Information
An unauthorized entity alters messages or values generated by an authorized entity in the system.

Masquerade
An unauthorized entity assumes the identity of an authorized entity.

Message Stream Modification
Malicious reordering, delaying, or replaying of messages that result in the disruption of normal sub-network service operation. This disruption could bring about unauthorized management operations.

Disclosure
Eavesdropping on the exchanges between SNMPv3 engines.

SNMPv1

SNMPv1 is the original request-response protocol and framework of the Simple Network Management Protocol. The Network Management System (NMS) issues a request, and the managed devices return responses. Four protocol operations are used in an SNMPv1 framework:

- GET
- GETNEXT
- SET
- TRAP

SNMPv2

SNMPv2 improves upon the existing SNMPv1 and adds two new protocol operations: GETBULK and INFORM.

SNMPv3

In comparison to SNMPv2, SNMPv3 offers greater capability to protect your resources against threats.

SNMPv3 supports authentication and encryption, and is specified in its User-Based Security Model (USM). The View-based Access Control Model (VACM) is an SNMPv3 approach for Management Information Base (MIB) access control.

Reliable fault information is also a part of SNMPv3. It involves utilizing INFORMs to reliably deliver fault information to a management entity.

SNMPv3 has three security levels. The following table explains which SNMPv3 security levels require authentication and privacy passphrases.

Table 1: SNMPv3 Security Levels

Security Level	AuthProtocol and AuthPassphrase	PrivProtocol and PrivPassphrase
NoAuthNoPriv	No	No
AuthNoPriv	Yes	No
AuthPriv	Yes	Yes

Web Service Protocol

Web Service protocols are used to communicate with VMware devices such as ESXi and vCenter. The protocols are based on Simple Object Access Protocol (SOAP) and offer authentication and encryption over SSL.

1.3 Reliable Communication

A network element and the Element Management System (EMS) communicate with each other, exchange information, and acknowledge the exchange of messages.

Reliable communication devices use INFORMs, which are the messages (events or alarms) sent by the network element to the management entity. INFORMs are applicable to the network element that uses either SNMPv2 or SNMPv3.

1.4 Agents

An agent is software that runs within each device. It responds to all protocols supported by the Unified Event Manager (UEM) server and reports all the events of interest to the management entity.

1.5 Redundancy Management

Redundancy is the backup mechanism which takes over the function of a device in case it fails to provide its core services, for example due to malfunction. Redundancy management includes the capability of the network element and the management entity to provide and report such a failover condition.

1.6 Synchronization

UEM performs synchronization automatically, by validating the health of a device with the information stored in the fault management database.

If UEM finds a discrepancy, it generates an event or an alarm. Synchronization can also be:

- Periodic synchronization triggered by the system clock
- New device discovery
- Rediscovery of an existing device
- User-initiated synchronization (see Synchronizing Managed Resources on page 196)

NOTICE: The synchronization process only generates an alarm when it detects that the state of a device differs from the state currently reported by UEM.

1.7 Supervision

Unified Event Manager (UEM) periodically checks its ability to communicate with the devices it manages.

This operation is referred to as supervision and is used to determine the following:

- Whether communication with the device is lost
- For SNMPv3 devices that support reliable communication, whether UEM is supposed to initiate synchronization with the device

If a device does not respond to the supervision query in a timely manner, UEM generates a **Communication Loss** event or alarm against the managed device.

1.8 North Bound Interface

North Bound Interface (NBI) describes an interface offered by many Network Management System (NMS) products, such as Unified Event Manager (UEM). NBI allows for NMS features, functions, and data to be accessible for Operations Support System (OSS) and Manager of Managers (MoM). The OSS can use the NBI to retrieve information from NMS. It uses SNMP which is a standardized protocol. It is also typical for NMS to forward information automatically to the OSS. An example of such notification is the trap forwarding function available in most NMS products.

The customer NBI Manager of Managers (MoM) interface is a licensed UEM service that is available only for users with a feature license for the NBI service. For more information about licenses, see the *License Manager* manual.

Unified Event Manager (UEM) supports the capability to send up events to hosts that support data processing by applications other than Motorola Solutions applications. An example of such a host is the Manager of Managers (MoM). The customer-processed data is typically viewed as reports by managers who are interested to see a summary of information from the NMS.

UEM supports North Bound Interface (NBI) for sending up notifications to the registered MoMs. Currently, there are four interfaces that are supported; two for the Motorola Solutions Support Center (SSC) interface and two for the customer MoM interface. NBI uses SNMPv3 and the User-Based Security Model (USM) to provide secure communication between UEM and NMS.

NBI services are:

Getting QuickSync events
UEM provides the means for NMS to query and obtain a set of events from the UEM datastore. This feature is typically used when the missed trap is within the last five minutes or among the most recent 5000 traps captured in NMS.

NBI Alarm Synchronization
UEM provides the means for NMS to query and obtain a set of alarms from the UEM datastore. This feature is typically used to re-synchronize fault information on the NMS after an extended outage.

NBI Event Forwarding
The events reported on UEM are sent to registered NMS using SNMPv3 traps.

NBI Event Synchronization
UEM provides the means for NMS to query and obtain a set of events from the UEM datastore. This feature is typically used to obtain events missed due to lost traps or when connectivity between UEM and NMS is lost temporarily.

NBI Notification Persistence
UEM stores events from the last five minutes or the last 5000 events forwarded to enable NMS to quickly retrieve any events it may have missed.

REST Inventory
This service allows NMS to retrieve a full or filtered list of managed Network Elements from UEM.

1.9 Secure E-mail Communication

Secure e-mail communication is a solution certified by Motorola Solutions. The solution provides encrypted notifications by using Simple Mail Transfer Protocol (SMTP) over Transport Layer Security (TLS), that is STARTTLS. Unified Event Manager (UEM) allows for secure e-mail communication. The secure e-mail communication takes place through an encrypted tunnel from UEM to a mail transfer agent, an e-mail server.

SMTP over TLS has an Internet Engineering Task Force (IETF) standard (RFC 2487) and is supported by a wide range of e-mail vendors including Microsoft Exchange, Lotus Domino, and Sendmail. Verify that your e-mail server vendor supports SMTP over TLS. SMTP over TLS prevents e-mail sniffing in transit, since the messages are encrypted during transmission.

UEM sends outgoing mail only. It does not receive incoming mail, and does not use Post Office Protocol (POP) or Internet Message Access Protocol (IMAP).

Secure and non-secure e-mail communication is a licensed UEM service that is available only for users with a feature license for the e-mail notification service. For more information about licenses, see the *License Manager* manual.

1.10 UEM Overview

Unified Event Manager (UEM) is a fault management application designed for critical fault management.

UEM primary functions are:

- Processing fault notifications
- Detecting and reporting loss of communication with managed devices (see Supervision on page 40)
- Making sure that the status reported is up-to-date (see Synchronization Operations on page 196)
- Discovering a device within the system
- Troubleshooting faults
- Sending commands to network elements
- Displaying values for network elements

UEM presents the faults and, in general, the status of the network elements in the following views:

- Alarms
- Maps
- Network Events

- Network Database
- Network Elements
- Sites

These views and their operations are explained in detail in Fault Management Operations on page 153.

UEM user accounts are managed within the application. You can set up system partitions and assign management responsibility to one or more administrators. The setup and maintenance of accounts are explained in UEM Configuration on page 81 and Security Management Operations on page 217. UEM also controls critical management operations invoked by operators within the application.

UEM provides the capability to manage devices securely (using SNMPv3). UEM can detect and report loss of fault notifications. It can quickly update without constantly polling the devices.

UEM North Bound Interface (NBI) supports notifications in the form of SNMPv3 traps to registered managers and access to management data. The NBI uses SNMPv3 and the User-Based Security Model (USM) to provide a secure communication between UEM and Network Management System (NMS).

For details on the devices and subsystems that UEM manages, see Groups of Network Elements Managed by UEM on page 42.

1.10.1
Dynamic System Resilience

In systems with the Dynamic System Resilience (DSR) feature, there are two operational Unified Event Manager (UEM) servers in each zone. The UEM servers are placed in the primary and backup zone cores, which are usually geographically separated. The UEM servers also have different host names and IP addresses. Both UEMs manage zone-level fault information. However, the two UEMs are not synchronized and operate independently. Changes made to one UEM do not affect the operation of the other UEM.

In case of a failure at the primary zone core, log on to UEM located in the backup core. For more information, see UEM Client Operations on page 123.

In DSR systems, perform discovery for all devices separately for each UEM. Managed devices send notifications to both UEMs independently.

For more information on the DSR feature, see the *Dynamic System Resilience Feature Guide*.

1.10.2
Groups of Network Elements Managed by UEM

Unified Event Manager (UEM) manages numerous groups of network elements. When you discover a whole group of network elements, you are asked to specify the discovery type for the group of network elements. When you discover a single network element, you can use the discovery type of the network element to identify the network element parent network type. Learn more about discovery (management) types for specific network element.

Related Links

SNMPv3 Devices Troubleshooting on page 264

1.10.2.1

Backhaul Network Elements

Unified Event Manager (UEM) manages Backhaul network elements. See the list of Backhaul network elements and their management type.

Table 2: Network Elements Managed in the Backhaul Discovery Type

Network Element Name	Management Type
Core Backhaul Switch 1-2	SNMPv3
Extreme E4G Switches	SNMPv3
HP Switches	SNMPv3
Point-To-Point (PTP) network elements	SNMPv3
Site Backhaul Switches	SNMPv3

1.10.2.2

Circuit Multisite Subsystem Network Elements

Unified Event Manager (UEM) manages Circuit Multisite Subsystem network elements. See the list of Circuit Multisite Subsystem network elements and their management type.

Table 3: Network Elements Managed in the Circuit Multisite Subsystem Discovery Type

Network Element Name	Management Type
Conventional Channel Gateway (CCGW)	SNMPv3
Ethernet Switch	SNMPv3
G-Series Sub-site Link Converter	SNMPv3
GCM 8000 Comparator	SNMPv3
GCM 8000 Conventional Comparator	SNMPv3
GCP 8000 HPD Site Controller	SNMPv3
GCP 8000 Repeater Site Controller	SNMPv3
GPB 8000 Reference Distribution Module (RDM)	SNMPv3
GRV 8000 Conventional Comparator	SNMPv3
GTR 8000 Base Radio (for HPD)	SNMPv3
GTR 8000 Base Radio (for Multisite)	SNMPv3
GTR 8000 Base Radio (Trunked or Conventional)	SNMPv3
GTR 8000 Repeater Base Radio	SNMPv3
ISSI/MPTT Gateway	SNMPv3
ISSI/MPTT Site Relay	SNMPv3
Linear Simulcast Station	SNMPv3
MOSCAD NFM RTU	SNMPv3
Out-of-Band Management Terminal Server	SNMPv3
PSC 9600 Repeater Site Controller	SNMPv3

Table continued…

Network Element Name	Management Type
RF Site Generic Application Server (GAS)	SNMPv3
Site Router	SNMPv3
SmartX Site Converter	SNMPv3
Terminal Server	SNMPv3
TRAK (NTP Server)	SNMPv3
ISSI/MPTT Firewall Fault Management	IP management only
MPTT iLO	IP management only
NTP Server	IP management only

1.10.2.3

Console Site Network Elements

Unified Event Manager (UEM) manages Console Site network elements. See the list of Console Site network elements and their management type.

Table 4: Network Elements Managed in the Console Site Discovery Type

Network Element Name	Management Type
Console Alias Manager (CAM) Server	SNMPv3
Conventional Channel Gateway (CCGW)	SNMPv3
Conventional Site Controller	SNMPv3
Domain Controllers	SNMPv3
Ethernet Switch	SNMPv3
G-Series Sub-site Link Converter	SNMPv3
GCM 8000 Comparator	SNMPv3
GCM 8000 Conventional Comparator	SNMPv3
Group Data Gateway (GDG)	SNMPv3
GRV 8000 Conventional Comparator	SNMPv3
GTR 8000 Base Radio (Trunking or Conventional)	SNMPv3
MCC 7500 AUX I/O Server	SNMPv3
MCC 7500 IP Logging Recorder	SNMPv3
MCC 7500 VPM	SNMPv3
MOSCAD NFM RTU	SNMPv3
Site Router	SNMPv3
Virtual Server Platform	SNMPv3
Backup and Restore Server	IP management only
CADI Client	IP management only
Computer Telephony Integration (CTI)	IP management only
Computer Telephony Integration (CTI) Client	IP management only

Table continued…

Network Element Name	Management Type
Computer Telephony Integration (CTI) Server	IP management only
Console Proxy	IP management only
Console Telephony Media Gateway	IP management only
MOSCAD NFM Graphical Workstation Computer (GWC)	IP management only
NICE Inform Server	IP management only
NICE Replay Station	IP management only
NM Clients	IP management only
Printer	IP management only
Replay Stations	IP management only
Software Console Dispatch Operator Position	IP management only
Virtual Server iLO	IP management only

1.10.2.4

Conventional Subsystem Network Elements

Unified Event Manager (UEM) manages Conventional Subsystem network elements. Conventional Subsystems consist of conduit hubs, hubs, and base repeater sites. See the list of Conventional Subsystem network elements and their management type.

Table 5: Network Elements Managed in the Conventional Subsystem Discovery Type

Network Element Name	Management Type
Backup – Conventional Site Controller	SNMPv3
CAM Server	SNMPv3
Configuration Manager	SNMPv3
Console Alias Manager (CAM) Server	SNMPv3
Console Manager	SNMPv3
Conventional Channel Gateway (CCGW)	SNMPv3
Conventional Site Controller	SNMPv3
Domain Controller	SNMPv3
Ethernet Switch	SNMPv3
G-Series Sub-site Link Converter	SNMPv3
GCM 8000 Comparator	SNMPv3
GCM 8000 Conventional Comparator	SNMPv3
GRV 8000 Conventional Comparator	SNMPv3
GTR 8000 Base Radio (Trunking or Conventional)	SNMPv3
MCC 7500 AUX I/O Server	SNMPv3
MCC 7500 IP Logging Recorder	SNMPv3
MCC 7500 VPM	SNMPv3

Table continued…

Network Element Name	Management Type
MOSCAD NFM RTU	SNMPv3
Out-of-Band Management Terminal Server	SNMPv3
Site Router	SNMPv3
Terminal Server	SNMPv3
Virtual Server Platform	SNMPv3
Backup and Restore Server	IP management only
CADI Client	IP management only
Computer Telephony Integration (CTI) Client	IP management only
Console Proxy	IP management only
Console Telephony Media Gateway	IP management only
IP Link Converters (channel endpoints at hub and base radio sites)	IP management only
IP Link Converters (physical Ethernet port addresses)	IP management only
MOSCAD NFM Graphical Master Computer (GMC)	IP management only
MOSCAD NFM Graphical Workstation Computer (GWC)	IP management only
NICE Inform Server	IP management only
NICE Replay Station	IP management only
NM Clients	IP management only
Replay Stations	IP management only
Printer	IP management only
Software Console Dispatch Operator Position	IP management only
Virtual Server iLO	IP management only

1.10.2.5

Customer Enterprise Network (CEN) Network Elements

Unified Event Manager (UEM) manages CEN network elements. See the list of CEN network elements and their management type.

Table 6: Network Elements Managed in the Customer Enterprise Network Discovery Type

Network Element Name	Management Type
Border Router	SNMPv3

1.10.2.6

Dynamic System Resilience Shared Network Network Elements

Unified Event Manager (UEM) manages Dynamic System Resilience (DSR) Shared Network network elements. See the list of DSR Shared Network network elements and their management type.

Table 7: Network Elements Managed in the DSR Shared Network Discovery Type

Network Element Name	Management Type
Backup – Core Backhaul Switch	SNMPv3
Core Backhaul Switch	SNMPv3
Exit Routers (1-4)	SNMPv3
Gateway Router	SNMPv3
GGSN	SNMPv3
LAN Switch Network Management Interface (Backup/ Tertiary/Primary)	SNMPv3
Mediation LAN Switch	SNMPv3
Out-of-Band Management Terminal Server	SNMPv3
Terminal Server	SNMPv3
Terminal Server Remote Analog Access IP	SNMPv3

1.10.2.7

IP Multisite Subsystem Network Elements

Unified Event Manager (UEM) manages IP Multisite Subsystem network elements. See the list of IP Multisite Subsystem network elements and their management type.

Table 8: Network Elements Managed in the IP Multisite Subsystem Discovery Type

Network Element Name	Management Type
Conventional Channel Gateway (CCGW)	SNMPv3
Ethernet Switch	SNMPv3
G-Series Sub-site Link Converter	SNMPv3
GCM 8000 Comparator	SNMPv3
GCM 8000 Conventional Comparator	SNMPv3
GCP 8000 HPD Site Controller	SNMPv3
GCP 8000 Repeater Site Controller	SNMPv3
GPB 8000 Reference Distribution Module (RDM)	SNMPv3
GRV 8000 Conventional Comparator	SNMPv3
GTR 8000 Base Radio (for HPD)	SNMPv3
GTR 8000 Base Radio (Trunking or Conventional)	SNMPv3
GTR 8000 Multisite Base Radio (MSBR)	SNMPv3
GTR 8000 Repeater Base Radio	SNMPv3

Table continued…

Network Element Name	Management Type
IP Simulcast Backhaul Switch	SNMPv3
ISSI/MPTT Gateway	SNMPv3
ISSI/MPTT Site Relay	SNMPv3
MOSCAD NFM RTU	SNMPv3
MTC 9600 Multisite Controller	SNMPv3
Out-of-Band Management Terminal Server	SNMPv3
PSC 9600 Repeater Site Controller	SNMPv3
Remote Site Router	SNMPv3
RF Site Generic Application Server (GAS)	SNMPv3
Site Router	SNMPv3
SmartX Site Converter	SNMPv3
Terminal Server	SNMPv3
TRAK (NTP Server)	SNMPv3
ISSI/MPTT Firewall Fault Management	IP management only
MPTT iLO	IP management only
NTP Server	IP management only

1.10.2.8
Primary Zone Core Network Elements

Unified Event Manager (UEM) manages Primary Zone Core network elements. See the list of Primary Zone Core network elements and their management type. For all primary zone core network elements, in the system, there are backup zone core network elements of the same management type.

Table 9: Network Elements Managed in the Primary Zone Core Discovery Type

Network Element Name	Management Type
Air Traffic Router (ATR)	SNMPv3
Backup and Restore Server	SNMPv3
Conventional Packet Data Router	SNMPv3
Core Router (RP 1–8)	SNMPv3
Direct Attached Storage (DAS) Management Controller	SNMPv3
Domain Controller	SNMPv3
Dynamic Transcoder	SNMPv3
Exit Routers 1–4	SNMPv3
Fortinet Firewall	SNMPv3
Gateway Router #1	SNMPv3
Gateway Router #2	SNMPv3
Generic Application Server (GAS)	SNMPv3

Table continued…

Network Element Name	Management Type
GGSN	SNMPv3
HPD Packet Data Router	SNMPv3
ISGW Network Management Interface	SNMPv3
IVD Packet Data Router	SNMPv3
LAN Switch Network Management Interface (Backup/ Tertiary/Primary)	SNMPv3
License Manager	SNMPv3
Intersystem Gateway	SNMPv3
IP Packet Capture (IPCAP)	SNMPv3
Mediation LAN Switch #1	SNMPv3
Mediation LAN Switch #2	SNMPv3
MOSCAD NFM RTU	SNMPv3
Out-of-Band Management Terminal Server	SNMPv3
Remote Analog Access Server	SNMPv3
Service Server	SNMPv3
Terminal Server	SNMPv3
Terminal Server Remote Analog Access IP	SNMPv3
TMG	SNMPv3
TRAK (NTP Server)	SNMPv3
Unified Event Manager (UEM) (NM Server)	SNMPv3
vCenter Server	SNMPv3
Virtual Server Platform	SNMPv3
Zone Controller	SNMPv3
Zone Database Server (NM Server)	SNMPv3
Zone Statistics Server (ZSS) (NM Server)	SNMPv3
Firewalls	IP management only
Fortinet Firewall Manager	IP management only
IP PBX	IP management only
IP PBX Media Gateways	IP management only
MOSCAD NFM Graphical Master Computer (GMC)	IP management only
MOSCAD NFM Graphical Workstation Computer (GWC)	IP management only
NM Clients	IP management only
NTP Server	IP management only
Printer	IP management only
Security Manager Client	IP management only
Syslog Server	IP management only
Virtual Center VM	IP management only

1.10.2.9

Primary Operations Support Systems Network Elements

Unified Event Manager (UEM) manages Primary Operations Support Systems network elements. See the list of Primary Operations Support Systems network elements and their management type. For all primary operations support systems network elements, in the system, there are backup operations support systems network elements of the same management type.

Table 10: Network Elements Managed in the Primary Operations Support Systems Discovery Type

Network Element Name	Management Type
Authentication Server (AuC)	SNMPv3
Backup and Restore Server (BAR)	SNMPv3
Core Security Management Server (CSMS)	SNMPv3
Domain Controller	SNMPv3
Generic Application Server (GAS)	SNMPv3
Performance Manager (InfoVista Server)	SNMPv3
System Statistics Server (SSS) (NM Server)	SNMPv3
Unified Network Configurator (UNC)/Unified Network Configurator Device Server (UNCDS) (NM Server)	SNMPv3
User Configuration Server (NM Server)	SNMPv3
Fortinet Firewall Manager	IP management only
NM Client	IP management only
Printer	IP management only
Virtual Server Platform	IP management only

1.10.2.10

RF Site Network Elements

Unified Event Manager (UEM) manages Radio Frequency (RF) Site network elements. See the list of RF Site network elements and their management type.

Table 11: Network Elements Managed in the RF Site Discovery Type

Network Element Name	Management Type
Conventional Channel Gateway (CCGW)	SNMPv3
Ethernet Switch	SNMPv3
GCM 8000 Comparator	SNMPv3
GCM 8000 Conventional Comparator	SNMPv3
GCP 8000 Repeater Site Controller	SNMPv3
GCP 8000 Simulcast Site Controller	SNMPv3
GPB 8000 Reference Distribution Module (RDM)	SNMPv3
GTR 8000 Base Radio (for HPD)	SNMPv3
GTR 8000 Base Radio (Trunking or Conventional)	SNMPv3

Table continued…

Network Element Name	Management Type
GTR 8000 Repeater Base Radio	SNMPv3
IntelliSite Repeater channels	SNMPv3
ISSI/MPTT Gateway*	SNMPv3
MOSCAD NFM RTU	SNMPv3
Out-of-Band Management Terminal Server	SNMPv3
PSC 600 Site Controller	SNMPv3
PSC 9600 Repeater Site Controller	SNMPv3
RF Site Generic Application Server (GAS)	SNMPv3
Site Controller (for High Performance Data (HPD))	SNMPv3
Site Relay	SNMPv3
Site Router	SNMPv3
SmartX Site Converter	SNMPv3
TRAK (NTP Server)	SNMPv3
ISSI/MPTT Firewall Fault Management	IP management only
MPTT iLO	IP management only
NTP Server	IP management only

* The MPTT Gateway refers to the Public Safety Push-To-Talk (PTT) Gateway.

1.10.2.11

Trunking Subsystem Network Elements

Unified Event Manager (UEM) manages network elements in Trunking Subsystems (Tsub).

A Tsub consists of the Tsub prime site and remote sites supporting any of the following site types:

- Centralized Conventional Site
- Console Site (NM/Dispatch Site)
- RF sites:
  - ASTRO® 25 Site Repeater (ASR) site
  - High Performance Data (HPD) Site
  - IP Simulcast Subsite

When Tsub local area operation occurs due to loss of transport connectivity to the zone core, any further failures that occur within the Tsub are not visible to UEM. In addition, remote configuration of Tsub devices while operating in this state is not possible unless the Tsub prime site is equipped with a Terminal Server.

Table 12: Network Elements Managed in the Trunking Subsystem Discovery Type

Network Element Name	Management Type
Console Alias Manager (CAM) Server	SNMPv3
Conventional Channel Gateway (CCGW)	SNMPv3
Conventional Site Controller	SNMPv3

Table continued…

Network Element Name	Management Type
Domain Controller	SNMPv3
Dynamic Transcoder	SNMPv3
Ethernet Switch	SNMPv3
G-Series Sub-site Link Converter	SNMPv3
GCM 8000 Comparator	SNMPv3
GCM 8000 Conventional Comparator	SNMPv3
GCP 8000 HPD Site Controller	SNMPv3
GCP 8000 Repeater Site Controller	SNMPv3
GCP 8000 Simulcast Site Controller	SNMPv3
GPB 8000 Reference Distribution Module (RDM)	SNMPv3
GRV 8000 Conventional Comparator	SNMPv3
GTR 8000 Base Radio (for HPD)	SNMPv3
GTR 8000 Base Radio (Trunking or Conventional)	SNMPv3
GTR 8000 Repeater Base Radio	SNMPv3
GTR 8000 Multisite Base Radio (MSBR)	SNMPv3
IntelliSite Repeater channels	SNMPv3
IP Packet Capture	SNMPv3
IP Simulcast Backhaul Switch	SNMPv3
MCC 7500 AUX I/O Server	SNMPv3
MCC 7500 IP Logging Recorder	SNMPv3
MCC 7500 VPM	SNMPv3
MOSCAD NFM RTU	SNMPv3
MTC 9600 Multisite Controller	SNMPv3
Out-of-Band Management Terminal Server	SNMPv3
Remote Site Router	SNMPv3
Site Router	SNMPv3
Terminal Server	SNMPv3
TRAK (NTP Server)	SNMPv3
Virtual Server Platform	SNMPv3
Zone Controller	SNMPv3
CADI Client	IP management only
Computer Telephony Integration (CTI)	IP management only
Computer Telephony Integration (CTI) Client	IP management only
Computer Telephony Integration (CTI) Server	IP management only
Console Proxy	IP management only
Console Telephony Media Gateway	IP management only

Table continued…

Network Element Name	Management Type
NICE Inform Server	IP management only
NICE Replay Station	IP management only
NM Clients	IP management only
NTP Server	IP management only
Printer	IP management only
Replay Stations	IP management only
Software Console Dispatch Operator Position	IP management only
Virtual Server iLO	IP management only

1.10.2.12

Network Elements Reported in UEM through MOSCAD RTUs

Unified Event Manager (UEM) manages network elements reported through MOSCAD Remote Terminal Units (RTUs). See the list of network elements reported through MOSCAD RTUs and their management type.

Table 13: Network Elements Managed through MOSCAD RTUs

Network Element Name	Hardware Type	Management Type
Alcatel Fial Polling Engine	N/A	SNMP over SCADA
Alcatel Microwave Radio DMX-3003	N/A	SNMP over SCADA
Alcatel Microwave Radio MDR-4000	N/A	SNMP over SCADA
Alcatel Microwave Radio MDR-5600	N/A	SNMP over SCADA
Alcatel Microwave Radio MDR-6000	N/A	SNMP over SCADA
Alcatel Microwave Radio MDR-7000	N/A	SNMP over SCADA
Alcatel Microwave Radio MDR-8000 DS1	N/A	SNMP over SCADA
Alcatel Microwave Radio MDR-8000 DS3	N/A	SNMP over SCADA
Alcatel Microwave Radio RDI-3100	N/A	SNMP over SCADA
Aviat Microwave Radio – Constella-tion	N/A	SNMP over SCADA
Aviat Microwave Radio – MicroStar	N/A	SNMP over SCADA
Aviat Microwave Radio – DVT	N/A	SNMP over SCADA
Aviat Microwave Radio – MegaStar	N/A	SNMP over SCADA
Aviat Microwave Radio – Truepoint	N/A	SNMP over SCADA
Eclipse Microwave Radio – AUX	AUX_6TTL AUX_4TTL AUX_2TTL	SNMP over SCADA

Table continued…

Network Element Name	Hardware Type	Management Type
Eclipse Microwave Radio – DAC	DAC 4x DAC 16xV2 DAC3xE3DS3M_ANSI DAC3xE3DS3M_ETSI DACGE DACES	SNMP over SCADA
Eclipse Microwave Radio – Eclipse FAN	FAN_2RU FAN_1RU	SNMP over SCADA
Eclipse Microwave Radio – Eclipse NCC	NCC	SNMP over SCADA
Eclipse Microwave Radio – Eclipse NPC	NPC	SNMP over SCADA
Eclipse Microwave Radio – IDU	IDU_300_20xV2 IDU_ES IDU_GE_20x	SNMP over SCADA
Eclipse Microwave Radio – INU	INU INUe	SNMP over SCADA
Eclipse Microwave Radio – RAC	RAC30v3 RAC40 RAC60_ODU RAC6x_ODU RAC4x RAC3x RAC60_IRU600 RAC6x_IRU600	SNMP over SCADA
Efratom GNSS	N/A	SNMP over SCADA
MNI Microwave Radio – CM	N/A	SNMP over SCADA
MNI Microwave Radio – Proteus	N/A	SNMP over SCADA
Motorola Base Radio – RF Distribution System (RFDS)	RF Distribution System	SNMP over SCADA
Motorola Base Radio – CS	GPW8000 GTR8000 Mutual Aid Quantar	SNMP over SCADA
Motorola Base Radio – MS	GPW8000 GTR8000 Quantar STR3000	SNMP over SCADA
Motorola Base Radio – RS	GTR8000 Quantar IR	SNMP over SCADA

Table continued…

Network Element Name	Hardware Type	Management Type
	Quantar 9600 Receiver STR3000	
Motorola Site Controller – RS	N/A	SNMP over SCADA
Motorola Comparator - ATAC 3000 (AstroTac)	N/A	SNMP over SCADA
Motorola MOSCAD RTU - Environmental Analog Inputs	N/A	SNMP over SCADA
Motorola MOSCAD RTU - Environmental Digital Inputs	N/A	SNMP over SCADA
Motorola MOSCAD RTU - Environmental Digital Outputs	N/A	SNMP over SCADA
Motorola Receiver - ATAC 3000 (AstrotacRx)	N/A	SNMP over SCADA
TRAK GNSS - 9100 (Moscad)	N/A	SNMP over SCADA
TeNSr/IMACS Channel Bank (Premisysis)	N/A	SNMP over SCADA

1.11
UEM Client Overview

The UEM client application provides an end-user interface for the UEM Fault Manager. The UEM client is launched through a web browser which provides starting point and flexibility in application deployment.

When used for the first time, the application is downloaded from the server onto the local machine using Java WebStart technology. For subsequent uses, the application is launched from the local workstation.

To meet security requirements, the UEM client application uses SSL and SSL over HTTP (HTTPS) for client-server communication and secure web browser connection. HTTP access is not supported.

To provide seamless access to the UEM client, it is recommended to install the SSL certificate for the UEM application first. The certificates are installed with PRNM Client application.

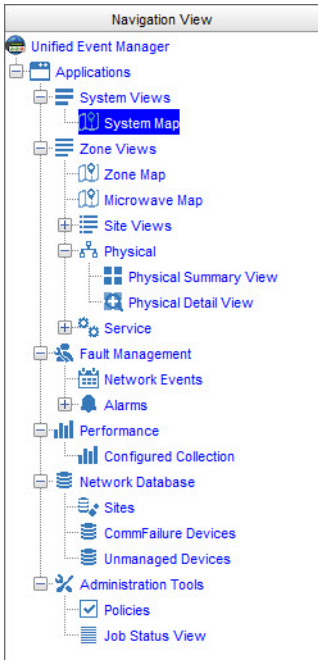
1.12
Navigation Tree

The navigation tree on the left-hand side in the main UEM panel enables you to quickly select different fault management views.

Selecting nodes in the tree opens the associated view on the right-hand side of the main panel. **Site Views** nodes are added to the tree automatically during the discovery of particular site types. They can be removed from the tree by deleting sites (see Deleting Zones or Sites on page 188). By default, when no sites are discovered, empty **Site Views** nodes are displayed in the tree.

Nodes may be added to the tree by creating custom views (see Adding Custom Views on page 128). Similarly, only the nodes associated with custom views can be removed from the tree (see Deleting Custom Views on page 131).

Figure 1: UEM – Navigation Tree



1.13 Maps Overview

Maps are the graphical representations of managed resources. These maps are maintained at the zone and system levels.

There are five types of maps maintained by UEM:

System Map

This map provides a status overview of all zones in the system and is especially useful in multi-zone systems. It is a system-level view so the information presented is partially based on the data retrieved from other zones. The map displays the name of each zone as a label. Zones are represented by basic map objects. A zone boundary is represented by an area associated with a particular zone and defined by the user.

System maps are available in all system configurations under additional licenses.

Zone Map

This map presents zone-level information and provides a status overview of all discovered sites within the zone (for example, Console Sites, RF Sites or Core Sites). The map displays the name of each site as a label. Sites are represented by basic map objects. A site boundary is represented by an area associated with a particular site and defined by the user.

Zone maps are available in the basic version of UEM in L and M core system configurations. For K core or standalone channel system configurations zone maps are available under additional licenses.

Microwave Map

This map presents the microwave radio infrastructure managed directly by UEM or through RTUs at the zone level. Each microwave radio is represented by a basic map object. Additionally, the connection between a pair of microwave radios is represented by a line.

Microwave maps are available in all system configurations under additional licenses.

Physical Map

This map provides a quick status summary of devices in the network subnets. Each icon represents a network subnet (or a group of subnets) containing the devices managed by UEM. There are two views of the zone physical map: a summary view and a detail view. Both views provide an overall status of the subnets. The **Physical Summary View** uses smaller icons to allow more subnets to be displayed without scrolling. It is useful in systems with multiple subnets within a zone. The **Physical Detail View** uses distinctive icons for different subnet types and displays the name of each subnet as a label. It is useful in systems with a smaller number of subnets. Typically an operator uses only one of the two views, based on the number of subnets within the zone.

Service Map

This map provides a quick summary of the service status of all sites in a zone. A failure in the service map view typically means degradation or loss of service in the coverage area of the associated site. There are two views of the zone service map: a summary view and a detail view. Both views provide an overall service status of the sites. The **Service Summary View** uses smaller icons to allow more sites to be displayed without scrolling. It is useful in systems with multiple sites within a zone. The **Service Detail View** uses larger icons and displays the name of each site as a label. It is useful in systems with a smaller number of sites. Typically an operator uses only one of the two views, based on the number of sites within the zone.

Different icons are used to represent different sites (or subnets) in your system. By default a map contains one symbol for each map element, for example, a site or a subnet.

Table 14: UEM Icons on System, Zone and Microwave Maps

UEM Icon	Description
	Zone
	Zone (no connection to the corresponding UEM)
	• Backhaul Subsystem • Trunking Subsystem (Tsub)
	• Primary Operation Support System • Backup Operation Support System
	• Primary Zone Core • Backup Zone Core

Table continued…

UEM Icon	Description
	Customer Enterprise Network (CEN)
	Console Site
	Conventional Subsystem
	DSR Shared Network Devices
	• IP Multisite Subsystem Prime Site • Circuit Multisite Subsystem Prime Site

	• IP Multisite Subsystem Remote Site:
	  - IP Simulcast Subsite
	  - Subsite in a Trunking Subsystem (Tsub)
	• Circuit Multisite Subsystem Remote Site

	RF Site
	Other devices
	Microwave Radio
	Trunking Subsystem (Tsub)

Table 15: UEM Icons on Physical and Service Maps

UEM Icon	Description
	• Primary/Backup Zone Core Subnet • Primary/Backup Operations Support Systems Subnet • DSR Shared Network Devices Subnet • Zone
	• Console Site Subnet
	• RF Site Subsystem • IP Multisite Subsystem • Circuit Multisite Subsystem • Repeater site • Data Site • Site • Simulcast Prime Site • Standalone HPD Site • IP Simulcast Site • Multisite Prime Site • Conventional Site • SmartZone Site • Interconnectivity Site **NOTICE:** Interconnectivity Site refers to the Interoperability Site. • Conventional Subsystem • Backhaul Subsystem • Map Group

1.13.1

Map Modes

System maps, zone maps and microwave maps work in two modes: static and geographical.

Static Map

In this mode an empty background (default) or an image-based background is used.

Geographical Map

In this mode a standard map format based on map tiles is used as a background. It replaces empty or image-based backgrounds. The map object locations are represented by geographical coordinates.

1.13.2
Map Object Types

The maps display the following types of objects:

Basic object (point icon)
Represents a single location of radio network infrastructure, for example, a zone, a site, a microwave radio, or a network. The location of such objects is based only on the user input.

Area (filled polygon)
Represents an area related to the radio system structure, for example, zone boundaries or site boundaries. The shape and location of such objects is based only on the user input. These objects are not available for physical and service maps.

Line
Represents the connection between two basic objects, for example, a link between microwave radios. The location of such objects and the configuration of associated objects is based only on the user input. These objects are only available for microwave maps.

Basic objects and areas use a severity color scheme to indicate the highest severity of the associated managed objects (zones, sites, networks, microwave radios).

1.13.2.1
Basic Objects Display

There are two methods of displaying basic objects (points) on a map.

Basic objects can be displayed in the following ways:

Co-locating
Displaying objects placed in the same location as a group of distinguishable objects organized in a grid structure. This method can be used for displaying co-located radio system elements where it is important to show all statuses at the same time, for example, an RF site co-located with a console site. Co-located objects have the same geographical coordinates.
Not available for physical and service maps.

Grouping
Displaying a group of multiple objects as a single object. Selected objects are merged into a single object based on the user input.
Available **only** for physical and service maps

1.14
Site Views Overview

Site views display the overall status of site infrastructure. They contain physical network elements managed within a particular site directly by UEM and through Remote Terminal Units (RTUs), and additional information, for example, redundancy group association, services status, digital output/input status, or analog input values.

Each site view contains up to four sections:
General Information
Main information for each site, for example, the name of the managed resource, the name of the subsystem, or the class name.

More Information
Additional information, for example, location tags.

Note
An editable area where users can enter and save any text (maximum 1024 characters long).

Objects
A tree containing up to three groups of objects associated with the site.

SERVICE
The status of all services within the site.

ENVIRONMENTAL
The status of digital/analog inputs and digital outputs directly configured through SDMB configuration file.

NOTICE: The template devices built based on mixed environmental objects are not included.
Motorola SDM3000 RTU Fault Object (entity) values reflect the most recent values sent by the SDM3000 to UEM. UEM does **not** initiate a real-time poll of current Logical Managed Resource (LMR) values when the view is opened. Changes to Digital I/O values are always sent from the SDM3000 to UEM. However, changes to Analog Inputs are only sent to UEM when the configured threshold or delta change is triggered. The accuracy of the Analog Input values depends on how the SDM3000 is configured to send threshold and delta change updates to UEM. For example, if the SDM3000 is configured to send an update to UEM on a delta change of 1 for a temperature analog input, the value reported by UEM will be within 1 degree accuracy of the current temperature at a site.

EQUIPMENT
The status of all physical devices managed directly by UEM and devices managed through a Remote Terminal Unit (RTU) – devices are grouped by type and the status is aggregated from physical and logical parts of a particular device.

NOTICE: For sites that do not have service or environmental related information, corresponding groups are not displayed.

Figure 2: Unified Event Manager – Site View

When discovered, sites are added dynamically to the navigation tree. The list of sites is divided into the following fixed categories:

Console Sites
All discovered console sites.

Conventional Subsystem
All discovered conventional subsystems.

Core Sites
All discovered core sites (Primary Zone Core, Backup Zone Core, Primary Operations Supports Systems, Backup Operations Supports Systems, DSR Shared Devices, Backhaul Devices, Customer Enterprise Network).

RF Sites
All discovered RF sites.

Simulcast Sites
All discovered multisite subsystems (prime and remote sites).

Trunking Subsystems
All discovered Trunking Subsystems (Tsubs). This includes the prime site and remote sites supporting any of the following site types: ASTRO® 25 Site Repeater (ASR) Site, Centralized Conventional Site, Console Site (NM/Dispatch Site), High Performance Data (HPD) Site, or IP Simulcast Subsite.

1.15
Fault Management Overview

Fault management in the UEM application includes processing and presentation of events sent by a network element in the form of a Simple Network Management Protocol (SNMP) trap or inform, or a Simple Object Access Protocol (SOAP) message.

Failures in the network, network elements, and communication links can interrupt routine activities. In such situations, UEM reports events.

1.15.1
UEM Events

An event is a basic unit of management information.

Events relate to an occurrence, such as:

- Initial discovery or rediscovery of an element
- Status update of an element
- Deletion of an element
- Failure in an element

Events form a repository of information for all the occurrences in the system. A UEM event contains many attributes, including the managed resource impacted, the associated entity or component, textual description, and the severity of the occurrence.

1.15.1.1
Unknown Events

UEM could display an **Unknown Event** against a discovered device. UEM displays such events with the warning severity and the informational event category when discovered devices send a notification that is not recognized by UEM (UEM has no rules to process and display a received notification type).

The message of this type of event contains:

- The text **Unknown Event**
- The type SnmpTrap (for SNMP notifications)
- Variable bindings (varbinds) together with received values in the format **<*varbind*>** = **<*value*>**

NOTICE: SnmpTrap type and varbinds can be presented as:

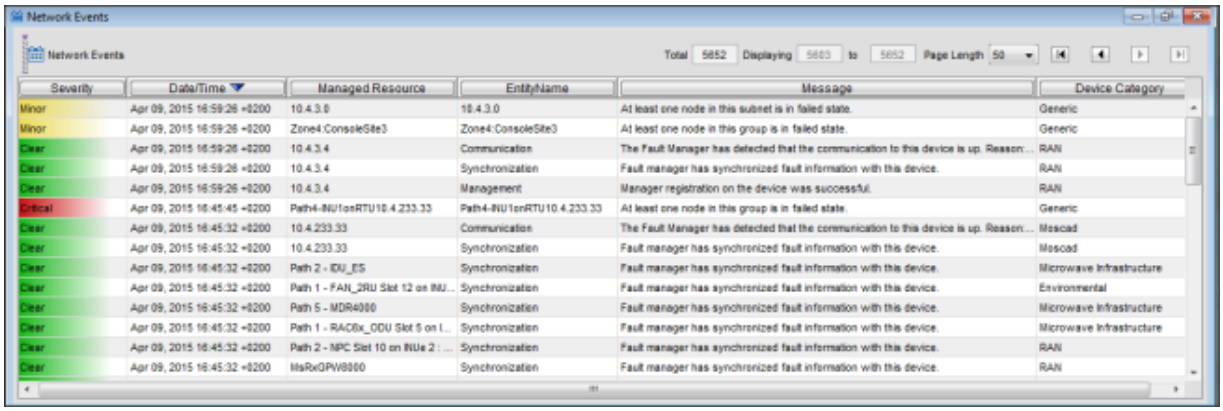
- text when UEM has MIBs to translate the object identifier (OID) to an exact name
- a raw OID if OIDs are from MIB and are not supported by UEM

1.15.1.2
Network Events Window

You open the **Network Events** window from the **Navigation View** by clicking the **Network Events** node under the **Fault Management** node. The window displays all notifications received or generated by Unified Event Manager (UEM). The notifications include various properties related to events that are raised against devices. You can open the detailed view of an event by double-clicking an entry in the window. By default, you can view 50 events on a single page. You can customize the number of events displayed on the page. The maximum number of events on a page is 1,000. The database stores maximum 10,000 newest events. The oldest events are moved to the events archive and can be viewed using the **Events Archive** browser.

The default sorting criterion in the **Network Events** window is the **Date/Time** column. You can sort the events by any attribute by clicking the associated column heading. To toggle between ascending and descending sort orders, click the column again.

Figure 3: Network Events Window



Related Links

Severity Definitions on page 65
Event and Alarm Category Definitions on page 65
Accessing and Retrieving Events Archives in UEM on page 246
Viewing Archived Events in UEM on page 252

1.15.2
UEM Alarms

An alarm results from an event in a managed resource. It occurs as a result of a pre-determined significant state (a failure or a fault) that may require user attention. Alarms are raised within UEM based on notifications from the network element, or by UEM to report failures associated with fault management functions.

Alarms can fall into the following general categories (for more information, see Event and Alarm Category Definitions on page 65):

- Communication alarms
- Equipment alarms
- Quality-of-service alarms

Alarms across a network are commonly related to:

- Resources that have failed
- Connectivity issues
- Devices malfunctioning
- Threat assessment reports
- SNMPv3 or Web Service credentials failure

1.15.2.1
Alarms Summary

Alarm summary is used to display the count of the total number of alarms organized by device categories and/or severities. It is positioned just below the navigation tree in the main window. Each severity is represented in a single cell or graph, depending on the presentation that is selected. The view is updated automatically and the counts can be seen at all times, irrespective of the view that is currently open.

The presentation of the alarm summary can be modified by clicking the buttons at the top of the summary panel. Three different presentations are available:

- Table view
- Bar graph view
- Pie chart view

Clicking a particular severity symbol opens an alarms window with the corresponding alarm type filtered.

1.15.2.2
Alarms Window

You open the **Alarms** window from the **Navigation View** by clicking the **Alarms** node under the **Fault Management** node. In the window, only active alarms of devices are displayed, that is the latest failure or an event clearing a failure.

You can open the detailed view of an alarm by double-clicking an entry in the window. By default, you can view 25 alarms on a single page. You can customize the number of alarms displayed on the page. The maximum number of alarms on a page is 1,000. The **Alarm Details** window allows the Unified Event Manager user to perform the following functions:

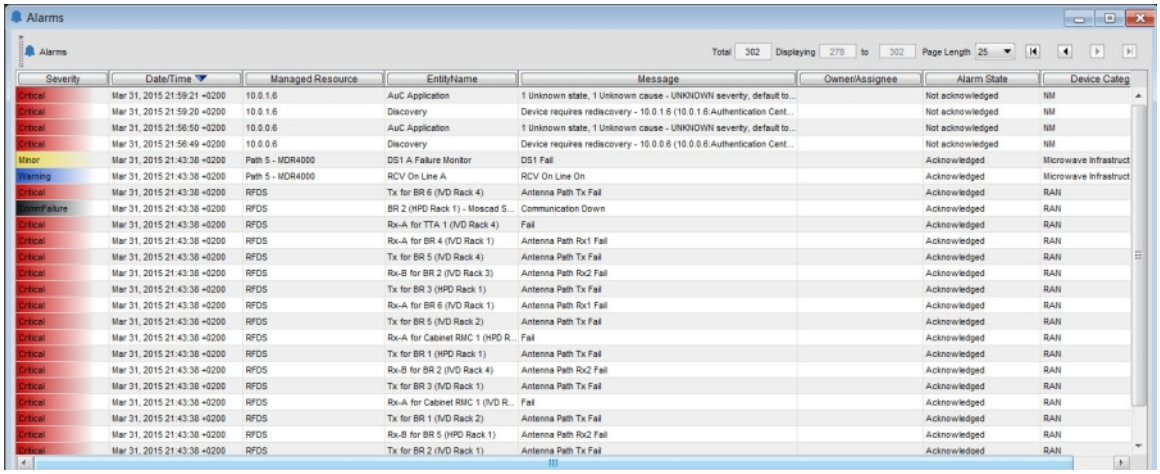
- Assign/Unassign an alarm
- Acknowlegde/Unacknowledge an alarm
- Annotate an alarm
- View the history of the selected alarm

For more information, see Alarm Operations on page 165.

To view the failure or fault history of a network element, look at the **Network Events** window. For more information, see Network Events Window on page 63.

The default sorting criterion in the **Alarms** window is the **Date/Time** column. You can sort the events by any attribute by clicking the associated column heading. To toggle between ascending and descending sort orders, click the column again.

Figure 4: Alarms Window



1.15.3
Severity Definitions

Alarms and events are assigned with severity levels, indicated by a severity color and an alarm or event message. The action required depends on the severity of the alarm.

Table 16: Severity Categories

Severity	Value	Color
CommFailure	1 (highest severity)	Black
Critical	2	Red
Major	3	Orange
Minor	4	Yellow
Warning	5	Blue
Clear	6 (lowest severity)	Green
Info	7	Light blue
Unknown	8	Gray

NOTICE:
When a managed resource is in an unmanaged state, its status (severity) is *unknown*. Only a device in an unmanaged state uses this status.

The *info* severity level is only used for events, never alarms.

1.15.4
Event and Alarm Category Definitions

Network elements detect and report to UEM conditions that have caused or can cause an interruption in the operation of network elements. Such conditions can be related to physical failures of a device, for example of a fan.UEM may also report certain conditions that it detects within the application or on

the device. In all cases, UEM inspects the reported condition and categorizes the event or alarm as one of the items in the following table.

Table 17: Event Category

Description	Condition
Attribute Value Change Event	An important parameter value has changed.
Communication Alarm	A communication/synchronization loss or regain is detected.
Equipment Alarm	An equipment or link failed or a previously reported failure is cleared.
Informational Event	A condition that is important, but is not a failure at this time. **NOTICE:** Some informational events report conditions that may cause a failure in the future. These events are normally reported with a severity higher than 'Info'.
Management Event	A condition is detected and reported by UEM and is related to a critical function of UEM.
Quality of Service Alarm	A service-impacting condition is detected.
Security Violation	A credential mismatch condition is detected by UEM. Typically associated with devices that use SNMPv3 to communicate with UEM.
Object Creation Event	A discovery or re-discovery of a managed resource is detected.
Object Deletion Event	A deletion of a managed resource or an entity is detected.
Processing-Error Alarm	A device report processing error.

1.15.5
Network Database

Network database serves as an inventory view for the resources that are currently present in the Unified Event Manager (UEM) database.

By default, network database displays certain critical properties associated with these resources. Entries in the Network Database can be:

Device Managed Resources (DMRs)
Physical devices (for example a Repeater Site Controller)

Network Managed Resources (NMRs)
Networks

Logical Managed Resources (LMRs)
Logical entities (for example a site)

Group Managed Resources (GMRs)
Groups of resources

Generic Nodes (GNs)
Unknown physical devices (IP managed devices, SNMP managed generic switches and routers)

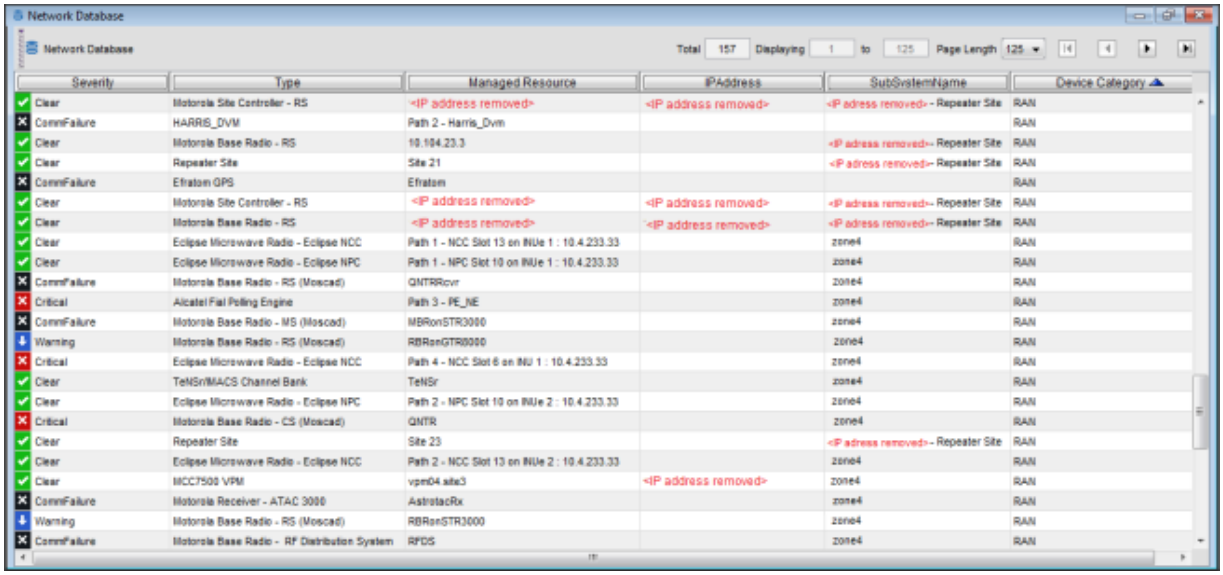
The contents are presented in a tabular format with each row corresponding to a resource. The default page size of this view is 25 entries, but it can be modified to show more or fewer entries in one page. The maximum number of events on a page is 125.

Network database displays a status value for each resource. This value is calculated based on the highest severity of the alarms that are currently outstanding against the resource. Only DMRs and LMRs can report alarms, so their state is directly based on the highest severity of the alarm they report. If a DMR has LMRs associated with it (for example Sites in a Zone Controller), the state of the LMRs is

ncluded in the calculation of the DMR state. The state of DMRs and LMRs is propagated further to associated NMRs and GMRs.

The unknown state value indicates that UEM does not currently manage the resource.

Figure 5: Network Database Window



1.15.5.1
Device Categories

Each Device Managed Resource (DMR) and each Logical Managed Resource (LMR) have an assigned category. All events and alarms for the DMRs and LMRs are marked with this particular category. The device category is visible in the **Network Database**, **Network Element View**, **Network Events**, and **Alarms** windows.

Network elements in UEM are grouped in 10 categories.

Application
This category includes additional components in the system, not related directly to its basic capabilities.

Core
This category includes core equipment and applications in the system.

Environmental
This category includes digital/analog inputs and digital outputs.

Microwave Components
This category includes microwave components equipment (PTP800 LMRs).

Microwave Infrastructure
This category includes all microwave radios.

Moscad
This category includes represents Moscad Remote Terminal Unit (RTU) devices.

NM (Network Management)
This category includes all network management devices, for example, NM Servers.

RAN (Radio Access Network)
This category includes all radio network devices, for example, Site Controllers or Zone Controllers.

Transport
This category includes the transport infrastructure: switches, routers and gateways.

Generic
This category includes all devices not included in other categories, for example, Generic Nodes or Generic SNMP Nodes.

NOTICE: The category of an LMR may differ from the category of the DMR to which it is assigned.

1.15.5.2
Network Element View

This view is used to display the status of a particular network element.

Each network element view contains up to seven sections:

General Information
Main information for each site, for example, the name of the managed resource, the name of the subsystem, or the class name.

More Information
Additional information, for example, location tags.

Microwave Information
Information available only for microwave radios, for example, the microwave path or location parameters.

Relationships
Information regarding the redundancy state, redundancy groups and related managed resources.

Commands and Metering Information
Available only for devices supporting commands or values; from this section users can issue commands to devices (for Network Managment Alliance devices, the commands are scheduled as jobs) or read values from devices.

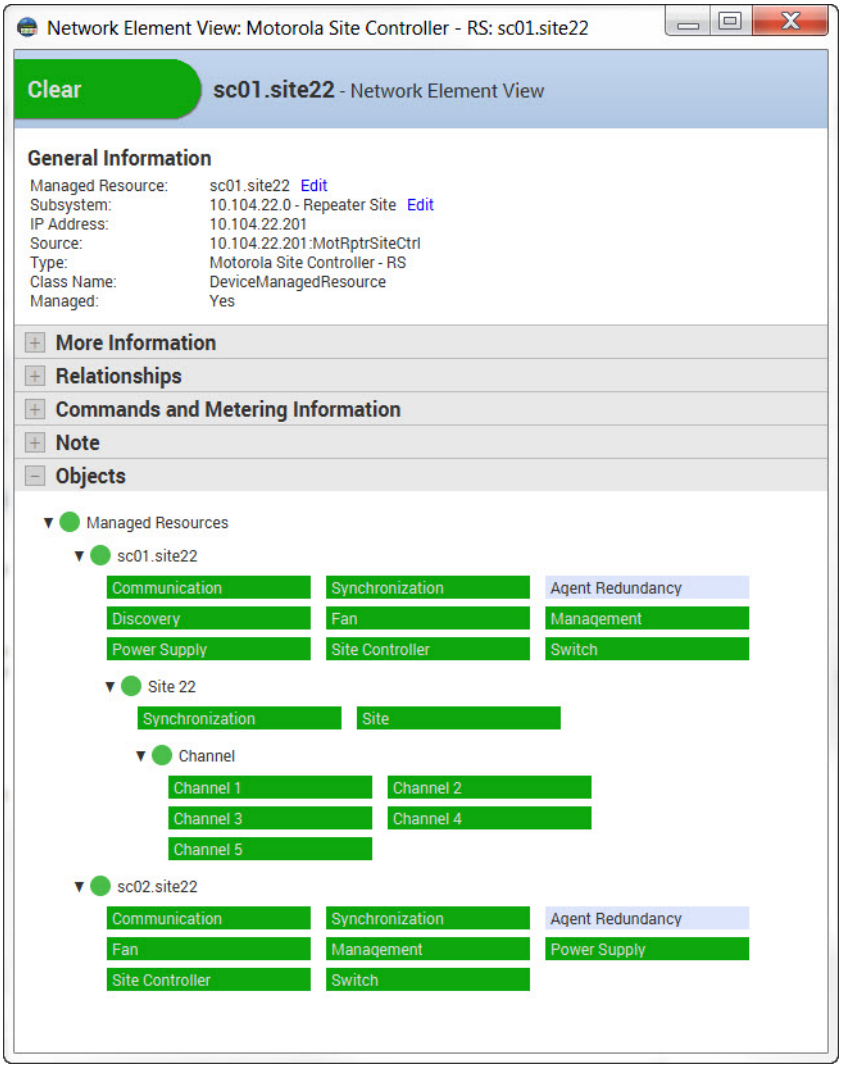
NOTICE:
Motorola SDM3000 RTU Fault Object (entity) values reflect the most recent values sent by the SDM3000 to UEM. UEM does **not** initiate a real-time poll of current Logical Managed Resource (LMR) values when the view is opened. Changes to Digital I/O values are always sent from the SDM3000 to UEM. However, changes to Analog Inputs are only sent to UEM when the configured threshold or delta change is triggered. The accuracy of the Analog Input values depends on how the SDM3000 is configured to send threshold and delta change updates to UEM. For example, if the SDM3000 is configured to send an update to UEM on a delta change of 1 for a temperature analog input, the value reported by UEM will be within 1 degree accuracy of the current temperature at a site.

Note
An editable area where users can enter and save any text (maximum 1024 characters long).

Objects
A tree of managed objects and their statuses, grouped by type and hierarchy. If applicable, the status of a redundant network element (a device which is in the same redundancy group) is also displayed.

NOTICE: NOTE: When a **Synchronization** or **Communication** object for a managed resource is in the **CommFailure** state, all other managed objects under this managed resource are displayed as striped to indicate that their status is not up-to-date.

Figure 6: Unified Event Manager – Network Element View



1.15.5.3
Commands

You can use the command window or the network element view to send commands to a selected managed resource.

For Network Management Alliance (NMA) devices, commands issued from the **Commands and Metering Information** section in the **Network Element View** window are scheduled – a job is created. These commands can be sent to multiple instances of entities at the same time.

For devices reporting to UEM through Remote Terminal Units (RTUs), commands issued both from the command window and from the **Commands and Metering Information** section in the **Network Element View** are sent to RTUs and no job is created.

Commands issued from the command window are sent immediately and no job is created. These commands can only be sent to a single entity at a time. If multiple instances of an entity can exist (for example, channels at a site), a combo box is displayed next to the entity type. The list in the combo box contains all possible IDs for the entity type. The entities are sorted in alphabetical order.

- If the command window is invoked from the **Alarms** window, the entity associated with the selected alarm is selected.

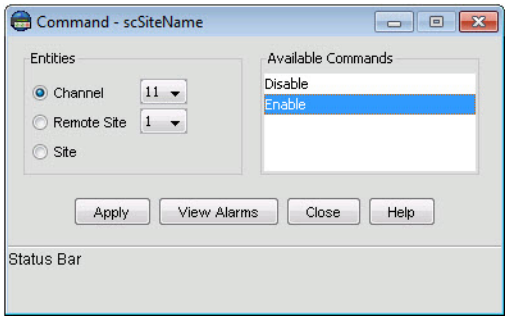
- If the command window is invoked from the **Network Database** window, the first entity in the list is selected.

NOTICE: If the entity has only one instance, no instance ID is displayed.

For commands issued from the command window the status of a command request is displayed in the multi-line status bar at the bottom of the command window. The managed resource typically responds to a command by changing the state of one or more entities. These changes are reported to UEM and are displayed in the **Alarms** window. To view these alarms, click **View Alarms** or select **Alarms** from the navigation tree.

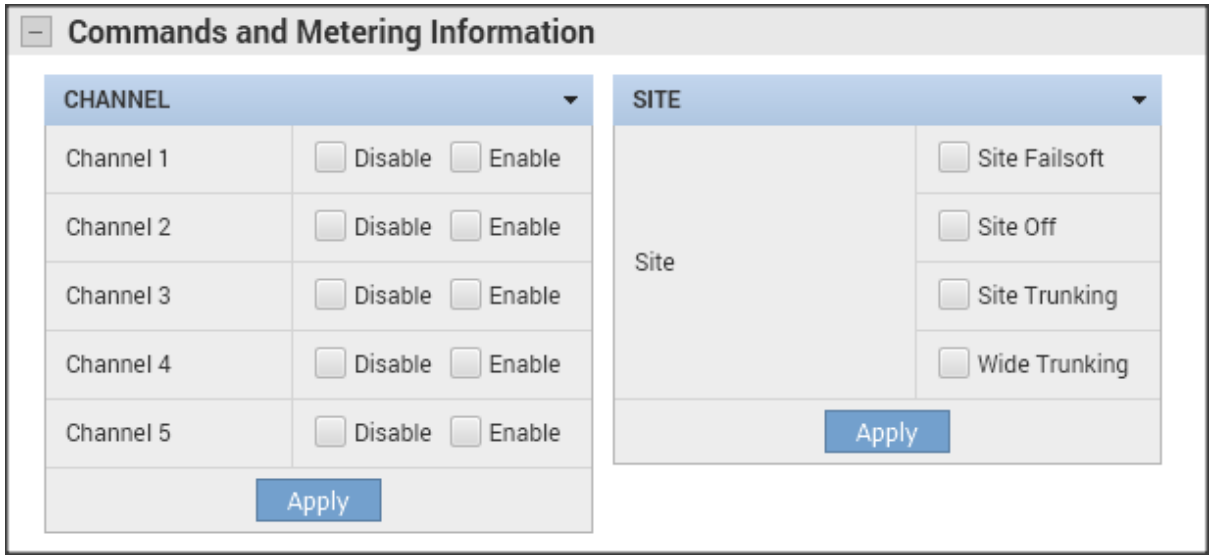
NOTICE: Clicking **View Alarms** automatically filters the alarms to display only the alarms associated with the selected managed resource.

Figure 7: Unified Event Manager – Command Window



For commands issued from the **Network Element View** window the status of a command request is displayed in in the multi-line status bar at the bottom of the box. If a job is created the detailed status is displayed in the **Job Status View** window.

Figure 8: Unified Event Manager – Commands and Metering Information Section



1.15.6

Centralized Fault Management Solution

The Centralized Fault Management solution changes the fault management subsystem by rearranging and merging the fault management functionality of two products: Moscad NFM and Unified Event Manager (UEM).

In this solution UEM has the ability to manage various devices through SDM Remote Terminal Units (RTUs) and can be established as the main fault manager, aggregating all health information from the system. Depending on the features available with your system, UEM can provide an integrated and more centralized fault management solution with enhanced views and optional integrated support as a replacement for MOSCAD Graphical Management Computer (GMC) and Graphical Workstation (GWS). In the centralized mode, the GMC/GWS/SNT components are retired, while SDM Builder and SDM3000 RTU are reused. The SDM3000 Advanced unit includes eight analog inputs (–5 VDC to +5 VDC). Both NFM managers (GMC or UEM in Centralized UEM Mode) support a range of 0 VDC to +5 VDC.

For more information on the transition from UEM and MOSCAD Network Fault Management to a centralized and integrated fault management solution, see the *UEM/GMC Transition Setup Guide*.

1.16

Performance Management Overview

Unified Event Manager (UEM) can collect and plot statistical data. You can use the data to analyze functions and performance of your system. The data collection for these statistics is triggered 10 minutes after the server application startup time.

The following statistics are available for collection and plotting:

- Host Resource Statistics on page 72
- Ethernet Link Statistics on page 72

NOTICE: Collecting statistics is disabled by default, but you may enable it. For more information, see Enabling Collections on page 210.

Performance Management Terminology

The following are terms and definitions used within the performance management functions of UEM:

Polled Data or Statistics
The pattern in which data is collected from a device is defined in a variable called Statistics (also called Polled Data).

A statistic is the basic object used for data collection. It contains details such as, for example, the contacted device, the data collected, and the time interval. The Statistics object does not store the collected data.

Polling
The process of contacting the device and collecting the data for the specified statistics.

Polling Period
The interval in which the device is polled for the statistical data.

Collected Statistics
The statistics collected and stored in the database at the specified polling period.

Current Statistics
The statistics polled instantly from the device. This data is not stored in the database.

1.16.1
Host Resource Statistics

Selected devices support the following Host Resource Statistics (HRS):

Processor Load
A graph shows Central Processing Unit (CPU) usage in percentage points at a given time. You can set the polling interval according to your preferences. If multiple CPUs are involved, the average value is presented here.

RAM Usage
A graph shows RAM usage in kilobytes at a given time. You can set the polling interval according to your preferences.

Devices listed in the table support HRS configured collections only on the Linux platform; the Solaris platform does not support HRS for these devices. The difference between Linux and Solaris platforms is the following:

- On Linux, devices run on a virtual server with the Linux operating system which supports HRS.
- On Solaris, devices run on General Application Server (GAS) which does not provide correct HRS data for single containers.

Although the listed devices are displayed as configured collections for Solaris and you can configure HRS for them, no data are collected.

Table 18: Devices that Do Not Support HRS on the Solaris Platform

Device Type	Device Name
Motorola Conventional IVD Packet Data Gateway	ConventionalIvdPacketDataGateway
Motorola HPD Packet Data Gateway	HpdPacketDataGateway
Motorola IVD Packet Data Gateway	IvdPacketDataGateway

1.16.2
Ethernet Link Statistics

The polling interval for Ethernet link statistics is set to 15 minutes by default. It can be configured at runtime.

The Motorola Network Resource (MNR) is the only device that supports Ethernet link statistics. The following statistics are enabled by default for all Ethernet WAN IF objects:

- IP Packet Transfer Delay (IPTD) Average
- IPTD Minimum
- IPTD Maximum
- IP Packet Delay Variation (IPDV) Average
- IPDV 99% Average
- IP Packet Loss Rate (IPLR)

All other statistics are disabled by default.

Table 19: Ethernet Link Statistics Configured for Data Collection

Statistic Name	Unit of Measurement	Description
Ethernet WAN IF: IPTD Number	Number of measurements	Number of successful round-trip IP Packet Transfer Delay (IPTD) measurements for the last interval.
Ethernet WAN IF: IPTD Sum	Milliseconds	Sum of the round-trip IPTD measurements for the last interval.
Ethernet WAN IF: IPTD Average	Milliseconds	Average value of the round-trip IPTD measurements for the last interval.
Ethernet WAN IF: IPTD Sum Squares	Milliseconds squared	Sum of squares of the round-trip IPTD measurements.
Ethernet WAN IF: IPTD Maximum	Milliseconds	Maximum round-trip IPTD measurement for the last interval.
Ethernet WAN IF: IPTD Minimum	Milliseconds	Minimum round-trip IPTD measurement for the last interval.
Ethernet WAN IF: IPDV Number	Number of measurements	Number of successful Internet Protocol Packet Delay Variation (IPDV) measurements for the last interval.
Ethernet WAN IF: IPDV Sum	Milliseconds	Sum of the IPDV measurements for the last interval.
Ethernet WAN IF: IPDV Average	Milliseconds	Average value of the IPDV measurements for the last interval.
Ethernet WAN IF: IPDV Sum Squares	Milliseconds squared	Sum of squares of the IPDV measurements for the last interval.
Ethernet WAN IF: IPDV 99% Number	Number of measurements	Number of successful measurements of the 99th percentile IPDV for the last interval.
Ethernet WAN IF: IPDV 99% Sum	Milliseconds	Sum of the measurements of the 99th percentile IPDV for the last interval.
Ethernet WAN IF: IPDV 99% Average	Milliseconds	Average value of the 99th percentile IPDV measurements for the last interval.
Ethernet WAN IF: IPDV 99% Maximum	Milliseconds	Maximum 99th percentile IPDV measurements for the last interval.
Ethernet WAN IF: IPDV 99% Minimum	Milliseconds	Minimum 99th percentile IPDV measurements for the last interval.
Ethernet WAN IF: IPLR TX Packet	Number of packets	Number of packets transmitted by the source end point in successful IP Packet Loss Rate (IPLR) measurement attempts for the last interval.
Ethernet WAN IF: IPLR Packet Not Received	Number of packets	Number of packets not received by the receiving end point for the last interval.
Ethernet WAN IF: IPLR Loss Rate	Hundredths percent (basis points)	IP packet loss rate (the number of packets not received divided by the number of packets transmitted) for the last interval.

1.17
Discovery Overview

In Unified Event Manager (UEM), discovery is adding devices and logical resources associated with them into the UEM database.When discovering the site, UEM attempts to discover a pre-defined list of IP addresses, based on the network design of the system.

Once the devices are discovered, UEM reads and stores critical parameters. It also determines the current health (status) of the devices and their components. Then, it starts monitoring the connectivity (supervision) to the devices.

NOTICE: In systems with Dynamic System Resilience (DSR), devices in both the primary and backup zone cores are discovered separately. UEMs in different zone cores do not share or exchange information.

As a result of a device discovery, additional resources are displayed in the UEM**Network Database** window. These resources are referred to as logical managed resources (LMR). The device itself is a device managed resource (DMR). LMRs typically represent a set of related services or components that a device reports on. They can be managed independently due to their physical or logical relationship. An example of a physical relationship is a separate device connected to the device. A logical relationship can be an active device in a redundant configuration. For a list of resources associated with a device, see “Alarms and Events” in the *UEM Online Help*.

You initiate the discovery of a device or a site/network from the Discovery Configuration user interface. You specify a unique identifier, for example the IP address or DNS name, and start the discovery process. You can also set SNMPv3 and/or Web Service credentials for a discovery job. For more information see Discovery Job Credentials Configuration on page 88.

Re-discovering a device is functionally the same as first-time discovery. However, the term is used to describe the discovery operation performed on a device that is already in the UEM database. During a rediscovery, UEM adds the resources of a device that are not present in the UEM database. UEM also verifies the current resources of the device. If the verification fails, an alarm is raised against the resource to indicate that the device does not respond to queries. To remove such alarms, you can verify the configuration of the device and invoke rediscovery at a later time. If the resource is no longer active in the system, you can delete it.

For more information, see Aborting Discovery Jobs on page 204.

1.17.1
Devices Discovered by UEM

For a list of devices managed by Unified Event Manager (UEM) and the alarms and events connected, see “Alarms and Events” in the *UEM Online Help*.

The Key Management Facility (KMF) and PDEG are fault-managed by KMF.

1.17.2
Post-Discovery Synchronization

Devices that are discovered successfully are automatically synchronized (see Synchronization Operations on page 196 section for more information) by Unified Event Manager (UEM) on a regular basis. Synchronization is done in the background, but the status is automatically updated and displayed in the following windows:

- **Alarms**
- Maps
- **Network Database**
- **Site Views**

- **Network Element View**

A device sends traps or informs to UEM. The UEM server application must continuously communicate with the devices to ensure that status information is up-to-date. Therefore, UEM also monitors its connectivity to the device (see Supervision on page 40).

1.18

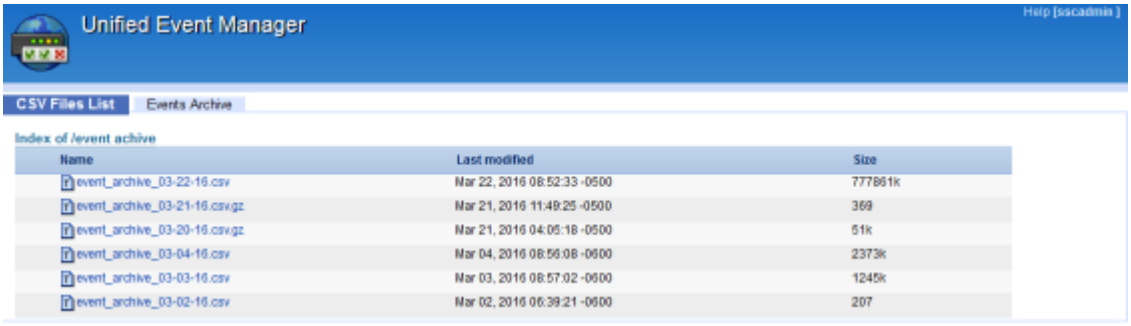
Events Archive

In Unified Event Manager (UEM), you can view the latest 10,000 events sent to UEM. Events that are logged after the first 10,000 events are automatically cleaned up (purged). In some cases, it is possible to store in the event archives more than 10,000 events that are kept in the UEM client file system. UEM periodically archives received events in two ways: in the UEM file system and in a database.

Archivization in the UEM file system

Event archive files contain all event fields that are defined in the event database. The event archive file format contains one event with all its attributes. The format uses a comma as a delimiter between event fields within the line (`.csv` format). UEM maintains one event file a day. If event archive files are older than 31 days, UEM cleans them up.

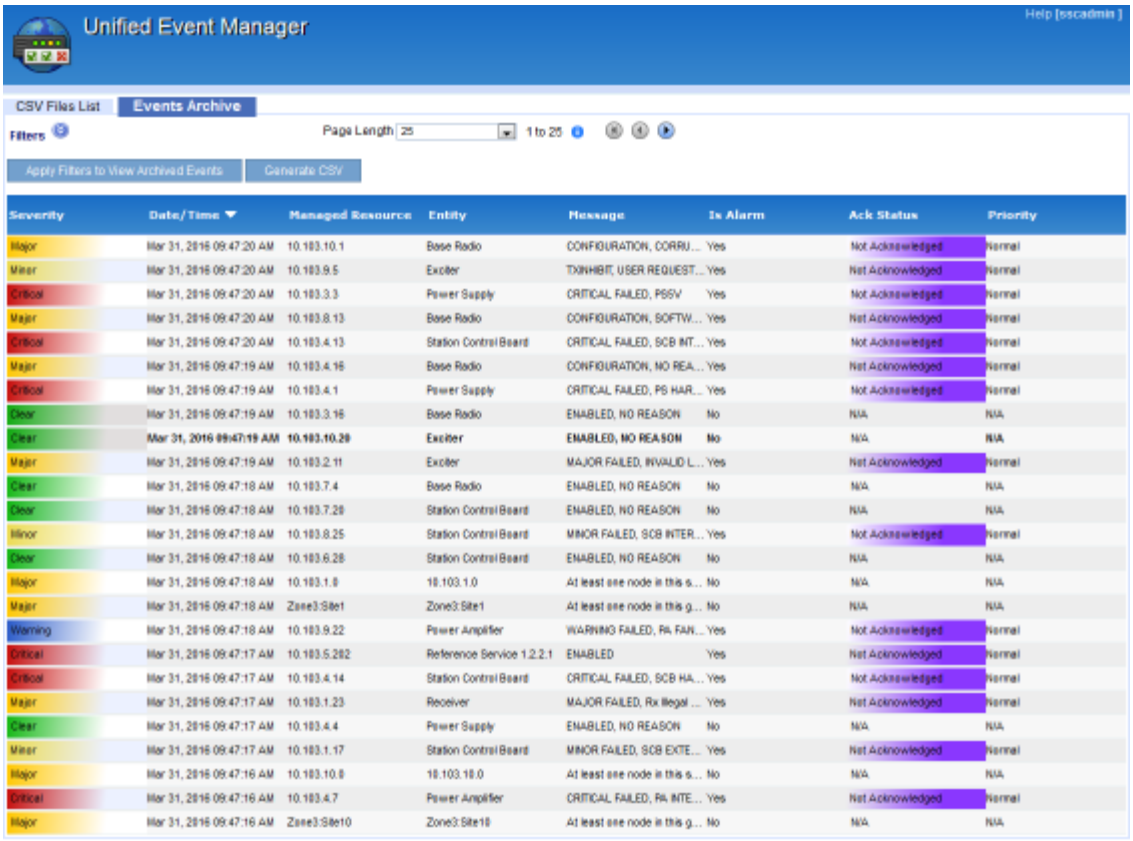
Figure 9: UEM File System – CSV Files List



Archivization in a Database

All events that UEM receives are automatically forwarded to a separate table. From that table, Fault Manager can get information about all past events that do not exceed the number of seconds defined in the ArchiveCleanupPolicy. Through the UEM client web interface, you can display archived events or export them to `.csv` files based on the provided filtering criteria. You can save the filter criteria you provide.

Figure 10: Events Archive – UEM Client Web Interface



Archived Events Properties

Severity
The severity of an event.

Date/Time
The time at which an event is generated in UEM. It is displayed in the **Date/Time** field in the **Network Database** window.

Managed Resource
A user-friendly name of a managed object which a particular event corresponds to.

Entity
A user-friendly name of a failure object which a particular event is associated with.

Message
A descriptive text message about an event.

Archive ID
A unique, sequential ID of an archived event. UEM assigns it to all archived events.

Event ID
A unique, sequential ID of an event. UEM assigns it to all each events.

Category
The category of the event. For example:

- Information event
- Attribute Value Change Event
- Equipment Alarm

- Quality of Service Alarm
- Communication Alarm
- Processing Error Alarm
- Object Creation Event
- Object Deletion Event
- Management Event
- Security Violation

Node
The name of the corresponding network element which a particular event is being generated for.

Failure Object
A failure object responsible for the creation of an event. The internal name is derived by UEM.

Source
The managed object which an event corresponds to. Generally, it is the name of a managed object.

Reporting Agent
The IP address of a device (agent) that sends an event.

NE Timestamp
The time at which an event is generated in a device (agent). If the device does not send this timestamp in the event, there is no value assigned to this attribute.

Identifier
An internal attribute that uniquely identifies a particular event.

Is Alarm
An event can be classified as an alarm, or as an event. This classification applies separately to every instance.

Ack Status
The acknowledgement status of an alarm (only applicable to alarms).

Ack Date/Time
The date and time an alarm was acknowledged or unacknowledged in UEM (only applicable to acknowledged and unacknowledged alarms).

Ack User
The name of the user who acknowledged or unacknowledged an alarm (only applicable to acknowledged and unacknowledged alarms).

Priority
The priority of an alarm (only applicable to alarms). Priority of an alarm in event archive is set while the alarm is generated, and is not updated later.

Related Links

Severity Definitions on page 65
Event and Alarm Category Definitions on page 65
Accessing and Retrieving Events Archives in UEM on page 246
Viewing Archived Events in UEM on page 252

This page intentionally left blank.

Chapter 2

UEM Installation

For information about the Unified Event Manager (UEM) installation, see the *Private Network Management Servers* manual.

This page intentionally left blank.

Chapter 3

UEM Configuration

Configuration procedures enable you to configure Unified Event Manager (UEM) for your specific network.

3.1

Account Management

Unified Event Manager (UEM) accounts are managed by administrators. The administrators assign privileges to users and groups. In UEM, there are pre-configured groups and user accounts that cannot be deleted.

Account Management Functions

The primary function of the Unified Event Manager (UEM) administrators is the management of UEM users and their privileges. Privilege assignments are primarily used to enable authentication and authorization of services on UEM. The account management function includes the management of the following items:

User
A UEM user configured for performing operations on the system.

Group
A logical set of configured users who access common information or perform similar tasks. Administration settings of a group apply to individual members or users of the group.

Operation
A task or a function allowed in UEM.

Authorized Scope/Authorized View
A set of criteria that restrict the configured user to perform operations only for data that match those criteria.

Pre-Configured Groups

By default, UEM is pre-configured with groups that cannot be deleted. If you attempt to delete any of these groups, an error message appears. The pre-configured groups are:

SuperUser
A user responsible for day-to-day monitoring and administration of the Radio System.

SecurityAdmin
A user responsible for the creation and maintenance of user accounts.

MotorolaSSC
A user responsible for the administration of the Motorola Solutions Support Center (SSC) accounts on the customer system.

TechnicianGroup
A user responsible for troubleshooting issues within the Radio System.

UpgradeGroup
A group of users responsible for upgrading the system.

Pre-Configured Users

By default, UEM is pre-configured with default local user accounts that cannot be deleted. If you attempt to delete any of the default local user accounts, an error message appears. You can create other local user accounts. The pre-configured default user accounts are:

root
A user account with the SuperUser role assigned.

admin
A user account with the SecurityAdmin role assigned.

sscadmin
A user account with the MotorolaSSC role assigned.

technician
A user account with the TechnicianGroup role assigned.

upgrade
An upgrade operator account used to upgrade UEM.

3.2 Communication Credentials Configuration

The configuration of inbound and outbound credentials includes the configuration of Simple Network Management Protocol version 3 (SNMPv3), WebService, and North Bound Interface (NBI).

3.2.1 SNMPv3 Credentials Configuration

Unified Event Manager (UEM) supports SNMPv3 communication to the network elements and Network Management System (NMS).

UEM is configured with default SNMPv3 credentials that are used for:

- Outbound communication to the devices
- Inbound communication from the devices
- Communication with NMS by using North Bound Interface (NBI)

By default, UEM restricts configuration of SNMPv3 credentials for those three types of communication to the SuperUser and SecurityAdmin groups. The configuration of Motorola Solutions Support Center (SSC) NBI SNMPv3 credentials (MotoNorthMotorola) is restricted to users belonging to the MotorolaSSC group only.

There are three types of SNMP credentials configuration:

- Global SNMPv3 credentials configuration
- Network element SNMPv3 credentials configuration
- Discovery session SNMPv3 credentials configuration

Network element SNMPv3 credentials can be configured after the network element/device has been successfully discovered.

NOTICE: If credentials for the discovery job were not configured, network elements are discovered with Global MotoMaster SNMPv3 credentials.

3.2.1.1

Configuring Global SNMPv3 Credentials for the MotoMaster User

Configure the global SNMPv3 credentials for communication by modifying the MotoMaster user credentials.

Credentials that you can configure for the MotoMaster user are the following security levels:

NoAuthNoPriv
A security level with no authentication and privacy passphrases defined.

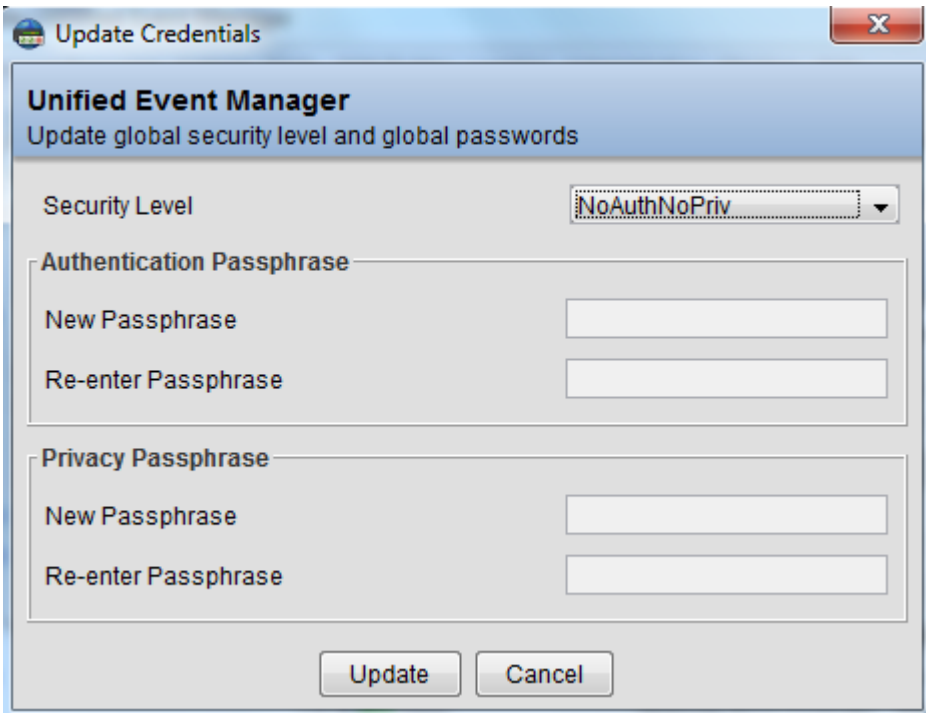
AuthNoPriv
A security level with an authentication passphrase defined but with no privacy passphrase.

AuthPriv
A security level with authentication and privacy passphrases defined.

Procedure:

1. From the main menu, select **Tools** → **Configure Global SNMPv3 Credentials**.
2. In the **Global SNMPv3 Credentials Configuration** dialog box, select **MotoMaster**. Click **Update Credentials**.
3. In the **Update Credentials** dialog box, select the security level that you want to update:
   - **NoAuthNoPriv**
   - **AuthNoPriv**
   - **AuthPriv**

   Figure 11: Update Credentials Dialog Box



4. Modify the security level information and click **Update**.

NOTICE: No passphrase fields are needed with the **NoAuthNoPriv** security level. Fill the **Authentication Passphrase** fields for the **AuthNoPriv** security level. Fill both the **Authentication Passphrase** and the **Privacy Passphrase** fields for the **AuthPriv** security level.

3.2.1.2
Configuring Global SNMPv3 Inform Credentials

Configure global SNMPv3 credentials for inbound communication by modifying the MotoInformA or MotoInformB user credentials.

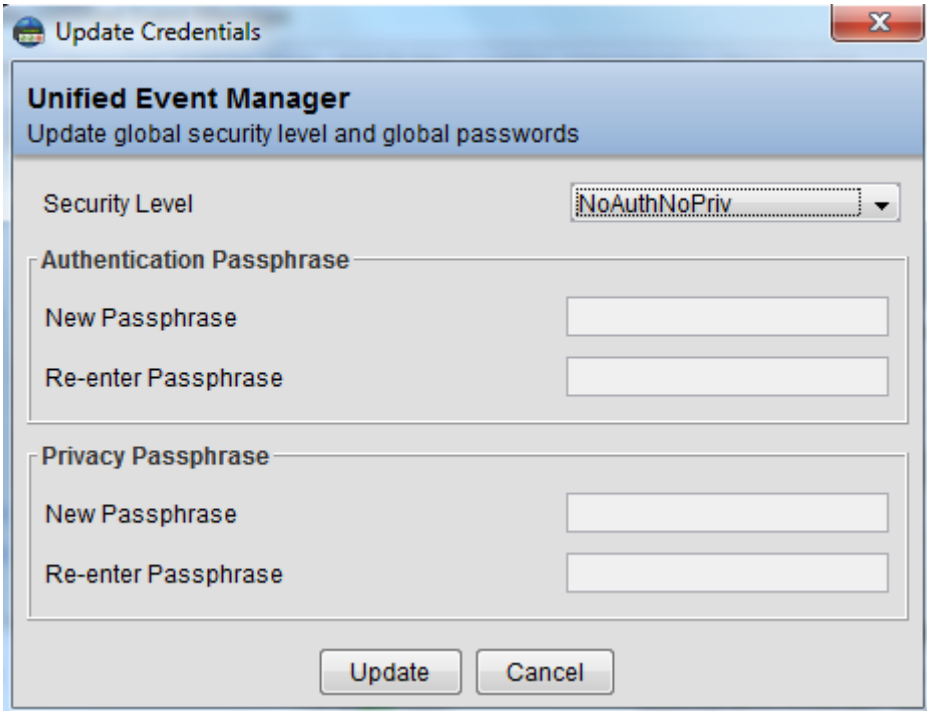
Procedure:

1. Log on to UEM as admin, security admin or any user who can change credentials.
2. From the main menu, select **Tools** → **Configure Global SNMPv3 Credentials**.

   The **Global SNMPv3 Credentials Configuration** window appears, displaying the default credentials.

3. Select **MotoInformA** or **MotoInformB** inform users and click **Update credentials**.

   Figure 12: Update Credentials Dialog Box



   The **Update Credentials** dialog box appears.

4. Modify the security level information and click **Update**.

   NOTICE: No passphrase fields are needed with the **NoAuthNoPriv** security level. Fill the **Authentication Passphrase** fields for the **AuthNoPriv** security level. Fill both the **Authentication Passphrase** and the **Privacy Passphrase** fields for the **AuthPriv** security level.

3.2.1.3
Updating the Network Element SNMPv3 Credentials

You update the network element SNMPv3 credentials for outbound communication by changing the MotoMaster credentials for a specific network element.

Credentials that you can update for the MotoMaster user are the following security levels:

NoAuthNoPriv
A security level with no authentication and privacy passphrases defined.

AuthNoPriv
A security level with an authentication passphrase defined but with no privacy passphrase.

AuthPriv
A security level with authentication and privacy passphrases defined.

Procedure:

1. In the **Navigation View** panel, highlight the **Network Database** node.
2. In the **Network Database** window, right-click a network element and select **Update SNMPv3 Credentials**.
3. In the **Update SNMPv3 Credentials** dialog box, select **MotoMaster**. Click **Update Credentials**.
4. In the **Update Credentials** dialog box, select the security level that you want to update:
   - **NoAuthNoPriv**
   - **AuthNoPriv**
   - **AuthPriv**
5. Modify a security level. Click **Update**.
   - For the **NoAuthNoPriv** security level, make no passphrase updates.
   - For the **AuthNoPriv** security level, update the **Authentication Passphrase** pane.
   - For the **AuthPriv** security level, update the **Authentication Passphrase** and **Privacy Passphrase** panes.

3.2.1.4 Testing any Device SNMPv3 Configuration

Testing the SNMPv3 configuration of devices involves communication with the MotoMaster user only. Other SNMPv3 users do not participate in this configuration test.

Procedure:

1. From the main menu, select **Tools** → **Test Any Device SNMPv3 Configuration**.

   The **Test Any Device SNMPv3 Configuration** dialog box appears.

2. In the **IP Address or Hostname** field, enter the IP address of the device you want to test. Click **Start**.

The status of the request appears in the status bar.

3.2.1.5 Testing SNMPv3 Communication Between Network Elements and UEM

Using this procedure, you can test if the MotoMaster account is configured properly.

Procedure:

1. In the **Navigation View** panel, click the **Network Database** node.
2. In the **Network Database** view, right-click a managed resource, and select **Test SNMPv3 Configuration**.
3. In the **Test SNMPv3 Configuration** dialog box, click **Start**.

   The **IP Address and Hostname** field is populated automatically.

   The status of the request appears in the status bar.

3.2.2
Web Service Credentials Configuration

Unified Event Manager (UEM) supports communication with Web Service over Simple Object Access Protocol (SOAP). UEM is configured with default Web Service credentials.

Web Service credentials are used for outbound communication to the devices. Neither the UEM server nor the UEM client exposes any Web Service, so no configuration for inbound traffic is necessary. By default, UEM restricts configuration of Web Service credentials to the members of the SuperUser and SecurityAdmin groups.

By using Web Service, the following network elements can be managed:

- ESXi (using VMware vSphere Web Services)
- vCenter (using VMware vSphere Web Services)

Configuring Web Service credentials can be classified into three types:

- Global Web Service credentials configuration
- Network element-specific Web Service credentials configuration
- Web Service credentials for a discovery session

Related Links

Configuring Global Web Service Credentials for the MotoMaster User on page 86
Updating Network Element Web Service Credentials on page 86
Configuring Discovery Job Credentials on page 88

3.2.2.1
Configuring Global Web Service Credentials for the MotoMaster User

You can configure the Web Service credentials for outbound communication, by updating the MotoMaster user credentials.

Procedure:

1. From the main menu, select **Tools** → **Configure Global Web Service Credentials**.
2. In the **Global Web Service Credentials Configuration** dialog box, modify the authentication passphrase. Click **Update**.

3.2.2.2
Updating Network Element Web Service Credentials

You can configure the credentials of network element-specific Web Service after the successful discovery of a network element or device.

Procedure:

1. In the **Navigation View** panel, click the **Network Database** node.
2. In the **Network Database** window, right-click a network element and click **Update Web Service Credentials**.
3. In the **Update Web Service Credentials** dialog box, modify the password. Click **Update**.

3.2.2.3
Testing any Device Web Service Configuration

Procedure:

1. From the main menu, select **Tools** → **Test Any Device Web Service Configuration**.

   The **Test Any Device Web Service Configuration** dialog box appears.

2. In the **IP Address or Hostname** field, enter the IP address of the device you want to test. Click **Start**.

The status of the request appears in the status bar.

3.2.2.4
Testing the Web Service Communication Between Network Elements and UEM

Procedure:

1. In the **Navigation View** panel, click the **Network Database** node.
2. In the **Network Database** view, right-click a managed resource and select **Test Web Service Configuration**.
3. In the **Test Web Service Configuration** dialog box, click **Start**.

   The **IP Address and Hostname** field is populated automatically.

The status of the request appears in the status bar.

3.2.3
Configuring North Bound Interface

Unified Event Manager (UEM) supports North Bound Interface (NBI) for sending up notifications to the registered Manager of Managers (MoM). Currently, there are four interfaces that are supported; two for the Motorola Solutions Support Center (SSC) interface and two for the customer MoM interface. NBI uses SNMPv3 and the User-Based Security Model (USM) to provide secure communication between UEM and Network Management System (NMS).The customer NBI MoM interface is a licensed UEM service that is available only for users with a feature license for the NBI service. For more information about licenses, see the *License Manager* manual.

Procedure:

1. From the main menu, select **Tools** → **Configure North Bound Interface**.
2. In the **NBI Configuration** dialog box, click **Register NMS**.
3. In the **Register NMS** dialog box, perform the following actions:
   a. In the **NMS IP Address** field, enter the IP address of the NMS to which you want to send the events.
   b. In the **Port Number** field, enter the port number of the NMS to which you want to send the events.
   c. From the **Operational state** list, select **Enabled**.

      NMS can receive events.

d Optional: Verify the NMS IP address by clicking **Send test trap**.

If the NMS IP address is correct, the trap is sent over the NBI interface to the MoM or SSC application. You can verify that the trap is sent in the MoM or SSC application.

e Click **Register**.

The NMS is registered and appears in the **NBI Configuration** window.

3.3 Discovery Job Credentials Configuration

With permissions to configure the MotoMaster credentials and to perform a discovery, you can configure and disable credentials for a single discovery job. You can configure Web Service and SNMPv3 discovery job credentials for a discovery job.

3.3.1 Configuring Discovery Job Credentials

When you initiate a discovery job with custom credentials set, the credentials are used to discover new devices and rediscover existing devices. Existing credentials for discovered devices are overwritten and rediscovery is performed.

If this rediscovery fails due to a credentials mismatch, additional rediscovery with the proper credentials set may be needed.
When you start a discovery job with custom credentials, settings in the **Update Credentials** window are not set back to their default values as long as the **Discovery Configuration** window remains open. This allows you to start multiple discovery jobs with the same customized credentials set.

Procedure:

1. From the main menu, select **Tools** → **Discovery**.
2. In the **Discovery Configuration** window, click **Credentials**.
3. In the **Update Credentials** window, perform one of the following actions:

If…	Then…
If you want to discover an SNMPv3 device,	perform the following actions: **a** In the **SNMPv3** tab, select the **Use the following credentials** check box. **b** From the **Security Level** list, select a SNMPv3 security level. **c** Enter the respective passphrases. Click **OK**.
If you want to discover a Web Service device,	perform the following actions: **a** In the **Web Service** tab, select the **Use the following credentials** check box. **b** Enter the respective passphrases. Click **OK**.

If the **Use the following credentials** check box is selected for either SNMPv3 or Web Service, in the header of the **Discovery Configuration** window, a message appears informing you that the customized credentials apply to devices discovered in earlier and recent discoveries.

3.3.2
Disabling Discovery Job Credentials

After you configure discovery job credentials, you can restore their default values.

Prerequisites: Configure discovery job credentials. See Configuring Discovery Job Credentials on page 88.

Procedure:

1. From the main menu, select **Tools** → **Discovery**.
2. In the **Discovery Configuration** window, click **Credentials**.
3. In the **Update Credentials** window, perform one of the following actions:
   - To disable discovery credentials of an SNMPv3 device, in the **SNMPv3** tab, clear the **Use the following credentials** check box. Click **OK**.
   - To disable discovery credentials of a Web Service device, in the **Web Service** tab, clear the **Use the following credentials** check box. Click **OK**.
4. In the **Discovery Configuration** window, click **Close**.

Discovery job credentials are restored to their default values.

3.4
Application Configuration

The following configuration operations can be made to the Unified Event Manager (UEM) interface:

- User preferences configuration
- Maps configuration
- Network Database configuration
- Alarm filters configuration
- Event filters configuration

3.4.1
User Preferences Configuration

All users can configure the initial Unified Event Manager (UEM) view and login information.

3.4.1.1
Setting the Initial View

Procedure:

1. From the main menu, select **Administration** → **User Preferences**.

   The **User Preferences** dialog box appears.

2. In the **Initial View on Login** drop-down menu, select the view you want to see each time you log on. The following views are available:
   - Physical Summary View
   - Physical Detail View
   - Service Summary View
   - Service Detail View

- Alarms
- Network Events
- Network Database
- System Map
- Zone Map
- Microwave Map

3 Click **OK**.

Your preference is saved. The **User Preferences** dialog box displays the currently saved option each time you open it.

3.4.1.2
Enabling or Disabling the Login Info Window at the Start-Up

Procedure:

1 From the main menu, select **Administration** → **User Preferences**.

The **User Preferences** dialog box appears.

2 From the **Display login info at startup** drop-down menu, select **Yes** to display the window at the start-up or select **No** not to display it.

3 Click **OK**.

Your preference is saved.

3.4.1.3
Setting a New Alarm Blinking Indication

New alarms can be indicated by blinking. This setting affects the System Map, the Zone Map, Site Views and Network Element Views.

Procedure:

1 Select **Administration** → **User Preferences**.

The **User Preferences** dialog box appears.

2 To define how long the new alarm indication lasts, in the **Blinking time for new alarm** field enter the appropriate number of seconds.

3 Click **OK**.

Every new alarm is blinking for the specified time.

3.4.2
Maps Configuration

Maps are the graphical representations of managed resources.

There are five types of maps:

- System Map
- Zone Map
- Microwave Map
- Physical Map (summary and details)

- Service Map (summary and details)

3.4.2.1

System, Zone and Microwave Maps Configuration

The system map displays the status of zones in the system (primary and backup cores) for each zone. The zone map displays the status of sites in the zone. The microwave map displays status of microwave radios in the zone.

NOTICE: When another user changes the map mode or tries to edit an element that is currently edited, a notification is displayed.

3.4.2.1.1

Setting the Map Mode

Choose between the geographical map and the static map. In the geographical mode users define geographical coordinates (latitude and longitude).

Procedure:

1 Perform one of the following actions:

If…	Then…
If you want to set the map mode for a system map,	go to **System Views** → **System Map**.
If you want to set the map mode for a zone map,	go to **Zone Views** → **Zone Map**.
If you want to set the map mode for a micro-wave map,	go to **Zone Views** → **Microwave Map**.

2 Click the **Map Mode** icon .

3 Select the desired mode and click **Save**.

Related Links

System, Zone and Microwave Map Operations on page 144

3.4.2.1.2

Changing the Map Background in the Static Mode

Background display can differ from one map to another. Backgrounds are images in the `.bmp`, `.gif`, `.jpg`, `.jpeg`, `.png`, or `.wbmp` format. The minimum size of the image is 256 pixels x 256 pixels, the maximum size of the image is 2048 pixels x 2048 pixels. You can change backgrounds according to your requirements.

Procedure:

1 Perform one of the following actions:

If…	Then…
If you want to change the map background for a system map,	go to **System Views** → **System Map**.
If you want to change the map background for a zone map,	go to **Zone Views** → **Zone Map**.

If…	Then…
If you want to change the map background for a microwave map,	go to **Zone Views** → **Microwave Map**.

2 Click the **Load Image File** icon  .

3 Perform one of the following actions:

If…	Then…
If you want to set a new background,	perform the following actions: **a** Click **Choose file**. **b** Navigate to the desired image and click **Open**. **c** Click **Save**.
If you want to remove the current background,	click **Clear background**.

Related Links

System, Zone and Microwave Map Operations on page 144

3.4.2.1.3

Loading and Updating Map Tiles in the Geographical Mode

In geographical mode, users define geographical coordinates (latitude and longitude).

In this mode a geographical map following the slippy map convention based on map tiles is used as a background and replaces an empty or image-based background.
To use the geographical map, the user needs to load the map tiles for a specific region on the UEM server. Motorola Solutions delivers the tiles for zoom levels 0–12, but the user may provide their own tiles in the proper format (***<zoom_level>/<x>/<y>***`.png`). The map tiles should be loaded onto the server from a CD/DVD. Motorola Solutions is not responsible for preparing map tiles from external vendors.

The user can perform this procedure to update the map tiles already installed on the UEM server by loading a new archive containing map tiles for the same zoom levels. The content of the newly loaded archive overwrites the corresponding map tiles existing on the UEM server.

NOTICE: All the map tiles loaded on the UEM server are stored in the `/opt/Motorola/geomap/storage/tiles` folder. The UEM partition can store up to 35 GB of data (it is the disk space dedicated only for the map tiles). The tiles archive is available for all maps.

Procedure:

1 Prepare a folder containing the map tiles, which should be loaded on the UEM server.

The structure of this folder must be ***<zoom_level>***/***<x>***/***<y>***.png, where:

- ***<zoom_level>*** is one of zoom level folders (UEM supports the zoom levels 0–18)
- ***<x>*** is the subfolder name, which is also the tile number on the x-axis,
- ***<y>*** is the name of the `.png` file containing 256 x 256 px map tile graphics (the name is also the tile number on the y-axis).

Step example:
The map tile image corresponding to zoom level 0, x-coordinate 0, and y-coordinate 1 would be stored with the following directory structure and filename: `0/0/1.png`.

2 Compress the content of the prepared folder to a `.zip` archive.

3 Burn the file to the CD/DVD.

NOTICE: The size of folders containing the map tiles for high zoom levels can be significant, so it may be necessary to compress individual groups of the zoom level folders to separate `.zip` archives and use more than one CD/DVD for storing them.

4 Log on to the UEM server using your Active Directory account.

5 Insert the CD/DVD with the tiles archive file in to the optical drive of the PC.

6 On the UEM server, run the admin menu.

7 Go to **Application Administration** → **Load Map Tiles from CD/DVD**.

8 Enter the number corresponding to the archive you want to load.

9 Confirm you want to unpack the archive by pressing **y**.

10 Repeat step 4 to step 6 for each CD/DVD disc containing the map tiles.

Related Links

System, Zone and Microwave Map Operations on page 144

3.4.2.1.4

Deleting Map Tiles

In order to free up space in the UEM server map tiles folder, or to remove map tiles for certain geographic locations, the UEM provides a function to delete map tiles. The following procedure removes all map tiles installed on the UEM server.

Procedure:

1 Log on to the UEM server using your Active Directory account.

2 Go to **Application Administration** → **Remove All Map Tiles**.

3 Confirm you want to remove all the installed map tiles by pressing **y**.

The system confirms that the map tiles storage on the server has been cleaned.

3.4.2.1.5

Setting Zones Visibility on System Maps

Use the visibility setting to hide selected zones on the system map.

Procedure:

1 In the **Navigation View** panel, go to **System Views** → **System Map**.

2 Click the **Zones Visibility** icon  .

3 Select and/or clear the required check boxes representing connections to UEMs in other zones.

4 Click **Save**.

NOTICE: If a zone icon is gray and crossed out, there is no connection to the UEM in that zone.

Related Links

System, Zone and Microwave Map Operations on page 144

3.4.2.1.6

Configuring the Map Center

Procedure:

1 Perform one of the following actions:

If…	Then…
If you want to configure the center of a system map,	go to **System Views** → **System Map**.
If you want to configure the center of a zone map,	go to **Zone Views** → **Zone Map**.
If you want to configure the center of a microwave map,	go to **Zone Views** → **Microwave Map**.

2 Click the **Map Configuration** icon .

3 In the **Default Map Center** section, enter the required latitude and longitude values.

4 Click **Set Properties To Map**.

Related Links

System, Zone and Microwave Map Operations on page 144

3.4.2.1.7

Configuring Zoom Levels

When a map is opened, the default zoom level is used. The minimum and maximum zoom levels available are 0 and 18 respectively.

Procedure:

1 Perform one of the following actions:

If…	Then…
If you want to configure the zoom levels of a system map,	go to **System Views** → **System Map**.
If you want to configure the zoom levels of a zone map,	go to **Zone Views** → **Zone Map**.
If you want to configure the zoom levels of a microwave map,	go to **Zone Views** → **Microwave Map**.

2 Click the **Map Configuration** icon .

3 3)In the **Zoom Level** section, enter the required minimum, maximum and default zoom values.

4 Click **Set Properties To Map**.

Related Links

System, Zone and Microwave Map Operations on page 144

3.4.2.1.8

Configuring Max Bounds

Procedure:

1 Perform one of the following actions:

If…	Then…
If you want to configure the max bounds of a system map,	go to **System Views** → **System Map**.
If you want to configure the max bounds of a zone map,	go to **Zone Views** → **Zone Map**.
If you want to configure the max bounds of a microwave map,	go to **Zone Views** → **Microwave Map**.

2 Click the **Map Configuration** icon  .

3 3)In the **Max Bounds** section, enter the required minimum and maximum latitude and longitude values.

4 Click **Set Properties To Map**.

Related Links

System, Zone and Microwave Map Operations on page 144

3.4.2.1.9

Adding Areas on Maps

An area can be defined by the user for each zone or site. In multi-zone systems, users can only add areas to the zone element assigned to their UEM.

Procedure:

1 Perform one of the following actions:

If…	Then…
If you want to add a zone area on a system map,	go to **System Views** → **System Map**.
If you want to add a site area on a zone map,	go to **Zone Views** → **Zone Map**.

2 Right-click the icon of the zone or site that you want to surround by an area and select **Add Area**.

3 To start drawing the area boundary, click the selected spot on the map.

4 Specify the remaining boundary points by clicking the map.

There can be maximum 100 boundary points.

5 To finish drawing the area boundary, click the first point.

6 Optional: If needed, re-arrange the boundary by dragging specific white points on the map, clicking a white point to remove it, or a transparent point to add two new points.

7 To confirm the area drawn, click **Save**.

Related Links

System, Zone and Microwave Map Operations on page 144

3.4.2.1.10

Editing Areas on Maps

Procedure:

1 Perform one of the following actions:

If…	Then…
If you want to edit a zone area on a system map,	go to **System Views** → **System Map**.
If you want to edit a site area on a zone map,	go to **Zone Views** → **Zone Map**.

2 Right-click the area that you want to edit and select **Edit Area**.

NOTICE: In multi-zone systems, users can only edit zone elements assigned to their UEM.

3 Re-arrange the boundary by dragging specific white points on the map, clicking a white point to remove it, or a transparent point to add two new points.

4 To confirm the area, click **Save**.

Related Links

System, Zone and Microwave Map Operations on page 144

3.4.2.1.11

Removing Areas from Maps

Procedure:

1 Perform one of the following actions:

- If you want to remove a zone area from a system map, go to **System Views** → **System Map**.
- If you want to remove a site area from a zone map, go to **Zone Views** → **Zone Map**.

2 Perform one of the following actions:

- Right-click the area that you want to delete and select **Remove Area**.
- Unassign all the sites or zones assigned to that area. Right-click the icon of each site or zone and select **Un-Assign Site from Area** or **Un-Assign Zone from Area**. When you unassign the last site or zone assigned to the area, the area is removed.

Related Links

System, Zone and Microwave Map Operations on page 144

3.4.2.1.12

Editing Map Elements Coordinates

Procedure:

1 Perform one of the following actions:

If…	Then…
If you want to edit the coordinates of a system map element,	go to **System Views** → **System Map**.
If you want to edit the coordinates of a zone map element,	go to **Zone Views** → **Zone Map**.
If you want to edit the coordinates of a microwave map element,	go to **Zone Views** → **Microwave Map**.

2 Right-click the element whose coordinates you want to edit and select **Edit Coordinates**.

3 Enter the coordinates as specified in the dialog box and click **OK**.

Related Links

System, Zone and Microwave Map Operations on page 144

3.4.2.1.13

Renaming Map Elements

Procedure:

1 Perform one of the following actions:

If…	Then…
If you want to rename a system map element,	go to **System Views** → **System Map**.
If you want to rename a zone map element,	go to **Zone Views** → **Zone Map**.
If you want to rename a microwave map element,	go to **Zone Views** → **Microwave Map**.

2 Right-click the element you want to rename and select **Rename**.

3 Enter the new name and click **OK**.

NOTICE: On the system map in a multi-zone system, users can only rename the zone element assigned to their UEM.

Related Links

Site Operations on page 136
System, Zone and Microwave Map Operations on page 144
Site Operations on page 136

3.4.2.1.14

Moving Elements on the Map

Procedure:

1 Perform one of the following actions:

If…	Then…
If you want to move a system map element,	go to **System Views** → **System Map**.
If you want to move a zone map element,	go to **Zone Views** → **Zone Map**.
If you want to move a microwave map element,	go to **Zone Views** → **Microwave Map**.

2 Click **Edit Coordinates** icon  .

All movable elements are highlighted.

3 Drag a specific element to a selected location.

4 To confirm the new location of the element, click **Save**.

Related Links

System, Zone and Microwave Map Operations on page 144

3.4.2.1.15

Assigning Sites to Areas on Zone Maps

When an area is already created for a site, other sites can be assigned to this area. Among the elements assigned to an area, the element with the highest severity level defines the severity level for the whole area.

Procedure:

1 In the **Navigation View** panel, go to **Zone Views** → **Zone Map**.

2 Right-click the icon of the site that you want to assign to an area and select **Assign to Area**.

3 Click the area to which you want to assign the site.

4 To confirm the assignment, click **Save**.

5 Optional: To view the list of sites assigned to the area, right-click the area.

The sites are listed at the top of the dialog box, in the **GROUP AREA** section.

Related Links

System, Zone and Microwave Map Operations on page 144

3.4.2.1.16

Adding a Link Between Microwave Radios on Microwave Maps

Procedure:

1 In the **Navigation View** panel, go to **Zone Views** → **Microwave Map**.

2 Right-click the icon of the radio that you want to link to another radio and select **Add Link**.

3 Hover the pointer over the target radio, a green line indicates a valid link. Click the target radio.

The radios are linked as indicated by a black line.

Related Links

System, Zone and Microwave Map Operations on page 144

3.4.2.1.17

Removing a Link Between Microwave Radios on Microwave Maps

Procedure:

1 In the **Navigation View** panel, go to **Zone Views** → **Microwave Map**.

2 Right-click the icon of one of the linked radios.

The link is highlighted.

3 Right-click the link and select **Remove Link**.

4 Confirm the action by clicking **Yes**.

Related Links

System, Zone and Microwave Map Operations on page 144

3.4.2.1.18

Unassigning Sites or Zones from Areas on Maps

You can unassign Sites from Areas on Zone Maps, and you can unassign Zones from Areas on System Maps.

Procedure:

1 Depending on whether you want to unassign a Site or a Zone, perform one of the following actions:

If…	Then…
If you want to unassign a Site,	perform the following actions: **a** In the **Navigation View** panel, go to **Zone Views** → **Zone Map**. **b** Right-click the icon of the site that you want to unassign from an area and select **Un-Assign Site from Area**
If you want to unassign a Zone,	perform the following actions: **a** In the **Navigation View** panel, go to **System Views** → **System Map**. **b** Right-click the icon of the zone that you want to unassign from an area and select **Un-Assign Zone from Area**

NOTICE: If you unassign the last site or zone assigned to an area, the area is removed.

Related Links

System, Zone and Microwave Map Operations on page 144

3.4.2.2

Physical and Service Maps Configuration

Physical and service maps can be configured to desired specifications.

The configuration of these maps includes changing the background image, grouping, ungrouping, and updating related information from the **Symbol Properties** window.

3.4.2.2.1

Maps Layout Configuration

Unified Event Manager (UEM) supports overlaying the map symbols on a background image. You can save the position of the anchored map symbols with respect to the background.

3.4.2.2.1.1

Changing Physical and Service Maps Background

Background display can differ from one map to another, between physical and service map types, and so on. Backgrounds are images in the `.png` or `.jpg` format. You can change backgrounds according

to your requirements. You can, for example, use your area map and move the icons in the view to reflect their physical location. You can also add a background image. For information and procedures on adding images, see “Loading Image and Audio Files from a CD/DVD” in the *Private Network Management Servers* manual.

Procedure:

1. In the **Navigation View** panel, highlight the map for which you want to change the background.
2. Double-click the background of the map.
3. In the **Map Properties** window, in the **Image Name** field, click the **Select a File** icon .
4. In the **Unified Event Manager File Dialog** dialog box, select a file that you want to set as the map background. Click **Open**.
5. In the **Map Properties** window, click **Modify**.

The background display of the map is changed.

3.4.2.2.1.2
Saving Physical and Service Maps Layout

After you modify your map, for example, you create groups or rearrange map symbols, save the map to retain the changes. If you do not save the map layout, when you reopen the client, the changes are lost.

Procedure:

From the main menu, select **Map** → **Save Map**.

The map changes are saved.

3.4.2.2.1.3
Refreshing Physical and Service Maps Layout

Use the refresh option to reset the map layout to the last saved layout. Unlike the relayout option that restores default layout of the application client to your map, the refresh option restores the last saved layout to your map.

Procedure:

From the main menu, select **View** → **Refresh**.

The last saved map layout is restored.

Example: You create two groups in your default map and save the map. In the same map, you perform further operations, for example, you add more groups or rearrange map symbols. If you want to restore the last saved map display, that is the one with the two groups saved, use the **Refresh** option.

3.4.2.2.1.4
Resetting Physical and Service Maps Layout

Unified Event Manager (UEM) has a default map layout in which the symbols in a map are arranged based on the order of discovery. You use the **Relayout** option after you rearrange symbols in the map to restore the symbols to their default position.

IMPORTANT: If you perform this operation, you lose your customized map layout. This operation cannot be reversed.

Procedure:

1. From the main menu, menu, select **Map** → **Relayout Map**.
2. In the confirmation dialog box, click **Yes** to restore default map layout.

Map elements are restored to their default position.

3.4.2.2.1.5
Physical and Service Maps Zooming Options

You can zoom in on the map to focus on a specific symbol or zoom out to see more map elements.

Table 20: Zoom Options

The following table contains zoom options available in the toolbar.

Toolbar Option	Description
Select Mode	This option is used to select a map symbol in the map view. This operation is indicated by enclosing it within four blocks.
Zoom Window	This option displays the Zoom Overview window highlighting the area of the map (with red bars) which is being zoomed.
	Click and drag the red bar to run through the open map.
	This option is useful when there are many map symbols displayed in the map view. You can find the exact location of a map symbol.
Zoom Mode	This tool enables you to zoom in on map symbols in a map. This option is used for viewing the enlarged version of a specific map symbol.
	When using this option, the map symbols cannot be selected. They can only be enlarged. If you want to select map symbols in the enlarged view, click **Select Mode** and then select the map symbols.
Zoom In	Click **Zoom In** for an enlarged view of the selected map. The selected map is zoomed at the center.
	Use the Zoom Mode to enlarge a specific map symbol or an area of the map. Use the Zoom In option to enlarge the complete map at the center.
Zoom Out	Retracts the zoomed map. With every click, the Map retracts by one size.
Group View	Goes back to Group View. If you are inside an Expanded View, click this icon to go back to Group View.
Expand Selected Groups	Expands the selected group. Click this icon to show all the map symbols that are under this group.
Group Selected Symbols	Combines the selected map symbols under one group. Click this icon to group the selected map symbols under a specific group.

3.4.2.2.2

Changing the Symbol Label Property for Physical and Service Maps

The map view shows symbols that are associated with the managed resources in the network database. In the map view, the label property of a symbol can be changed to exhibit a more meaningful name.

Procedure:

1. On the symbol icon in the map view window, highlight a symbol icon, right-click it, and select **Symbol Properties**.

   The **Symbol Properties** window appears.

2. In the **Label** text box, type the name of the symbol you want to be displayed for the symbol and click **Modify**.

The property is changed.

3.4.2.2.3

Changing the Managed Resource Name for Physical and Service Maps

After you discover managed resources in UEM, you can view them in the **Network Database** window. For most managed resources, the **Managed Resource** value is meaningful, and for some the value is the IP address of a managed resource, for example for backhaul firewalls. Additionally, network and logical-managed resources that are displayed in the **Network Database** window are associated with symbols displayed in the maps windows, for example in the **Physical Summary View** and **Service Detail View** windows. You can change the value of a managed resource to be more meaningful than, for example, an IP address.

Procedure:

Open the properties window of the object whose name you want to change:

If…	Then…
If you want to change the name of a map symbol on a physical or service map,	see the Changing the Symbol Label Property for Physical and Service Maps on page 102 procedure.
If you want to change the name of the network,	see the Renaming Managed Resources on page 103 procedure.

3.4.2.2.4

Updating Map Symbols and Managed Resource Names for Physical and Service Maps

Managed resources in the network database can be associated with symbol icons displayed in customized maps. You can update the symbol label to match the display name of a managed resource.

When updated, the display name of a managed resource is used for the symbol label name.
For symbols in the **Service Detail View**, the symbol label is updated first with the managed resource display name of the site controller in the group. The symbol name is updated with the managed resource display name of the site reported by the zone controller if the group does not contain any of the following:

- Site Controller
- SmartX Site Converter

- Site Link Relay Module

Procedure:

1. In the **Navigation View** panel, highlight a physical or service map node.

   The map nodes are:

   - **Physical Summary View**
   - **Physical Detail View**
   - **Service Summary View**
   - **Service Detail View**

2. Right-click the map symbol that you want to synchronize and select **Update Symbol Name**.

   You cannot update symbol names of user-created group symbols.

   The symbol label is synchronized with the managed resource display name.

3.4.3
Network Database Configuration

You can configure the network database by changing the display names of managed resources and by changing the names of subsystems.

3.4.3.1
Renaming Managed Resources

Follow this procedure to edit managed resource display names in the **Managed Resource Properties** window.

NOTICE: For user-created groups, the Synch Name command for synchronization of the Managed Resource Display Name with Symbol Property Label is not supported.

Procedure:

1. In the **Navigation View** panel, click the **Network Database** node.
2. In the **Network Database** window, highlight a row, right-click it, and select **Managed Resource Properties**.

   The **Managed Resource Properties** window appears.

3. In the **Managed Resource** field, type the name of the node you want to see displayed in the **Network Database View** and click **Modify**.

   NOTICE: The length of the name cannot exceed 100 characters. If the **Managed Resource** field is left blank, UEM uses the default managed resource name.

The device displays the updated name in the **Managed Resource** field.

3.4.3.2
Setting Default Names for Managed Resources

Procedure:

1. In the **Navigation View** panel, highlight the **Network Database** node.
2. In the **Network Database** window, double-click an element.
3. In the **Network Element View** window, go to the **Objects** section.

4 Right-click the managed resource to which you want to set the default name and select **Set Default Name**.

NOTICE: The default name for **Logical Managed Resources** is taken from UEM metadata and may be different than the name set on device side.

3.4.3.3
Renaming Subsystems

In Unified Event Manager (UEM), you can edit subsystem names so that Logical Managed Resources (LMR) and Device Managed Resources (DMR) are segregated into appropriate groups.

Procedure:

1 In the **Navigation View** panel, click the **Network Database** node.

2 In the **Network Database** window, right-click an item and select **Managed Resource Properties**.

3 In the **Managed Resource Properties** dialog box, click the **Relationships** tab.

4 Type the new name in the **Subsystem Name** field and click **Modify**.

NOTICE:
The length of the subsystem name cannot exceed 100 characters.

If the **Subsystem Name** field is left blank, UEM uses the default subsystem name.

The subsystem name is changed.

3.4.3.4
Network Element Configuration

Network elements are used to display the status of the managed resources and their entities.

Users can rename a managed resource, a single entity in the managed resource, and a subsystem, or change the hardware type and card configuration for managed resources supporting such functionality.

3.4.3.4.1
Renaming Entities

Procedure:

1 In the **Navigation View** panel, highlight the **Network Database** node.

2 In the **Network Database** window, double-click an element.

3 In the **Network Element View** window, go to the **Objects** section.

4 Right-click the entity that you want to rename and select **Rename**.

5 Enter a new name for the entity and click **Save**.

3.4.3.4.2
Setting Default Names for Entities

Procedure:

1 In the **Navigation View** panel, highlight the **Network Database** node.

2 In the **Network Database** window, double-click an element.

3 In the **Network Element View** window, go to the **Objects** section.

4 Right-click the entity to which you want to set the default name and select **Set Default Name**.

3.4.3.4.3
Changing the Hardware Type

Procedure:

1. In the **Navigation View** panel, highlight the **Network Database** node.
2. In the **Network Database** window, double-click an element.
3. In the **Network Element View** window, click **Edit** next to the **Hardware Type** value.
4. Enter a new name for the hardware type and click **Save**.

3.4.3.4.4
Changing the Card Configuration

Procedure:

1. In the **Navigation View** panel, highlight the **Network Database** node.
2. In the **Network Database** window, double-click an element.
3. In the **Network Element View** window, go to the **More Information** section.
4. Click **Edit** next to the **Card Configuration** value.
5. From the drop-down list, select the required option and click **Save**.

3.4.4
Alarm Filters Configuration

When an alarm is created, the occurrence of the alarm can be associated with some actions. Unified Event Manager (UEM) provides alarm filters to send e-mails to an administrator on occurrence of an alarm. This action is called a notification.

By configuring alarm filters you can filter alarms based on certain match criteria. With this tool you can add, modify, or delete filters and filter actions.

You can configure Unified Event Manager (UEM) to send notifications to users when alarms are generated from devices in a network. You can use alarm filters, also referred to as alert filters, to configure UEM to automatically initiate actions for selected alarms.

NOTICE:
When specifying property names, use only alphanumeric characters and underscores. Do not start property names with digits.

When used for filtering, property names are case-sensitive and should be used exactly as specified when typing in the name of the additional property criterion to filter on. For more information, see Alarm Properties on page 166.

UEM supports only the **Sending e-mails** built-in filter notification. Other notification types that can be associated with the filter are **Suppressing events**, **Sending custom trap**, and **Running Custom Code**. Even though these notifications are available on the user interface, **Sending e-mails** is the only notification type recommended for use during filter configuration on UEM. Do not add/delete or modify other notification types. These notification schemes require advanced knowledge and privileges and therefore are not recommended for general use. Contact Motorola Solutions Support Center (SSC) for information on the use of notification schemes other than e-mail notification scheme.

Match Criteria Property Overview

The managed resource and severity criteria determine whether the incoming alarm or event can be filtered or not. If any field is left blank, it is not considered matching criteria. For the alarm or event filter

to be applied, it must satisfy all the match criteria specified. If even one of the criteria fails, the filter is not applied. You can use wildcard characters and expressions to specify the match criteria.

UEM accepts any match criteria you enter. However, if you want to make sure that your criteria are valid for the system, enter them into a custom view. Criteria specified for custom views take immediate effect, while an alarm or event filter only works when new alarms or events of the specified type occur. For more information on how to add a custom view, see Custom View Operations on page 127.

Manage/Unmanage
Option that enables you to manage or unmanage UEM resources. For example, you can unmanage resources that are broken so that they do not send many traps to the trap buffer and take a lot of the trap buffer capacity. After the resources are fixed, you can manage the fixed resources to enable UEM to receive traps from them.

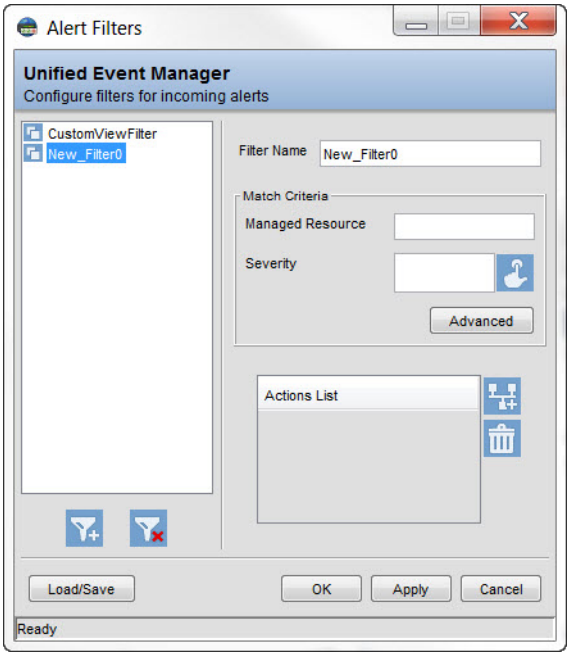
Clean Trap Buffer & Sync
Option that enables you to clear the trap buffer of all traps UEM received from a managed resource. After the trap buffer is cleared, UEM schedules synchronization with managed resources whose traps you removed. As a result, UEM receives up-to-date information from the managed resources.

3.4.4.1 Adding Alarm Filters

Procedure:

1. In the **Navigation View** panel, select **Fault Management** → **Alarms**.
2. From the main menu, select **Edit** → **Alarm Filters**.
3. In the **Alert Filters** window, click **Add Filter**.

   Figure 13: Alert Filters Window



   The **Actions List** panel options become active.

4. In the **Filter Name** field, specify the name of the filter.
5. In the **Match Criteria** pane, specify the **Managed Resource** and **Severity** criteria.
6. Optional: Configure additional match criteria by clicking **Advanced**.

In the **Match Criteria Properties** dialog box, you can configure the following match criteria:

- **Message**
- **Category**
- **Domain**
- **Network**
- **Node**
- **Failure Object**

7 Optional: Configure a filter by using an alarm property that is not displayed on the user interface:

a In the **Match Criteria Properties** dialog box, click **More Properties**.

b In the **Property Name** and **Property Value** fields, specify filter properties. Click **OK**.

The value must be the same as the one listed in the Property name for the filtering column. To modify an existing property, in the **Property Name** field, enter the same value again and in the **Property Value**, enter a new value. To remove a property, in the **Property Name** field, enter the same value again and leave the **Property Value** field blank.

c Close the **More Properties** dialog box. In the **Match Criteria Properties** dialog box, click **OK**.

8 In the **Actions List** panel, click **Add Action**  .

9 In the **Add Action** window, add an action related to the notification.

A filter must have at least one notification associated with it.

10 Finish adding filters and notifications by clicking **Apply**. Click **OK**.

3.4.4.2
Configuring E-mail Notifications for Alarm Filters

You can configure the e-mail notification to receive e-mails from Unified Event Manager (UEM) about incoming alarms or events that matches your filter criteria. You configure e-mail notifications by adding an e-mail action to an alarm filter and defining match criteria for the filter. Your notification settings and the certificate that you need for secure communication are backed up during your backup process.

The e-mail notification service has limited capacity and is designed for sending individual notifications rather than forwarding entire events. If the rate of notifications matching the filter pattern is high, some e-mails may not be sent to the SMTP server.

Secure and non-secure e-mail communication is a licensed UEM service that is available only for users with a feature license for the e-mail notification service. For more information about licenses, see the *License Manager* manual.

You can configure UEM to send paging notifications instead of e-mails. This requires PageGate software to be installed and running on your system. See Installing and Configuring PageGate Server on page 285.

NOTICE: When specifying property names, use only alphanumeric characters and underscores. Do not start property names with digits.

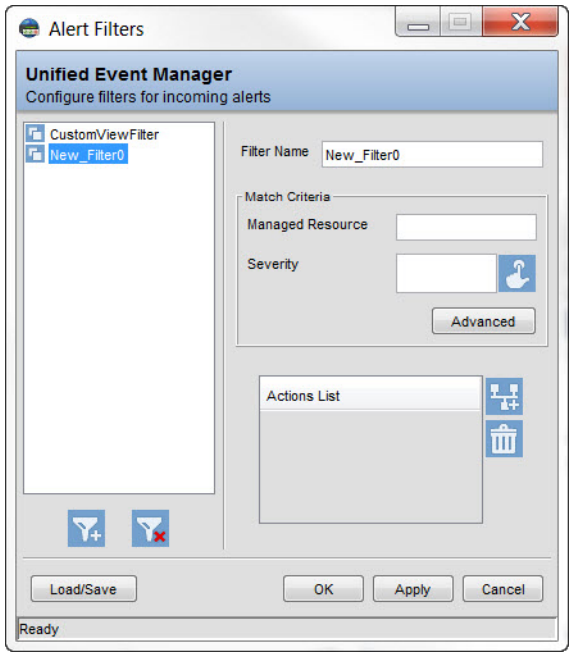
Procedure:

1 In the **Navigation View** panel, select **Fault Management** → **Alarms**.

2 From the main menu, select **Edit** → **Alarm Filters**.

3 In the **Alert Filters** window, click **Add Filter**  .

Figure 14: Alert Filters Window

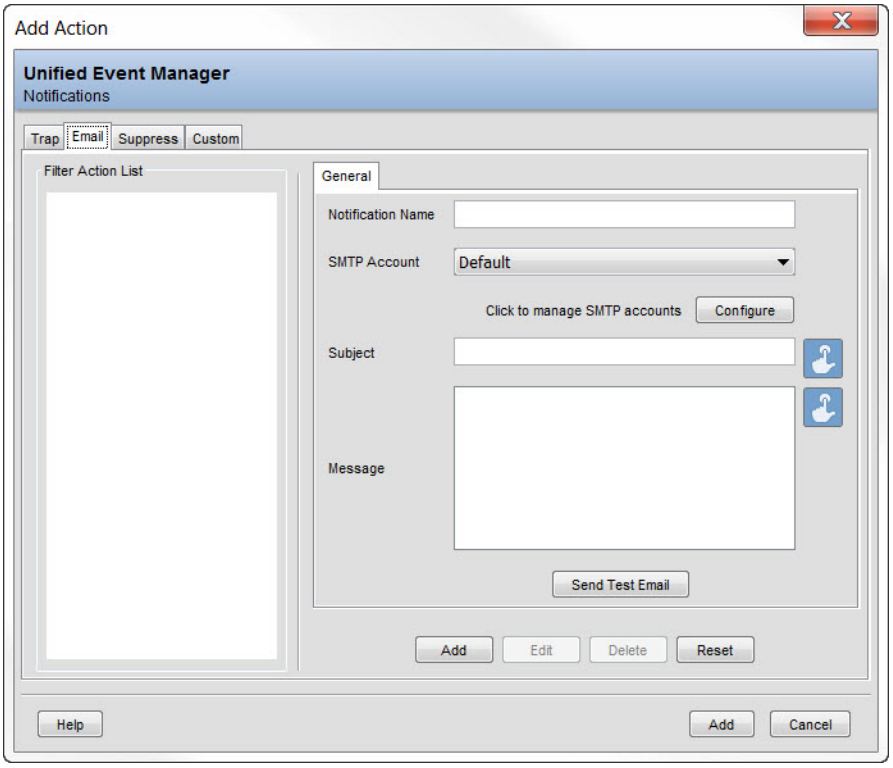


The **Actions List** panel options become active.

4 In the **Actions List** panel, click **Add Action** .

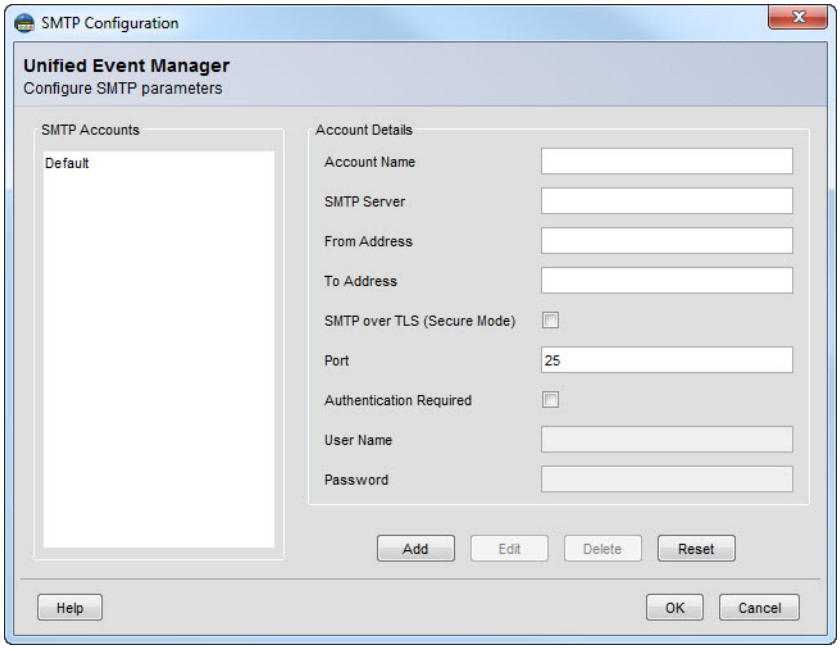
5 In the **Add Action** window, click the **Email** tab.

Figure 15: Add Action Window – Email Tab



6 In the **Notification Name** field, enter the name of the e-mail notification. Click **Configure**.

Figure 16: SMTP Configuration Dialog Box



7 In the **SMTP Configuration** dialog box, enter the following account details:

a In the **Account Name** field, enter an SMTP account name.

b In the **SMTP Server** field, enter a server name.

For paging notifications, enter the IP address of the PC that is hosting the PageGate application.

c In the **From Address** field, enter a source e-mail address.

For paging notifications, this field is not relevant, but may be useful in multi-zone systems to identify the zone the UEM is in.

d In the **To Address** field, enter a target e-mail address.

For paging notifications, enter the recipient name, as defined in PageGate, followed by the at-sign and the e-mail server domain as setup in PageGate.

Step example: pageall@uempagegate.com

e Optional: Enable the secure mode, select the **SMTP over TLS (Secure Mode)** check box.

f Optional: Enable obligatory authentication, select the **Authentication Required** check box. Enter your user name and password.

g Click **Add**. Click **OK**.

8 Optional: Test the e-mail notification by performing the following actions:

a In the **Add Action** window, from the **SMTP Account** list, select an SMTP account.

b In the **Subject** field, click **Append Property** and select the properties you want to receive. Click **Send Test Email**.

In the **Message** field, a default message is added.

c In the confirmation window, click **Yes**.

UEM sends a test notification to the specified e-mail address. The test notification does not contain the properties that you specified in the e-mail notification configuration.

9 In the **Alert Filters** window, click **Advanced**.

10 Optional: In the **Match Criteria Properties** dialog box, configure the match criteria of your choice.

You can configure the following match criteria:

- **Message**
- **Category**
- **Domain**
- **Network**
- **Node**
- **Failure Object**

11 Configure a filter by using an alarm property that is not displayed on the user interface:

a In the **Match Criteria Properties** dialog box, click **More Properties**.

b In the **Property Name** and **Property Value** fields, specify filter properties. Click **OK**.

The value must be the same as the one listed in the Property name for the filtering column. To modify an existing property, in the **Property Name** field, enter the same value again and in the **Property Value**, enter a new value. To remove a property, in the **Property Name** field, enter the same value again and leave the **Property Value** field blank.

c Close the **More Properties** dialog box. In the **Match Criteria Properties** dialog box, click **OK**.

3.4.4.3 Modifying Alarm Filters

Procedure:

1 In the **Navigation View** panel, select **Fault Management** → **Alarms**.

2 From the main menu, select **Edit** → **Alarm Filters**.

3 In the **Alert Filters** window, select the alarm filter you want to modify.

4 Optional: In the **Filter Name** field, modify the filter name.

5 Optional: In the **Match Criteria** pane, modify the **Managed Resource** and **Severity** criteria.

6 Optional: Configure additional match criteria by clicking **Advanced**.

In the **Match Criteria Properties** dialog box, you can configure the following match criteria:

- **Message**
- **Category**
- **Domain**
- **Network**
- **Node**
- **Failure Object**

7 Optional: Configure a filter by using an alarm property that is not displayed on the user interface:

a In the **Match Criteria Properties** dialog box, click **More Properties**.

b In the **Property Name** and **Property Value** fields, specify filter properties. Click **OK**.

The value must be the same as the one listed in the Property name for the filtering column. To modify an existing property, in the **Property Name** field, enter the same value again and in the **Property Value**, enter a new value. To remove a property, in the **Property Name** field, enter the same value again and leave the **Property Value** field blank.

c Close the **More Properties** dialog box. In the **Match Criteria Properties** dialog box, click **OK**.

8 In the **Alert Filters** window, click **Apply**. Click **OK**.

The window closes.

3.4.4.4
Modifying Alarm Filter Notifications

Regional and system administrators can modify alarm filter notifications.

Procedure:

1 In the **Navigation View** panel, select **Fault Management** → **Alarms**.

2 From the main menu, select **Edit** → **Alarm Filters**.

3 From the left panel of the **Alert Filters** window, select the alarm filter whose notification you want to modify.

4 In the **Actions List** panel, click **Add Action**  .

5 In the **Add Action** window, select the tab corresponding to the notification that you want to modify.

- **Trap**
- **Email**
- **Suppress**
- **Custom**

6 From the **Filter Action List**, select the notification that you want to modify.

7 Edit the notification properties. Click **Save**.

3.4.4.5
Loading Alarm Filter Files

Procedure:

1 In the **Navigation View** panel, select **Fault Management** → **Alarms**.

2 From the main menu, select **Edit** → **Alarm Filters**.

3 In the **Alert Filters** dialog box, click **Load/Save**.

4 In the **Filter Details** dialog box, specify the file name and click **Load**.

3.4.4.6
Deleting Alarm Filters

Procedure:

1 In the **Navigation View** panel, select **Fault Management** → **Alarms**.

2 From the main menu, select **Edit** → **Alarm Filters**.

3 In the **Alert Filter** dialog box, select the alarm filter you want to delete. Click **Delete Filter**  .

4 In the confirmation dialog box, confirm the deletion by clicking **Yes**.

The alarm filter disappears from the list of alarm filters.

3.4.4.7
Deleting Alarm Filter Notifications

Procedure:

1. In the **Navigation View** panel, select **Fault Management** → **Alarms**.
2. From the main menu, select **Edit** → **Alarm Filters**.
3. In the **Alert Filters** dialog box, select the alarm filter whose notification you want to delete.
4. From the **Actions List** panel, select the notification you want to delete. Click **Delete Action**  .
5. In the confirmation dialog box, confirm the deletion by clicking **Yes**.

The notification disappears from the **Actions List** panel.

3.4.5
Event Filters Configuration

When an event is created, the occurrence of the event can be associated with some actions. Unified Event Manager (UEM) provides event filters to send e-mails to an administrator on occurrence of an event. This action is called a notification.

By configuring event filters you can filter events based on certain match criteria. With this tool you can also add, modify, or delete filters and filter actions.

You can configure UEM to send notifications to users when events are generated from devices in a network. Use event filters to configure UEM to automatically initiate actions for selected events.

NOTICE:
When specifying property names, use only alphanumeric characters and underscores. Do not start property names with digits.

When used for filtering, property names are case-sensitive and should be used exactly as specified when typing in the name of the additional property criterion to filter on. For more information, see Event Properties on page 158.

UEM supports only the **Sending e-mails** built-in filter notification. Other notification types that can be associated with the filter are **Suppressing events**, **Sending custom trap**, and **Running Custom Code**. Even though these notifications are available on the user interface, **Sending e-mails** is the only notification type recommended during filter configuration on UEM. Do not add/delete or modify other notification types. These notification schemes require advanced knowledge and privileges and therefore are not recommended for general use. Contact Motorola Solutions Support Center (SSC) for information on the use of notification schemes other than e-mail notification scheme.

IMPORTANT: By default, UEM is configured with a filter named **TopoSupress** and its associated action named **suppressTopoEvent** to suppress someUEM internal events. When configuring the event filter, do not modify or delete the in-built **TopoSupress** event filter or **suppressTopoEvent** action configuration. Modifying or deleting this in-built configuration may lead to incorrect display of device statuses.

Match Criteria Property Overview

The managed resource and severity criteria determine whether the incoming alarm or event can be filtered or not. If any field is left blank, it is not considered matching criteria. For the alarm or event filter to be applied, it must satisfy all the match criteria specified. If even one of the criteria fails, the filter is not applied. You can use wildcard characters and expressions to specify the match criteria.

UEM accepts any match criteria you enter. However, if you want to make sure that your criteria are valid for the system, enter them into a custom view. Criteria specified for custom views take immediate

effect, while an alarm or event filter only works when new alarms or events of the specified type occur. For more information on how to add a custom view, see Custom View Operations on page 127.

Manage/Unmanage

Option that enables you to manage or unmanage UEM resources. For example, you can unmanage resources that are broken so that they do not send many traps to the trap buffer and take a lot of the trap buffer capacity. After the resources are fixed, you can manage the fixed resources to enable UEM to receive traps from them.

Clean Trap Buffer & Sync

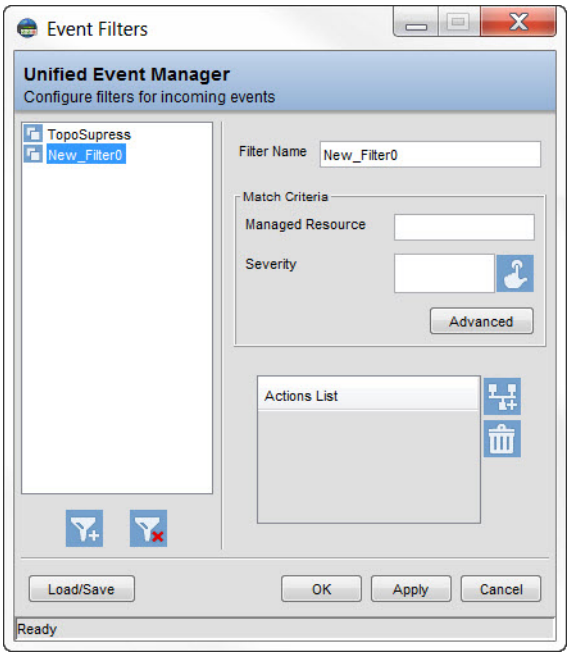
Option that enables you to clear the trap buffer of all traps UEM received from a managed resource. After the trap buffer is cleared, UEM schedules synchronization with managed resources whose traps you removed. As a result, UEM receives up-to-date information from the managed resources.

3.4.5.1 Adding Event Filters

Procedure:

1. In the **Navigation View** panel, select **Fault Management** → **Network Events**.
2. From the main menu, select **Edit** → **Event Filters**.
3. In the **Event Filters** window, click **Add Filter**.

   Figure 17: Event Filters Window



4. In the **Filter Name** field, specify the name of the filter.
5. In the **Match Criteria** pane, specify the **Managed Resource** and **Severity** criteria.
6. Optional: Configure additional match criteria by clicking **Advanced**.

   In the **Match Criteria Properties** dialog box, you can configure the following match criteria:

   - **Message**
   - **Category**
   - **Domain**
   - **Network**

- **Node**
- **Failure Object**

7 Optional: Configure a filter by using an alarm property that is not displayed on the user interface:

a In the **Match Criteria Properties** dialog box, click **More Properties**.

b In the **Property Name** and **Property Value** fields, specify filter properties. Click **OK**.

The value must be the same as the one listed in the Property name for the filtering column. To modify an existing property, in the **Property Name** field, enter the same value again and in the **Property Value**, enter a new value. To remove a property, in the **Property Name** field, enter the same value again and leave the **Property Value** field blank.

c Close the **More Properties** dialog box. In the **Match Criteria Properties** dialog box, click **OK**.

8 In the **Actions List** panel, click **Add Action**  .

9 In the **Add Action** window, add an action related to the notification.

A filter must have at least one notification associated with it.

10 Finish adding filters and notifications by clicking **Apply**. Click **OK**.

3.4.5.2
Configuring E-mail Notifications for Event Filters

You can configure the e-mail notification to receive e-mails from Unified Event Manager (UEM) about incoming alarms or events that matches your filter criteria. You configure e-mail notifications by adding an e-mail action to an event filter and defining match criteria for the filter. Your notification settings and the certificate that you need for secure communication are backed up during your backup process.

The e-mail notification service has limited capacity and is designed for sending individual notifications rather than forwarding entire events. If the rate of notifications matching the filter pattern is high, some e-mails may not be sent to the SMTP server.

Secure and non-secure e-mail communication is a licensed UEM service that is available only for users with a feature license for the e-mail notification service. For more information about licenses, see the *License Manager* manual.

You can configure UEM to receive paging notifications instead of e-mails. This requires PageGate software to be installed and running on your system. See Installing and Configuring PageGate Server on page 285.

NOTICE: When specifying property names, use only alphanumeric characters and underscores. Do not start property names with digits.

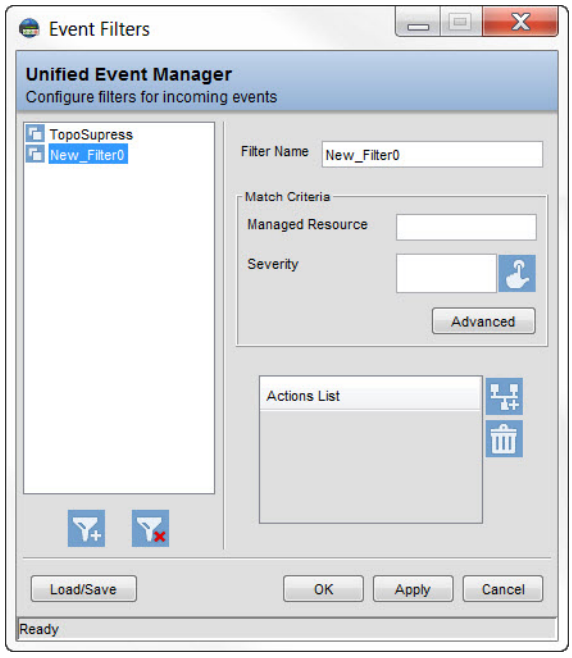
Procedure:

1 In the **Navigation View** panel, select **Fault Management** → **Network Events**.

2 From the main menu, select **Edit** → **Event Filters**.

3 In the **Event Filters** window, click **Add Filter**  .

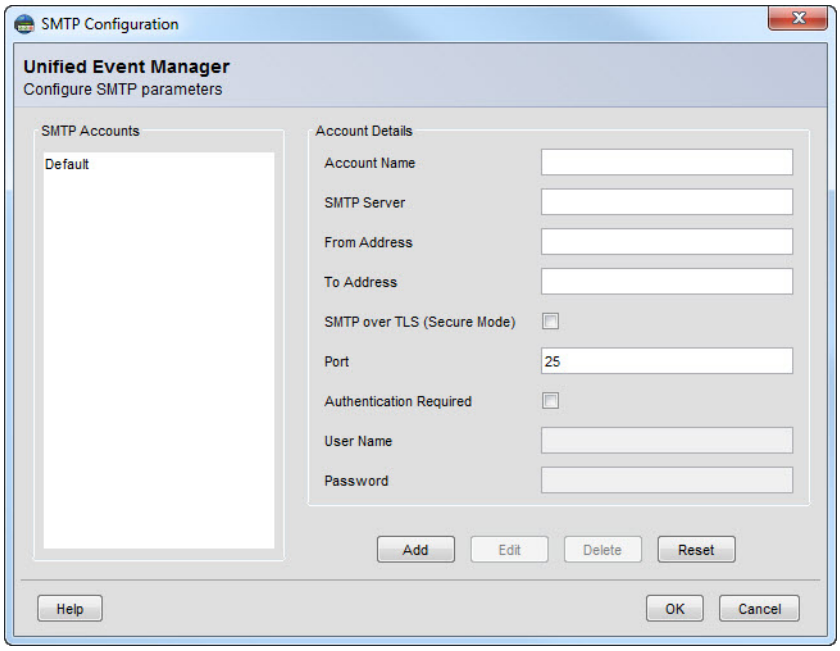
Figure 18: Event Filters Window



4 In the **Actions List** panel, click **Add Action** .

5 In the **Notification Name** field, enter the name of the e-mail notification. Click **Configure**.

Figure 19: SMTP Configuration Dialog Box



6 In the **SMTP Configuration** dialog box, enter the following account details:

a In the **Account Name** field, enter an SMTP account name.

b In the **SMTP Server** field, enter a server name.

For paging notifications, enter the IP address of the PC that is hosting the PageGate application.

c In the **From Address** field, enter a source e-mail address.

For paging notifications, this field is not relevant, but may be useful in multi-zone systems to identify the zone the UEM is in.

d In the **To Address** field, enter a target e-mail address.

For paging notifications, enter the recipient name, as defined in PageGate, followed by the at-sign and the e-mail server domain as setup in PageGate.

Step example: pageall@uempagegate.com

e Optional: Enable the secure mode, select the **SMTP over TLS (Secure Mode)** check box.

f Optional: Enable obligatory authentication, select the **Authentication Required** check box. Enter your user name and password.

g Click **Add**. Click **OK**.

7 Optional: Test the e-mail notification by performing the following actions:

a In the **Add Action** window, from the **SMTP Account** list, select an SMTP account.

b In the **Subject** field, click **Append Property** and select the properties you want to receive. Click **Send Test Email**.

In the **Message** field, a default message is added.

c In the confirmation window, click **Yes**.

UEM sends a test notification to the specified e-mail address. The test notification does not contain the properties that you specified in the e-mail notification configuration.

8 In the **Alert Filters** window, click **Advanced**.

9 Optional: In the **Match Criteria Properties** dialog box, configure the match criteria of your choice.

You can configure the following match criteria:

- **Message**
- **Category**
- **Domain**
- **Network**
- **Node**
- **Failure Object**

10 Configure a filter by using an alarm property that is not displayed on the user interface:

a In the **Match Criteria Properties** dialog box, click **More Properties**.

b In the **Property Name** and **Property Value** fields, specify filter properties. Click **OK**.

The value must be the same as the one listed in the Property name for the filtering column. To modify an existing property, in the **Property Name** field, enter the same value again and in the **Property Value**, enter a new value. To remove a property, in the **Property Name** field, enter the same value again and leave the **Property Value** field blank.

c Close the **More Properties** dialog box. In the **Match Criteria Properties** dialog box, click **OK**.

3.4.5.3
Modifying Event Filters

Procedure:

1 In the **Navigation View** panel, select **Fault Management** → **Network Events**.

2 From the main menu, select **Edit** → **Event Filters**.

3 In the **Event Filters** window, select the event filter you want to modify.

4 Optional: In the **Filter Name** field, modify the filter name.

5 Optional: In the **Match Criteria** pane, modify the **Managed Resource** and **Severity** criteria.

6 Optional: Configure additional match criteria by clicking **Advanced**.

In the **Match Criteria Properties** dialog box, you can configure the following match criteria:

- **Message**
- **Category**
- **Domain**
- **Network**
- **Node**
- **Failure Object**

7 Optional: Configure a filter by using an alarm property that is not displayed on the user interface:

a In the **Match Criteria Properties** dialog box, click **More Properties**.

b In the **Property Name** and **Property Value** fields, specify filter properties. Click **OK**.

The value must be the same as the one listed in the Property name for the filtering column. To modify an existing property, in the **Property Name** field, enter the same value again and in the **Property Value**, enter a new value. To remove a property, in the **Property Name** field, enter the same value again and leave the **Property Value** field blank.

c Close the **More Properties** dialog box. In the **Match Criteria Properties** dialog box, click **OK**.

8 In the **Event Filters** window, click **Apply**. Click **OK**.

The window closes.

3.4.5.4
Modifying Event Filter Notifications

Procedure:

1 In the **Navigation View** panel, select **Fault Management** → **Network Events**.

2 From the main menu, select **Edit** → **Event Filters**.

3 From the left panel of the **Event Filters** window, select the event filter whose notification you want to modify.

4 In the **Actions List** panel, click **Add Action**  .

5 In the **Add Action** window, select the tab corresponding to the notification that you want to modify.

- **Trap**
- **Email**
- **Suppress**
- **Custom**

6 From the **Filter Action List**, select the notification that you want to modify.

7 Edit the notification properties. Click **Save**.

3.4.5.5
Loading Event Filter Files

Procedure:

1. In the **Navigation View** panel, select **Fault Management** → **Network Events**.
2. From the main menu, select **Edit** → **Event Filters**.
3. In the **Event Filters** dialog box, click **Load/Save**.
4. In the **Filter Details** dialog box, specify the file name and click **Load**.

3.4.5.6
Deleting Event Filters

Procedure:

1. In the **Navigation View** panel, select **Fault Management** → **Network Events**.
2. From the main menu, select **Edit** → **Event Filters**.
3. In the **Event Filters** dialog box, select the event filter you want to delete. Click **Delete Filter**  .
4. In the confirmation dialog box, confirm the deletion by clicking **Yes**.

The event filter disappears from the list of event filters.

3.4.5.7
Deleting Event Filter Notifications

Procedure:

1. In the **Navigation View** panel, select **Fault Management** → **Network Events**.
2. From the main menu, select **Edit** → **Event Filters**.
3. In the **Event Filters** dialog box, select the event filter whose notification you want to delete.
4. From the **Actions List** panel, select the notification you want to delete. Click **Delete Action**  .
5. In the confirmation dialog box, confirm the deletion by clicking **Yes**.

The notification disappears from the **Actions List** panel.

3.5
Configuration from SDM3000 Builder

In the integrated and centralized fault management solution, the SDM3000 Builder application is used to configure SDM3000 Remote Terminal Units (RTU) and the configuration needs to be loaded into UEM to allow UEM to manage SCADA components through the RTUs.

3.5.1
Importing Configuration from SDM3000 Builder

You can import a `.zip` or an `.sbz` configuration file created in SDM3000 Builder.For information and procedure on exporting configuration files, see “Exporting UEM Configuration Data” in the *SDM3000 Builder User Guide*.

Procedure:

1. From the main menu, select **SDM Builder** → **Import SDM Builder Configuration File**.

2 Navigate to the configuration file and click **Open**.

The SDM3000 Builder configuration data is imported into UEM.

Postrequisites: Re-discover the SDM3000 Remote Terminal Units (RTU) to apply the new settings. See Discovering Network Elements on page 198

3.5.2
Exporting SDM3000 Builder Configuration

You can export a `.zip` or an `.sbz` file from UEM, containing an SDM300 Builder configuration file and SDM3000 Builder project files. For more information, see the *SDM3000 Builder User Guide*.

Procedure:

1 From the main menu, select **SDM Builder → Export SDM Builder Configuration File**.

A web browser window opens.

2 In the web browser window, confirm the download of the exported file.

3.5.3
Importing Customization from GMC

You can import an `.xml` customization file created in GMC.For information and procedure on exporting customization files, see “Configuring SDM3000 Builder Projects for the Centralized UEM Mode” in the *MOSCAD Network Fault Management Feature Guide*.

Procedure:

1 From the main menu, select **SDM Builder → Import GMC Customization File**.

2 Navigate to the configuration file and click **Open**.

The GMC customization data is imported into UEM.

This page intentionally left blank.

Chapter 4

UEM Optimization

No optimization procedures are required for Unified Event Manager (UEM).

This page intentionally left blank.

Chapter 5

UEM Operation

Operation procedures help you work with Unified Event Manager (UEM) effectively.

5.1
UEM Client Operations

If the Network Management client is a part of a domain, you can modify the security policies (for given devices) to allow the addition of trusted site information. When the configuration is completed, the system administrator must restore security settings. The security administrator may refer to the Active Directory information provided by Microsoft for details on editing security policies.

NOTICE:
It is recommended to install the PRNM suite which contains Unified Event Manager (UEM) client certificates. The certificates are installed into the web browser and eliminate security warnings. See the *Private Network Management Client* manual.

UEM uses the HTTPS protocol (HTTP over SSL) to provide improved security. The HTTP protocol is **not** supported.

5.1.1
Starting the UEM Client

Unified Event Manager (UEM) requires the Java Runtime Environment (JRE) 1.8_72 version or higher. If you have no JRE installed or your JRE version is not compatible with UEM, UEM does not start.

Procedure:

1. Open the 32-bit version of Internet Explorer on the client computer.
2. In the browser address field, enter the URL of the UEM client: `https://uem01.zone<zone ID>:9090`

   To start the backup zone core UEM, change the `uem01` prefix to `uem02`.
3. In the UEM welcome page, click **Launch Client**.
   - If the **Security Warning** dialog box appears, select the **I accept the risk and want to run this application** check box. Click **Run**.
   - If you are requested to accept the SSL certificate, accept it.
4. In the **Unified Event Manager Authentication** dialog box, enter a valid UEM client user name and password. Click **Connect**.

   NOTICE: Entering an invalid password three times in a row locks the user account. Wait 1hour or contact the administrator to unlock the account. To manually remove the account lock, see Unlocking the User Account on page 231.

The UEM client console appears. A splash screen with a status bar is shown and the UEM client user interface appears.

5.2
Work Area Overview

Follow procedures in this section to navigate through the Unified Event Manager (UEM) application and to perform basic UEM operations.

5.2.1
Work Area Operations

This section provides information on basic Unified Event Manager (UEM) operations.

5.2.1.1
Navigating Through Active Windows

When many windows are open in the display panel, you can easily navigate to the next or the previous active screen.

You may open up to the following number of windows at one time:

- three **Network Element View** windows
- three **Site View** windows
- three map windows
- three **Alarm details** windows
- three **Event details** windows

Procedure:

Navigate to a window:

- To go back to the previous window, from the **File** menu, select **Back**.
- To go to the next window, from the **File** menu, select **Forward**.

The window appears.

5.2.1.2
Detaching a Window from the Client

You can detach a window from the display panel of the UEM client and view it as a separate window.

Procedure:

In the **Window** menu, select **Detach Current Window**.

You restore the window to its default position by closing the detached window.

5.2.1.3
Arranging Windows

Procedure:

Arrange windows horizontally, vertically, or as a cascade of windows:

- To tile all open windows horizontally, from the **Window** menu, select **Tile Windows Horizontally**.
- To tile all open windows vertically, from the **Window** menu, select **Tile Windows Vertically**.
- To display a cascade of all open windows, from the **Window** menu, select **Cascade**.

Windows are arranged according to your requirements.

5.2.2

Work Area Components

Title Bar

The title bar displays the user logged on , the core where UEM is installed (**Primary** or **Backup**), and the current zone.

Menu Bar

A rectangular component that is positioned at the top edge of the display area. By clicking the menu and selecting a particular menu item, the associated function can be performed.

The menu bar differs from screen to screen, based on the functions and on your privileges as a user. For instance, the Fault Management module has additional menu items, such as Actions and Custom Views. However, certain menu items, such as **File**, **Tools**, **SDM Builder**, **Administration**, **Window**, and **Help** are common for the entire UEM client.

Toolbar

A component that displays a collection of actions, commands, or control functions; useful to display the frequently used components. It is placed below the menu bar and consists of various tools for different nodes. A tool tip is provided for each tool, which indicates the operations performed by them.

To hide the toolbar, perform one of the following steps:

- Click the icon with the tool tip Hide Toolbar.
- From the **Window** menu, select **Show Toolbar**.

The toolbar differs from screen to screen, based on the functions of the module. For instance, the Fault Management module has additional toolbar options, such as **Add Custom View**, **Modify Custom View**, and so on. Toolbar options, such as **Go Back to Previous**, **Go Forward to Next**, **Help**, and so on, are common for the entire UEM client.

Map Toolbar

Maps have a separate toolbar that is located above the display panel.

Navigation View (Navigation Tree)

The tree present on the left-hand side of the UEM client displays a set of hierarchical data. The fundamental object in a tree is called a node, which represents a data item in a given hierarchical set. The root node is the top node of the hierarchical data. Nodes inside the root nodes are called child nodes. Nodes that contain no child nodes are called leaf nodes. When you select a particular node, the corresponding window is displayed on the right-hand side display panel.

Alarm Summary View

An overall summary of the alarms that can be viewed. It is based on severity. The **Alarm Count** panel is located below the **Navigation View** panel. When you click the count displayed in the **Alarm Count** panel, the alarms of specific severity are displayed in the corresponding **Alarm** panel. This panel is updated automatically. The counts can be seen all the time, regardless of the functional view.

Status Bar

The status bar is displayed at the bottom of the window. It indicates the status of ongoing processes.

Display Panel

The display panel is displayed on the right-hand side of the UEM client and appears as a window within the main window. This panel is shown when a tree node is selected. For example, if you select **Fault Management → Network Events** in the navigation tree, the Events display panel is displayed on the right-hand side.

5.2.3
Broadcasting Messages

You can send messages to all clients connected to the Unified Event Manager (UEM) server.

Procedure:

1. From the main menu, select **Tools** → **Broadcast Message**.
2. In the **Message** field, enter the message you want to broadcast. Click **Broadcast**.
3. In the pop-up window with your message, click **OK**.

The message is delivered to the clients that are connected to the UEM server.

5.2.4
Table View Operations

The Table view panel displays details of various application elements, for example alarms and events.

Table view is available on the right-hand side of the Unified Event Manager (UEM) client for elements in the **Fault Management**, **Network Database**, and **Configured Collections** nodes.

5.2.4.1
Table Navigation

The table views are available only in the **Fault Management**, **Network Database**, and **Configured Collections** nodes.

The navigator buttons, **First Page**, **Previous Page**, **Next Page**, and **Last Page** are located at the top of each table.

First Page
The first page of the window that displays the data retrieved from the database.

Previous Page
The previous page of the window that displays the data retrieved from the database.

Next Page
The next page of the window frame that displays the data retrieved from the database.

Last Page
The last page of the window that displays the data retrieved from the database.

5.2.4.2
Setting the Page Length

For **Navigation View** panel elements that belong to the **Fault Management** and **Network Database** nodes, you can set the number of table rows that are displayed. This option is available to all users and helps you adjust the views to your needs.

Procedure:

In the **Page Length** drop-down menu, select the number of rows you want to display.

The table displays the desired number of rows.

5.2.4.3
Sorting Table Details

All users can sort the data in a table based on the column type. The details can be viewed either in ascending or descending order. Arrows indicate the type of sorting order (ascending or descending).

There are two types of sorting:

Sort all
Sorts all data in the Unified Event Manager (UEM) server and is not restricted to the data visible on the currently displayed page.

Sort currently displayed
Sorts only the data that is displayed in the UEM client. For example, if there are 50 alarms in the UEM server and only 25 are visible on the currently displayed page, the table sorts only the 25 visible alarms.

Procedure:

1. Sort your table details.
   - To sort the data, click the column header.
   - To sort the data in reverse order, click the same header once again.

   IMPORTANT: When you sort the column header on the client side, hold CTRL.

5.2.4.4
Rearranging and Resizing Table Columns

You can modify table columns according to your preferences. After you modify table columns, your settings remain unchanged until the UEM client is open. When you reopen the UEM client, your settings are lost.

Procedure:

1. In the **Navigation View** panel, go to the **Fault Management** or **Network Database** node and click the element that you want to modify.
2. Rearrange the columns by dragging the column header and moving it to the desired place in the table.
3. Resize the column header by dragging the right edge of a column.
4. Optional: Retain the size of columns, by selecting **Custom Views** → **Save Custom View State**.

5.2.5
Custom View Operations

In Unified Event Manager (UEM), custom views are tailored views that you can create to display a subset of data that satisfies specific criteria. You can use custom views, for example, to monitor a specific group of managed resources; instead of performing search on the resources multiple times, you can define a custom view for them.

You can create custom views in the **Network Events**, **Alarms**, **Network Database**, and **Configured Collection** windows. You can create custom views only if your account is privileged to do so. For information about your user privileges, contact your system administrator.

You can open up to seven **Network Events** custom view windows. When you open another **Network Events** custom view window, the **Network Events** custom view window opened as the first one closes.

5.2.5.1

Adding Custom Views

You can add or create a view by specifying various criteria and providing a name for the view. The views you create allow you, for example, to quickly monitor only the devices you need.

Procedure:

1. In the **Navigation View** panel, click one of the following nodes:
   - **Network Events**
   - **Alarms**
   - **Network Database**
   - **Configured Collection**
2. From the main menu, select **Custom Views** → **Add Custom View**.
3. In the **Show objects with these Properties** dialog box, specify the object properties you want to use to filter the data.

   For example, to show only **Network Events** or **Alarms** for Element Management Toolkit devices, in the **Source** field enter `*FMT*`

   IMPORTANT:
   Custom view names, that you can modify in the **Filter View Name** field, are not case-sensitive. On the same custom view tree level, you cannot add two custom view names whose names differ only by the size of letters. You can add such custom view names on different custom view tree levels.

   NOTICE:
   The properties differ for each node. For more information, see Event Properties on page 158, Alarm Properties on page 166, Managed Resource Properties on page 155, Data Collection Detailed Properties on page 207. For information about wildcard characters and operators that can be used to define match criteria, see Filtering Quick Reference on page 132.
4. Optional: Specify the columns you want to view:
   a. In the **Show objects with these Properties** dialog box, click **Select Props To View**.

      The **Select Table Columns** dialog box appears. The selected fields are the columns that you see in your table view.

   b. In the **Select Table Columns** dialog box, specify the columns you want to view by selecting or clearing check boxes next the column names. Click **OK**.

      You can also define new columns by clicking **Additional table columns**.
5. In the **Show objects with these Properties** dialog box, click **Apply Filter**.

   NOTICE: Within this master (parent) custom view, you can create more views, for example child custom views. Deleting the master custom view deletes its child custom views.

A new node with the custom name you have configured is created on the tree. When you click it, your custom view is displayed on the display panel.

Related Links

Renaming Custom Views on page 129

5.2.5.2

Modifying Custom Views

You can modify user-defined custom views to expand or limit the amount of information it displays. Follow this procedure to modify custom view properties, not custom view names.

Procedure:

1. In the **Navigation View** panel, click a user-defined custom view under one of the following nodes:
   - **Network Events**
   - **Alarms**
   - **Network Database**
   - **Configured Collection**
2. From the main menu, select **Custom Views** → **Modify Custom View**.
3. In the **Properties** pane of the **Show object with these Properties** dialog box, specify the match criteria you want to use to filter the data.

   NOTICE:
   The criteria differ for each node. For more information, see Event Properties on page 158, Alarm Properties on page 166, Managed Resource Properties on page 155, Data Collection Detailed Properties on page 207. For information on wildcard characters and operators that can be used to define match criteria, see Filtering Quick Reference on page 132.
4. Optional: Specify the columns you want to view:
   a. In the **Show object with these Properties** dialog box, click **Select Props To View**.

      The **Select Table Columns** dialog box appears. The selected fields are the columns that you see in your table view.

   b. In the **Select Table Columns** dialog box, specify the columns you want to view by selecting or clearing check boxes next the column names. Click **OK**.

      You can also define new columns by clicking **Additional table columns**.
5. In the **Show objects with these Properties** dialog box, click **Apply Filter**.

Related Links

Renaming Custom Views on page 129

5.2.5.3

Renaming Custom Views

You can rename custom views to make them more meaningful.

NOTICE: Custom view names are not case-sensitive. You cannot add two custom view names whose names differ only by the size of letters on the same custom view tree level. You can add such custom view names on different custom view tree levels.

Procedure:

1. In the **Navigation View** panel, click a user-defined custom view under one of the following nodes:
   - **Network Events**
   - **Alarms**

- **Network Database**
- **Configured Collection**

2 From the main menu, select **Custom Views** → **Rename Custom View**.

The custom view name is editable. To quit the custom view name edit field, press ESC.

3 Modify the custom view name. Press ENTER.

The name cannot exceed the limit of 50 characters.

5.2.5.4
Moving Custom Views

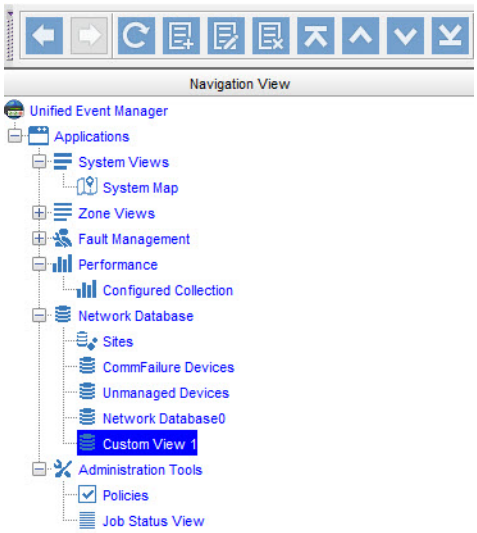
All users can move both pre-defined and user-defined custom views. You can move custom views for network events, alarms, and the network database.

Procedure:

1 In the **Navigation View** panel, click a custom view under one of the following nodes:

- **Network Events**
- **Alarms**
- **Network Database**
- **Configured Collection**

Figure 20: Navigation View Panel – Custom View



2 Move the node by using one of the action icons available on the toolbar:

- Move the custom view to the first position by using the **Move to the Top** icon .
- Move the custom view up by using the **Move Up** icon .
- Move the custom view down by using the **Move Down** icon .
- Move the custom view to the last position by using the **Move to the Bottom** icon .

5.2.5.5
Saving Custom View State

All users can save the state of both pre-defined and user-defined custom views. You can save custom views for network events, alarms, and the network database. You can configure filter criteria during the

configuration of custom views and custom view scopes by using the properties.See Managed Resource Properties on page 155. If the property is not available in the filter configuration user interface, use the mechanism provided to add more properties to the filter criterion. The name used for the additional property should match, including case-sensitivity, the name specified in the **Property name for filtering** column of the table in Managed Resource Properties on page 155.

Procedure:

1. In the **Navigation View** panel, click one of the following nodes or a custom view under one of these nodes:
   - **Network Events**
   - **Alarms**
   - **Network Database**
   - **Configured Collection**
2. From the main menu, select **Custom Views** → **Save Custom View State**.

In the status bar, a message appears informing that the custom view state is saved.

5.2.5.6
Deleting Custom Views

All users can delete user-defined custom views. You can delete custom views for network events, alarms, and the network database. You cannot delete custom views that are pre-defined in Unified Event Manager (UEM). You can delete single custom views or master (parent) custom views in which other custom views are nested. When you delete a master custom view, you also delete all its child custom views. For example, you create a custom view named `Master` (parent) and nest in it more custom views named Master1 and Master2. When you delete the `Master` custom view, you also delete the Master1 and Master2 child custom views.

Procedure:

1. In the **Navigation View** panel, click a user-defined custom view under one of the following nodes:
   - **Network Events**
   - **Alarms**
   - **Network Database**
   - **Configured Collection**
2. From the main menu, select **Custom Views** → **Remove Custom View**.
3. In the confirmation dialog box, click **Yes**.

5.2.5.7
Exporting Custom Views

All users can export both pre-defined and user-defined custom views. You can export custom views for network events, alarms, and the network database. By default, all pre-defined custom views are exported. You can select the user-defined custom views that you want to export. You can export your custom views to a `.cv` file and import them to another client application. Custom views are structured hierarchically and displayed in the form of a tree. The structure of your exported custom views depends on which custom views you select.

Procedure:

1. In the **Navigation View** panel, select one of the following nodes:

- **Network Events**
- **Alarms**
- **Configured Collection**
- **Network Database**

2 From the main menu, select **Custom Views** → **Export Custom View**.

3 In the **Export Custom Views** dialog box, select check boxes corresponding to custom views that you want to export. Click **OK**.

4 In the **Save Custom View(s) File** dialog box, select a destination folder. Click **Save**.

A `.cv` file with custom views is saved in the selected folder. You can use the file to import the custom views.

5.2.5.8
Importing Custom Views

All users can import both pre-defined and user-defined custom views. You can import custom views for network events, alarms, and the network database. You can import your custom views from a `.cv` file. Custom views are structured hierarchically and displayed in the form of a tree. You can import single custom views or the whole structure of your exported custom views.

Procedure:

1 In the **Navigation View** panel, select one of the following nodes:

- **Network Events**
- **Alarms**
- **Configured Collection**
- **Network Database**

2 From the main menu, select **Custom Views** → **Import Custom View**.

3 In the **Open Custom Views File** dialog box, select a `.cv` file with custom views you want to import. Click **Open**.

4 In the **Import Custom Views** dialog box, select check boxes corresponding to custom views that you want to import. Click **OK**.

CAUTION: If a custom view of the same name as any of the ones you import exists in the same hierarchy, name conflict information is displayed in the dialog box in red. If you continue to import this custom view, the custom view on the client is overwritten.

Selected custom views from the `.cv` file are imported.

5.2.5.9
Custom View Operations Interactions with Trunking Subsystem

During Trunking Subsystem (Tsub) expansion, specific Custom View definitions can become invalid. Custom Views, especially those defined to filter out RF Sites, Console Sites, Remote Sites, and Prime Sites by any property, should be checked and modified to work under the Tsub.

5.2.6
Filtering Quick Reference

Most of the properties listed while adding a custom view are string-based. Some of the properties can be displayed with a drop-down list. A single value can be selected from the drop-down list. Multiple

values can be typed in by using the operators and expressions available for filtering. When you choose **all**, the property is not included.

String-based property values are case-sensitive. For example, the string **Router** matches the exact word with capital R only.

Expressions like **Status** or **Severity** are also treated as strings. Hence, for a filter of Alarms with critical severity, specify `crit*`.

Leave unnecessary fields blank.

Depending on the total number of objects/elements, the complexity of the filter criteria, and the mode of storage, the time taken for filtering varies.

Custom views continue to be updated and navigable for additions/deletions until the Unified Event Manager (UEM) client is closed. You can either save your views (see Saving Custom View State on page 130) or remove them (see Deleting Custom Views on page 131).

Wildcard characters can be used for effective filtering. For a list of wildcard characters that can be used, see Wildcard Characters for Filtering on page 133.

5.2.6.1
Wildcard Characters for Filtering

You can use wildcard characters to define filtering expressions. Except for `<between>“value1” and “value2”`, the expressions that you create by using wildcard characters should include no spaces between the value and the wildcard characters or operators. For example, the expression `abc* && *xyz` is invalid. A valid definition for this expression is `abc*&&*xyz`.

`*` (Asterisk)
It is used to match zero or more characters. The character works only for text strings. Example:

- To view all objects whose names start with `test`, enter: `test*`
- To view all objects that end with `com`, enter: `*com`

`!` (Exclamation Mark)
It is used for filtering the search using the NOT operand. The character works only for text strings. Example:

- To view all objects whose names do not start with `test`, enter: `!test*`
- To view all alarms except the ones with the warning severity, enter: `!war*` (or) `!warning`

`,` (comma)
It is used for specifying multiple criteria for the same property. It is the equivalent of the OR operand. Example: To view objects named nms-server1, nms-server2, or nms-server3, enter: `nms-server1,nms-server2,nms-server3`

`&&` (two ampersands)
It is used to match a single value with many patterns. It is the equivalent of the AND operand. The character works only for text strings. Example: If all the objects with names starting with `abc` and ending with `xyz` are required, enter: `abc*&&*xyz`

`<between>“value1” and “value2”`
It is used to get objects with some numeric values within a specific range. Example: If object names with poll interval value ranging from `300` to `305` is required, enter: `<between>300 and 305`

5.2.6.2

Examples of Filtering with Wildcard Characters

Table 21: Filtering Site Trunking Condition Example

Filter site trunking condition due to site control path or core router failure on all Repeater sites. Temporarily exclude Repeater site 5 which is being upgraded. Filter on the following two fields:

Field	Value
identifier	`isr_site_fault:51.6,isr_site_fault:51.11`
source	`*:Rptr_Site&&!*X.X.X:Rptr_Site`
	For exact values for ***<X>***, see your System Configuration Plan.

Table 22: Filtering Transient Illegal Carrier Events Example

Filter transient illegal carrier events from channel 5 (High Performance Data (HPD)) and channel 21 (Repeater) at host site 32. Include a special note. Filter on the following three fields:

Field	Value
identifier	`Transient*receiver_fault.1`
entityDisplayName	`Channel 5,Channel 21`
source	`*X.X.X:*Site`
	For exact values for ***<X>***, see your System Configuration Plan.

Table 23: Filtering Station Alarms on Chosen Sites Example

View all station (Base Radio) alarms on site1. View all station alarms on site2 except stations 2 and 10. View all station alarms on site 3. Filter on the following value:

Field	Value
source	`X.X.X.*BaseRadio,X.X.X.*BaseRadio&&!X.X.X.X:*&&!X.X.X.X:*,X.X.X.*BaseRadio`
	For exact values for ***<X>***, see your System Configuration Plan.

5.2.7

Manager Registration on the Oracle Server

The Oracle server must be configured to send the traps to Unified Event Manager (UEM). This configuration should be performed by Motorola Solutions Support Center (SSC) personnel during system installation, but it might get corrupted or changed during system usage. UEM detects incorrect configuration and raises a warning alarm indicating, that a manager registration is not found on the device and that the manual registration is required.

For a discovered Oracle Server, Oracle Integrated Lights Out Manager can be opened in a web browser from UEM.

For more information, see the *Virtual Management Server Software* manual.

5.2.7.1
Launching Web Management Application

Procedure:

1. In the **Navigation View** panel, highlight the **Network Database** node.
2. Right-click an Oracle server you want to configure and select **Launch Web Management Application**.

   You may need to accept additional certificates.

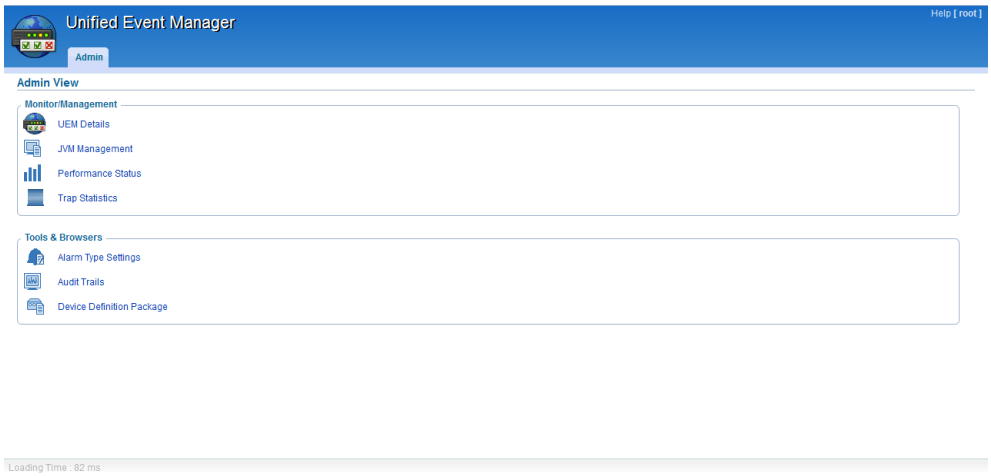
The **Oracle Integrated Lights Out Manager** window appears in the web browser.

5.3
Active Users Operations

Administrators can view the list of current active UEM clients.

Unified Event Manager (UEM) responds to the request by displaying the list of current active users who are logged on in the UEM client web interface. You access the system administration panel by selecting **Administration → System Administration** from the main menu.

Figure 21: System Administration – UEM Client Web Interface

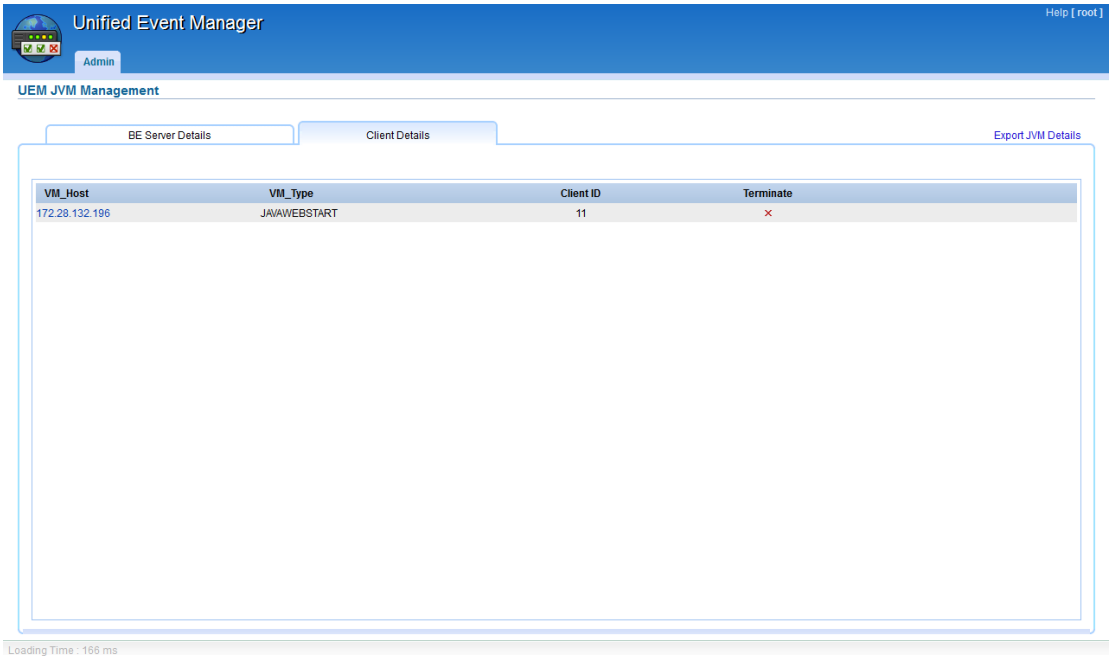


5.3.1
Viewing the Active Users List

Procedure:

1. From the main menu, select **Administration → System Administration**.
2. In the **Monitor/Management** pane, click **JVM Management**.
3. In the **UEM JVM Management** window, select the **Client Details** tab.

Figure 22: Client Details – UEM Client Web Interface



4 Optional: Terminate client sessions by clicking **Terminate** for a client.

UEM displays the list of current active clients.

5.4 Site Operations

The site and its associated devices can be discovered using the Site/Network discovery tab in the Discovery Configuration user interface. See Discovering Groups of Network Elements on page 200. The type of Site and its ID are used to determine the list of devices for which discovery is attempted.

Set up the SNMPv3 configuration (see SNMPv3 Credentials Configuration on page 82) to match the configuration of the devices at the Site.

UEM can also provide the service state as reported by the Zone Controller. For this purpose, it is necessary to invoke the re-discovery operation on the Zone Controller device after the site link has been established. After successfully re-discovering the Zone Controller, a new Site-managed resource is added to the Network Database. Then, the status is propagated to the map symbol representing the site in the Service Map Views.

NOTICE: The Site managed resource is discovered only when the active controller (Zone Controller, Site Controller, or SmartX Site Converter) is discovered. The active controller reports the status of the Site and its Channels. Discovering an inactive controller or just the base radios does not discover and add the site to the Network Database.

Related Links

Deleting Zones or Sites on page 188
Renaming Map Elements on page 97

5.5
Administration Tools

This section captures information about the Policies and the View Job Status features of Unified Event Manager (UEM).

Policies
A set of rules predefined against an activity; for example, a policy can be written for archiving events and viewing job status. For more information, see Policies Overview on page 137.

Viewing job status
The Job Status View provides user feedback and status of jobs initiated. For more information, see Viewing Job Status on page 141.

5.5.1
Policies Overview

Policies are a set of predefined rules which can be triggered as:

- Non-periodic action (policy can be scheduled for specified date and time)
- Periodic action (server application performs an action at regular intervals, defined in seconds)

Unified Event Manager (UEM) defines and supports ten predefined policies. All predefined policies are described by custom parameters (to check the value of a parameter, see Viewing Policy Details on page 140.

5.5.1.1
Policies Description

Table 24: Policies Description

The following parameters are defined for all predefined policies.

Policy	Description	Additional Parameters
Archive cleanup (ArchiveCleanupPolicy)	A pre-defined policy to periodically remove from the archive database events that are older than given time.	**Min Event Storage Size** Minimum number of events, that should be retained during clean-up. **Min Event Storage Period** The time events can exist in the archive database (in days).
Audit Trails cleanup (AuditTrailsCleanupPolicy)	A pre-defined policy to periodically remove from the database audit trails that are older than 5 years and save them to the `/opt/Motorola/nms/logs/archivedAuditTrails/auditTrails.csv` file.	N/A
Cleared Alarm cleanup (AlarmCleanupPolicy)	A pre-defined policy to periodically clean up alarms with the *clear* severity. The cleaned alarms are no longer displayed in the **Alarms** window.	**Period for Clear Acknowledged Alarms** The time (in seconds) counted from the last modification of

Table continued…

Policy	Description	Additional Parameters
		alarm time. As a result of the modification, acknowledged alarms with the clear severity are listed in the **Alarms** window. After the set time passes, the alarms are removed from the **Alarms** window during the next policy execution. The default time value is one hour, that is 3600 seconds. The minimum time value is 15 minutes, that is 900 seconds. The maximum time value is 24 hours, that is 86400 seconds. **Period for Clear Non-Acknowledged Alarms** The time (in seconds) counted from the last modification of alarm time. As a result of the modification, not acknowledged alarms with the clear severity are listed in the **Alarms** window. After the set time passes, the alarms are removed from the **Alarms** window during the next policy execution. The default time value is one hour, that is 3600 seconds. The minimum time value is 15 minutes, that is 900 seconds. The maximum time value is 24 hours, that is 86400 seconds. **Period** The time (in seconds) in which the policy is executed. Period is always 15 minutes and it starts when the fault manager server is enabled. Parameter is not editable by user. Example 1: The fault manager server is enabled at 8.12 a.m.; the policy execution starts. The clear alarm cleanup delay is set to one hour. An alarm is set to the clear severity at 8.28 a.m. Because period is set to 15 minutes, policy is run six times to remove all cleared alarms. Time of the policy execu-

Table continued...

Policy	Description	Additional Parameters
		tion: 8.27, 8.42, 8.57, 9.12, 9.27, 9.42. At 9.42 a.m. the alarm set to the clear severity at 8.28 is removed from the **Alarms** window. Example 2: For the same conditions as in example 1, except with the clear alarm cleanup delay set to 15 minutes, the alarm set to clear severity at 8.28 a.m. is removed from the **Alarms** window at 8.57 a.m.
Events cleanup (EventCleanupPolicy)	A pre-defined policy to periodically remove the oldest *current* events when their number exceeds the configurable maxEventNumber parameter value.	**Event Storage size** Maximum number of events; when total number of *current* events exceeds a given value, the oldest events are removed.
Event archive and purge (EventLoggingPolicy)	A pre-defined policy to periodically archive events from the UEM event database to a file on the UEM application server. This policy also periodically purges the archived events from the UEM event database.	**lastId** The id of the last event in the previous file (updated after policy execution). **lastTime** The time (in milliseconds) in which the last file is created (updated after policy execution).
Export Events to CSV File (EventLoggingPolicy)	A pre-defined policy to periodically copy the latest events to a `.csv` file and compress old `.csv` files to `.zip` archives.	**lastId** The ID of the last event copied to the file; do not modify this parameter. **lastTime** The time (ms since EPOCH) of the last policy execution; do not modify this parameter.
Export Statistical Data to CSV File (StatsDataExportPolicy)	A pre-defined policy to periodically archive collected statistics from the UEM StatsData database to a `.csv` file on the UEM application server. This file is then archived and stored.	**lastTime** The time of last execution. Before first execution, it is equal to server start time.
Jobs View Cleanup (JobsCleanupPolicy)	A pre-defined policy to periodically clean up the completed jobs from the UEM Job Status View. All jobs with End Time older than 24 hours and with status Failure or Success or Aborted will be deleted from Job View and archived on UEM server for 30 days.	N/A

Table continued…

Policy	Description	Additional Parameters
NBI File Purge (NbiFilePurgePolicy)	A pre-defined policy to periodically clean up files generated by the North Bound Interface functionality during Event Synchronization or Alarm Synchronization with the Manager of Managers.	**File History Time** The maximum age (in seconds) of the file preventing that processed file from being deleted by this policy.
NBI Storage (NbiNotiStoragePurgePolicy)	A pre-defined policy to periodically clean up database storage used to keep sent notifications generated by the North Bound Interface (NBI) functionality.	N/A
Performance Archive Purge (PerfArchivePurgePolicy)	A pre-defined policy to periodically purge the archived statistical data files from the UEM application server older than 31 days.	N/A
Statistics Data Cleanup (StatsDataCleanupPolicy)	A pre-defined policy to periodically clean up any collected statistical data stored on UEM. This policy triggers the clean-up of data from the STATSDATA% table in the database to ensure that the database does not get smothered by the large amount of data collected every day. The administrator decides on the frequency of cleanup.	**Delete data after (days)** The frequency of cleanup. **Cleanup Hour** An hour of date to execute policy.
Trap Overload Relieve (TrapStoreOverloadRelievePolicy)	A pre-defined policy to periodically detect trap overload condition (constant very high load of SNMP traps to be processed) and clean up the oldest unprocessed trap files when overload is detected.	N/A

5.5.1.2

Viewing Policy Details

IMPORTANT: Any user changes made in the predefined policy parameters shipped with Unified Event Manager (UEM) can seriously damage the UEM application.

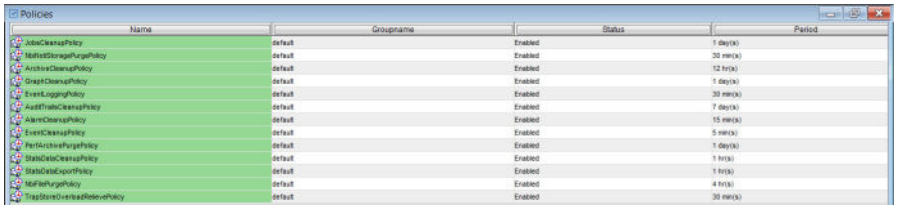
NOTICE:
Do not delete any policies.

Time intervals to trigger the predefined policies are maintained on UEM. You can update/execute the policies. Use the Policy user interface to set a different trigger time. Unless necessary, do not change the trigger time.

Procedure:

1 In the **Navigation View** panel, click the **Policies** node.

Figure 23: Policies Window



The **Policies** window appears.

2 Optional: Right-click a policy to perform the following actions:

- **Update**
- **Delete**
- **Execute**
- **Stop**

3 Double-click the row of a policy whose details you want to view.

In the **Policy Item Details** dialog box, the policy details appear.

5.5.1.3
Default Policy Parameters

Name
The policy display name

GroupName
The policy group name

Period
Period for policy execution in seconds

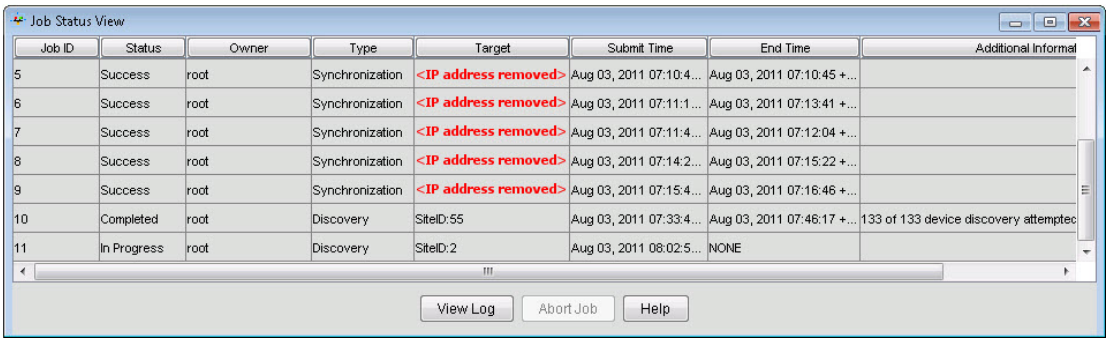
Severity
Switch to enable or disable policy

5.5.2
Viewing Job Status

You can view the statuses of the jobs initiated by the operator. All jobs listed in the **Job Status View** are user-initiated. However, not all user-initiated jobs are maintained in the **Job View**.

Jobs that are maintained in the **Job View** are jobs that do not have immediate user feedback. They take longer time to provide user feedback on the job disposition.

Figure 24: Job Status View Window



Procedure:

1. In the **Navigation View** panel, click the **Job Status View** node.
2. In the **Job Status View** window, perform the following actions:

If…	Then…
If you want to access job logs,	select a row and click **View Log**.
If you want to display job status details fields,	double-click a row. The **Job Status Details** dialog box appears.
If you want to abort an unfinished discovery job,	select a row and click **Abort Job**. For more information, see Aborting Discovery Jobs on page 204.

5.6 Fault Management Toolkit Operations

This section describes Fault Management Toolkit operations available in the Unified Event Manager (UEM). The Fault Management Toolkit capacity allows the provisioning of UEM Configurable Traps for third-party network elements. Provisioning of the Fault Management Toolkit requires an enforce, perpetual, capacity license. For more information about licenses, see the *License Manager* online help.

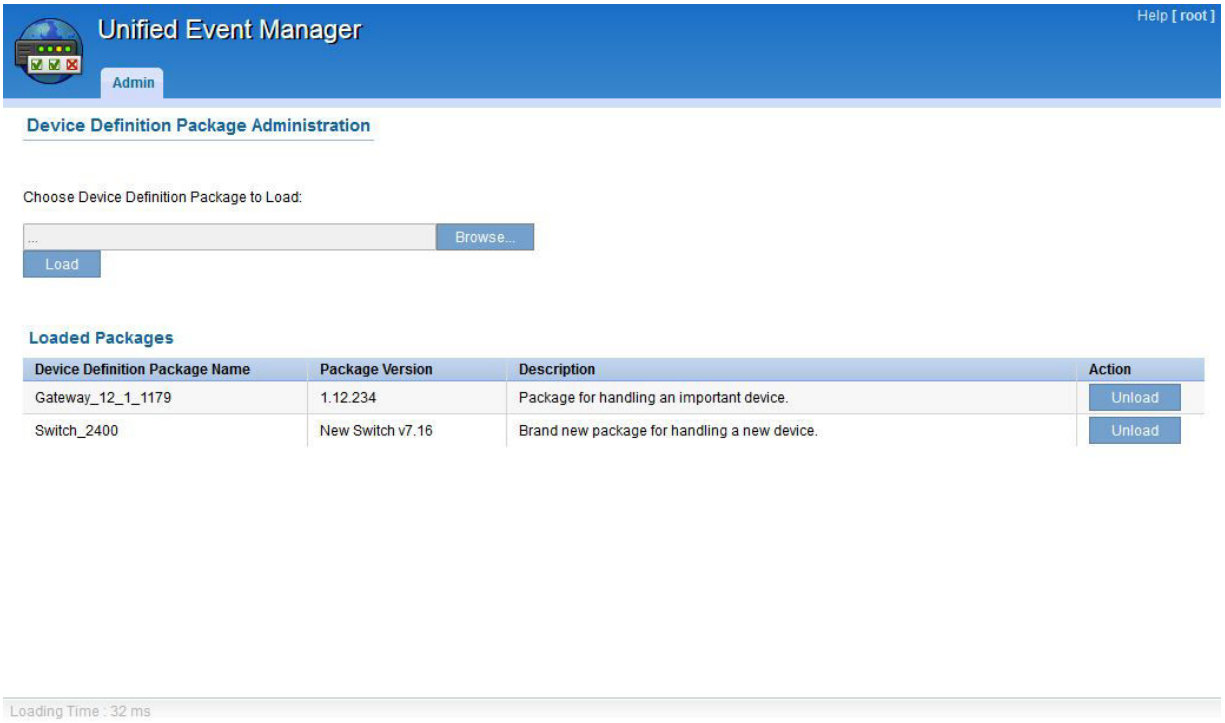
UEM management of third-party elements starts with importing a Device Definition Package (DDP). The DDP (`.ddp` file) contains the device definition which includes set of parameters to discover and manage device

For information about creating DDP files, see *Fault Management Toolkit Developer Guide*.

5.6.1 Device Definition Package Administration Page Overview

The **Definition Package Administration** allows administrators to view, load, and unload Device Definition Packages (DDPs) in the UEM database.

Figure 25: Device Definition Package Administration Page



An administrator can access the **Definition Package Administration** page from the **Administration** menu of the Unified Event Manager. See Loading DDPs on page 143.

DDPs selected by using the **Browse** option, can be loaded in the UEM database by clicking **Load**.

DDPs loaded in the UEM database are displayed in the **Loaded Packages** table. The table displays the name, version, and description for each DDP. DDPs can be unloaded by clicking **Unload** from the **Action** column. When a DDP is successfully unloaded, the page reloads.

5.6.2
Loading DDPs

The Unified Event Manager supports third party devices imported as Device Definition Packages (DDPs) and allows administrators to load DDPs into the database.

NOTICE: This procedure cannot be performed at the same time as discovery device/subnet procedure. Performing one of these procedures while the other is performed results in failure.

Procedure:

1. From the main menu, select **Administration** → **System Administration**.
2. In the **Tools & Browsers** pane, click **Device Definition Package**.
3. On the **Device Definition Package Administration** page, click **Browse**, and in the new window, select the .ddp file to load.
4. On the **Device Definition Package Administration** page, click **Load**.

   CAUTION: If a DDP already exists in the UEM database under the same sysObjectID, it is replaced by the loaded DDP. Any devices in managed state that are using this DDP, become unmanaged before replace and managed again after replace is completed.

The selected DDP is saved in the UEM database.

Postrequisites:

- Discover the added network elements. See Discovering Network Elements on page 198
- Verify the communication between UEM and the added network elements. See Testing SNMPv3 Communication Between Network Elements and UEM on page 85 and Testing the Web Service Communication Between Network Elements and UEM on page 87.
- Customize the displayed element names, if needed. See Renaming Managed Resources on page 103
- View alarms for the added elements. See Alarm Operations on page 165

5.6.3
Unloading DDPs

The Unified Event Manager supports third party devices imported as Device Definition Packages (DDPs) and allows administrators to unload Device Definition Packages (DDPs) from the database.

NOTICE: This procedure cannot be performed at the same time as discovery device/subnet procedure. Performing one of these procedures while the other is performed results in failure.

Procedure:

1. From the main menu, select **Administration** → **System Administration**.
2. In the **Tools & Browsers** pane, click **Device Definition Package**.
3. On the **Device Definition Package Administration** page, in the **Loaded Packages** table, locate the DDP you want to unload and in the **Action** column, click **Unload**.

Any devices in managed state that are using this DDP, become unmanaged. The DDP is removed from the UEM database, and the **Device Definition Package Administration** page reloads.

5.7
System, Zone and Microwave Map Operations

The system map displays the status of zones in the system (primary and backup cores) for each zone. The zone map displays the status of sites in the zone. The microwave map displays status of microwave radios in the zone.

Depending on a map, users can change the map mode, set the background image, rename a map element, change the visibility of elements on the map or filter map elements, add an area to a zone and site, or define links between microwave radios. In the geographical mode users can set such parameters as the map center, zoom level, or map bounds.

Related Links

Setting the Map Mode on page 91
Changing the Map Background in the Static Mode on page 91
Loading and Updating Map Tiles in the Geographical Mode on page 92
Setting Zones Visibility on System Maps on page 93
Changing Sites Filtering on Zone Maps on page 145
Configuring the Map Center on page 94
Configuring Zoom Levels on page 94
Configuring Max Bounds on page 95
Adding Areas on Maps on page 95
Editing Areas on Maps on page 96
Removing Areas from Maps on page 96
Adding Site Areas on Zone Maps
Editing Site Areas on Zone Maps

5.7.1
Changing Sites Filtering on Zone Maps

Use the filtering setting to hide selected site categories on the zone map.

Procedure:

1. In the **Navigation View** panel, go to **Zone Views** → **Zone Map**.
2. Click the **Sites Filtering** icon  .
3. Select and/or clear the required check boxes representing categories of sites.
4. Close the dialog box.

NOTICE: The filtering is applied only to the current map view – it is not saved.

Related Links

System, Zone and Microwave Map Operations on page 144

5.8
Physical and Service Maps Operations

5.8.1
Physical and Service Map Properties

Table 25: Map Properties

Property	Description
Name	Specifies a unique name of the map.
Label	Specifies the label of the map, as displayed in the tree and on the display panel (internal frame). Edit this field to change the name of the map as displayed in the tree, and then click **Modify** to apply the change.
Tree Icon Name	Specifies the image name and location of the icon representing the map in the tree. Edit this field to provide the background image from the `<UEM Home>/image` directory, and click **Modify** to apply the change.
Image Name	Specifies the image name and location of the background image for that map. If nothing is specified in this field, a blank white background is set to the map. Edit this field to provide the background image from the `<UEM Home>/image` directory, and click **Modify** to apply the change.

Table continued…

Property	Description
MapLinkRenderer	Specifies the Map Link Renderer that renders the links in the map.
MapSymbolRenderer	Specifies the Map Symbol Renderer that renders the symbols in the map.
Menu Name	Specifies the map-specific menu file (XML) name. This menu is shown in the menu bar when the map is selected, or as a pop-up when you right-click the map.
Current Topology	Edit this field to change the type of the topology: grid, star, ring, or flow, and click **Modify** to apply the change.
Anchored	If this field is selected (click **Modify** for the change to take effect), you are not able to edit that map anymore.
AutoPlacement	When set to **true**, the map layout is set with the CurrentTopology.
HelpDoc	Specifies the URL for the help documentation for the Map Properties dialog box.
Type	dit this field to change the list of types displayed on the map and click **Modify** to apply the change.
groupName	The name of the group.
Save changes on server	If you want to apply the changes you made to the fields in the **Map Properties** window, select this check box. As a result, changes from the currently open **Map Properties** window are saved on the server and applied to all connected clients. If you made changes without the **Save changes on server** check box selected, they are saved only on the client you are working on. You can save them on the server by clicking **Save Map**  . As a result, changes from the currently open **Map Properties** window and the previous changes are saved on the server and applied to all connected clients.

5.8.2

Physical and Service Maps Symbol Properties

Table 26: Map Symbol Properties

Property	Description
Name	Specifies the unique name of the map symbol.
Label	Specifies the label for the map symbol. Edit this field to change the label of the map symbol and click **Modify** for the change to take effect. **NOTICE:** If you want this change to apply to all the clients connected, save changes to the server.
Object Name	Specifies the object name of the selected symbol.
MapName	Specifies the map name in which the map symbol is located.
IconName	Specifies the image representing the map symbol. Edit the IconName to provide a new image for the map symbol from `<Web NMS Home>/images` directory, and click **Modify** to apply the change.

Table continued…

Property	Description
	NOTICE: If you want this change to apply to all the connected clients, save the changes to the server.
MenuName	Specifies the menu name in which the map symbol-related tasks are available.
Parent Symbol Name	Specifies the parent name of the selected symbol.
GroupName	Specifies the group name to which the map symbol belongs. Null is displayed if the link does not belong to any group.
Status	Specifies the status of the map symbol in that network.
Managed State	Specifies whether that map symbol is in a managed or an unmanaged state.
INITIAL_MIBS	Specifies the initial MIB associated with that map symbol.
Y	Specifies the current Y coordinate value where the map symbol is positioned. Edit this field to change the position. Click **Modify** to apply the change.
X	Specifies the current X coordinate value where the map symbol is positioned. Edit this field to change the position. Click **Modify** to apply the change.
Type	Specifies the type of the device associated with that map symbol.

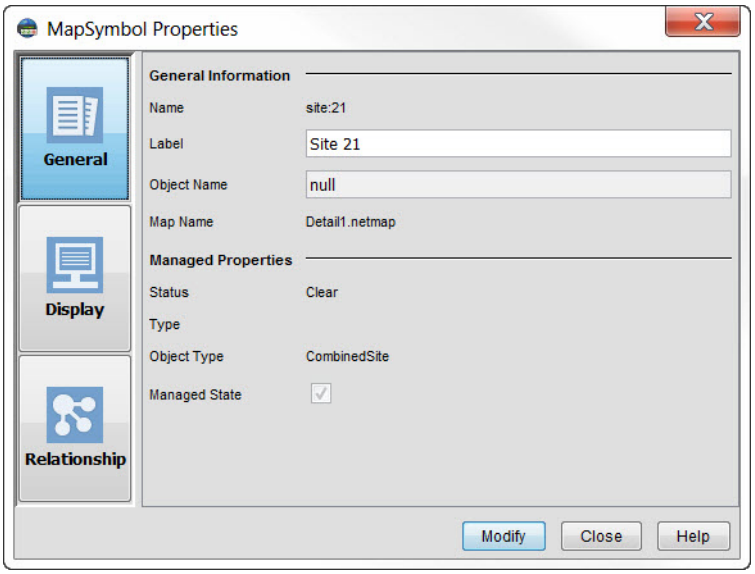
5.8.3
Viewing Physical and Service Map Symbol Properties

Procedure:

1. In the **Navigation View** panel, click a physical or service map view node.
2. In the map window, right-click a map symbol and select **Symbol Properties**.

The **MapSymbol Properties** window appears.

Figure 26: MapSymbol Properties Window



For information about the properties in this window, see Physical and Service Map Properties on page 145.

5.8.4

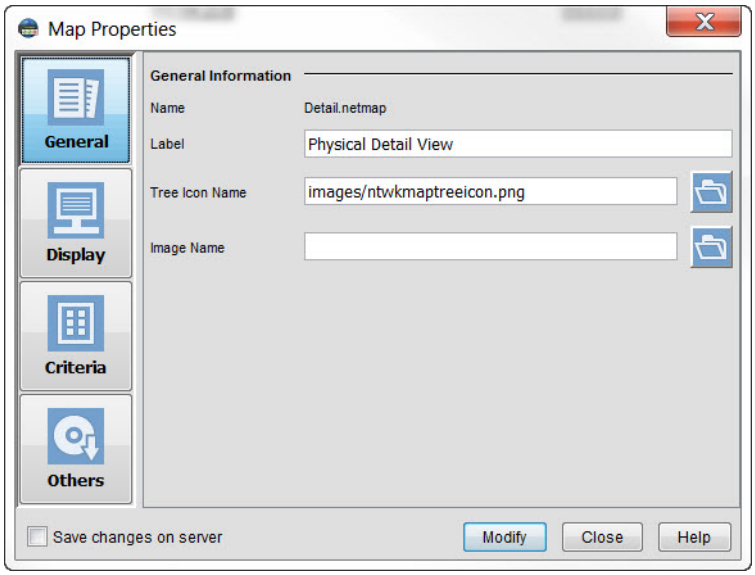
Changing Physical and Service Maps Properties

Procedure:

1. In the **Navigation View** panel, click the physical or service map view node.
2. In the map window, right-click the map and select **Map Properties**.

   The **Map Properties** window appears.

   Figure 27: Map Properties Window



3. In the **Map Properties** window, modify map properties:

If…	Then…
If you want to modify the current map properties and save them only on your local UEM client,	perform the following actions: **a** Modify the map properties you want. **b** Click **Modify**. Changes from the currently open **Map Properties** window are saved on the client you are working on.
If you want to modify the current map properties and save them on the server,	perform the following actions: **a** Modify the map properties you want. **b** Select the **Save the changes on server** check box. **c** Click **Modify**. Changes from the currently open **Map Properties** window without previous client changes are saved on the server and applied to all connected clients.
If you want to modify the current map properties and save the current and previous client changes on the server,	perform the following actions: **a** Modify the map properties you want. **b** On the toolbar, click **Save Map**  .

If…	Then…
	Changes from the currently open **Map Properties** window and the previous changes are saved on the server and applied to all connected clients.

For information about the properties in this window, see Map Properties.

5.8.5

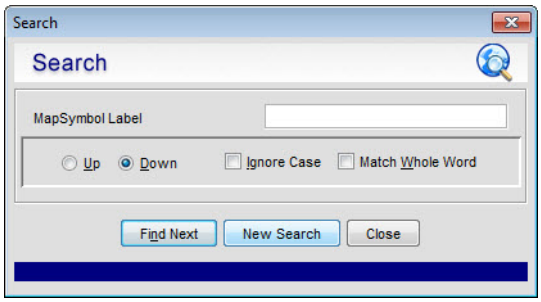
Searching Elements in Physical and Service Maps

You can search for an element, that is a map symbol, based on specific criteria.

Procedure:

1. Open the map in which you want to search for elements.
2. From the main menu, select **View** → **Search**.

   Figure 28: Search Dialog Box

   IMPORTANT: By clicking **New Search**, you reset the value to default. To close the **Find** dialog box, click **Close**. For more information, see **Help**.

   The **Search** dialog box appears.

3. In the **MapSymbolName** field, enter the label name of the symbol you are searching for.

   NOTICE: If you want to include any of the following characters in your search, enter a backslash \ before the character: `, \ * % _`

   Step example: You can enter `test-machine`, `test-server`.

4. Select **Up** or **Down** for the search pattern.

   Step example: If you are at the bottom of the map view, select **Up**. If you are at the top of the map view, select **Down**.

5. If you do not want to search the symbol based on case, select **Ignore case**.

   Step example: Enter `TEST` to search for instances of `test`, `Test`, and `TEST`, regardless of case.

6. If you want the search to be based on the complete label that you provide, select **Match whole word**.
7. Click **Find Next**. To skip a specific map and move to the next map available in the tree, click **Next Map**.

If a symbol that meets your criteria is found, you are taken to that symbol and it is automatically selected. If no symbols are found, use **Find Next**.

5.8.6
Changing Map Symbol Icons in Physical and Service Maps

You can change the icons for map symbols in the Service Detail View and Physical Detail View. You can use the available icons, and add you own. For information and procedures on adding custom images, see “Loading Image and Audio Files from a CD/DVD” in the *Private Network Management Servers* manual.

Procedure:

1. In the **Navigation View** panel, click the **Service Detail View** or **Physical Detail View** node.
2. In the corresponding window, right-click a map symbol and select **Symbol Properties**.
3. In the **MapSymbol Properties** dialog box, click **Display**.

   The display tab appears.
4. Click **Select a File** displayed next to the **Tree Icon Name** field.

   The **Unified Event Manager File Dialog** window appears.
5. Select the file you want to use and click **Open**.

   The **Unified Event Manager File Dialog** window closes.
6. Click **Modify**.

The **Map Symbol Properties** dialog box closes and the map symbol changes.

5.8.7
Launching the Network Database Window

Procedure:

1. In the main window, select **Zone Views** → **Physical** → **Physical Summary View** or **Physical Detail View**.

   The **Physical View** window appears.
2. Right-click a device or the subnet icon and select **View Device(s)**.

The **Network Database** window appears, displaying a list of events and alarms associated with the device or subnet you selected.
The window does not display some of the Logical Managed Resources representing services.

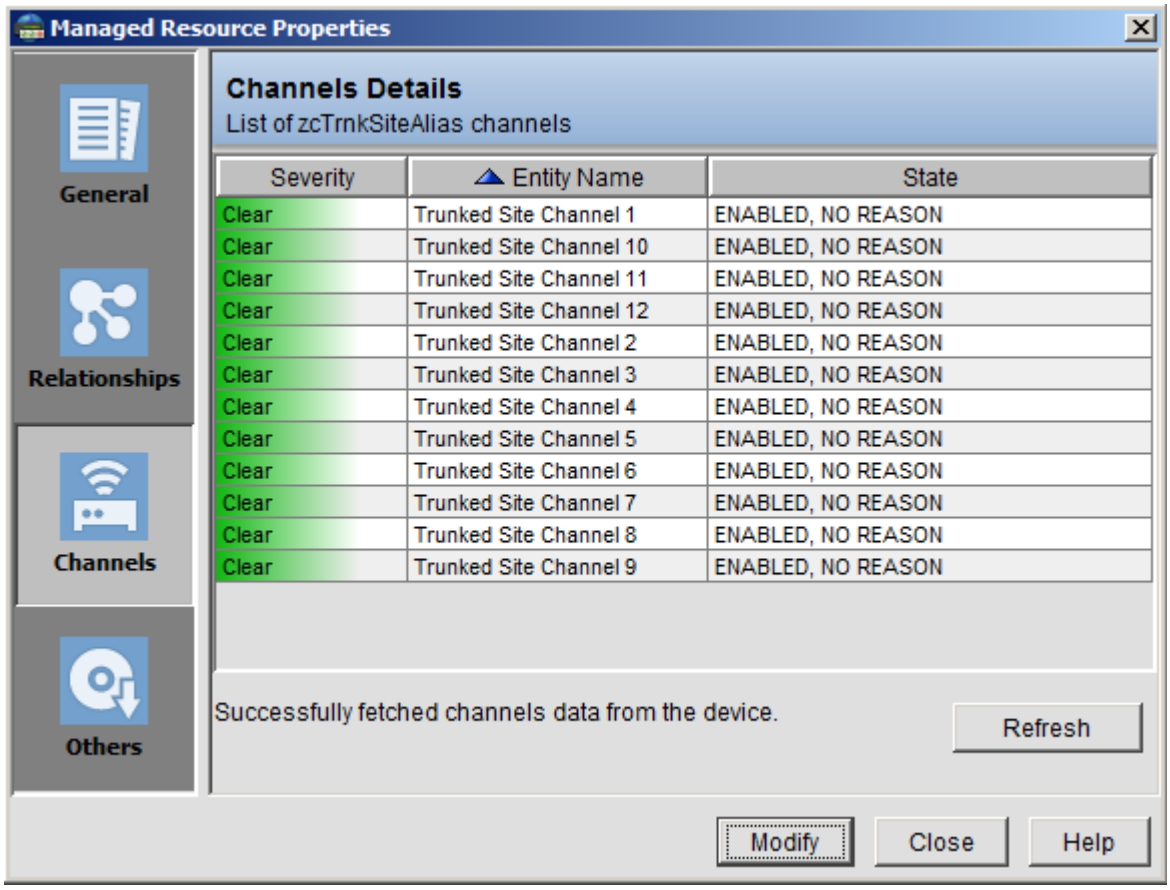
5.8.8
Viewing Channel Details from the Site Map

Procedure:

1. In the **Navigation View** panel, select **Service** → **Service Summary View**.
2. In the **Service Summary View** window, right-click a site icon and select **Site Channels View(ZC)** or **Site Channels View(SC)**.

The **Managed Resource Properties** window appears displaying a list of channels that belong to the site you selected. The channels are displayed from the zone controller or site controller perspective.

Figure 29: Managed Resource Properties Window – Channels Details



5.8.9

Map Grouping Operations

You can perform several operations to group devices within specific maps.

5.8.9.1

Grouping Specific Map Symbols

Procedure:

1. Open the desired map and select map symbols by clicking and dragging the mouse over a group of symbols. Press CTRL and click a map symbol to add it to the current selection.
2. After you select at least one map symbol, in the map toolbar, click **Group Selected Symbols**.

   NOTICE:
   You can group only individual map symbols. Grouping a map symbol with a group of map symbols is impossible.

   The group symbol shows the consolidated or the maximum severity of the group members. Even if only one of the nodes in a group is in the Critical state, the group symbol shows Critical.

   The map symbols are now grouped. UEM automatically assigns the group name.

3. To add more groups, repeat step 1 and step 2.

4 From the main menu, select **Map** → **Save Map**.

The custom map group is saved.

5.8.9.2
Viewing Symbols in a Specific Group in Physical and Service Maps

You can view all map symbols under a specific group.

Procedure:

1 Click a group in a map.

2 From the main menu, select **Group** → **Open Group**.

Devices under the selected group are displayed in the same window.

5.8.9.3
Ordering Symbols in Physical and Service Maps

By default, UEM arranges symbols in a map based on the order of discovery. However, you can order map symbols according to your requirements. You can manually drag and drop map symbols by using the mouse or order them automatically. Follow the procedure to order map symbols automatically.

Procedure:

1 From the main menu, select **Map** → **Order By**.

NOTICE:
If you order map symbols using **Order By**, they are aligned to a grid. The order you set is lost.

Devices discovered after ordering map symbols are not placed according to your preferences. They are added at the end of the map in the sequence of their discovery.

Postrequisites: Select one of the criteria from Map Symbol Criteria on page 152.

5.8.9.3.1
Map Symbol Criteria

Table 27: Map Symbol Criteria

Criteria	Description
Name	Sorts the map symbols based on their names. The order of sorting is A - Z.
label	Sorts the map symbols based on the label values of the symbol. The order of sorting is A - Z.
objName	Sorts the map symbols based on the name of the managed resource.
Severity	Sorts the map symbols based on the severity of the managed resources represented by the symbols. The order of sorting is from CommFailure to Clear, where symbols with CommFailure severity are listed first, followed by symbols with lower severity.
groupName	Sorts the map symbols based on the name of the group to which they belong.
objType	Sorts the map symbols based on the type of the managed resource represented by the symbols (node, network, router, switch, and so on).

5.8.9.4

Ungrouping Symbols in Physical and Service Maps

Procedure:

1. In the **Map** window, right-click a group and select **Ungroup**.
2. In the confirmation window, click **Yes**.

The group no longer exists and map symbols previously located in that group are now displayed in the main map area.

5.8.9.5

Changing Group Labels in Viewing Physical and Service Maps Symbol Properties

When creating a group, Unified Event Manager (UEM) automatically assigns a label to the group. For example, UEM labels groups as Group 1, Group 2, and so on. You can change the label name according to your preferences.Symbols in the Service Summary View and Service Detail View are group symbols that represent the site service status. UEM creates these symbols when sites are discovered. You can synchronize the label name for these site symbols with the display name of the site managed object reported by the Site Controller. For more information, see Updating Map Symbols and Managed Resource Names for Physical and Service Maps on page 102.

Procedure:

1. Right-click a group in the map and click **Symbol Properties**.

   The **Map Properties** dialog box appears.

2. In the **Label** field, enter the label name and click **Modify**.

The label of the group is changed.

5.9

Fault Management Operations

Fault management in Unified Event Manager (UEM) includes processing and presentation of events sent by a network element.

Failures in the network, network elements, as well as communication links can interrupt routine activities. When a failure occurs, events and alarms are reported in UEM, based on the criticality of the occurrence.

5.9.1

Displaying Alarm or Event Details from the Network Database Window

Procedure:

1. In the **Navigation View** panel, click the **Network Database** node.
2. In the **Network Database** window, highlight a row.
3. Perform one of the following actions:
   - If you want to display alarm details, from the main menu, select **Managed Resource → View Managed Resource Alarms**.

The **Alarms** window appears, displaying the alarms associated with the managed resource you selected.

- If you want to display Event details, from the main menu, select **Managed Resource → View Managed Resource Events**.

  The **Network Events** window appears, displaying the events associated with the managed resource you selected.

5.9.2
Displaying the Health of Sites

Procedure:

In the **Navigation View** panel, go to **Zone Views → Zone Map**.

The **Zone Map** window appears, displaying the discovered sites along with their health status. A colored icon indicates the health status (severity) of the sites.

5.9.3
Displaying the Health of Subnets

Procedure:

In the navigation tree, select **Zone Views → Physical → Physical Summary/Physical Detail View**.

The **Physical Summary/Physical Detail View** window appears, displaying the list of discovered subnets along with their health status. A colored icon indicates the health status (severity) of the subnet.

5.9.4
Displaying the Health of Network Elements

Procedure:

1. In the **Navigation View** panel, click **Network Database**.
2. In the **Network Database** window, double-click a selected network element.

   The **Network Element View** window opens. The **Object** section shows the health status of the network element. A colored icon indicates the health status (severity) of the element.

5.9.5
Displaying the Service State of All Sites

Procedure:

From the main navigation tree, select **Zone Views → Service → Service Summary/Service Detail View**.

The **Service Summary/Service Detail View** window appears, displaying the list of discovered sites along with their state details.

5.9.6

Managed Resource Properties

The following table describes various properties of managed resources. The properties are displayed in the **Managed Resource Properties** window. The **Field** column contains the name, as shown in the **Managed Resource Properties** window. You can also use the table to configure **Custom Views** and **Custom View Scopes** (see Security Management Operations on page 217). During the configuration of network database custom views, you can configure filter criteria for any of the properties. If the name of the property is not available, the custom view user interface supports defining additional properties. Use the additional property, based on the **Property name for filtering** column.

The **Property name for filtering** column contains case-sensitive data and is typically used in the configuration of custom views and custom view scopes (see Security Management Operations on page 217).

Table 28: Managed Resource Properties

This table contains various fields of the **Managed Resource Properties** window.

NOTICE: Properties that are not listed in the table are either not used or internal to Unified Event Manager. Do **not** use the unlisted properties.

Field	Description	Property name for filtering
	General Tab	
Name	Displays the unique Managed Resource internal name.	name
Managed Resource	Displays the name of the Managed Resource (this name is configurable).	displayName
Manager IP address	Displays the UEM IP address to which network elements send traps.	managerIpAddr
Type	Displays the network element type.	type
Class Name	Displays the managed resource type.	classname
Severity	Displays the present status of the device.	status
Managed	Displays the state of the device (managed or unmanaged).	managed
IP Address	Displays the IP address of the device.	ipAddress
Netmask	Displays the subnet to which the IP address belongs.	netmask
	SNMP Tab	
SNMP Port	Displays the port at which the device is running.	snmpport
Base Mibs	Displays the name of the management information base (MIB) to which the query is sent.	baseMIBs
Read Community	Displays the value of the read community.	community
Write Community	Displays the value of the write community.	writeCommunity
SNMP Version	Displays the SNMP Version of the device.	version
System Contact	Displays the system contact name for the device.	sysContact
System Location	Displays the location of the network element.	sysLocation

Table continued…

Field	Description	Property name for filtering
System Object Identifier	Displays the system object identifier (OID) of the device.	sysOID
System Name	Displays the system name of the device. For Trunking Subsystems (Tsubs), this field includes the Tsub ID and subsite ID (when applicable) along with other device information.	sysName
System Description	Displays the system description of the device.	SysDescr
	Channels Tab	
Severity	Displays the present status of a channel.	N/A
EntityName	Displays the name of a channel.	N/A
State	Displays the state of a channel and/or state explanation.	N/A
	Relationships Tab	
Parent Resource	Displays the name of the parent resource.	N/A
Subsystem Name	Displays the subsystem name for the device.	subSystemName
Red. Agent Group Name (optional)	Displays the redundant group name of a device.	nmaRedAgntGrpName
Group Members	Displays managed resources that are associated with a particular device as its children.	N/A
Group Names	Displays managed resources a particular device is associated with.	N/A
Is Group	Displays whether the device is part of a group.	isGroup
	Others Tab	
Parent Network	Not used by UEM.	parentNet
Reliable Comm. Capable	Displays the reliableCommCapable status of the device. V3 = True and V1 = False.	reliableCommCapable
Last Successful Synchronization	Displays the last synchronization date and time for a particular device.	lastSuccessSyncTime
Last Successful Supervision	Displays the last supervision date and time for a particular device.	lastSuccessSupervisionTime
Username	Displays the user name of the device.	userName
Synchronization State	Displays the current synchronization state of the device.	syncRate
Site ID	Displays the value of the subsystem or site location identifier (applicable only to LogicalManagedResource).	siteID
Metadata Managed Resource Type	Displays the managed resource type, as specified in the metadata.	metadataManagedResourceType

Table continued...

Field	Description	Property name for filtering
NM Data Interface Version	Displays the interface version of the managed object.	nmDataIfcVersion
Managed as NM Data Interface Version	Displays the interface version that is used to manage the device. This property appears only if UEM does not recognize the interface version of the device.	N/A
Object location – Core	Displays the zone ID number.	N/A
Object location – Instance	Displays the site ID number.	N/A
Object location – Site	Displays the discovery type.	N/A
Object location – Subsite	Displays the discovery type.	N/A
Managed Resource Device Category	Displays the category of the managed resource.	N/A
Network ID	Displays the network to which the IP belongs.	N/A
Object location – Site Type	Displays the site type. **NOTICE:** The displayed site type is the site type for RTU, NOT the site type for the device set in the SDM Builder.	N/A

5.10
Network Events Operations

A network event is an occurrence within a defined network. It could be a discovery of an element, a status update of an element, or an element failure. Events form a repository of information for all the occurrences within the system.

The **Network Events** window provides a means of looking at all events, or a filtered subset of events that the system receives. Consolidated lists of events are displayed in the **Network Events** window. The event properties that are displayed include:

- Severity
- Managed Resource
- Message
- Entity
- Date/Time
- Device Category

The other properties are not automatically displayed on the **Network Events** window by default, but can be viewed on Event Details window

5.10.1

Event Properties

The following table describes various properties of an event. The **Field Name** column contains the name as shown on the **Managed Properties** window. The information in Managed Resource Properties on page 155 can also be used to configure custom views and custom view scopes (see Security Management Operations on page 217).

During the configuration of network database custom views, you can configure filter criteria on any of the properties. If the name of the property is not available, the custom view user interface supports defining an additional property. Use the additional property, based on the **Property Name for Filtering** column.

NOTICE:
When specifying property names, use only alphanumeric characters and underscores. Do not start property names with digits.

When used for filtering, property names are case-sensitive and should be used exactly as specified when typing in the name of the additional property criterion to filter on.

Properties that are not listed in the table are either not used or internal to Unified Event Manager. Do **not** use the unlisted properties.

Table 29: Event Details Overview

Field Name	Description	Property Name for Filtering
Event ID	The unique ID of an event. This ID is sequential and UEM assigns it for each event.	id
Message	Descriptive text message about the event.	message
Category	Category of the event. For example: • Information Event • Attribute Value Change Event • Equipment Alarm • Quality of Service Alarm • Communication Alarm • Processing Error Alarm • Object Creation Event • Object Deletion Event • Management Event • Security Violation For more information, see Event and Alarm Category Definitions on page 65.	category
Network	The associated network. Not used by UEM.	network
Node	Name of the corresponding network element for which an event is being generated.	node
Failure Object (also named as	Failure object which was responsible for the creation of the event. The internal name derived by UEM.	entity

Table continued...

Field Name	Description	Property Name for Filtering
Entity in Event Filter UI)		
Severity	Severity of the event. See Severity Definitions on page 65.	severity
Date/Time	The time at which the event was generated on UEM. The time displayed on the Date/Time field in the **Network Events** window.	time
Device Category	Logical category of an alarm. Alarms are assigned the following categories: • Environmental • Generic • Microwave Infrastructure • Moscad • NM • RAN • Transport • Application • Core • Microwave Components	deviceCategory
Source	The Managed Object to which the event corresponds. Generally, it is the name of the Managed Object	source
Identifier	An internal attribute that uniquely identifies a particular event. The northbound manager uses it to determine whether the event is a duplicate, without relying on the event text. This identifier is different from the Event ID field. Example: For a site controller power supply malfunction due to fan failure, the identifier is `csc_ps_fault.7.2` where 7 is the malfunction state number and 2 is the fan failure cause number. Similarly, for a site controller power supply malfunction due to excessive battery temperature the identifier is `csc_ps_fault.6.4`.. For unique identifiers of events supported on UEM, see “Alarms and Events” in the *UEM Online Help*.	identifier
Entity Name	User-friendly name of the Failure Object the event is associated with.	entityDisplayName **NOTICE:** Entity name is displayed on the top of the window.

Table continued…

Field Name	Description	Property Name for Filtering
Ne TimeStamp	Time at which the event was generated on the device. If the device does not send this timestamp in the event, this attribute has an empty value.	neTimeStamp
Managed Resource	User-friendly name of the managed object to which the event corresponds. The user-friendly name for the managed object name, defined by the **Source** attribute of the event, for example `chan3.ss2.site60.zone7`.	ManagedResource
Reporting Device	IP Address of the device (agent) sending the event.	reportingAgent
Event Age (modified time)	Property that is available only in the Event Custom View UI. This property is not applicable to Event Filters user interface and cannot be used in the filter criteria definition on the Event Filters UI.	N/A
	This property specifies the age of the event. Age of an event denotes the time elapsed since the last modification of the alarm on UEM.	
	By default, the value specified is `Any`, whereby events of any age are displayed.	
	Other options are: minutes, hours, days, today, and yesterday.	
	Example: Age in **hrs < 1** displays all the events that are less than an hour old. After this custom view is created, the events are dynamically added to the view when they meet the criteria of being less than one hour old. In this case, the old events remain in the view. If you require to delete the old events and want to view only those currently meeting the criteria, set **Refresh period in minutes**. By default, it is set to one minute. When you set it, the server application sends data automatically at the specified time interval.	
System Name	The system name configured on the device.	sysName

NOTICE: The following parameters that are listed in Additional Criteria are not used by UEM: help URL, network.

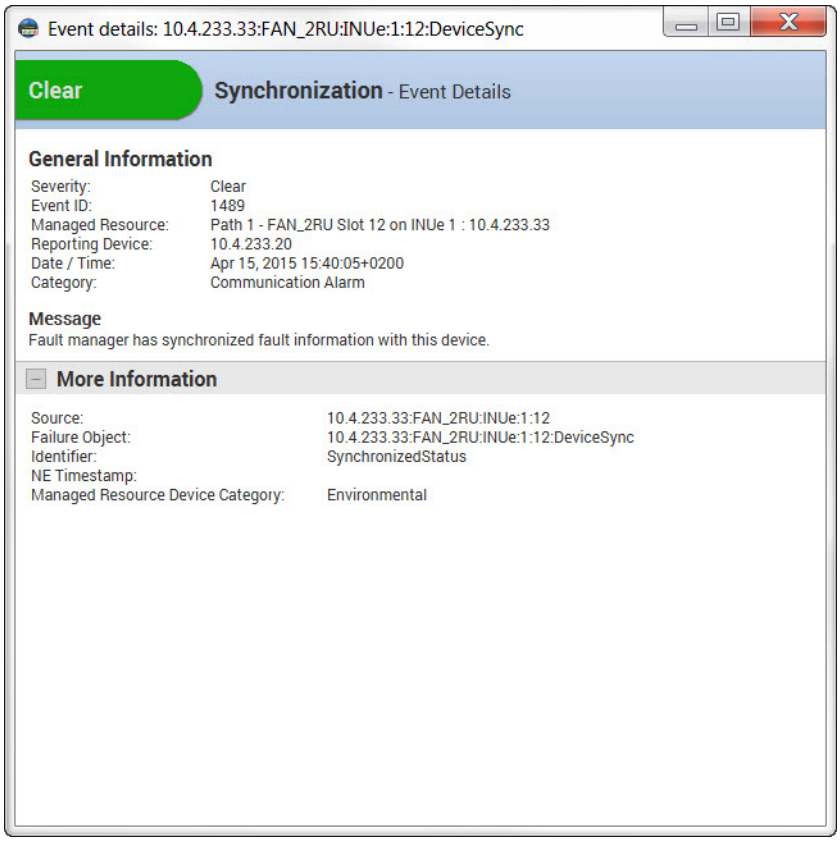
5.10.2
Viewing Event Details

All events received by Unified Event Manager (UEM) are based on the status of recognized devices. Event details display the property names and their values.

Procedure:

1. In the **Navigation View** panel, select **Fault Management** → **Network Events**.
2. In the **Network Events** window, double-click an event to view its details.

Figure 30: Event Details Window



The **Event details** window appears, displaying the details pertaining to the event you selected.

5.10.3
Viewing Related Alarms for an Event

Procedure:

1. In the **Navigation View** panel, select **Fault Management** → **Network Events**.
2. In the **Network Events** window, right-click an event and click **View Alarms**.

   The **Alarms** window displaying related alarms opens.
   For Logical Managed Resource (LMR) - only alarms for LMR are displayed.

   For Device Managed Resource (DMR) - alarms for DMR and related LMRs are displayed.

5.10.4
Viewing Related Managed Resources for an Event

Procedure:

1. In the **Navigation View** panel, select **Fault Management** → **Network Events**.
2. In the **Network Events** window, right-click an event and click **View Associated Managed Resources**.

   The **Network Database** window displaying related managed resources opens.

5.10.5
Viewing Group Events

Procedure:

1. In the **Navigation View** panel, select **Service** → **Service Detail View**.
2. In the **Service Detail View** window, right-click a group. From the context menu, select **View Group Events**

The **Network Events** window appears displaying the events for the selected group.

5.10.6
Exporting Events

Follow this procedure to export events to a `.csv` (Comma Separated Value) file and save it to the local client PC.

Procedure:

1. In the **Navigation View** panel, select **Fault Management** → **Network Events**.
2. From the main menu, select **Actions** → **Export Events**.
3. In the **Save File** window, perform the following actions:
   a. Select the destination directory.
   b. Enter a file name followed by `.csv`.
   c. Click **Save**.

   NOTICE: To print the events, open the saved file on the client and use the **Print** option in the application you are using.

The `.csv` file is saved to the local client PC.

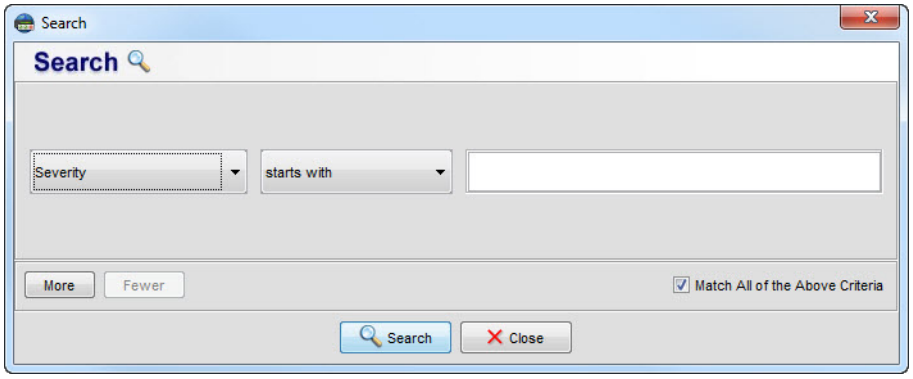
5.10.7
Searching Events

The search option is useful when you are looking for a particular event in the list of events. Search operations are performed in the database and are not restricted only to the events that you see in Unified Event Manager (UEM).

Procedure:

1. In the **Navigation View** panel, select **Fault Management** → **Network Events**.
2. To open the **Search** dialog box, press CTRL + F

Figure 31: Search Dialog Box



3 In the **Search** dialog box, set your search options:

   a From the first drop-down list, select the property you want to base your search on.

   b From the second drop-down list, select the condition based on which you want to restrict your search.

   c In the text field, enter the exact information you are looking for.

   NOTICE: If you want to include any of the following characters in your search, enter a backslash \ before the character: `, \ * % _`

   Step example:
   If you selected a severity from the first drop-down list, in the text field, specify the severity value, for example, `critical` or `major`.

   If you selected date or time-related properties, the **Date/Time** spin box to set date and time is available.

4 Define which criteria you want to include in the search:

   - To perform a search operation that meets any of the matching criteria that you specify, clear the **Match All of the Above Criteria** check box.
   - To include all matching criteria in your search operation, select the **Match All of the Above Criteria** check box.

5 Optional: Specify more criteria by clicking **More** and repeating step 3 through step 4.

6 Optional: Remove some of the criteria by clicking **Fewer**.

   The last criterion on the list is removed.

7 To begin the search, click **Search**.

   NOTICE: If you want to view all events after performing the search, in the **Network Events** window, click **Show All**.

Events meeting the configured criteria are displayed in the same view.

5.10.8
Launching Events View from the Network Database View

You can view events for a selected managed resource by opening the Events view from the Network Database view.

Procedure:

1 In the **Navigation View** panel, highlight the **Network Database** node.

2 Right-click a specific managed resource.

3 Select **View Managed Resource Events**.

The **Network Events** window opens.

5.10.9

Launching Events View from the Network Element View

You can view events for a selected managed resource or entity by opening the **Network Events** view from the **Network Element** view.

Procedure:

1 In the **Navigation View** panel, highlight the **Network Database** node.

2 Double-click a managed resource.

3 In the **Objects** section of the **Network Element View** window, right-click a specific resource.

4 Select **View Associated Events**.

The **Network Events** window opens.

5.10.10

Launching Events from Maps

You can view events for a selected map elements by opening the Events view from the Map view.

Procedure:

Navigate to the events for a selected map:

If…	Then…
If you want to launch the events window from a system, zone or microwave map,	**a** In the **Navigation View** panel select a specific Map. **b** Right-click the icon of a specific map element and select **View Associated Events**.
If you want to launch the events window from a physical map,	**a** In the **Navigation View** panel, go to → **Zone Views** → **Physical** → **Physical Summary View / Physical Detail View**. **b** Perform one of the following actions: • If the map element is not a group, right-click the icon of the specific map element and select **View Managed Resource Events** • If the map element is a group, right-click the icon of the element and select **View Group Events**
If you want to launch the events window from a service map,	**a** In the **Navigation View** panel, go to **Zone Views** → **Service** → **Service Summary View / Service Detail View**. **b** Perform one of the following actions: • If the map element is not a group, right-click the icon of the specific map element and select **View Managed Resource Events**

If…	Then…
	• If the map element is a group, right-click the icon of the element and select **View Group Events**

The **Network Events** window opens.

5.10.11

Launching Events View from a Custom Event Panel

Procedure:

1. In the **Navigation View** panel, expand the **Network Events** node.

   The **Network Events** node expands and a list of custom views appears.

2. From the list of custom views, select a previously created custom view.

In the **Network Events** window, the filtered list of events for the specified criteria appears.

5.11

Alarm Operations

In Unified Event Manager (UEM), specific network events are converted to alarms. UEM displays alarms in a separate window.

Figure 32: Alarms Window

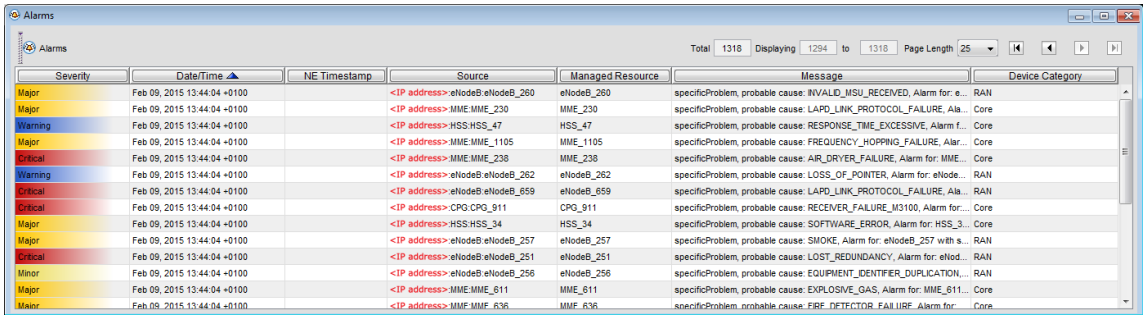
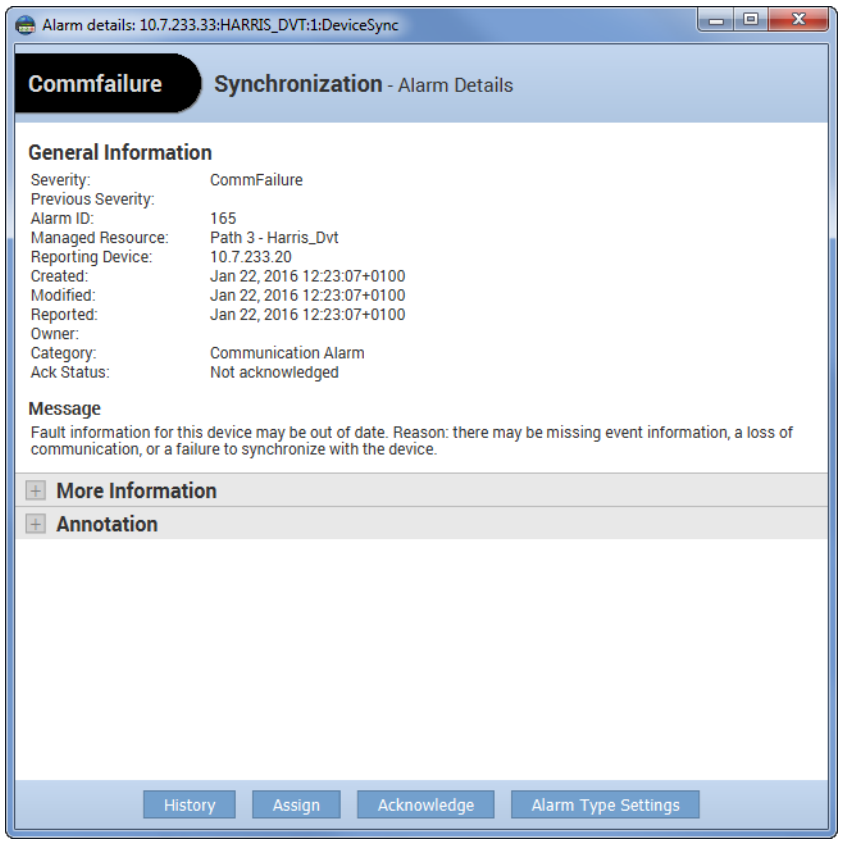


Figure 33: Alarm Details Window

You can see details of a specific alarm by double-clicking an alarm. A window with alarm details appears.



5.11.1
Alarm Properties

The following table describes various fields of an alarm. The **Field Name** column contains the name as shown on the **Managed Properties** window.

Managed Resource Properties can also be used to configure custom views and custom view scopes (see Security Management Operations on page 217). During the configuration of alarm custom views, you can configure filter criteria on any of the properties.If the name of the property is not available, the custom view user interface supports defining an additional property. Use the additional property, based on the **Property Name for Filtering** column.

NOTICE:
When specifying property names, use only alphanumeric characters and underscores. Do not start property names with digits.

When used for filtering, property names are case-sensitive and should be used exactly as specified when typing in the name of the additional property criterion to filter on.

Properties that are not listed in the table are either not used or internal to Unified Event Manager. Do **not** use the unlisted properties.

In property names, do not use the following characters:

```
white space
empty space
> < & $ # ^ - " ' ""
a digit at the beginning of the name
* ! @ ( + ~ { [ | \ ; , . ? / % `
```

Table 30: Alarm Details Overview

Field Name	Description	Property Name for Filtering
Annotations	Additional information about an alarm that you can add. The length of an annotation cannot exceed 4,096 characters.	annotations
Alarm ID	The unique ID of an alarm. Since every alarm on Unified Event Manager (UEM) is generated from a corresponding event, this ID is the same as the ID of the corresponding event.	id
Message	Descriptive text message about an alarm.	message
Category	Category of an alarm. The value can be one of the following: • Equipment Alarm • Quality of Service Alarm • Communication Alarm • Processing Error Alarm • Security Violation For more information, see Event and Alarm Category Definitions on page 65.	category
Failure Object	Failure object or entity which has the problem indicated by this alarm. The entity and failure object refer to the same property.	entity
Severity	Severity of an alarm. For more information, see Severity Definitions on page 65.	severity
Reported	Custom alarm property that indicates the time and date of the last event reported for a given alarm by UEM. The property is used by the Cleared Alarm cleanup policy (AlarmCleanupPolicy).	lastReportedNotificationTime

Table continued…

Field Name	Description	Property Name for Filtering
Created	The time at which an alarm was created on UEM. It is the time displayed in the **Date/Time** field in the **Alarms** window.	createTime
Source	The name of a managed object to which an alarm corresponds.	source
Previous severity	Previous severity of an alarm, that is, the severity of the alarm before it was updated.	previousSeverity
Modified	The time at which an alarm was last modified.	modTime
Identifier	An internal attribute that uniquely identifies a particular alarm. The northbound manager uses the Identifier to determine whether the event is a duplicate, without relying on the alarm text. This identifier is different from the **Alarm ID** field. Example: For a site controller power supply malfunction due to fan failure, the identifier is `csc_ps_fault.7.2` where 7 is the malfunction state number and 2 is the fan failure cause number. Similarly, for a site controller power supply malfunction due to excessive battery temperature the identifier is `csc_ps_fault.6.4`. For unique identifiers of events supported on UEM, see “Alarms and Events” in the *UEM Online Help*.	identifier
Name	User-friendly name of the Entity/Failure Object an event is associated with. The Entity name is displayed at the top of the window.	entityDisplayName
Managed Resource	The name of a managed object to which an event corresponds. It is an IP address, a DNS name or user provided name of the managed object, for example `uem01`.	managedResourceDisplayName
ReportingDevice	IP address of a device (agent) sending an alarm.	reportingAgent
Owner	Not used by UEM.	ownerName
GroupViewMode	This property is available only for alarm custom views. This property is not applicable to Alarm Filters user interface and cannot be used in the filter criteria definition on the Alarm Filters user interface. This user interface property defines the mode in which alarms in a custom view are grouped. The drop-down menu supports three modes of grouping. **max** The 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.	N/A

Table continued…

Field Name	Description	Property Name for Filtering
Alarm Age (modified time)	This property is available only for alarm custom views. This property is not applicable to Alarm Filters user interface and cannot be used in the filter criteria definition on the Alarm Filters user interface.	N/A
	This property specifies the age of the alarm for filtering. Age of an alarm denotes the time elapsed since the last modification of the alarm on UEM.	
	By default, the value specified is Any, whereby alarms of any age are displayed.	
	Other options are: minutes, hours, days, today, and yesterday.	
	For example, age in **hrs < 1** displays all the alarms that are less than one hour old. After this custom view is created, the alarms are dynamically added to the view when they satisfy the criteria of being less than one hour old. In this case, the old alarms remain in the view. If you require to delete the old alarms and want to view only those currently meeting the criteria, set **Refresh period in minutes**. By default, it is set as 1 minute. When you set it, the server application sends data automatically at the specified time interval.	

5.11.2
Viewing Alarm Details

Alarm details provide information about each of the alarm properties. All users can view alarm details.

Procedure:

1. In the **Navigation View** panel, select **Fault Management** → **Alarms**.
2. In the **Alarms** window, double-click an alarm row.

5.11.3
Viewing Related Events

Procedure:

1. In the **Navigation View** panel, select **Fault Management** → **Alarms**.
2. In the **Alarms** window, right-click an alarm row and select **View Events**.

The **Network Events** window appears with the events related only to the selected alarm.

5.11.4
Viewing Alarm History

The alarm history gives the complete information on alarm status, such as added and updated alarms. For example, when a critical alarm is generated, in the **Alarms** window, an alarm status appears.

Procedure:

1. In the **Navigation View** panel, select **Fault Management** → **Alarms**.

2 In the **Alarms** window, double-click an alarm row.

3 In the **Alarm Details** window, click **History**.

The **Alarm History** window appears, displaying the alarm history that includes 20 last instances of the alarm, the time at which the alarm occurred, device. Ack State, and severity.

5.11.5
Adding Annotations to Alarms

You can add an annotation to alarms. An annotation is an extra piece of information that tells you how to deal with an alarm. Annotations can serve other functions as well. They are visible to other users.

Procedure:

1 In the **Navigation View** panel, select **Fault Management** → **Alarms**.

2 In the **Alarms** window, double-click an alarm row.

3 In the **Alarm Details** window, expand the **Annotations** section by clicking **+** icon.

4 In the text field, enter the annotation about the alarm. Click **Save**.

The annotation can be 4,096 characters long or shorter.

Your annotation is added to the alarm. The annotation is visible to other users. After saving an annotation, you can still modify it.

5.11.6
Viewing Group Alarms

Procedure:

1 In the **Navigation View** pane, select **Service Summary View**.

2 Right-click a group and select **View Group Alarms**.

The **Alarms** window appears displaying the alarms for devices in the selected group.

5.11.7
Exporting Alarms

Follow this procedure to export alarms to a `.csv` (Comma Separated Value) file. Only visible alarms are exported.

Procedure:

1 In the **Navigation View** panel, click the **Alarms** node.

2 From the main menu, select **Actions** → **Export Alarms**.

3 In the **Save File** window, perform the following actions:

a Select a destination directory.

b Enter a file name followed by `.csv`. Click **Save**.

NOTICE: To print the alarms, open the saved file on the client and use the **Print** option in the application you are using.

The `.csv` file is saved to the local client PC.

5.11.8

Searching Alarms

The procedure for searching alarms is the same as the procedure for searching events. For more information, see Searching Events on page 162.

5.11.9

Displaying Alarms Summary

Procedure:

1 In the **Alarm Summary View** panel, perform one of the following actions:

- Click the **Severity and Category – Tabular View** icon  .
- Click the **Severity and Category – Graphical View** icon  .
- Click the **Severity alone** icon  .

Alarms appear in the selected view in the **Alarm Summary View** panel.

2 Depending on your view, perform one of the following actions:

If…	Then…
If you are using the Severity and Category – Tabular View,	click a severity or a category.
If you are using the Severity and Category – Graphical View or Severity alone,	click a severity.

The **Alarms** window appears, displaying the filtered alarms.

3 In the **Alarms** window, perform one of the following actions:

- To view alarm details, double-click an alarm.
- To view events related to the selected alarm, right-click an alarm and from the context menu select **View Events**.

5.11.10

Assigning Audio Notifications to Alarms

Audio notification for an alarm associates an audio file with a severity.

When an alarm with that severity is raised, you can hear the associated audio notification. You can also mute audio notifications and configure the playback time of the audio file.
There are six severity levels that can be associated with an audio file. If it is not necessary to audibly distinguish severities, you can configure the same audio file for all severities. You can add custom audio notifications.

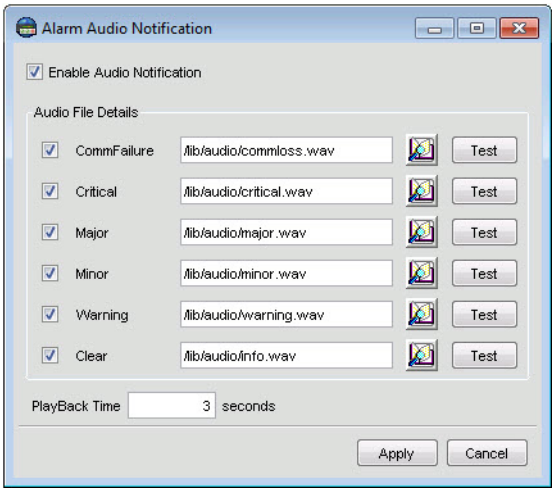
For information and procedures on adding custom alarm tones to UEM, see “Loading Image and Audio Files from a CD/ DVD” in the *Private Network Management Servers* manual.

Prerequisites: Ensure that the **Alarms** window that is open is not filtered to exclude the alarm to which you want to assign an audio notification. For more information, see Custom View Operations on page 127.

Procedure:

1. In the **Navigation View** panel, select **Fault Management** → **Alarms**.
2. From the main menu, select **Actions** → **Alarms Notifier**.

   Figure 34: Alarm Audio Notification Dialog Box



3. In the **Alarm Audio Notification** dialog box, make sure the **Enable Audio Notification** check box is selected.

   The options in the **Audio File Details** field are enabled.
4. Select a severity to which you want to associate an alarm.
5. Click **Browse** and select the audio file you want to associate with an alarm.
6. To play the audio file, click **Test**.
7. Click **Apply**. Repeat the steps to assign alarms for other severity levels.

   NOTICE: You can set the playback time for an alarm by specifying the duration in seconds. The alarm is not played longer than the duration of the audio file itself.

5.11.11
Launching the Alarms View from the Network Database View

You can view alarms for a selected device by opening the **Alarms** view from the **Network Database** view.

Procedure:

1. In the **Navigation View** panel, click the **Network Database** node.
2. In the **Network Database** window, right-click a managed resource. From the context menu, select **View Managed Resource Alarms**

The **Alarms** window appears, displaying the alarm (if any) for the device you selected.

5.11.12
Launching Alarms View from the Network Element View

You can view alarms for a selected managed resource or entity by opening the **Alarms** window from the **Network Element View** window.

Procedure:

1. In the **Navigation View** panel, highlight the **Network Database** node.
2. Double-click a managed resource.
3. In the **Objects** section of the **Network Element View** window, right-click a specific resource.
4. Select **View Associated Alarms**.

   The **Alarms** window opens.

5.11.13

Launching Alarms from Maps

You can view alarms for a selected map elements by opening the **Alarms** window from a map.

Procedure:

Navigate to the alarms for a selected map:

If…	Then…
If you want to launch the alarms window from a system, zone or microwave map,	**a** In the **Navigation View** panel, go to **System Views** or **Zone Views**, and select a specific map. **b** Right-click the icon of a specific map element and select **View Associated Alarms**.
If you want to launch the alarms window from a physical map,	**a** In the **Navigation View** panel, go to → **Zone Views** → **Physical** → **Physical Summary View / Physical Detail View**. **b** Perform one of the following actions: • If the map element is not a group, right-click the icon of the specific map element and select **View Managed Resource Alarms** • If the map element is a group, right-click the icon of the element and select **View GroupAlarms**
If you want to launch the alarms window from a service map,	**a** In the **Navigation View** panel, go to **Zone Views** → **Service** → **Service Summary View / Service Detail View**. **b** Perform one of the following actions: • If the map element is not a group, right-click the icon of the specific map element and select **View Managed Resource Alarms** • If the map element is a group, right-click the icon of the element and select **View GroupAlarms**

The **Alarms** window opens.

5.11.14
Launching Alarms View from a Custom Alarm Panel

Procedure:

1. In the **Navigation View** panel, expand the **Alarms** node.

   The **Alarms** node expands and a list of custom views appears.

2. From the list of custom views, select a previously created custom view.

In the **Alarms** window, the filtered list of alarms for the specified criteria appears.

5.11.15
Environmental Alarms

The **Environmental Alarms** window lists all the alarms related to the environmental entities (Environmental Digital Input and Environmental Alarms Output). A Remote Terminal Unit (RTU) at the site usually monitors and reports these entities. This default custom alarms view ensures quick access to environmental alarms, by filtering them from all the outstanding alarms existing in the system.

5.11.16
Alarms Ownership

You can take assignin an alarm you own to a resolver.

The alarm ownership operation can be invoked from:

- The **Alarm details** window
- The main menu **Edit** → **Assign/Unassign**

After an alarm is assigned, Unified Event Manager (UEM) stores the data of the user assigned to an alarm and a timestamp in audit trails.

Batch Assignments

If you select a list of alarms and invoke the Assign/UnAssign operation, all the selected alarms are assigned the same owner and assignee.

Related Links

Audit Trails Operations on page 218

5.11.16.1
Assigning Ownership to Alarms from the Alarms Details Window

All users can own and assign ownership of an alarm or a group of alarms.

Procedure:

1. In the **Navigation View** panel, select **Fault Management** → **Alarms**.
2. In the **Alarms** window, double-click an alarm row.
3. In the **Alarm Details** window, click **Assign**.
4. In the **AlarmAssignDialog** dialog box, type the assigned user name and click **OK**.
5. In the **Alarm Details** window, click **Close**.

In the **Alarm Details** window, the assignment appears in the **Owner/Assignee** field.

5.11.16.2

Assigning or Unassigning Ownership to Alarms from the Main Menu

Procedure:

1. In the **Custom Alarm** window, highlight an alarm.
2. From the main menu, select **Actions** → **Assign/Unassign**.

5.11.17

Acknowledging Alarms

You can acknowledge alarms from map, **Site Views**, **Zone Views** or the **Alarms** nodes. You can acknowledge alarms for single network elements and entities or for a whole site or zone. The information about whether the alarm is acknowledged or not is displayed in the **Alarms** window in the **Ack Status** column.

Procedure:

1. In the **Navigation View** panel, select **Alarms**.
2. Right-click an alarm and click **Acknowledge Alarm**.
3. If prompted to confirm, click **OK**.

   The **Ack Status** is updated to **Acknowledged**.

5.11.18

Unacknowledging Alarms

You can unacknowledge alarms previously acknowledged. The information about whether the alarm is acknowledged or not is displayed in the **Alarm View** window in the **Ack Status** column.

Procedure:

1. In the **Navigation View** panel, select **Alarms View**.
2. Right-click an alarm and click **Unacknowledge Alarm**.
3. If prompted to confirm, click **OK**.

   The **Ack Status** is updated to **Unacknowledged**.

5.11.19

Audit Report Viewer Functionalities and Layout

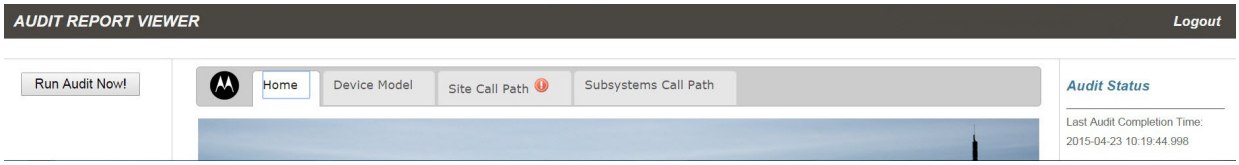
The Audit Report Viewer is a web application that allows you to see the details of model audit report or call path audit report alarms that appear in the Unified Event Manager (UEM).

Inconsistencies between the system configuration and the transport configuration can result in insufficient call paths in the system, and may cause system outages. To prevent system outages, the system weekly audits the current Transport Network configuration and compares it to the current system configuration. When an inconsistency is detected, the UEM displays an audit alarm. Information about the cause of the alarm is accessible in the Audit Report Viewer.

The Home Tab

From the **Home** tab, which displays after you launch the application, you can access the **Device Model**, **Site Call Path**, and **Subsystems Call Path** tabs, check the current audit status, or run a manual audit.

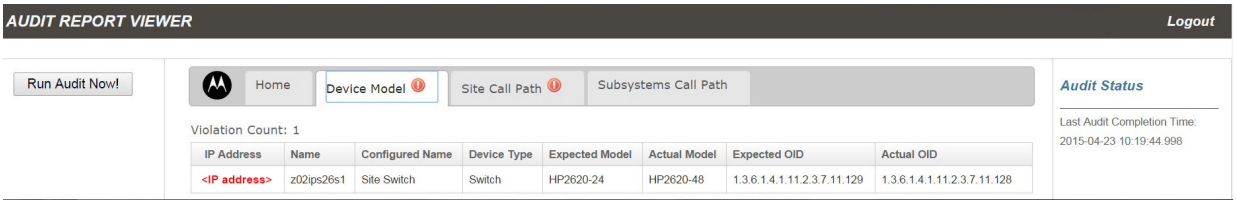
Figure 35: Audit Report Viewer Window — Home Tab



The Device Model Tab

The **Device Model** tab displays information about model and OID inconsistencies between the transport configuration and the device as discovered by the Unified Network Configurator (UNC). When there is a violation, the tab displays a red exclamation point icon.

Figure 36: Audit Report Viewer Window — Device Model Tab



Viewing the following fields helps to understand the reasons of inconsistencies and determine the appropriate corrective actions:

IP Address
The IP address of the device in violation. This field links the data in the Transport Network configuration to the data in the UNC configuration.

Name
The host name of the device as discovered by the UNC.

Configured Name
The host name of the device in the Transport Network configuration, used to confirm that the IP is consistent in the Transport Network configuration and in the UNC configuration.

Device Type
The type of device audited.

Expected Model
The model number as entered in the Transport Network configuration.

Actual Model
The model number as read from the device by the UNC.

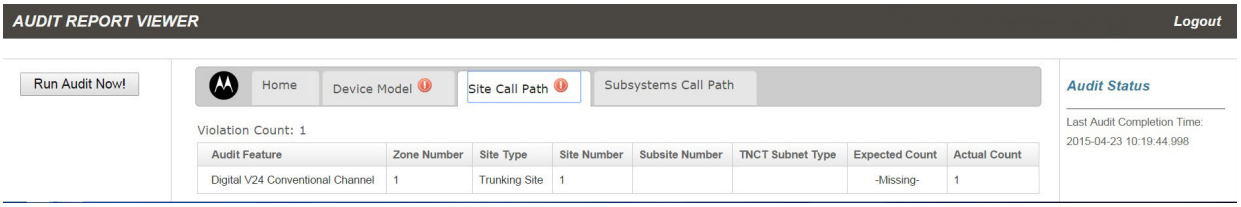
Expected OID
The OID for the device as entered in the Transport Network configuration.

Actual OID
The OID for the device as read from the device by the UNC.

The Site Call Path Tab

The **Site Call Path** tab displays information about call path shortages that occur in the system in relation to sites or subsites. When there is a violation, the tab displays a red exclamation point icon.

Figure 37: Audit Report Viewer Window — Site Call Path Tab



Viewing the following fields helps to understand the causes of such shortages and determine the appropriate corrective actions:

Audit Feature
The currently audited feature of the Transport Network configuration.

Zone Number
The zone ID for the device. Viewing this field helps to identify the instance of site involved in the violation.

Site Type
The type of site for the device.

Site Number
The site ID for the device. Viewing this field helps to identify the instance of site involved in the violation.

Subsite Number
The subsite number for simulcast devices. Viewing this field helps to identify the instance of site involved in the violation.

TNCT Subnet Type
The subnet type of the device.

Expected Count
The number of call paths available per the Transport Network configuration.

NOTICE: If a device is found in the system, but not in the Transport Network configuration, this field displays the value `Missing`.

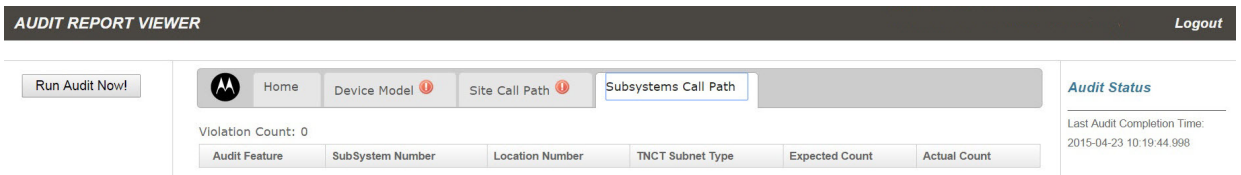
Actual Count
The required number of call paths as calculated from the current system configuration.

NOTICE: This number must either be equal to, or smaller than the expected count.

The Subsystems Call Path Tab

The **Subsystems Call Path** tab displays information about call path shortages that occur in the system in relation to a subsystem. When there is a violation, the tab displays a red exclamation point icon.

Figure 38: Audit Report Viewer Window — Subsystems Call Path



Viewing the following fields helps to understand the causes of such shortages and determine the appropriate corrective actions:

Audit Feature
The currently audited feature of the Transport Network configuration.

Subsystem Number
The subsystem ID for the device.

Location Number
The location ID within the conventional subsystem.

TNCT Subnet Type
The subnet type of the device.

Expected Count
The number of call paths available per the Transport Network configuration.

NOTICE: If a device is found in the system, but not in the Transport Network configuration, this field displays the value `Missing`.

Actual Count
The required number of call paths as calculated from the current system configuration.

NOTICE: This number must either be equal to, or smaller than the expected count.

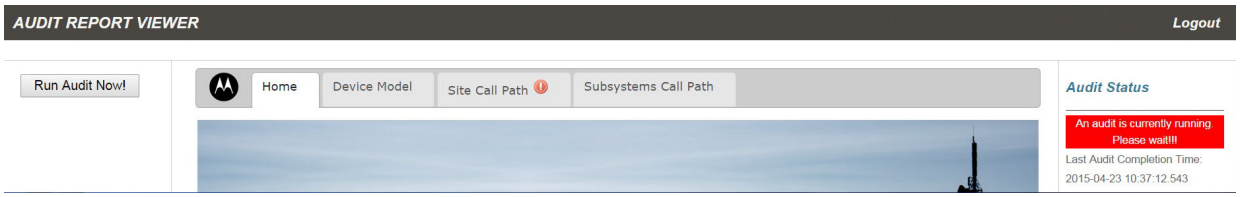
The Audit Status Panel

The **Audit Status** panel displays the `Last Audit Completion Time`, which indicates the last time the system searched for violations.

If an audit did not run after you corrected a violation, the UEM still displays an alarm. Viewing the `Last Audit Completion Time` helps you to understand why the alarm still displays in the UEM.

When an audit is running, the **Audit Status** panel displays a red warning message.

Figure 39: Audit Report Viewer Window During an Audit



Manual Audit

The **Run Audit Now** button on the left of the Home tab allows you to run an audit whenever needed. You can run a manual audit to:

- Confirm the correction of a previously reported violation, and clear the pending alarm on the UEM
- Ensure that the addition or change of a system, subsystem, or network configuration does not result in inconsistencies between the transport configuration and the impacted devices

5.11.19.1
Diagnosing Audit Alarms

Follow the procedure to navigate from Unified Event Manager (UEM) to the Audit Report Viewer (ARV) application, diagnose the cause of an audit alarm, and run a manual audit.

Prerequisites: In the **Navigation View** panel, highlight the **Network Database** node.

Procedure:

1 In the **Network Database** window, locate the **Audit Report** managed resource, and right-click on it. From the context menu, select **Launch Web Management Application**.

NOTICE: You may also access the ARV by entering a URL in the address field of your browser. For customer systems, enter: https://ucs01.ucs:49309/arv/. For Dynamic System Resilience sys tems, enter: https://ucs02.ucs:49309/arv/

The ARV interface is displayed.

2 To diagnose the cause of the alarm, view the **Device Model**, **Site Call Path**, and **Subsystems Call Path** tabs.

NOTICE: When any of these tabs contains violations, it displays a red exclamation point icon.

3 Optional: To run a manual audit, click the **Run Audit Now** button.

NOTICE:
You can run only one manual audit at a time. Therefore when an audit is running, the **Run Audit Now** button is disabled.

Due to the amount of data that is processed, the completion of the audit takes several minutes.

The **Run Audit Now** button is re-enabled, and the ARV displays the results of the audit.

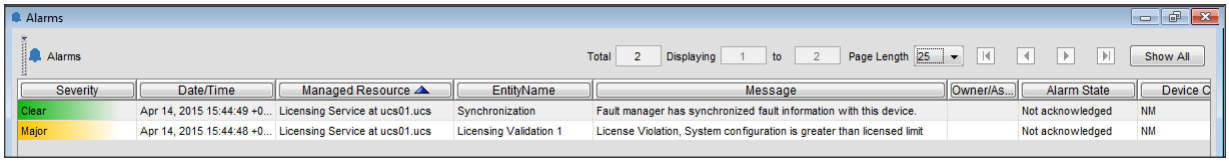
5.11.19.2
Audit Alarm Types

There are two managed resources that report license status:

- **Licensing Service** – reports the result of a license compliance audit that compares the configuration with the installed licenses.
- **Audit Report** – reports the result of a compliance audit that compares the Transport Network Configuration Tool audit file with the devices discovered in the system.

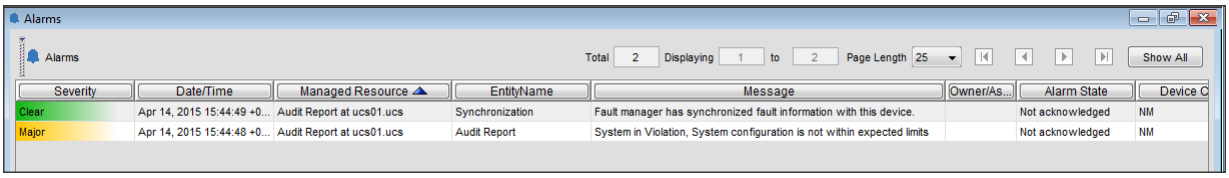
When the system configuration is greater than licensed limit, a license violation occurs and an alarm reported by the **Licensing Service** managed resource is displayed in the Unified Event Manager (UEM) **Alarms** view.

Figure 40: UEM Alarms View – Sample License Service Alarm



When the system configuration is not within expected limits, a system audit violation occurs and an alarm reported by the **Audit Report** managed resource is displayed in the UEM **Alarms** view.

Figure 41: UEM Alarms View – Sample Audit Report Alarm

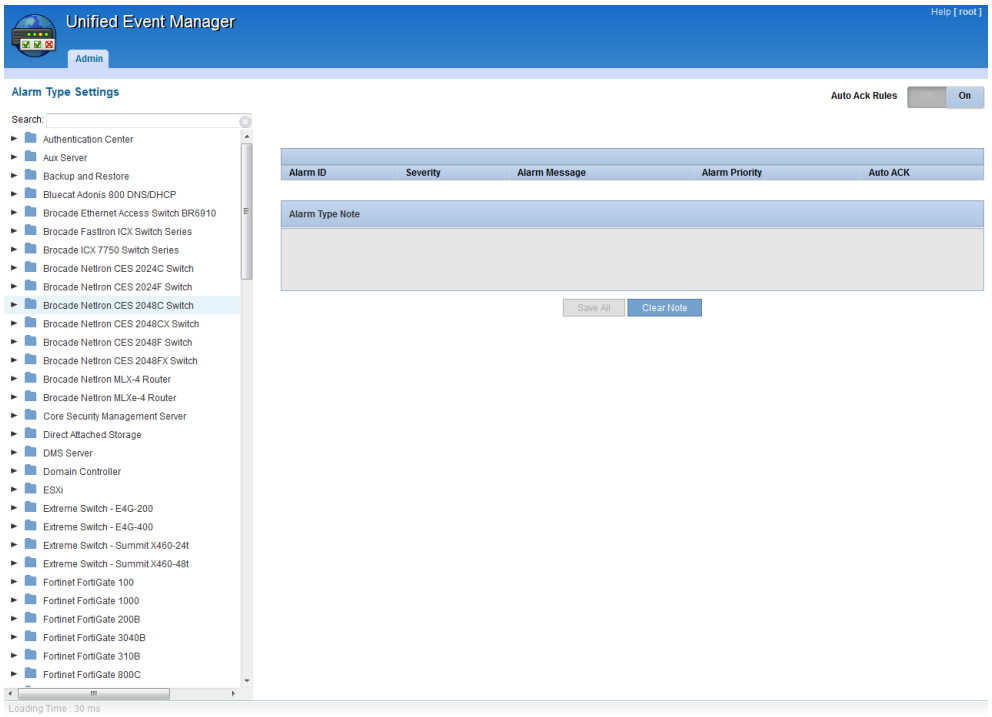


5.11.20
Alarm Type Settings

The **Alarm Type Settings** window displays details about alarm types generated for specific network elements and for UEM itself.

Only system administrators and users with appropriate permissions can view the **Alarm Type Settings** window. You can access it from the **Admin** view available from **Administration** → **System Administration**, or from the **Alarm details** window.

Figure 42: Alarm Type Settings Window



The window displays all pre-defined alarm types per network element. For some network elements, alarm types are not pre-defined. For those elements, the **Alarm Type Settings** window displays only the alarm type information based on the alarms already received by UEM.

Using the **Search** text field, you can search for specific alarm types.

In the **Alarm Type Settings** window, you can set the priority for a given alarm type or add a note for it. You can also set automatic acknowledgement for an alarm type, which means that the alarms of the given type are automatically acknowledged without requiring any actions from the users.

When you change settings for an alarm type, all of the existing alarms of a given type become updated with the new settings, and all of the newly generated alarms have the new settings.

To set auto acknowledgement for an alarm type, the **Auto Ack Rules** option in the upper right-hand corner of the window must be enabled. Only the system administrator can enable and disable this option.

NOTICE: The following table contains manager generated alarms that are not presented in the Alarm Type Settings window (unless they had Auto Acknowledgement enabled):

Table 31: Alarms Not Present in the Alarm Type Settings Window

Alarm Name	Alarm Message
EntityStatusClear	Entity has been removed:
EntityUnmanagedStatusClear	Entity has been unmanaged {0}:{1}
EntityNotConfiguredStatusClear	Configuration has been changed. The following entity is no longer reported: {0}:{1}.
UserRequestedAlarmStatusClear	Alarm has been cleared by {0}. Previous message: {1}
DiscUnManClearAll	Failure cleared by user un-management request.
PortDeletedClear	Port status is clear. Reason: Port is no longer reported.
PortStatusDisabled	Port status is clear. Reason: Port has been administratively disabled.

5.11.20.1

Setting Auto Acknowledgement for Alarm Types

You can set automatic acknowledgement of selected alarm types in the **Alarm Type Settings** window.

If you set automatic acknowledgment for an alarm type, it means that all alarms of a given type become acknowledgement by the system without any action from the user.

For the setting of automatic acknowledgement to be possible, the system administrator must enable the **Auto Ack Rules** option located in the upper right-hand corner of the window. When the system administrator disables the **Auto Ack Rules** option, the system saves the current settings for automatic acknowledgement, but disables further editing of the **Auto Ack** column.

Procedure:

1. From the main menu, select **Administration** → **System Administration**.

   A web browser window opens displaying UEM client web interface.

2. From the **Tools & Browsers** pane, select **Alarm Type Settings**.
3. In the panel on the left, expand the tree and navigate to the element for which you want to edit an alarm type.
4. Ensure that the **Auto Ack Rules** option is enabled.

   Only system administrators can enable or disable the **Auto Ack Rules** option.
5. In the **Auto Ack** column, select the check boxes for the alarm types which you want to be automatically acknowledged.
6. Optional: To cancel auto acknowledgement for an alarm type, clear the check box in the **Auto Ack** column.
7. Click **Save All**.

5.11.20.2

Setting Alarm Type Priority

You can set an alarm type for a given network element as **High**, **Normal**, or **Low** priority. The priority helps you filter and sort the alarms.

Procedure:

1. From the main menu, select **Administration** → **System Administration**.

   A web browser window opens displaying UEM client web interface.

2. From the **Tools & Browsers** pane, select **Alarm Type Settings**.
3. In the panel on the left, expand the tree and navigate to the element for which you want to edit an alarm type.
4. In the **Alarm Priority** column, set the priority for a selected alarm type to one of the available values:
   - **Low**
   - **Normal**
   - **High**
5. Click **Save All**.

5.11.20.3

Adding Notes to Alarm Types

You can add a note to an alarm type. It is later displayed in the **Alarm Details** window, and, optionally, in the **Alarms** window.

Procedure:

1. From the main menu, select **Administration** → **System Administration**.

   A web browser window opens displaying UEM client web interface.

2. From the **Tools & Browsers** pane, select **Alarm Type Settings**.
3. In the panel on the left, expand the tree and navigate to the element for which you want to edit an alarm type.
4. Highlight a selected alarm type.
5. In the **Alarm Type Note** text box located under the table, enter your note.

   The maximum length for a note is 4096 characters.
6. Optional: To delete an existing note, click **Clear Note**.
7. Click **Save All**.

5.12

Network Elements Management Operations

Unified Event Manager (UEM) uses the discovery process to find devices that are managed in a system. Device management in UEM controls whether a device in the ASTRO® 25 system is in one of two states: MANAGED or UNMANAGED.

Whenever a managed resource is discovered (or rediscovered) successfully, UEM designates the management state of that resource as MANAGED.

There are two types of managed resources: device managed resources and logical managed resources. Logical managed resources are non-physical managed resources, for example, a site. Device managed resources are physical managed resources, for example, a base radio or a site controller.

Once a device is marked as MANAGED, UEM starts periodic supervision and synchronization. UEM also starts displaying events sent by this device. It raises active alarms against a specific entity within this device whenever any displayed event requires user attention.

If you have administrative privileges, you can unmanage a managed resource in UEM. Once a device is in an unmanaged state, UEM:

- Does not supervise the device.
- Does not synchronize the device.
- Does not diagnose the device.
- Does not perform rediscovery.
- Does not allow any user to view any new events or alarms of any entity from this device.

5.12.1
Managing Resources

Device management provides administrators or MotorolaSSC administrators with the ability to start managing a previously unmanaged device. Managing an unmanaged device automatically invokes device rediscovery.

By default, all resources are managed. Only Device Managed Resources (DMRs) can be unmanaged. The **Manage** option is only available for unmanaged DMRs. If a DMR is unmanaged, all its LMRs are also unmanaged. Managing a previously unmanaged DMR will also manage all its LMRs.

Procedure:

1. In the **Navigation View** panel, click the **Network Database** node.
2. In the **Network Database** window, search for the DMR you need.

   The DMR severity should be **Unknown**.
3. Right-click the selected DMR, and select **Manage**.

The DMR and its Logical Managed Resources (LMRs) become managed. UEM starts state synchronization and traps processing for that device.

5.12.2
Unmanaging Resources

Device unmanagement gives the privileged operator, that is the administrators or MotorolaSSC administrators, the ability to stop the managemeny of a non-critical device managed resource in the system.

You can unmanage a resource if it fails or is at fault. For example, when the managed resource is interfering with the display of the system health by retaining long-standing high-priority alarms or generating an excessive number of events.

By default all resources are managed. Only Device Managed Resources (DMRs) can be unmanaged. The **Unmanage** option is only available for managed DMRs. If a DMR is managed, all its LMRs are also managed. Unmanaging a previously managed DMR will also unmanage all its LMRs.

Neither events nor alarms are processed for an unmanaged resource.

Procedure:

1. In the **Navigation View** panel, click the **Network Database** node.
2. In the **Network Database** view, search for the DMR you need.

   Every DMR has a defined IP address.
3. Right-click the selected DMR, and click **Unmanage**.

The DMR, and its Logical Managed Resources (LMRs) become unmanaged. Their severity changes to Unknown. UEM stops state synchronization and traps processing for that device.

5.12.3
Managing Entities

Entity management gives the privileged operator, that is the administrators or MotorolaSSC administrators, the ability to start managing a previously unmanaged entity. Managing an unmanaged entity automatically invokes synchronization.

Procedure:

1. In the **Navigation View** panel, click the **Network Database** node.
2. In the **Network Database** window, double-click a managed resource whose entity you want to manage.
3. In the **Network Element View** window, in the **Objects** section, perform the following actions:
   a. Expand the node of the managed resource whose entity you want to manage.
   b. Right-click the entity and select **Manage**.

The entity becomes managed. UEM starts state synchronization and traps processing for the managed resource.

5.12.4
Unmanaging Entities

Entity unmanagement gives privileged operators, that is administrators or MotorolaSSC administrators, the ability to stop the management of a non-critical managed resource entity in the system. Entities can be unmanaged indefinitely or temporarily.

You can unmanage an entity if it fails or is at fault. For example, when the managed entity interferes with the display of system health by retaining long-standing high-priority alarms or generating an excessive number of events.
Alarms are not processed for unmanaged entitties, but events are.

NOTICE: You cannot manage the communication, synchronization, management, agent redundancy, and discovery entities.

Procedure:

1. In the **Navigation View** panel, click the **Network Database** node.
2. In the **Network Database** window, double-click a managed resource whose entity you want to unmanage.
3. Depending on your preference, in the **Objects** section of the **Network Element View** window, perform the following actions:

If…	Then…
If you want to unmanage an entity,	Perform the following actions: **a** Expand the node of the managed resource whose entity you want to unmanage. **b** Right-click the entity and select **Unmanage**
If you want to temporarily unmanage an entity,	Perform the following actions: **a** Expand the node of the managed resource whose entity you want to unmanage. **b** Right-click the entity and select **Temporary Unmanage** **c** In the **Temporary unmanage entity** window, set an unmanage time and click **Unmanage**.

The entity is grayed out and becomes unmanaged. Temporarily unmanaged entities return to the managed state when the set time expires.

5.12.5

Launching Remote Connector Terminal Sessions

Unified Event Manager (UEM) allows you to launch terminal sessions for some network elements. The network elements are managed on UEM through SDM3000 SCADA.

You can launch terminal sessions for the following network elements:

- Motorola Base Radio - CS (MOSCAD)
- Motorola Receiver - ATAC 3000
- TeNSr/IMACS Channel Bank

You can establish terminal sessions from the PC on which UEM is running by using Remote Connector and additional software. The sessions are realized by tunneling serial interface through IP protocol to RTU which proxies that over physical serial interface to the target device.

Only one concurrent terminal session is supported. Due to limitations of components used to set up a terminal session, in some cases, multiple attempts at launching a session are required. There must be at least a 90-second interval between two consecutive attempts at launching a terminal session.

Prerequisites:
Ensure that the PC has the appropriate software and Windows system installed as indicated in the following table:

Table 32: Software and System Requirements for Remote Connector Terminal Sessions

Network Element	Terminal Session Software	System
Motorola Base Radio - CS (MOSCAD)	Remote Connector Radio Service Software Serial/IP (Tactical Serial/IP Redirector)	Windows 7
Motorola Receiver - ATAC 3000		
TeNSr/IMACS Channel Bank	Remote Connector HyperACCESS	Windows 7 or Windows 10

Procedure:

1 In the UEM **Navigation View** panel, click the **Network Database** node.

2 In the **Network Database** window, double-click a network element for which you want to launch a terminal session.

3 In the **Network Element View** window, in the **Objects** section, right-click the network element and select **Launch Terminal Session**.

4 In the **NFM Remote Connector Login** window, enter SDM3000 **rss** user name and password.

5 Establish a terminal session for a network elelement by performing one of the following actions:

If…	Then…
If you are launching a terminal session for TeNSr/IMACS Channel Bank,	in the **NFM — HyperACCESS** window, close the welcome message by pressing ENTER.
If you are launching a terminal session for Motorola Base Radio - CS (MOSCAD) or Motorola Receiver - ATAC 3000,	perform the following actions: **a** In the **RSS** window, click **Continue**. **b** From the **Radio Service Software** main screen, navigate to **Tools** → **Connection Configuration**. **c** On the **Connection Screen**, click **Connect/Dial**.

6 To end the terminal session, close HyperACCESS or RSS.

If the Remote Connector did not close properly after the first launch and at the next launch attempt you are prompted that Remote Connector is already running, you must end one or both of the following processes in the Windows Task Manager:

- `NFM_RemoteConnector.exe`
- `plink.exe`

Related Links

Terminal Session Software Installation on page 289

5.12.6
Point-to-Point Devices Management

Cambium Networks Point-to-Point (PTP) devices operate as wireless bridges in the ASTRO® 25 Network. You can open a direct browser connection to a particular PTP device in order to manage and configure it. This web browser connection is possible through the PTP Web Management Application. You can open it either from the Network Database View or the Alarms View.

NOTICE: If PTP certificates are not installed, opening the PTP Web Management Application generates security warnings. For more information on PTP certificates, see the *Private Network Management Client* manual.

5.12.6.1
Opening the PTP Web Management Application for Alarms

Procedure:

1 In the **Navigation View** panel, click the **Alarms** node.

2 In the **Alarms** window, right-click a Point-to-Point (PTP) alarm and select **Launch Web Management Application**.

NOTICE: If PTP certificates are not installed, opening the PTP Web Management Application generates security warnings. For more information on PTP certificates, see the *Private Network Management Client* manual.

The PTP web management application opens with the device details.

5.12.6.2

Opening the PTP Web Management Application for Network Database Devices

Procedure:

1. In the **Navigation View** panel, click the **Network Database** node.
2. In the **Network Database** window, right-click a Point-to-Point (PTP) device and select **Launch Web Management Application**.

   NOTICE: If PTP certificates are not installed, opening the PTP Web Management Application generates security warnings. For more information on PTP certificates, see the *Private Network Management Client* manual.

The PTP web management application opens with the device details.

5.12.6.3

Warnings Related to PTP Web Management Application

If PTP certificates are not installed and you open the PTP Web Management Application, security warnings are generated. For more information on PTP certificates, see the *Private Network Management Client* manual.

If you try to launch the Web Management Application for a device that does not support it, a warning window appears.

You can launch the Web Management Application only for a single device. If you try to launch the application for multiple devices, a dialog box appears with the following message:

```
Please select only one device.
```

5.12.7

Deleting Network Elements

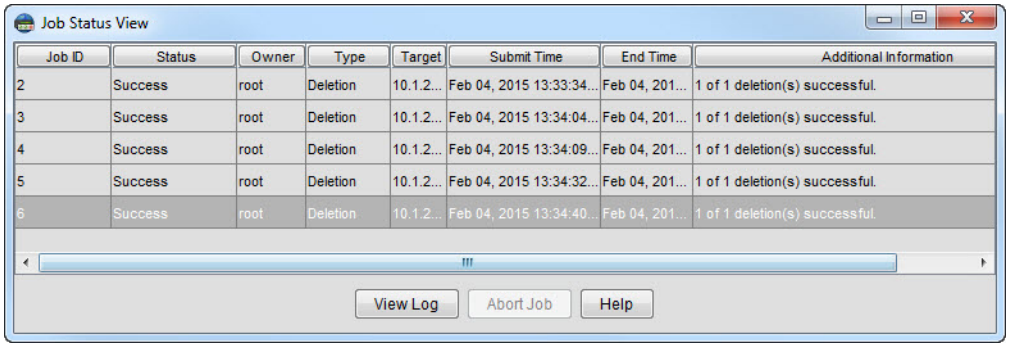
Users assigned to the SuperUser or MotorolaSSC group have the rights to permanently remove a managed resource from UEM. Administrators or MotorolaSSC administrators are allowed to request the deletion of managed resources.

Procedure:

1. In the **Navigation View** panel, click the **Network Database** node.
2. In the **Network Database** view, right-click a manager resource row and select **Delete Object and Traces**.
3. In the confirmation dialog box, click **Yes**.
4. In the **Deletion Status** dialog box, click **View Job Status**.

   A separate job is initiated for each deletion request. The status of the request appears in the **Job Status View** window.
5. In the **Job Status View** window, verify the deletion status.

Figure 43: Job Status View Window



NOTICE: If you delete a single network, the network name appears in the **Target** column in the **Job Status View** window. If you delete multiple networks, **Multiple nodes** message appears in the **Target** column.

If the job status is **Success** or **Completed**, the managed resource or node and the alarms associated with it are also deleted. Events are not deleted, as events are part of the history and they are deleted only when the database is reinitialized.

6 If the **Warning Discovery in progress** dialog box appears, to the view active jobs that are related to the object being deleted, click **Open Job View**.

NOTICE: Once a managed resource is deleted, you cannot restore its alarms.

Job View with the first job highlighted appears.

Postrequisites: If a managed resource was deleted accidentally, to rediscover the managed resource, see Discovering Network Elements on page 198.

5.12.7.1

Deleting Zones or Sites

Procedure:

1 Perform one of the following actions:

If…	Then…
If you want to delete a zone,	go to **System Views → System Map**.
If you want to delete a site,	go to **Zone Views → Zone Map**.

2 Right-click the element you want to delete and select **Delete Object and Traces**.

3 Confirm the operation by clicking **Yes**.

Related Links

Site Operations on page 136
Site Operations on page 136

5.12.7.2

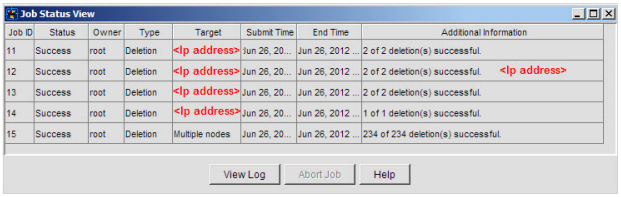
Deleting a Network

Procedure:

1. Navigate to the **Zone Views** → **Physical** → **Physical Summary View/Physical Detail View** window, right-click the managed resource, and select **Delete Object and Traces**.
2. In the confirmation dialog box, click **Yes**.
3. In the **Deletion Status** dialog box, click **View Job Status**.

   A separate job is initiated for each deletion request. The status of the request appears in the **Job Status View** window.
4. In the **Job Status View** window, verify the deletion status.

   Figure 44: Job Status View for Deletion Jobs Window



NOTICE: If you delete a single network, the network name appears in the **Target** column in the **Job Status View** window. If you delete multiple networks, **Multiple nodes** message appears in the **Target** column.

If the job status is **Success** or **Completed** the network, node or device and the alarms and events associated with it are also deleted. If a DMR is deleted, the associated LMR is also deleted. For example, the site is deleted when the active site controller is deleted.

5.12.7.3

Deletion Status

Deletion job status is displayed in the **Job Status View** window.

In progress
The job submission recognized and is in the queue. To determine, whether the job has started executing and to get information about the progress, view the job log.

Success
The deletion job completed successfully. All devices/nodes scheduled for deletion have been deleted. The Additional Comments field and detailed information is available in the job log.

Completed
The deletion job completed, but not all devices/nodes scheduled for deletion have been deleted; during the deletion process, devices/nodes were not present in the database. Detailed information is available in the job log.

Failure
The deletion job failed. The job terminated incorrectly, because a deletion failed for one or more devices/nodes. Detailed information is available in the job log.

5.12.8

Device Commands and Metering

To fault-manage devices and their entities, you can issue commands from Unified Event Manager (UEM) to a device or a specific entity of the device.UEM supports, for example, enable, disable, and

restart commands. After you issue a command, command status is displayed on the status bar or in a created job and UEM receives alarms about the device state change.

5.12.8.1

Issuing Commands from the Alarms Window

Procedure:

1. In the **Navigation View** tree, select the **Alarms** node.
2. In the **Alarms** window, select the alarm for which you want to issue a command.
3. In the main menu, select **Actions** → **Issue Command**.
4. In the **Command** dialog box, perform the following actions:
   a. Select an entity for which you want to issue a command.
   b. Optional: If a list with entity instances is available, select an entity instance.
   c. In the **Available Commands** pane, select a command.
   d. Click **Apply**.

   NOTICE: When you issue a command for entities that do not support diagnostics, a warning message appears.

On the multi-line status bar, the system displays one of the following command statuses:

Execution time
Indicates that the command is being processed: `Sending command`.

Successful command
Indicates that the command status is successful.

Failed command
Indicates that the command status is unsuccessful. A message displays the status as failed and the reasons of failure.

5.12.8.2

Issuing Commands from the Network Database Window

Procedure:

1. In the **Navigation View** tree, select the **Network Database** node.
2. In the **Network Database** window, select the entity for which you want to issue a command.
3. In the main menu, select **Managed Resource** → **Issue Command**.
4. In the **Command** dialog box, perform the following actions:
   a. Select an entity for which you want to issue a command.
   b. Optional: If a list with entity instances is available, select an entity instance.
   c. In the **Available Commands** pane, select a command.
   d. Click **Apply**.

   NOTICE: When you issue a command for entities that do not support diagnostics, a warning message appears.

On the multi-line status bar, the system displays one of the following command statuses:

Execution time
Indicates that the command is being processed: `Sending command`.

Successful command
Indicates that the command status is successful.

Failed command
Indicates that the command status is unsuccessful. A message displays the status as failed and the reasons of failure.

5.12.8.3
Issuing Commands from the Network Element View

Procedure:

1. In the **Navigation View** panel, highlight the **Network Database** node.
2. Double-click a network element.
3. In the **Network Element View** window, expand the **Commands and Metering Information** section.
4. Issue specific commands by clicking relevant buttons.

   A job is created unless the device reports to UEM through a Remote Terminal Unit (RTU).

5.13
Network Database Operations

Network Database serves as an inventory of network resources. It maintains the properties of all the managed resources, including network, physical devices and logical entities. These managed resources and their properties are listed in a tabular format in the Network Database View. Each row in the list corresponds to a managed resource.

For information on configurable aspects on Network Database, see Renaming Managed Resources on page 103.

5.13.1
Viewing Managed Resource Properties

Procedure:

1. In the **Navigation View** panel, click the **Network Database** node.
2. In the **Network Database** window, double-click a managed resource.

The **Managed Resource Properties** window appears, displaying the properties of the network element you selected.

5.13.2
Launching VMware vSphere Client

You can connect to the vSphere client for **ESXi** and **VMware vCenter Server** from the **Network Database** window.

Procedure:

1. In the **Navigation View** panel, highlight the **Network Database** node.
2. In the managed resources list, right-click an **ESXi** or **VMware vCenter Server** resource type.
3. Select **Launch VMware vSphere Client**.

   The **VMware vSphere Client** login window opens.

4 Enter the correct IP address or select one from the drop-down list, if available.

5 Enter the user name and password values, and click **Login**.

The vSphere client launches.

5.13.3
Determining Reliable Communication Capability of a Managed Resource

Some devices managed by Unified Event Manager (UEM) are capable of Reliable Communication. This means that they are able to communicate with UEM sending informs by using a separate SNMP user, that is MotoInform. Devices incapable of Reliable Communication use MotoMaster and communicate by sending traps.

All users can verify if managed resources are capable of Reliable Communication. For more information about Reliable Communication, see Reliable Communication on page 39

Prerequisites: Viewing Managed Resource Properties on page 191

Procedure:

1 In the **Navigation View** panel, click the **Network Database** node.

2 In the **Network Database** window, double-click a managed resource.

3 In the **Managed Resource Properties**, perform the following actions:

a Select the **Others** tab.

b In the **Other Properties** area, search for the **Reliable Comm Capable** property.

If the property value is **true**, the managed resource is capable of reliable communication.

5.13.4
Sites Window

The **Sites** window displays filtered **Network Database** window information and contains all sites within a zone that UEM discovers. For each site, you can view the managed resource (name of the site), severity, subsystem name, and site type information. Severity depicts the overall service status of the site by displaying the highest severity of the current failures for this entity. For more information on the fields displayed, see Managed Resource Properties on page 155.

The status of a site is reported by both the site controller and zone controller. UEM maintains different managed resources to track the site status as reported by the site and the zone controllers. In the **Sites** window, you can see both the site managed resources reported by a site controller and site managed resources reported by a zone controller.

5.13.5
Changing Managed Resource Manager IP Address

The Unified Event Manager (UEM) IP address is the address to which network elements send traps. This IP address is used by managed resources that are Device Managed Resources (DMR). You change the manager IP address before you change the configuration of the Network Address Translation (NAT) protocol.

Procedure:

1 In the **Navigation View** panel, click the **Network Database** node.

2 In the **Network Database** window, double-click a DMR.

3 In the **Managed Resource Properties** window, in the **Manager IP Address** field, modify the IP. Click **Modify**.

5.13.6
Exporting Network Inventory Data

Procedure:

1 In the **Navigation View** panel, click the **Network Database** node, or any custom network database node.

2 Select **Actions** → **Export Topology Data**.

The **Export Topology Data** window appears.

3 Specify a file name for your selection and click **Save**.

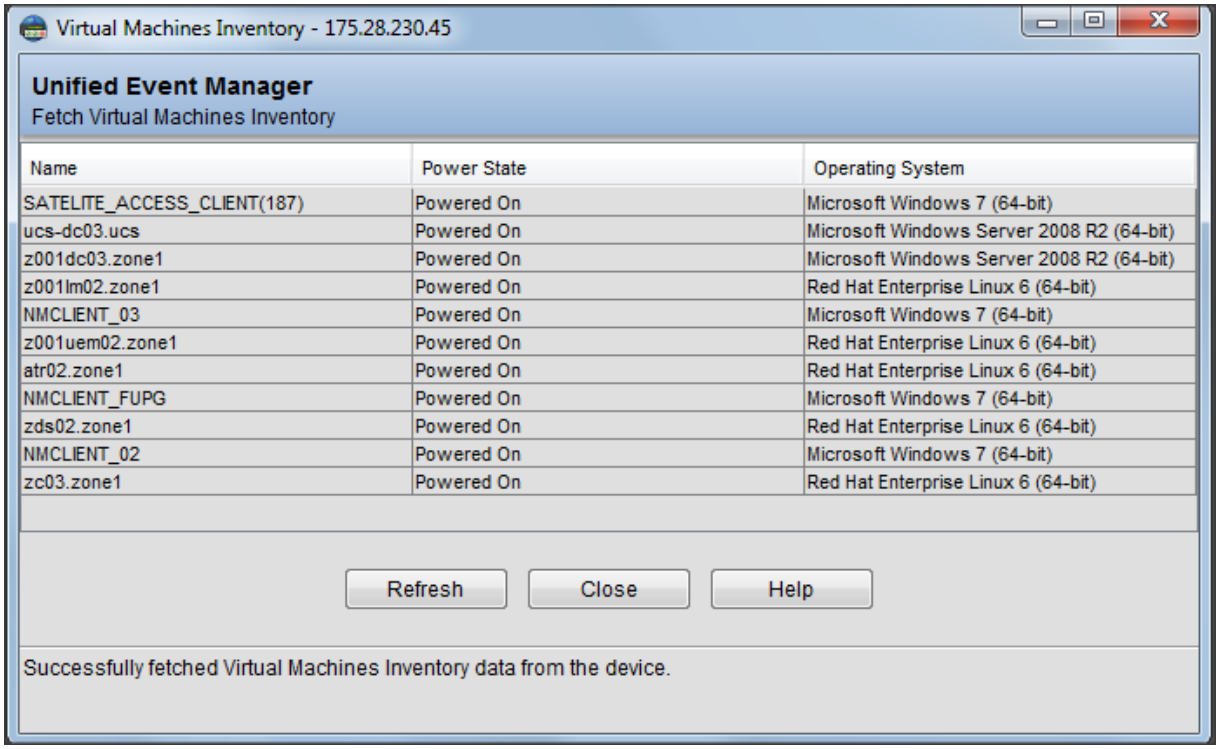
The file is saved to the local client PC.

5.13.7
Application Inventory Operations

For devices that support the application inventory it is possible to view the servers installed on the machine.

The data is retrieved dynamically – it is not necessary to rediscover a device when the displayed values change. Refreshing data can be done by clicking the **Refresh** button in the Application Inventory window.

Figure 45: Application Inventory



Application Inventory View is supported by Generic Application Server (GAS) and ESXi.

5.13.7.1

Viewing Inventory from the Network Database View

Procedure:

1. From the **Network Database** window, select a resource managed by Generic Application Server (GAS).
2. Right-click the resource and click **Show Application Inventory**.

   NOTICE: The location of a particular software application determines the managed resource name. The specific instance of the Generic Application Server software is used as part of the unique service/application name. For example, Zone Controller 01 uses the name `z00Xgas01.zoneX`. The `X` stands for the unique number given to the zone where the Generic Application Server is installed.

The **Generic Application Server Inventory** window appears.

5.13.7.2

Viewing Inventory from the Alarms View

Inventory View is supported by Generic Application Server (GAS) and ESXi and may be invoked from **Network Database** or **Alarms** window.

Procedure:

1. From the **Alarms View** window, select an alarm for an entity that belongs to a device capable of displaying **Application Inventory View**.

   NOTICE: If no such entity exists, use the **Network Database View** to access the Application Inventory. For more information, see Viewing Inventory from the Network Database View on page 194 and Viewing ESXi Inventory from the Network Database View.
2. Select **Actions** → **Show Application Inventory** or press CTRL+I.

   NOTICE: If you use the **Show Application Inventory** option for an entity that does not belong to the device supporting such a feature, a message appears, saying that the operation is not supported. Inventory View is supported by Generic Application Server (GAS) and ESXi.

5.13.8

Viewing ESXi Inventory from the Network Database View

Procedure:

1. In the **Navigation View** panel, click the **Network Database** node.
2. In the **Network Database** window, right-click an ESXi-managed resource and select **Show Application Inventory**

The **Virtual Machines Inventory** window appears.

5.13.9

Asset Management Information Operations

For devices that support asset management information it is possible to view the values of specific properties that describe the versions of software or hardware installed on the device. The data is fetched dynamically, so if any of the displayed values change, the device does not require rediscovery. To refresh the displayed information, in the **Asset Management Information** window, click **Refresh** or reopen Asset Management Information. For more information, see Viewing Asset Management

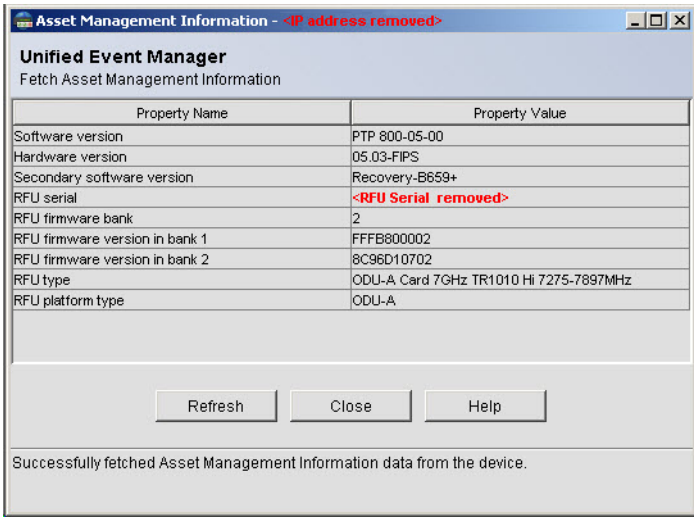
Information from the Alarm View and Viewing Asset Management Information from the Network Database View.

The status of the request is displayed at the bottom of the **Asset Management Information** window and contains information about the status of the acquiring data process.

Devices that support Asset Management Information are:

- Extreme Switches
- Point-To-Point (PTP) devices

Figure 46: Asset Management Information Window



5.13.9.1
Viewing Asset Management Information from the Alarms View

Procedure:

1. From the **Alarms** view, select an alarm for an entity that belongs to the device that is capable of displaying asset management information.

   NOTICE: If such an entity is not available from the **Alarms** view, use the **Network Database** view to see the asset management information. For more information, see Viewing Asset Management Information from the Network Database View on page 195.

2. Select **Actions** → **Show Asset Management Information**.

   NOTICE: If you use the **Show Asset Management Information** option for an entity that belongs to a device that does not support Asset Management Information, a message is displayed saying that the operation is not supported.

The **Asset Management Information** window appears.

5.13.9.2
Viewing Asset Management Information from the Network Database View

Procedure:

1. From the **Network Database** view, select a resource supporting asset management information.
2. Right-click the resource and select **Show Asset Management Information**.

The **Asset Management Information** window appears.

5.14
Synchronization Operations

In a large network, the network administrators store all the details of the device in a centralized database. When a device gets configured, the latest configuration changes must be updated in the database. This synchronization allows data integrity by keeping the latest device details up to date. Periodic synchronization on a device initiates the transfer of all previously unacknowledged state/cause redundant messages. A user-initiated synchronization or synchronization after discovery initiates the network element to send all current state/cause redundant messages. You can see the synchronization state of a device under the **Others** tab in the **Managed Resource Properties** of the device.

5.14.1
Synchronizing Managed Resources

Synchronization is the process in which the status of managed resource alarms is periodically checked. If you do not want to wait for periodic synchronization, you can initiate a synchronization request for the device with the manager. For RTU, the request interrupts the normal synchronization process and checks the status of a particular device. For Zone Controller, a job is created with `Synchronization already in progress`.

Procedure:

1. In the **Navigation View** panel, click the **Network Database** node.
2. In the **Network Database** window, right-click a row and select **Synchronize**.

The managed resource is synchronized. The **Synchronization Job Status** dialog box with a synchronization request summary appears. You can view the job status by clicking **Job Status View**.

5.15
CEN Network Elements Operations

In Unified Event Manager (UEM), network elements in the Customer Enterprise Network (CEN) subsystem must have the IP address of the Network Address Translation (NAT) protocol configured. The NAT IP address configuration is needed for UEM to be able to discover and manage network elements that are in the CEN subsystem.

For network elements in the CEN subsystem, a device managed resource (DMR) is created with the UEM NAT IP address instead of the UEM Radio Network Infrastructure (RNI) IP address. For network elements with subsystem different from CEN, a DMR is created with UEM RNI IP address.

You can configure single CEN network elements manually or you can configure multiple CEN network elements by loading an external NAT IP configuration file to UEM. The NAT IP configuration file is generated by Motorola Solutions Support Center (SSC) per request.

Related Links

Configuring NAT IP for Multiple CEN Network Elements on page 196
Configuring NAT IP for UEM on page 197

5.15.1
Configuring NAT IP for Multiple CEN Network Elements

Follow this procedure for expansion purposes only. In this procedure, you configure the IP address of the Network Address Translation (NAT) protocol of Customer Enterprise Network (CEN) network elements that are not managed by Unified Event Manager (UEM). You configure the NAT IP address in UEM to enable UEM to discover CEN network elements that use the NAT protocol. If the NAT IP

address is not configured in UEM, UEM discovers the network elements but they do not communicate with UEM.

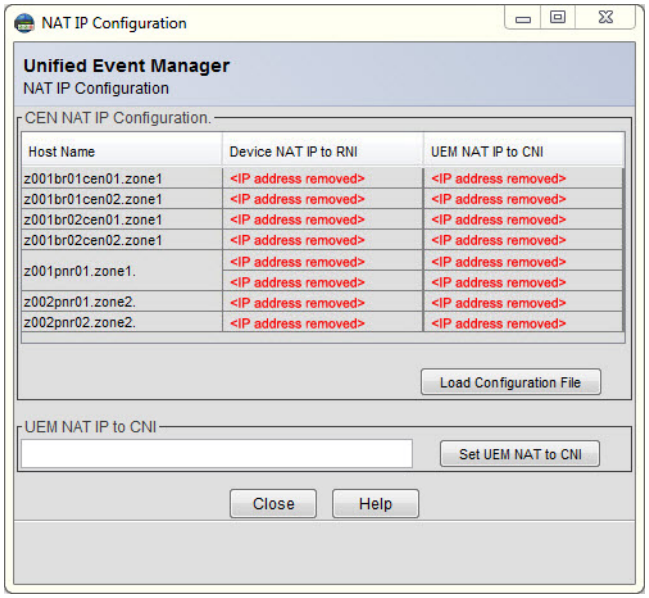
Prerequisites: Contact Motorola Solutions Support Center (SSC) and request the creation of a NAT IP configuration `.xml` file.

Procedure:

1. Save the NAT IP configuration `.xml` file on a PC with network access to UEM and log on to UEM from the PC.
2. In UEM, from the main menu, select **Tools** → **Configure NAT IP**.
3. In the **NAT IP Configuration** window, click **Load Configuration File**.
4. Navigate to the NAT IP configuration `.xml` file you want to load. Click **Open**.

IP addresses necessary for UEM and CEN network elements to communicate are loaded to UEM and appear in the **NAT IP Configuration** window.

Figure 47: NAT IP Configuration Window



Postrequisites: Discover reconfigured network elements to ensure correct communication with UEM.

1. If the reconfigured network elements are already discovered, delete them from UEM.
2. Discover the reconfigured network elements. See Discovering Network Elements on page 198 or Discovering Groups of CEN Network Elements on page 201.

5.15.2
Configuring NAT IP for UEM

Follow this procedure to configure the IP address of the Network Address Translation (NAT) protocol for Unified Event Manager (UEM). You configure the NAT IP address for UEM to enable UEM to discover CEN network elements that use the NAT protocol. If the NAT IP address is not configured for UEM, UEM discovers the network elements but they do not communicate with UEM.

Procedure:

1. From the main menu, select **Tools** → **Configure NAT IP**.

2 In the **UEM NAT IP to CNI** field, type the UEM NAT IP address for the customer enterprise network. Click **Set UEM NAT to CNI**.

IP address necessary for UEM to communicate with CEN devices is displayed in the **UEM NAT IP to CNI** field.

Postrequisites: Discover reconfigured network elements to ensure correct communication with UEM.

1 If the reconfigured network elements are already discovered, delete them from UEM.

2 Discover the reconfigured network elements. See Discovering Network Elements on page 198 or Discovering Groups of CEN Network Elements on page 201.

5.16
Discovery Operations

Discovery is the process of adding network elements to the Network Database. Discovered network elements are fault-managed by Unified Event Manager (UEM) and generate events and alarms. There are two ways of discovering network elements.

Discovering a Single Network Element (Node Discovery)

You can discover a particular network element based on Hostname or IP address. For more information, see Discovering Network Elements on page 198.

Discovering a Group of Network Elements (Subnet Discovery)

You can discover a group of network elements, such as an RF Site, the Primary Zone Core, a Console Site. You can discover what is generally understood as a site, or, in other words, a group of network elements that fulfill a particular function. For more information, see Discovering Groups of Network Elements on page 200.

NOTICE: In systems with Dynamic System Resilience (DSR), network elements in both the primary and the backup zone core are discovered separately. UEMs in different zone cores do not share or exchange information.

Discovering Groups of CEN Network Elements

You can discover a group of Customer Enterprise Network (CEN) network elements that perform a joint function or serve a single purpose.

See Discovering Groups of CEN Network Elements on page 201.

Discovering Tsub Sites

You can discover the network elements in the Trunking Subsystem (Tsub) prime site and remote sites.

See Discovering Tsub Sites on page 202.

You can abort both node discovery and subnet discovery. For more information, see Aborting Discovery Jobs on page 204.

5.16.1
Discovering Network Elements

Discovering a single network element, that is one network element at a time, is sometimes referred to as node discovery. Node discovery operations initiated for a single network element have priority over the subnet discovery option. Thanks to this priority, operators can discover single network elements before the subnet discovery is completed.

Prerequisites:

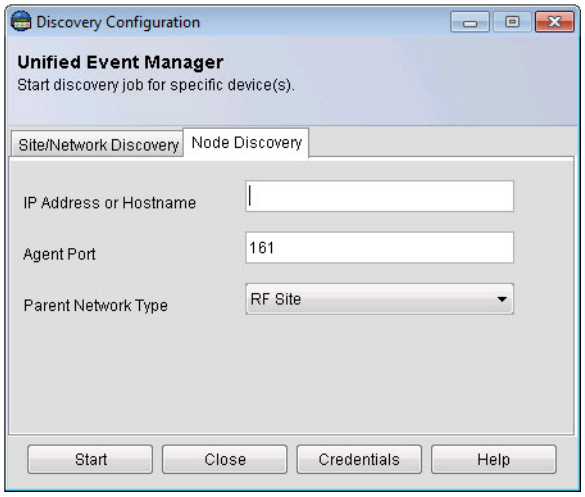
If you want to discover Customer Enterprise Network (CEN) network elements, first configure the IP address of the Network Address Translation (NAT) protocol of single CEN network elements. See Configuring NAT IP for UEM on page 197.

If you want to discover network elements other than CEN network elements, you do not need to perform any prerequisite actions.

Procedure:

1. From the main menu, select **Tools** → **Discovery**.
2. In the **Discovery Configuration** window, click the **Node Discovery** tab.

   Figure 48: Discovery Configuration – Node Discovery

3. In the **Node Discovery** tab, provide discovery credentials:
   a. In the **IP Address or Hostname** field, enter an IP address or hostname of the network element you want to discover.
   b. In the **Agent Port** field, enter an SNMP agent port.

      You can leave the default value unchanged as it applies to most of network elements.
   c. From the **Parent Network Type** list, select the parent network type. Click **Start**.

      NOTICE:
      The Parent Network Type value is used to create the appropriate Network managed resource. It applies when the IP address being discovered is the first node added to UEM in this subnet. The network type that the network element belongs to can be different from the physical location of the network element.

      For example, choose **RF Site** when discovering a base radio at a site that is physically located at the Primary Zone Core.
4. In the **Node Discovery Status** window, click **View Job Status**.

   For each discovery request, a separate job is initiated. You can view jobs statuses in the **Job Status View** window.

In the **Job Status View** window, the status of the discovery is displayed. If the discovery is based on hostname, the **TARGET** column shows the hostname with the IP address appended.

Related Links

Configuring NAT IP for Multiple CEN Network Elements on page 196
Configuring NAT IP for UEM on page 197

5.16.2

Discovering Groups of Network Elements

Discovering a group of network elements is referred to as site discovery. Sometimes one site consists of many networks. You can discover a group of network elements that perform a joint function or serve a single purpose, for example an RF Site, a Console Site, or Dynamic System Resilience (DSR) shared network elements.

For more information, see Groups of Network Elements Managed by UEM on page 42.

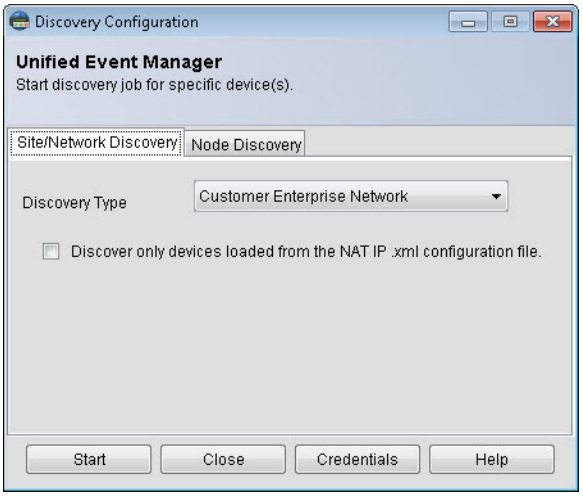
NOTICE: Some network elements discovered automatically do not require management. Check your System Configuration Plan to see the Management column to confirm which network elements are not managed. Remove network elements which are not managed (see Deleting Network Elements on page 187).

The **Discovery/Rediscovery** operation initiated for a single network element by using the **Node Discovery** option has higher priority over the **Site/Network Discovery** option. This is done so that the discovery of single network elements is performed before discovery of large numbers of network elements in functional groups.

Procedure:

1 From the main menu, select **Tools** → **Discovery**.

Figure 49: Discovery Configuration – Site/Network Discovery



2 In the **Discovery Configuration** window, from the **Discovery Type** list, select a site type. See Groups of Network Elements Managed by UEM on page 42.

- If in the **Site/Network Discovery** tab, there are no discovery type parameters available to set for the discovery type of your choice, click **Start**.
- If in the **Site/Network Discovery** tab, there appeared discovery type parameters to set for the discovery type of your choice, enter the parameters based on Discovery Type Parameters on page 203. Click **Start**.

UEM constructs the range of IP addresses for the selected discovery type. This operation depends on the system IP and the site identifier, if any, provided by the user. UEM attempts to discover all IP addresses (network elements) within the subnet, even though some network elements may not exist in the network.

3 In the **View Job Status** window, click **View Job Status**.

The **Job Status View** window appears, displaying the status of the subnet discovery.

5.16.3

Discovering Groups of CEN Network Elements

Discovering a group of network elements is sometimes referred to as subnet discovery. You can discover a group of Customer Enterprise Network (CEN) network elements that perform a joint function or serve a single purpose.

For more information, see Groups of Network Elements Managed by UEM on page 42.

NOTICE: Some network elements discovered automatically do not require management. Check your System Configuration Plan to see the Management column to confirm which network elements are not managed. Remove network elements which are not managed (see Deleting Network Elements on page 187).

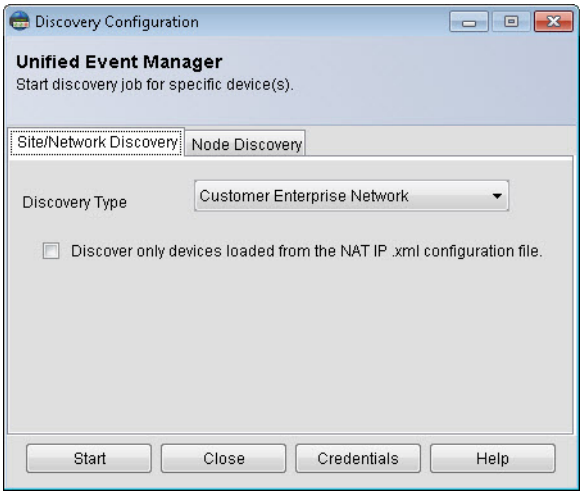
The **Discovery/Rediscovery** operation initiated for a single network element by using the **Node Discovery** option has higher priority over the **Site/Network Discovery** option. This is done so that the discovery of single network elements is performed before discovery of large numbers of network elements in functional groups.

Prerequisites: Configure NAT IP for multiple CEN network elements. See Configuring NAT IP for Multiple CEN Network Elements on page 196.

Procedure:

1 From the main menu, select **Tools** → **Discovery Configuration**.

Figure 50: Discovery Configuration – Site/Network Discovery



2 In the **Discovery Configuration** window, from the **Discovery Type** list, select**Customer Enterprise Network** and perform the following actions:

- To discover network elements defined in your System Configuration Plan, click **Start**.
- To discover only CEN network elements loaded from the NAT IP configuration `.xml` file, select the **Discover only network elements loaded from the NAT IP .xml configuration file** check box. Click **Start**.

UEM constructs the range of IP addresses for the CEN discovery type. UEM attempts to discover all IP addresses (network elements) within the CEN subnet, even though some network elements may not exist in the network.

3 In the **View Job Status** window, click **View Job Status**.

The **Job Status View** window appears, displaying the status of the subnet discovery.

Related Links

Configuring NAT IP for Multiple CEN Network Elements on page 196
Configuring NAT IP for UEM on page 197

5.16.4

Discovering Tsub Sites

A Trunking Subsystem (Tsub) consists of the Tsub prime site and remote sites supporting any of the following site types:

- Centralized Conventional Site
- Console Site (NM/Dispatch Site)
- RF sites:
  - ASTRO® 25 Site Repeater (ASR) site
  - High Performance Data (HPD) Site
  - IP Simulcast Subsite

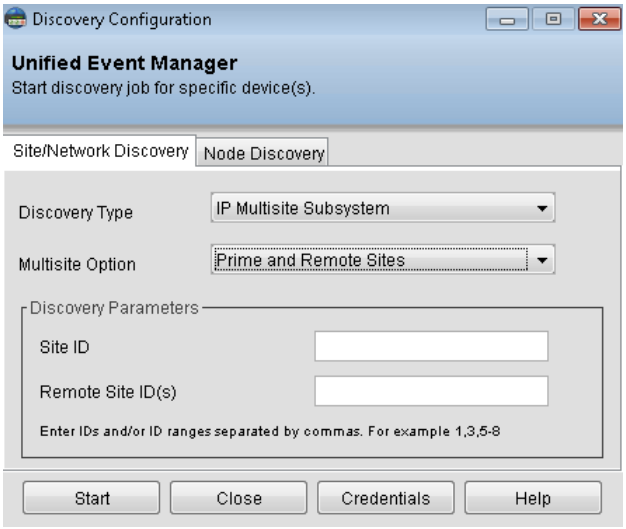
The discovery type used when discovering the site types listed above will differ from what is used in non-Tsub deployments. For the Tsub prime site and remote sites discovery, the **IP Multisite Subsystem** discovery type is used.

For proper discovery, all devices in the Tsub must have the sysName correctly configured and devices that require hostname configuration must be configured as well. This information is utilized during discovery to properly present sites in the Navigation View. The Navigation View conveys which sites reside outside of the Tsub and which sites reside inside the Tsub. In addition, the Tsub ID is presented in the view.

Procedure:

1. From the main menu, select **Tools** → **Discovery**.
2. On the **Site/Network Discovery** tab, from the **Discovery Type** list, select the **IP Multisite Subsystem** type.

   Figure 51: Discovery Configuration – Site/Network Discovery



3. From the **Multisite Option** list, select **Prime and Remote Sites**.
4. In the **Discovery Parameters** section, enter the correct parameters:

For more information, see Discovery Type Parameters on page 203.

a In the **Site ID** field, enter the the Tsub prime site ID.

b In the **Remote Site ID(s)** field, enter the Tsub remote site IDs.

You can enter multiple IDs or ID ranges separated by commas.

Step example: 1,3,5-8

c Click **Start**.

5 In the **View Job Status** window, click **View Job Status**.

The **Job Status View** window appears, displaying the status of the subnet discovery.

5.16.5
Discovery Type Parameters

Discovery Type Parameters are parameters for each discovery type. If you select a particular discovery type, some parameters are disabled (you cannot select any values for them). Other parameters have a limited range of values.

Table 33: Discovery Type Parameters

DiscoveryType	Zone ID	MultiSite Options	SiteID	Remote Site IDs
RF Site	unavailable	unavailable	1–150	unavailable
IP Multisite Subsystem	unavailable	Prime Site	1-64	unavailable
		Prime and Remote Sites	1-64	1-32
		Remote Site	1-64	1-32
Circuit Multisite Subsystem	unavailable	Prime Site	1-64	unavailable
		Prime and Remote Sites	1-64	1-15
		Remote Site	1-64	1-15
Console Site	unavailable	unavailable	1001-1191 or 1227-1230	unavailable
Primary Zone Core	unavailable	unavailable	unavailable	unavailable
Backup Zone Core	unavailable	unavailable	unavailable	unavailable
Primary Operations Support Systems	unavailable	unavailable	unavailable	unavailable
Backup Operations Support Systems	unavailable	unavailable	unavailable	unavailable
DSR Shared Network Devices	1-7	unavailable	unavailable	unavailable

Table continued…

DiscoveryType	Zone ID	MultiSite Options	SiteID	Remote Site IDs
Conventional Subsystem	unavailable	unavailable	1-47 Parameter name changes to Conventional Subsystem ID	1-255 Parameter name changes to Conventional Location ID
Backhaul Subsystem	unavailable	unavailable	unavailable	unavailable
Customer Enterprise Network	unavailable	unavailable	unavailable	unavailable

NOTICE:
UEM arrives at the list of device IPs or a range of IPs for the selected discovery type, based on the system System Configuration Plan. Provide the required information.

UEM attempts the discovery of all IP addresses, based on the list of device IP addresses derived from the System Configuration Plan. However, some IP addresses (devices) may not exist in the network. Check the Discovery Logs by selecting the Discovery Job in the Job Status View. It allows you to view details on IP addresses that are discovered and IP addresses that are not reachable. Confirm that IP addresses that are not reachable are not configured in the network. Check the network plan or execute an Internet Control Message Protocol (ICMP) ping on the unreachable IP addresses.

Related Links

Discovering Groups of Network Elements on page 200
Discovering Tsub Sites on page 202

5.16.6

Aborting Discovery Jobs

Procedure:

1. In the **Navigation View** panel, expand the **Job Status View** node.
2. Select a row with the discovery job you want to abort.

   If the selected job type is **Discovery** and its status is **In Progress**, the abort job option becomes active.
3. Click **Abort Job**.
4. In the confirmation dialog box, click **Yes**.

   NOTICE: Selected devices awaiting discovery are not discovered. Selected devices already processed are discovered with appropriate status (discovered, failed, or unreachable). Job status is set to `Aborted` if at least one device discovery is aborted during the operation.

Job status changes to `Aborting`.

5.16.7
Discovery Status

The status of a discovery job is displayed in the **Job Status View** window. Status messages include:

In progress
The job submission has been recognized and is in the queue. To determine if the job has started executing and to get information on the progress, view the job log.

Aborting
An authorized user has chosen to abort an unfinished discovery job. Discovery of devices awaiting in the queue is being aborted. Discovery of devices for which discovery process was initiated continues without any interruption. Job log contains details about status of each device (represent by IP address).

Success
The discovery job has completed successfully. One or more devices may still have not been found due to communication failures. This information is shown in the **Additional Information** field and detailed information is available in the job log.

Completed
The discovery job is complete but no devices defined for the discovery were available. Detailed information is available in the job log.

Failure
The discovery job has failed. The job has terminated abnormally. The job log provides additional details and it is necessary for the user to re-submit the job at a later time.

Aborted
An authorized user has aborted the discovery job. At least one device discovery was aborted. The **Additional Information** field contains detailed information about the number of discovered, failed, unreachable, and aborted devices.

After the job is complete, select the job and click **View Log**. Check the discovery logs for details on IP addresses that were discovered and IP addresses that are not reachable. Confirm that IP addresses that are not reachable are indeed not configured in the network. Check the network plan or, by executing an Internet Control Message Protocol (ICMP), ping on the unreachable IP addresses.

When you choose to abort a discovery job, the status is initially set to `Aborting`.

- If UEM aborts the job, status is set to Aborted.
- If UEM initiated discovery of some devices in the selected job, the status is set to Failure or Success. View the log for more details.

Summary information about the number of discovered, failed, unreachable and aborted jobs can be found in the Additional Comments column.

5.17
Performance Management Operations

Performance management includes all procedures necessary to monitor and collect information on devices fault managed by Unified Event Manager (UEM).

NOTICE: To avoid loss of functionality, only Motorola Solutions Support Center (SSC) personnel should edit configuration. You can perform the procedures in Enabling Collections on page 210 and Disabling Collections on page 211.

5.17.1

Viewing Configured Collections for a Device

The **Configured Collection** panel displays the list of statistics configured for a data collection. Based on the defined statistics, Unified Event Manager (UEM) collects the data from a device.

Procedure:

1. From the **Navigation View** panel, select **Performance** → **Configured Collection**.

   The **Configured Collection** window appears on the right-hand side of the panel, showing all the configured statistics for the selected device. The **Hosts** column lists all the devices on the network that are configured for data collection.

2. To view the list of statistics for a host, select the host from the **Host** column in the left panel.

   The statistics for the selected host are displayed in the right-hand column.

3. Double-click any statistic to view details for that statistic.

The **Data Collection Detailed Properties** window appears.

Postrequisites:
For information on searching in configured collections, see Searching Configured Collections on page 211.

For a list of properties and descriptions of the statistics information shown on the right-hand side of the panel, see Statistic Properties on page 206.

For a list of fields and descriptions of the object details displayed in the **Data Collection Detailed Properties** window, see Data Collection Detailed Properties on page 207.

5.17.2

Statistic Properties

Name
A unique name (string) to identify the statistic.

ID
A unique number generated automatically and associated with each statistic.

DNS Name
Host name (device name).

OID
A unique identification number of the device interface.

Community
The community used when sending the SNMP request for collecting the statistic.

Period
The interval at which data is collected for the statistic. For example, the value 300 indicates that data is collected every 300 seconds.

Active
Specifies whether data collection for the selected device is active or not. The possible values are true or false. If it is false, data collection is not performed for that device.

Multiple
Specifies the type used to poll columnar value of the tables.

User Name
One of the credentials required for querying SNMPv3 devices.

SNMP
Simple Network Management Protocol (SNMP) version of the device.

Context Name
One of the credentials required for querying SNMPv3 devices.

5.17.3
Data Collection Detailed Properties

Table 34: Data Collection Detailed Properties

Object Details Field	Description
Name	Specifies the name of the statistic.
	For example, if the statistic name is specified as `interface_in_octets`, then only devices with that statistic are displayed in the custom view.
	Specify multiple statistic names as comma-separated values. For example, `interface_in_octets`, `interface_out_octets`.
snmpVersion	Specifies the SNMP agent version, such as v1, v2, v3 data is collected from.
Username	User name of the user.
Context Name	Specifies the name for the custom view you are creating or modifying. If no value is specified in this field, default values such as `Configured Collection0`, `Configured Collection1`, or `Configured Collection2` are created.
agent	Specifies the agent name.
	For example, if the agent name is specified as `Node1agent`, then only statistics from the data that is collected from that agent is displayed.
port	Specifies the port number from which the agent is listening for data collection requests. **NOTICE:** The default SNMP agent port is 161.
ID	Specifies the Poll ID.
oid	Specifies the object identifier as reported by the SNMP agent.
active	Specifies whether a data collection for a selected device is active or not. Possible values are true or false. If the value is false, data collection is not available for the device.
period	Specifies the polling interval.
	Example: If the period is specified as 2, then the statistics that have been scheduled for data collection every 2 seconds are displayed.
threshold	Specifies whether to display data, based on the thresholds set.
	`All`: Displays all statistics, with and without thresholds.
	`True`: Displays only those statistics which have thresholds associated.
	`False`: Displays only those statistics which do not have thresholds associated.
DNS Name	Specifies the host (node).

Table continued…

Object Details Field	Description
	Example: If the dnsName is specified as `test-machine`, then all statistics pertaining to test-machine are displayed.
Last Counter Value	Specifies a numeric value. Those statistics (counter type OIDs only) whose last collected value equals the value specified are displayed.
lastTimeValue	The time at which the data collection was scheduled for in the previous cycle.
timeVal	The time at which the data collection is scheduled for in the subsequent cycle.
Policy Name	The default PollingObject name.
Save	A check box to enable or disable the save function.
Log File	Specifies a log filename (string), based on the statistics you want to display.
Parent Object	Specifies the name of the managed object whose statistics you view.
Threshold List	Specifies the name of the thresholds in comma-separated format.
Failure Count	Specifies the failure count as a numeric value.
	Example: If the failure count is set as 2, all statistics whose failure count is set as 2 are displayed.
protocol	Specifies the name of a protocol.
	Example:`SNMP`, `TL1`.
groupName	Specifies the group.
Save Poll Count	Specifies the save poll count (numeric value). All statistics with the specified save poll count are displayed.
Failure Threshold	Specifies the save failure threshold value (numeric value). All statistics with the specified failure threshold value are displayed.
Is Multiple Polled Data	Specifies the type used to poll the column value of the tables.
	`True`: Displays only those statistics which are of type MultiplePolledData.
	`False`: Displays statistics other than MultiplePolledData.
	`All`: Displays all statistics, irrespective of their type (node, interface, multiple).
Save On Threshold	Possible values are `true` or `false`. A true value indicates that the collected data is saved only when it exceeds the threshold. **NOTICE:** The default value is `false`.
ownerName	A string to denote the owner of the statistic.
timeAvg	Possible values are `true` or `false`. Calculated for Counter type OIDs. The collected data is an incremental value. At one point, it reaches the final value and resets to zero. As this reset happens soon and often, it is preferred that a delta value is derived from two consecutive polls. **NOTICE:** The default value is `false`.

5.17.4
Statistics Operations

Unified Event Manager (UEM) allows you to add, remove, and modify a statistic. However, you can add a statistic only if you are a member of Motorola Solutions Support Center (SSC) personnel.

IMPORTANT: Do not edit any fields in the Statistic Properties user interface. You can only perform the following actions:

- Enable or disable collection (the **Active** field of the Statistics Properties Table)
- Modify the collection interval (the **Period** field of the Statistics Properties Table)

5.17.4.1
Adding Statistics

Procedure:

1. In the main navigation tree, select **Performance** → **Configured Collection**.

   The **Configured Collection** window appears on the right-hand side of the panel, displaying all configured devices.

2. In the main menu, select **Edit** → **Add Statistic** or press CTRL + K.

   The **Object Details** dialog box appears.

3. Specify appropriate values in the fields and click **Next**.

   NOTICE: For information on each of the fields, see Viewing Configured Collections for a Device on page 206.

4. Optional: Add more properties by performing the following actions:

   a. In the **Object Details** dialog box, click **Additional Props**.

      The **Polled Data Additional Properties** dialog box appears.

   b. In the **Property Name** and **Value** fields, specify the property name and its value respectively.

5. Optional: In the **Polled Data Additional Properties** dialog box, add a property by clicking **More**.
6. Optional: In the **Polled Data Additional Properties** dialog box, remove rows of properties by clicking **Fewer**.
7. Optional: In the **Polled Data Additional Properties** dialog box, remove a property by selecting the property and clicking **Remove**.
8. Finish adding a new statistic by clicking **OK**.

In the **Configured Collections** panel, the statistic added for the device is displayed.

5.17.4.2
Modifying Statistics

Procedure:

1. From the main navigation tree, select **Performance** → **Configured Collection**.

   The **Configured Collection** window appears on the right-hand side of the panel, displaying all configured devices.

2 Select the statistic that you want to modify and select **Edit** → **Modify Statistic** or press CTRL + SHIFT + M.

   The **Object Details** dialog box appears.

3 Make appropriate changes. For information on each of the fields, see Viewing Configured Collections for a Device on page 206.

4 Click **Modify**.

The modifications are immediately applied to the statistic.

5.17.4.3
Removing Statistics

If you want to stop the data collection for a statistic temporarily, do not delete the statistic. Instead, you can disable (uncheck) the Active property of the statistic, temporarily stopping data collection for the device. You can check the Active property to enable data collection in the future.

Procedure:

1 From the **Navigation View** panel, select **Performance** → **Configured Collection**.

2 In the **Configured Collection** window, select the statistic that you want to delete.

3 From the main menu, select **Edit** → **Remove Statistic**.

4 In the confirmation dialog box, click **Yes**.

User properties associated with the statistics are deleted.

5.17.5
Enabling Collections

You can enable the data collection for a particular statistic during runtime.

Procedure:

1 From the main navigation tree, select **Performance** → **Configured Collection**.

   The **Configured Collection** window appears on the right-hand side of the panel, displaying all configured devices.

2 In the **Hosts** column, select the host that you want to enable.

3 Double-click the row a statistic that you want to enable.

   The **Object Details** window appears.

4 In the **Object Details** window, select the **Active** check box.

5 Click **Modify**.

Data collection for the selected device is enabled.

5.17.6

Disabling Collections

You can disable the data collection for a particular statistic during runtime.

Procedure:

1. From the main navigation tree, select **Performance** → **Configured Collection**.

   The **Configured Collection** window appears on the right-hand side of the panel, displaying all configured devices.

2. From the **Hosts** column, select the collection that you want to disable.
3. Double-click the row with a statistic that you want to disable.

   The **Object Details** window appears.

4. In the **Object Details** window, clear the **Active** check box.
5. Click **Modify**.

Data collection for the selected device is disabled.

5.17.7

Searching Configured Collections

You can search configured collections and view the statistics of individual devices. You can search configured collections by any of the statistics properties.

Procedure:

1. From the main navigation tree, select **Configured Collection**.
2. From the menu bar, select **View** → **Search**.

   The **Search** window appears.

3. Select a parameter.

   Step example: You can select **Name**, **ID**, **DNS Name**, and so on.

   NOTICE: You can also specify if the selected parameter starts with the name or ends with the name, and so on.

4. In the text field, enter your search phrase.

   NOTICE: If you want to include any of the following characters in your search, enter a backslash \ before the character: `, \ * % _`

5. Click **Search**.

The **Configured Collection** lists the statistics that match your search.

Postrequisites: To view a table of the parameters, see Viewing Configured Collections for a Device on page 206.

5.17.8

Plotting Collected Statistics

Follow this procedure to view a graph for the collected data within a certain date range. You can view the collected data (statistics) by using graphs and tables. They help to analyze the statistics gathered over a long period.

Procedure:

1. From the **Navigation View** panel, select **Performance** → **Configured Collection**.
2. In the **Configured Collection** window, in the **Host** column, click the host for which you want to plot collected statistics.

   The hosts are displayed on the right-hand side.
3. Right-click the row for which you want to plot collected statistics and from the main menu, select **Show Collected Statistic**.
4. Optional: In the **Collected Graph Viewer** window, change the chart type by clicking a chart icon of your choice.

   You can also view the collected data in the form of a table by selecting **Table**.

   NOTICE: By default, the line chart graph type is displayed. You can change the chart type to any of the following types:

   - Line chart
   - Bar chart
   - Area chart
   - Scatter chart
   - X-Y chart
   - Table
5. In the **Date Range Settings** area, select a date range. Click **Plot Chart**.
   - To view the graph for the last 24 hours, select the **Last 24hrs** option button.
   - To view the graph for today, select the **Today** option button.
   - To view the graph for data collected over the last seven days, select the **Last one week** option button.
   - To view a graph for a specific period, select the **Custom** option button and specify the dates in the **From** and **To** fields.

   The custom date range can be displayed for the period of 30 days or less. If you set a custom date range that is longer than 30 days, no statistics are displayed.
6. Optional: Save your plotted graph locally to a `.png` file by clicking **Save**  .

The graph appears along with a legend. The legend lists object identifiers (OIDs) that are unique identification numbers of the interface of a managed resource.

5.17.9

Plotting Current Statistics

Plotting current statistics (performance data) helps to view the updated data. In the collected statistics, only the past data is displayed and it is not updated. The current statistics are instantly collected from

the device and plotted in graphs. On request, Unified Event Manager (UEM) queries the devices and collects the data. You can view the current data (statistics) by using graphs or tables.

Procedure:

1. From the **Navigation View** panel, select **Performance** → **Configured Collection**.
2. In the **Configured Collection** window, in the **Host** column, click the host for which you want to plot current statistics.

   The hosts are displayed on the right-hand side.
3. Right-click the row for which you want to plot current statistics and from the main menu, select **Show Current Statistic**.
4. Optional: In the **Current Graph Viewer** window, change the chart type by clicking a chart icon of your choice.

   You can also view the current data in the form of a table by selecting **Table**.

   NOTICE: By default, the line chart graph type is displayed. You can change the chart type to any of the following types:

   - Line chart
   - Bar chart
   - Area chart
   - Scatter chart
   - X-Y chart
   - Table
5. Optional: Define how often data is gathered for the statistics by setting the **Polling interval** value.

   You can set the **Polling interval** value to 10 seconds or higher.

   Step example: Set the **Polling interval** value to 30 seconds to gather data for a managed resource statistics every 30 seconds.

   NOTICE: The number and frequency of the statistics data actually gathered depend both on UEM performance and on the device from which the data is retrieved. These values may differ from the ones set by the user.
6. Optional: Stop the process of gathering data for statistics by clicking **Stop Poller**  . To start the process again, click **Start Poller**  .
7. Optional: Clear your plotted graph by clicking **Clear Graph**  .

   Current statistics are collected all the time. With the **Clear Graph** option, you can clear the gathered data and start gathering statistics from a specific period.
8. Optional: Save your plotted graph locally to a `.png` file by clicking **Save**  .

The graph appears along with a legend. The legend lists object identifiers (OIDs) that are unique identification numbers of the interface of a managed resource.

5.17.10

Zooming in on Plotted Graphs

Unified Event Manager (UEM) allows you to zoom in on a graph for a better view. You can zoom in on one axis or on both axes of the graph, that is the Domain Axis and Range Axis.

Procedure:

Right-click the graph and select **Zoom In**:

- To zoom in on both axes, select **Both Axes**.
- To zoom in on the domain axis, select **Domain Axes**.
- To zoom in on the range axis, select **Range Axes**.

The axis or axes are zoomed in according to your requirements.

5.17.11

Zooming out on Plotted Graphs

Unified Event Manager (UEM) allows you to zoom out on a graph for a better view. You can zoom out on one axis or on both axes of the graph, that is the Domain Axis and Range Axis.

Procedure:

Right-click the graph and select **Zoom Out**:

- To zoom out on both axes, select **Both Axes**.
- To zoom out on the domain axis, select **Domain Axes**.
- To zoom out on the range axis, select **Range Axes**.

The axis or axes are zoomed out according to your requirements.

5.17.12

Viewing Performance Status of Managed Resources

You can view the performance status of a managed resource.

The following periods of time are available:

- Today
- Last 7 days
- Last 30 days
- Custom

NOTICE: Only nodes in the hosts section of the **Configured Collection** display are shown in this view.

Procedure:

1. From the main menu, select **Administration** → **System Administration**.
2. In the **Module Details** section, click **Performance Status**.
3. In the **Node Name** field, type the name of the device and click **View Status**.
4. Optional: View the performance status of a device for a period of time:
   a. In the **Period** field, select **Custom**.

      The **Start Date** and **End Date** text boxes are enabled.

b In the **Start Date** and **End Date** text boxes, select the dates and click **View Status**.

The **Performance Status Report** screen with the following details appears:

- Statistic name
- Data collection status
- Last collection time
- Next collection time

5.18

Associated Managed Resources Operations

To get a better idea of a fault that affects one or multiple devices or their particular components, you can filter the **Network Database** view to display only the associated objects, based on the selected alarms in the **Alarms** view or managed objects in the Network Database. When the list of managed resources is narrowed down only to the associated objects, fault tracking becomes easier.

The following rules define which elements are associated:

- All elements inside a subnet are related to a network element but not the other way round. For example, when you view associated managed resources for a network element, all devices that are located in the same network are displayed. However, when you view associated managed resources for a device, the network is not displayed.
- Generic SNMP Nodes, which represent IP managed devices, are associated only to a network they belong to.
- Device Managed Resources (DMR) are associated via redundancy groups. If two or more DMRs belong to the same redundancy group, they are considered associated.
- Two or more DMRs are associated if they belong to the same Ethernet Automatic Protection Switching (EAPS) domain, that consists of devices supporting EAPS.
- Logical Managed Resources (LMR) are related to DMRs that they belong to. When you view associated managed resources for an LMR, the DMR that the LMR belongs to is displayed. When you view associated managed resources for DMR, all LMRs that belong to this DMR are displayed.
- Group Managed Resourced (GMR) are related to DMRs and LMRs. When you view associated managed resources for a GMR, the GMR and all related LMRs and DMRs are displayed.
- Once a related element is displayed, all associated elements are also displayed.

5.18.1

Viewing Associated Managed Resources from the Network Database Window

Procedure:

1 In the **Navigation View** panel, click the **Network Database** node.

2 In the **Network Database** window, select one or multiple elements.

3 Right-click the selection and select **View Associated Managed Resources**.

In the **Network Database** window, a temporary custom view containing the associated managed resources appears.

5.18.2
Viewing Associated Managed Resources from the Network Events Window

Procedure:

1. In the **Navigation View** panel, highlight the **Network Database** node.
2. Right-click a specific resource.
3. Select **View Managed Resource Events**.
4. In the **Network Events** window, right-click a specific resource.
5. Select **View Associated Managed Resources**.

   A **Network Database** window containing all associated managed resources opens.

5.18.3
Viewing Associated Managed Resources from Maps

Procedure:

1. Navigate to the desired map:

If…	Then…
If you want to view associated managed resources for the Zone Map,	In the **Navigation View** panel, go to **Zone Views** → **Zone Map**.
If you want to view associated managed resources for the Physical Map,	**a** In the **Navigation View** panel, go to **Physical** → **Physical Summary View/Physical Detail View**. **b** Right-click a selected element and click **View Device(s)**. The **Network Database** window appears.
If you want to view associated managed resources for the Service Map,	**a** In the **Navigation View** panel, go to **Service** → **Service Summary View/Service Detail View**. **b** Right-click a selected element and click **View Device(s)**. The **Network Database** window appears.

2. Right-click a specific managed resource.
3. Select **View Associated Managed Resources**.

   A **Network Database** window containing all associated managed resources opens.

5.19
Unknown Devices

An unknown device is a device whose device type is unrecognizable, or a device that does not have a Simple Network Management Protocol (SNMP) agent running. These devices are discovered as generic nodes.

5.20
Generic SNMP Node, Switch and Router

If a device responds to Simple Network Management Protocol (SNMP) but the **sysObjectID** value (starting from 1.3.6.1.4.1.) does not match any device supported explicitly by UEM, such device falls into one of three generic categories.

Generic SNMP Router
Managed by UEM as any other **Transport** device (for example, a HP Switch). It synchronizes ports and interfaces of all types.

Generic SNMP Switch
Managed by UEM as any other **Transport** device (for example, a HP Switch). It synchronizes only Ethernet ports and interfaces.

Generic SNMP Node
Managed by UEM as a **GenericNode** device type, however, it uses the SNMP protocol instead of Internet Control Message Protocol (ICMP) to periodically check if the device is alive.

Otherwise the device is discovered as a Generic Node and managed using ICMP.
Generic SNMP Switch and **Generic SNMP Router** devices generate **Equipment Alarms** only if standard **linkUp** or **linkDown** traps are received. All other traps are handled as **Informational Events**.

For **Generic SNMP Node** all traps are handled as **Informational Events**.

You can manually change the automatically assigned generic categories. Changing the category requires a rediscovery operation. If during the rediscovery process the device is recognized as explicitly supported by UEM, the generic category is ignored and a specific category is assigned.

5.21
Security Management Operations

Security is the assurance of legitimate use, maintenance of confidentiality, data integrity, and ability to audit the Network Management operations. It involves identifying the assets, threats, and vulnerabilities of the system. As a result, you can take protective measures against unintended use of the system. The Security Administration module enables you to manage security information. Different users can perform different security operations, depending on their permissions.

This section helps the administrator to create new users, or new groups of users, enabling the administrator to control the different security levels. New users, or new groups of users are allowed to see only selected information.

After logging on, all the operations available to you are based on your group. Therefore, user administration is a prime function of the administrators.

The following functions can be managed under Security Management:

- Providing group-based authorization where users can be assigned to groups that have configured levels of access, and that provides only specific functions to them.
- Providing fine-grained access control for specific groups, views, and operations.
- Limiting the access for some users to specific subsets of objects or instances (for example, user access can be limited to a specific device).
- User activity log, called Audit Trails, containing:

- Operations invoked by the user.
- The name of the user who invoked the operation.
- Data and time of invocation.
- Target device/object on which the operation was invoked.
- The status of the operation.
- The category of invoked operation.

For information about tasks related to security management, see the following sections:

- Audit Trails Operations on page 218
- Groups Operations on page 220
- Users Management on page 228
- Operations Management on page 233

5.21.1

Audit Trails Operations

Audit trails enable you to view the operations performed in Unified Event Manager (UEM).

The audit trail identifies all operations that have been performed, displaying also:

- The time
- Whether the audit was successful
- The category
- The audited object
- User name
- Operation name

Clear the trails after they have been reviewed.

You can perform the following operations:

- View the audit trail details of all the users or a single user.
- Sort the details by user, operation, time, status, category, and audited object, by clicking the appropriate column heading.
- Search for audit details, based on the properties.
- Clear the audit trails when you no longer want to manage them.

Related Links

Alarms Ownership on page 174

5.21.1.1

Viewing Audit Trails for All and Single Users

You can view various operations performed by the users, along with the status of whether the operation was a success or failure. You can view the operation categories such as Fault, Topo, Provisioning, Configuration, or DEFAULT. For operations that involve adding objects, such as the **Add Node** operation, you can also view object details.

Procedure:

1. From the main menu, select **Administration** → **Security Administration**.
2. In the **Security Administration** window, perform one of the following actions:

If…	Then…
If you want to view Audit Trails for all users,	from the main menu select **View** → **Audit Trails**
If you want to view Audit Trails for single users,	Perform the following actions: **a** Expand the **Users** node. **b** Click the user

3 Optional: In the **Audit Screen** window, sort audit trails:

- To sort all audit trails, click a column header.
- To sort only the audit trails that are currently displayed, click a column header while holding CTRL.

4 Optional: Clear an audit trail by selecting an audit entry and clicking **Clear Audit**.

- To select a single audit trail, click it.
- To select contiguous audit trails, hold SHIFT and click audit trails.
- To select non-contiguous audit trails, hold CTRL and click audit trails.
- To view new records, click **Refresh**.

5.21.1.2
Viewing Audit Trails on the UEM Client Web Interface

Procedure:

1 From the main menu, select **Administration** → **System Administration**.

The UEM client web interface appears.

2 In the **System Administration** panel, click the **Audit Trails** icon.

5.21.1.3
Searching Audit Trails

Procedure:

1 From the main menu, select **Administration** → **Security Administration**.

2 In the **Security Administration** window, perform one of the following actions:

- To search audit trails for all users, from the main menu, select **View** → **Audit Trails**.
- To search audit trails for a specific user, expand the **Users** node, right-click a user and select **Audit Trails**.

3 In the **Auth Audit** window, select **Edit** → **Search**.

4 In the **Search** dialog box, perform the following actions:

a Select the property on which the search has to be performed.

b Select the condition from the combo box.

c Specify the value in the text box.

NOTICE: If you want to include any of the following characters in your search, enter a backslash \ before the character: , \ * % _

d Click **Search**.

NOTICE:
After viewing the audit details, you can view all the details again on the same page by clicking **Show All**.

To search the Audit Trails more precisely, click **More**. It allows you to define additional criteria. To remove additional criteria, click **Fewer**.

5.21.1.4
Exporting Audit Trails

Procedure:

1. From the main menu, select **Administration** → **Security Administration**.
2. In the **Security Administration** window, perform one of the following actions:
   - To export audit trails for all users, from the main menu, select **View** → **Audit Trails**.
   - To export audit trails for a specific user, expand the **Users** node, right-click a user and select **Audit Trails**.
3. In the **Auth Audit** screen, click **Export**.
4. Define the type of exported data by choosing the appropriate radio button.
5. Enter the file name. Click **Export**.

The file is exported on the server side.

5.21.2
Groups Operations

Unified Event Manager (UEM) enables you to organize different types of users into groups. You can classify them by a set of common operations, or provide specific permissions to various groups. This practice saves time when changing permissions for all users in a specific group. It also makes it easier to add a new user to an existing group.

A group is a logical collection of users grouped to access common information or perform similar tasks. Any administration done for the group is reflected in the individual members (or users) of the group.

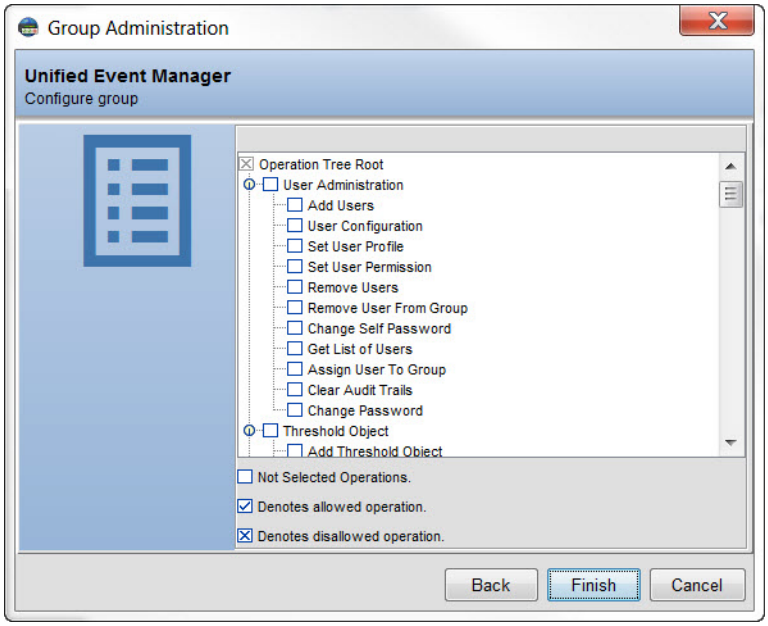
5.21.2.1
Adding Groups

You can add new groups to assign to it permissions that are different from those of an existing group.

Procedure:

1. From the main menu, select **Administration** → **Security Administration**.
2. In the **Security Administration** window, from the **File** menu, select **New** → **Add Group**.
3. In the **Enter a group name** field, enter the name of the group. Click **Next**.
4. From the **Operations Tree Root** list, select the permissions you want to allow or disallow for all users in this group. Click **Finish**.

Figure 52: Group Administration – Configure Group



The group is visible in the **Security Administration** window, under the **Groups** node.

5.21.2.2

Assigning Users to Groups

By assigning users to groups, you can limit access to specific functions of Unified Event Manager (UEM). The groups provide specific permissions and levels of permissions. For example, user access can be limited to specific types of devices. The users assigned to the group are displayed in the **Members** tab.

Procedure:

1. From the main menu, select **Administration** → **Security Administration**.
2. In the **Security Administration** window, perform the following actions:
   a. Expand the **Groups** node and click the group to which you want to assign users.
   b. Click the **Members** tab displayed on the right-hand side.
   c. Click **Setting Users**.
3. In the **Select Users** dialog box, assign one user or many users to a group:
   - To assign one user to a group, click the user in **All Users** and click the **Add** icon  .
   - To assign many users to a group, select multiple users by using SHIFT or CTRL.
4. Click **OK**.

The new group member appears in the **Members** tab.

5.21.2.3

Unassigning Users from Groups

Procedure:

1. From the main menu, select **Administration** → **Security Administration**.

2 In the **Security Administration** window, perform the following actions:
   a Expand the **Groups** node and click the group to which you want to assign users.
   b Click the **Members** tab displayed on the right-hand side.
   c Click **Setting Users**.
3 In the **Select Users** dialog box, in the **Selected Users** area, click the user you want to unassign and click **Remove**  .
4 Click **OK**.

The removed group member disappears from the **Members** tab.

5.21.2.4
Permitted Operations for Group

Scopes are used to set limits to a permission by applying one or more properties to a group permission.

The sets of properties are applicable only when the properties are valid. For example, if you assign a network to a particular IP address to a property, the scope of that associated operation is applicable only to this network.

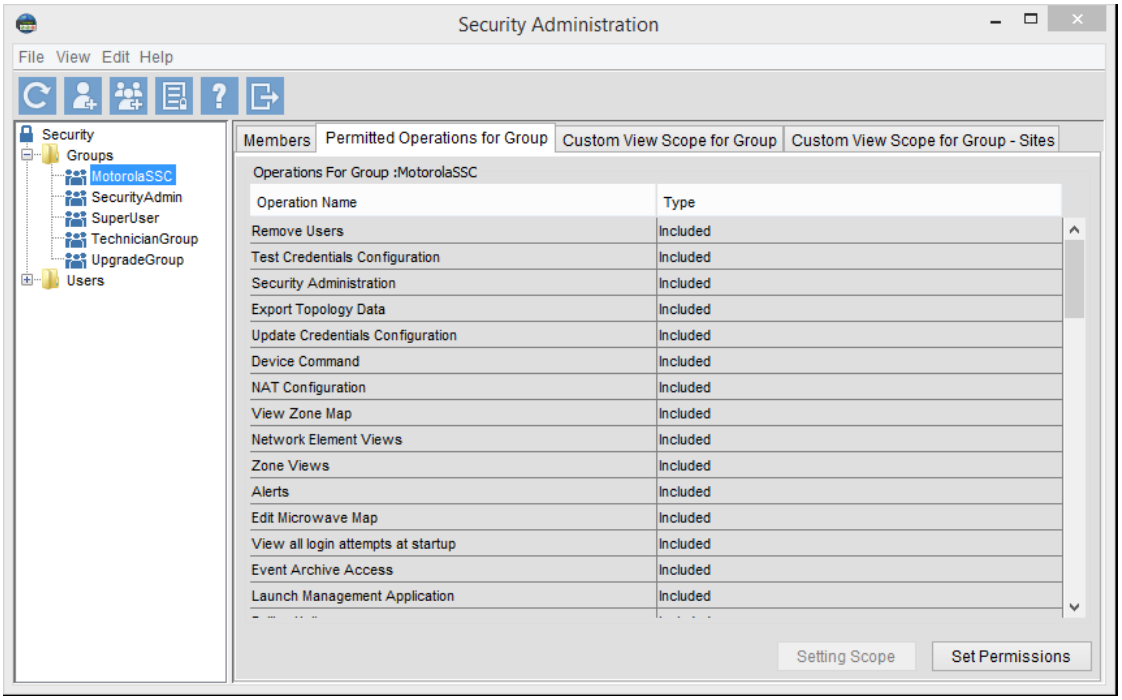
5.21.2.4.1
Adding Scopes

You can add a scope to a permission when you want to identify a specific object or a set of properties to which the group has permissions.

Procedure:

1 From the main menu, select **Administration** → **Security Administration**.
2 In the **Security Administration** window, expand the **Groups** node and select a group.
   In the **Permitted Operations for Group** tab, operations for the selected group appear.

Figure 53: Security Administration – Permitted Operations for Group



3 Click an operation for which you want to set a scope. Click **Setting Scope**.

4 In the **Scope Settings** dialog box, in the **Name** and **Value** fields, enter the property name and value for the scope. Click **Add**. Click **OK**.

5 Optional: Add more scopes by repeating step 2 through step 4.

5.21.2.4.2

Changing Scopes

You can change the scope of a permission when you want to change or identify a specific object to which the group has permissions.

Procedure:

1 From the main menu, select **Administration** → **Security Administration**.

2 In the **Security Administration** window, the **Security** tree, click the desired group.

3 Click the **Permitted Operations for Group** tab on the right-hand side.

The operation set for the selected group appears.

4 Click the operation for which you want to set a scope and click **Setting Scope**.

The **Scope Settings** dialog box appears.

5 Select a scope to modify and click **Edit**.

6 In the **Name** and **Value** fields, type the property name and value for the scope of the selected operation.

7 Click **Edit**. Click **OK**.

5.21.2.4.3
Deleting Scopes

You can delete a scope when you no longer want to specify certain properties for the permission.

Procedure:

1. From the main menu, select **Administration** → **Security Administration**.
2. In the **Security Administration** window , the **Security** tree, select the desired group.
3. Click the **Permitted Operations for Group** tab on the right-hand side.

   The operation set for the selected group appears.
4. Click the operation for which you want to set a scope and click **Setting Scope**.

   The **Scope Settings** dialog box appears.
5. Select a scope to delete.
6. Click **Delete**. Click **OK**.

5.21.2.5
Custom View Scope Operations

Setting Custom View Scopes (CVS) for groups enables you to filter the objects or whole sites. By specifying the custom view scope criteria, you can ensure that users view only the data for which they have authorization to perform these operations.

5.21.2.5.1
Custom View Scope for Sites Operations

Sites can be filtered for a group which is useful, for example, when the system is shared between a few agencies and one agency should be able to access only specific sites. Only checked sites and related elements are visible for a group.

5.21.2.5.1.1
Adding Custom View Scopes for Sites

You add custom view scopes for sites to control which sites are displayed in Unified Event Manager (UEM). You can add custom view scopes for sites only to groups in UEM, you cannot add them to users. By default, no custom view scopes are defined for sites so all sites are visible in UEM.

Procedure:

1. From the main menu, select **Administration** → **Security Administration**.
2. In the **Security Administration** window, expand the **Groups** node and select a group.
3. In the **Custom View Scope for Group - Sites** tab, perform the following actions:
   a. Clear check boxes for the sites you no longer want the see in UEM, if any.
   b. Click **Save Custom View Scope**.

Sites included in the custom view scope are still visible in UEM while the excluded ones are no longer visible in any of the UEM views.

NOTICE:
Saving custom view scopes for sites automatically creates authorized scopes for all UEM views. You can view the authorized scopes in the **Security Administration** window, under the **Custom View Scope for Group** tab.

By default, creating a custom view scope for sites for a specific group results in a new perspective of viewing historical events. As a result, previously generated events in the event view and the event archive view are not visible for that group.

Changing the properties of an existing custom view scope for sites affects only events generated after the changes are made. Historical events are unaffected.

A network element may be visible in UEM even if the custom view scope excludes the site that this network element belongs to. This exception applies to any network element which is in the same redundancy group as a network element at a site that is included in the custom view scope.

5.21.2.5.1.2
Deleting Custom View Scopes for Sites

Custom view scopes for sites enable you to control which sites are displayed in Unified Event Manager (UEM). By default, no custom view scopes are defined for sites so all sites are visible in UEM. You can delete the custom view scopes you added earlier.

Procedure:

1. From the main menu, select **Administration** → **Security Administration**.
2. In the **Security Administration** window, expand the **Groups** node and select a group.
3. In the **Custom View Scope for Group - Sites** tab, click **Delete Custom View Scope**.

All sites are visible in UEM.

5.21.2.5.2
Authorized Custom View Scope Operations

Custom view scope can be defined to filter objects for the following views: **Events**, **Network Database**, **Alerts**, **Maps** and **Stats Admin**.

5.21.2.5.2.1
Adding Authorized Custom View Scopes

You can add authorized custom view scopes to groups to ensure the group members can view only the authorized data.

Procedure:

1. From the main menu, select **Administration** → **Security Administration**.
2. In the **Security Administration** window, perform the following actions:
   a. Expand the **Group** node and click a group for which you want to add authorized custom view scopes.
   b. Click the **Custom View Scope for Group** tab on the right-hand side.
   c. From the **Custom View Scope Name** drop-down menu, select a module. Click **Add AuthorizedScope**.
3. In the **Scope Settings** dialog box, in the **Name** field, enter an authorized scope name.

4 From the **Name** drop-down menu, select the **Property** name. This drop-down menu lists the property names that can be used to create the authorized scopes and are specific to each of the custom view scope.

NOTICE:
The fields and properties displayed in this dialog box differ for Events, Alarms, and Network Database views.

For the description of Event, Alarm and Network Database properties, see Event Properties on page 158, Alarm Properties on page 166, and Managed Resource Properties on page 155.

5 In the **Value** field of the match criteria, enter the value for the property.

NOTICE: To define match criteria for more than one property value, separate each value according to the appropriate operator or wildcard characters. For information on Wildcard characters and Operators that can be used to define match criteria, see Filtering Quick Reference on page 132.

6 Click **Add**.

This operation adds the Authorized Scope for the selected Custom View Scope of the group. You can add more than one property criteria.

7 On adding the properties, click **OK** for making a permanent store.

5.21.2.5.2.2
Assigning Authorized Custom View Scopes

After you create an authorized custom view scope for a group, you can assign it to other groups as necessary.

Procedure:

1 From the main menu, select **Administration** → **Security Administration**.

2 In the **Security Administration** window, perform the following actions:

a Expand the **Group** node and click a group for which you want to assign authorized custom view scopes.

b Click the **Custom View Scope for Group** tab on the right-hand side.

c Click **Assign AuthorizedScope**.

3 In the **Select Authorized Scopes** window, from **All Authorized Scopes**, select an authorized scope and click **Add**  . Click **OK**.

The selected scopes are displayed in both the **All Authorized Scopes** list and in the **Selected Authorized Scopes** list.

5.21.2.5.2.3
Removing Authorized Custom View Scopes from Groups

Remove an authorized Custom View Scope from a group when it is no longer valid for that group. By removing the Custom View Scope, the properties themselves are not changed. The Custom View Scope is not deleted from the database.

Procedure:

1 From the main menu, select **Administration** → **Security Administration**.

2 In the **Security Administration** window, perform the following actions:

a Expand the **Group** node and click a group for which you want to remove authorized custom view scopes.

b Click the **Custom View Scope for Group** tab on the right-hand side.

c Click **Assign AuthorizedScope**.

3 In the **Select Authorized Scopes** window, from **Selected Authorized Scopes**, select an authorized scope and click **Remove**  . Click **OK**.

5.21.2.5.2.4
Changing Authorized Scope Properties

After you add properties to an authorized custom view scope, you can change them as appropriate.

NOTICE: If you have assigned the authorized custom view scope to other groups, any changes to the custom view scope affect those groups as well.

Procedure:

1 From the main menu, select **Administration** → **Security Administration**.

2 In the **Security Administration** window, perform the following actions:

a Expand the **Group** node and click a group for which you want to modify authorized custom view scopes.

b Click the **Custom View Scope for Group** tab on the right-hand side.

c In the **Authorized Scopes for CV** list, select the **Authorized Scope** you want to modify.

d Click **Set Scope Properties**.

3 In the **Scope Settings** dialog box, click **OK**.

5.21.2.5.2.5
Deleting Authorized Custom View Scopes

When an authorized custom view scope is no longer valid, you can delete it from the database. After you delete it, you can recreate it if you ever need it again.

Procedure:

1 From the main menu, select **Administration** → **Security Administration**.

2 In the **Security Administration** window, perform the following actions:

a Expand the **Group** node and click a group for which you want to delete authorized custom view scopes.

b Click the **Custom View Scope for Group** tab on the right-hand side.

c Right-click the **Authorized Scope** you want to delete from the **Authorized Scopes for CV** list and click **Delete AuthorizedView**.

After you confirm that you want to delete the custom view scope, it is deleted from the database and from any group to which it was associated.

5.21.2.5.3
Custom View Scope for Sites Operations Interactions with a Trunking Subsystem

Custom View Scope for Sites Operations supports all sites in a Trunking Subsystem (Tsub). This includes subsites that are not configurable otherwise.

When the parent of a discovered subsite changes to a corresponding Tsub, a new configuration option for Custom View Scopes for Sites Operations is added. The default value for the new option makes the subsite and its devices invisible for the user in the specific Custom View Scope.

5.21.2.5.3.1
Filtering Devices that Are Outside of Sites

Custom View Scope can be defined to show all devices in a Prime Site that work in a Trunking Subsystem (Tsub). Some of the devices discovered in this Prime Site are not assigned to a Prime Site Group Managed Resource but to a Trunking Subsystem Group Managed Resource. To be visible in the user's Custom View Scope for Group, those devices must be defnied using the **parentKey** property. This property should point to a Trunking Subsystem Group Managed Resource name that is parent of those devices.

5.21.2.6
Deleting Groups

Procedure:

1. From the main menu, select **Administration** → **Security Administration**.
2. In the **Security Administration** window, perfrom the following actions:
   a. Expand the **Group** node.
   a. Select a group you want to delete.
   a. Right-click the group, and from the menu select **Delete**.
3. Confirm the deletion by clicking **Yes**.

The group is removed from the database.

5.21.3
Users Management

A user is an individual who logs in to Unified Event Manager (UEM). The user account allows for performing only a specific set of functions.

Users can be given specific permissions, added to groups, and given specific permissions within the group.

5.21.3.1
Adding Users

You can add a user at any time. By default, the new user has login permissions only. You provide access to various functions by making the user a member of pre-configured groups, or by directly assigning permissions to the user.

You can add a new user from the:

- Application Client
- Command Line

5.21.3.1.1
Adding Users from the UEM Client

Procedure:

1. From the main menu, select **Administration** → **Security Administration**.

2 In the **Security Administration** window, click **Add User**.

3 In the **User Administration** dialog box, enter the user name and password. Click **Next**.

NOTICE: The password must meet the following criteria:

- must be at least 15 characters long
- cannot exceed 64 characters
- must have the following characteristics:
  - at least one lower case alphabet (a-z)
  - at least one upper case alphabet (A-Z)
  - at least one digit (0-9)
  - at least one of the following special characters: ` ! @ # $ % ^ & * ( ) _ - + = [ ] { } ; : ' \" \ | , < . > / ? "

4 In the **User Administration** window, set the expiration period. Click **Next**.

If…	Then…
If you want the user account to expire after a specific period,	perform the following actions: **a** Clear the **Account never expires** check box. **b** In the **This user account expires in** field, enter a number of days.
If you do not want the user account to expire,	leave the **Account never expires** check box selected.

NOTICE: By default, the user account never expires and the password always expires after 60 days.

5 Optional: Assign the user with an existing group:

a Select the **Group-based permissions** check box.

b In the **Assign groups for the user** panel, select the check boxes corresponding to the groups to which you want to assign the user.

NOTICE: Click the arrow in the panel to display a pop-up window with the permissions for the group. Based on the permissions, you can assign groups to the user.

6 Create a group to which you want to associate the user:

a In the **Enter the new group name** field, enter a group name.

b Click **Add Group**.

For information about selecting permissions for the new group in this dialog box, see Assigning Operations to Groups on page 242.

7 To directly assign permissions to the user, perform the following actions:

a Check the **Direct assignment** check box.

b Click **Permissions**.

For more information on selecting permissions in this dialog box, see Operations Assignment on page 242.

NOTICE: The operations assigned to the user are specific to that particular user.

The **Assign Permissions** dialog box appears.

8 When you finish assigning permissions to the user, click **Finish**.

A new user appears in the **Security** tree on the left-hand side of the **Security Administration** window.

5.21.3.1.2
Adding Users from the Command Line

Procedure:

1 Execute the `UserConfig.sh` file located in the ***<UEM Home>***`/bin/admintools` directory, from the command as follows: `UserConfig.sh Add` ***<UserName> <Password> <Group> <rmiPort>***

where:

`UserName` is the user name of the new user.

`Password` is the password to authenticate the user during login.

`Group` is the group to which the user should belong.

`rmiPort` (optional) is the RMI port number of UEM. If not specified, the default RMI port number: 1099 – is set.

IMPORTANT: To add a new user, the UEM server must be enabled.

NOTICE:
The password must meet the following criteria:

- must be at least 15 characters long
- cannot exceed 64 characters
- must have the following characteristics:
  - at least one lower case alphabet (a-z)
  - at least one upper case alphabet (A-Z)
  - at least one digit (0-9)
  - at least one of the following special characters: ` ! @ # $ % ^ & * ( ) _ - + = [ ] { } ; : ' \" \ | , < . > / ? "

Step example: `UserConfig.sh Add guest UlTr@STr0ngPa$$word! Admin 1099`

A new user: `guest` – is added to the `Admin` group with the password: `lTr@STr0ngPa$$word!`.

5.21.3.2
Changing the User Profile

You can change the profile of a user according to your requirements. For example, you can change a profile to modify the account expiration date or remove the temporary account lock caused by entering an invalid password several times in a row.

Procedure:

1 From the main menu, select **Administration** → **Security Administration**.

2 In the **Security Administration** window, expand the **Users** node and click the user whose profile you want to change.

The **Security Administration** tabs are displayed on the right-hand side.

3 Click the **User Profile** tab and select **Setting Profile**.

The **User Profile** dialog box appears.

4 To enable or disable the user, clear the **No change in status** check box and from the drop-down menu, select **enable** or **disable** as appropriate.

5 Change the account and password expiration date, and click **OK**.

The **Security Administration** window displays the **Groups** and **Users** nodes on the left-hand side.

5.21.3.3

Unlocking the User Account

You can unlock a user account that is temporarily locked for one hour due to entering an invalid password three times in a row.

Procedure:

1 From the main menu, select **Administration** → **Security Administration**.

2 In the **Security Administration** window, expand the **Users** node and click the user whose account you want to unlock.

The **Security Administration** tabs are displayed on the right-hand side.

3 Click the **User Profile** tab and select **Setting Profile**.

The **User Profile** dialog box appears.

4 To unlock the user account, clear the **Account locked** check box. Click **OK**.

The account locked check box is active only when a user account is locked.

The **Security Administration** window displays the **Groups** and **Users** nodes on the left-hand side.

5.21.3.4

Assigning Groups to Users

You can assign the users that you created to existing groups.

Procedure:

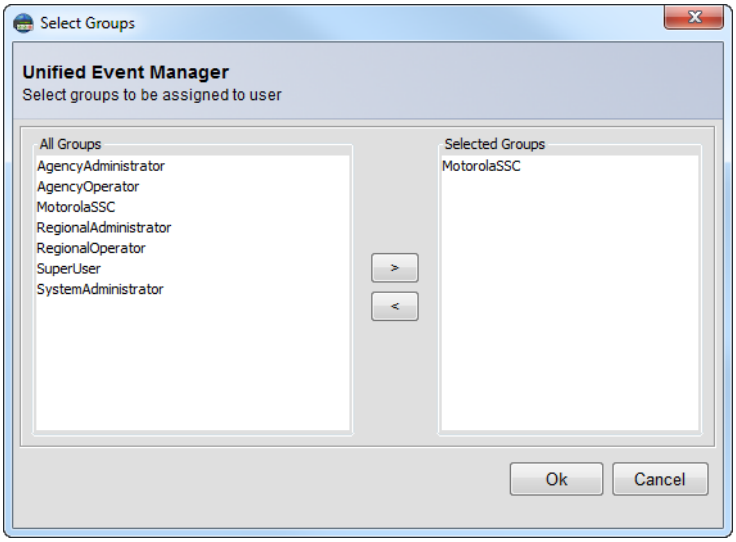
1 From the main menu, select **Administration** → **Security Administration**.

2 In the **Security Administration** window, expand the **Users** node and click the user whose profile you want to change.

The **Security Administration** tabs are displayed on the right-hand side.

3 Click the **Member Of** tab and select **Setting Groups**.

Figure 54: Select Groups Dialog Box



The **Select Groups** dialog box appears.

4 Assign one group or many groups to a user:

- To assign one group to a user, click the group in the **All Groups** list and click the **Add** icon  .
- To assign many groups to a user, select multiple groups by using SHIFT or CTRL.

5 Optional: Unassign a group from a user:

a In the **Selected Groups** list, click a group.

b Click the **Remove** icon  .

6 Click **OK**.

The groups assigned to the user are displayed in the **Groups For** list in the **Member Of** tab.

5.21.3.5

Changing the User Password

Within a 24-hour period, you can change your password only once. You cannot change passwords of domain users.

The password must meet the following criteria:

- must be at least 15 characters long
- cannot exceed 64 characters
- must have the following characteristics:
  - at least one lower case alphabet (a-z)
  - at least one upper case alphabet (A-Z)
  - at least one digit (0-9)

- at least one of the following special characters: ` ! @ # $ % ^ & * ( ) _ - + = [ ] { } ; : ' \" \ | , < . > / ? "

Procedure:

1. From the main menu, select **Administration** → **Change Password**.
2. In the **Password Configurator** window, enter the old and new passwords.

The password is changed.

5.21.3.6

Changing the User Password when in the Security Administrator Group

A user with the security administrator role or belonging to the security administrator group can change the passwords for any user at any time.

Procedure:

1. From the main menu, select **Administration** → **Security Administration**.
2. In the **Security Administration** window, expand the **Users** node and click the user whose password you want to change.

   The user details appear on the right-hand side.
3. From the **Security Administration** window, select **Edit** → **Change Password**.

   The **Change Password** dialog box appears.
4. In the password fields, enter the new password. Click **OK**.

5.21.3.7

Deleting Users

Delete a user when you no longer want the user to have access to the Unified Event Manager (UEM).

Procedure:

1. From the main menu, select **Administration** → **Security Administration**.
2. In the **Security Administration** window, expand the **Users** node, right-click a user you want to delete, and click **Delete**.
3. Confirm the deletion by clicking **Yes**.

5.21.4

Operations Management

The operations tree contains a list of operations (also referred to as permissions) that are provided by default in Unified Event Manager (UEM). The operations are logically arranged in a tree structure with

parent and child operations. You can add new operations when they are needed and delete obsolete operations.

5.21.4.1

Default Operations

The operations tree contains a list of operations that are provided by default in Unified Event Manager (UEM). Assigning different operations to different users is an administrative function.

Administrative Operation

Administrative Operation Services provide information on the operation and the description of administrative services.

Table 35: Security Administration

Security Administration provides the following security-related operations that can be configured in the table. You can provide permissions for users only for certain security operations and restrict other security functions. For instance, you can provide permissions for users to create groups, but restrict permissions to delete groups.

Operations		Description
Group Operations	Add Group	Disabling this operation prevents the user from adding a group.
	Remove Group	Disabling this operation prevents the user from removing a group.
	Set Permission	Disabling this operation prevents the user from setting permissions or operations to groups.
Scope Settings	Create Scope for Group	Disabling this operation prevents the user from adding a scope or setting the properties of a scope.
	Modify Group Scope Relation	Disabling this operation prevents the user from assigning a scope to a group in the Custom View Scope for Group UI.

Table 36: System Administration

Operations	Description
System Administration	Disabling the System Administration operation prevents the user from accessing the System Administration page in both the UEM client and UEM client web interface.

Table 37: Runtime Administration

Operations	Description
Runtime Administration	Disabling the Runtime Administration operation prevents the user from managing JVM in the UEM client web interface.

Table 38: Shutdown Web NMS Server

Operations	Description
Shutdown Web NMS Server	Shutdown Web NMS Server is an operation used internally only by the root user. Disabling this operation for the root user may cause problems with disabling the Server.

Table 39: Terminate Client

Operations	Description
Terminate Client	Disabling the Terminate Client operation prevents the user from shutting down connected Clients using System Administration.

Events

Table 40: Events

The Events operations provide permissions to work with event filters, export, and save events to file.

Operations	Description	
Event Filters	Get Event Filters	Disabling this operation prevents the user from viewing the existing event filters in UEM.
	Set Event Filters	Disabling this operation prevents the user from modifying or adding an event filter.
Export Events	Disabling this operation prevents the user from exporting the list of events.	
Save Events To File	Disabling this operation prevents the user from saving event filters to a file.	

Topology

Table 41: Topology

The Topology operations provide permissions to work with topology data displayed in the **Network Database** view.

Operations	Description
Modify Object	Disabling this operation prevents the user from altering Managed Resource properties.
Manage and Unmanage Objects	Disabling this operation prevents the user from managing or unmanaging an object or a network element.

Table continued…

Operations	Description
Discovery Configuration	Disabling this operation prevents the user from configuring the discovery process
Export Topology Data	Disabling this operation prevents the user from exporting the topology data
Modify Managed Resource Properties	Disabling this operation prevents user from modifying managed resource properties
Delete Object	Disabling this operation prevents the user from deleting an object or a network element.
Refresh Node	Disabling this operation prevents the user from refreshing a node. UEM does not manage devices that support this operation.
Manage and Unmanage Entities	Disabling this operation prevents the user from managing or unmanaging an entity.
Set Entities Alias	Disabling this operation prevents the user from setting an alias for an entity.

Policy

Table 42: Policy

The Policy operations provide permissions to work with policies.

Operation	Description
Add Policy	Disabling this operation prevents the user from adding a policy.
Delete Policy	Disabling this operation prevents the user from deleting an existing policy.
Update Policy	Disabling this operation prevents the user from updating an existing policy.
Execute Policy	Disabling this operation prevents the user from executing an existing policy.
Stop Policy	Disabling this operation prevents the user from stopping an existing policy.

User Administration

Table 43: User Administration

The User Administration operations provide permissions to work with local accounts, users, and groups.

Operation	Description
User Configuration	Disabling this operation prevents the user from modifying user configuration in the UEM client web interface.

Table continued…

Operation	Description
Add Users	Disabling this operation prevents the user from adding new users.
Assign User to Group	Disabling this operation prevents the user from assigning a user to a group.
Remove Users	Disabling this operation prevents the user from removing a user.
Remove User from Group	Disabling this operation prevents the user from removing a user from a group.
Change Password	Disabling this operation prevents the user from changing the password of a user.
Get List of Users	Disabling this operation prevents the user from viewing the list of users added. Applicable only to the UEM client web interface (the link to access the list is disabled).
Set User Permission	Disabling this operation prevents the user from setting operations or permissions for existing users.
Set User Profile	Disabling this operation prevents the user from setting profiles for existing users.
Clear Audit Trails	Disabling this operation prevents the user from clearing audit trails in the UEM client.
Change Self Password	Disabling this operation prevents the user from changing the password.

Alerts

Table 44: Alerts

The Alerts operations provide permissions to work with alarms displayed in the **Alarms** view and with alert filters.

Operations	Description	
Alarm Notifier	Disabling this operation prevents the user from modifying notifications assigned to Alarms.	
Acknowledge Alarm	Disabling this operation prevents the user from acknowledging and un-acknowledging alarms.	
Export Alarms	Disabling this operation prevents the user from exporting the list of alerts.	
Alarm Type Settings	Disabling this operation prevents the user from modifying alarm type settings.	
Alert Filters	Get Alert Filters	Disabling this operation prevents the user from viewing existing alert filters.
	Set Alert Filters	Disabling this operation prevents the user from setting new alert filters.

Table continued…

Operations	Description	
Alert User Operations	Set Alert Annotation	Disabling this operation prevents the user from annotating an alarm.
	Get Alert Details	Disabling this operation prevents the user from viewing the details of an alarm.
	Get Alert History	Disabling this operation prevents the user from viewing the history of an alarm.
	Alert Pickup	Disabling this operation prevents the user from picking up an alarm.
	Save Alerts To File	Disabling this operation prevents the user from saving alarm filters to a file.

Maps

Table 45: Maps

Operation	Description
Map Editing Operations	Disabling this operation prevents the user from adding or deleting symbols, links, areas, and containers, grouping symbols and configuring nodes in a map.
Modify Symbol Properties	Disabling this operation prevents the user from modifying the Map Symbol properties.
Sync Map Symbol Display Name	Disabling this operation prevents the user from updating the display name of a Map Symbol with the Managed Resource name.

NBI

Table 46: NBI

The NBI operations provide permissions to configure the North Bound Interface (NBI).

Operation	Description
NMS Configuration	Disabling this operation prevents the user from configuring the NBI.
NBI Rest	Disabling this operation prevents the user from accessing the NBI via the REST Interface.

Credentials Configuration

Table 47: Credentials Configuration

The Credentials Configuration operations provide permissions to update and test credentials configuration.

Operation	Description
Update Credentials Configuration	Disabling this operation prevents the user from modifying credentials configuration.
Test Credentials Configuration	Disabling this operation prevents the user from testing the credentials configuration.

Device Command

Table 48: Device Command Configuration

Operation	Description
Device Command	Disabling this operation prevents the user from issuing commands to the device.

Application Inventory

Table 49: Application Inventory Configuration

The Application Inventory operation provides permissions to access the application inventory.

Operation	Description
Application Inventory	Disabling this operation prevents the user from viewing the Application Inventory of a device managed by the Generic Application Server.

Device Synchronization

Table 50: Device Synchronization

The Device Synchronization operation provides permissions to manually synchronize fault managed devices.

Operation	Description
Device Synchronization	Disabling this operation prevents the user from performing force synchronization on the device.

Abort All Discovery Jobs

Table 51: Abort All Discovery Jobs Configuration

The Abort All Discovery Jobs operation provides permissions to abort discovery jobs started by other users.

Operation	Description
Abort All Discovery Jobs	Disabling this operation prevents the user from aborting a discovery job started by a different user. Users can always abort discovery jobs which they initiated themselves.

Server Logs Access

Table 52: Server Logs Access Configuration

The Server Logs Access operation provides access to server logs.

Operation	Description
Server Logs Access	Disabling this operation prevents the user from accessing the server logs by using a web browser. The access is available from **Tools** → **Server Logs**.

Event Archive Access

Table 53: Event Archive Access Configuration

Operation	Description
Event Archive Access	Disabling this operation prevents the user from accessing the event archives by using a web browser. The access is available from **Tools** → **Server Logs**.

Performance Archive Access

Table 54: Performance Archive Access Configuration

Operation	Description
Performance Archive Access	Disabling this operation prevents the user from accessing the performance archives by using a web browser. The access is available from **Logging** → **Performance Archive**.

Configure Logging

Table 55: Logging Configuration

Operation	Description
Configure Logging	Disabling this operation prevents the user from configuring the log information.

Launch Management Application

Table 56: Launch Management Application Configuration

The Launch Management Application operation provides access to the launch management application for fault managed devices.

Operation	Description
Launch Management Application	Disabling this operation prevents the user from accessing the management application.

View All Login Attempts at Startup

Table 57: View All Login Attempts at Startup Configuration

The View All Login Attempts at Startup operation allows you to view logon attempts for all users.

Operation	Description
View All Login Attempts at Startup	Disabling this operation prevents the user from being able to view login attempts for other users at startup of the application. You can view all login attempts by clicking **Details** in the **Last Login Information** dialog box that opens after starting the UEM client.

View Associated Managed Resources

Table 58: View Associated Managed Resources

The View Associated Managed Resources operation allows you to view all associated managed resources.

Operation	Description
View Associated Managed Resources	Disabling this operation prevents the user from viewing associated managed resources by using context menu in UEM.

Asset Management Information

Table 59: Asset Management Information Configuration

The Asset Management Information operation provides access to the asset management information for devices that support this operation, for example PTP, Extreme switches.

Operation	Description
Asset Management Information	Disabling this operation prevents the user from accessing asset management information for devices that support this operation.

Turn on/off Upgrade Mode

Table 60: Turn on/off Upgrade Mode Configuration

The Turn on/off Upgrade Mode operation allows you to configure the upgrade mode.

Operation	Description
Turn on/off Upgrade Mode	Disabling this operation prevents user from configuring the Upgrade Mode.

5.21.4.2

Operations Assignment

You can assign operations (include or exclude privileges) for a group or for a particular user. Assigning operations for a group automatically sets the same privileges for the users in that group.

5.21.4.2.1

Assigning Operations to Groups

Procedure:

1. From the main menu, select **Administration** → **Security Administration**.
2. In the **Security Administration** window, expand the **Group** node and click the group to which you want to assign operations.
3. Click the **Permitted Operations for Group** tab displayed on the right-hand side.

   All operations included or excluded for that group are displayed in the **Operations For Group** list.
4. Click **Set Permissions**.

   The **Assign Permissions** window appears.
5. To grant appropriate permissions, perform any of the following actions:
   - To include the permissions you want to grant to the group, select the check box so that a tick symbol is displayed.
   - If you do not want to grant specific permissions, select the check boxes next to these permissions.

   NOTICE: Leaving the check box empty for an operation is does not authorize the operation. For information on each of the operations, see Default Operations on page 234.
6. To reset the changes without closing the window, click **Reset**, to exit without saving, click **Cancel**.
7. Click **Done**.

5.21.4.2.2

Assigning Operations to Users

Procedure:

1. From the main menu, select **Administration** → **Security Administration**.
2. In the **Security Administration** window, expand the **Users** node and click the user to which you want to assign operations.
3. Click the **Permitted Operations for User** tab displayed on the right-hand side.

   All operations allowed or not allowed for that user are displayed in the **Permissions For User** list.
4. Click **Set Permissions**.
5. In the **Assign Permissions** window, grant the appropriate permissions:
   - To include the permissions you want to grant to the user, select appropriate check boxes so that a tick symbol is displayed.

- If you do not want to grant specific permissions, select the check boxes next to these permissions.

  NOTICE: Leaving the check box empty for an operation does not authorize the operation.

6. To reset the changes without closing the window, click **Reset**, to exit without saving, click **Cancel**.
7. Click **Done**.

5.22

Enabling the Upgrade Mode

The Upgrade Mode is a functionality that allows automatic rediscovery of the devices that are already discovered by UEM. Rediscovery is necessary when the device was upgraded or downgraded (the device interface version (DIV) was modified).

Procedure:

1. Log on to the UEM client with an **upgrade** account.

   NOTICE: Use the same password as the default one for the **root** account.

2. Select **Administration** → **Upgrade Mode**.

   The **Upgrade Mode Configuration** window appears.

3. Select the **Enable Upgrade Mode** check box. Click **Apply**.

   The Upgrade Mode is enabled and the **Status: Enabled** notification is displayed.

   NOTICE: The Upgrade Mode is disabled automatically after two weeks.

4. Close the window.

5.23

Disabling the Upgrade Mode

The Upgrade Mode is a functionality that allows automatic rediscovery of the devices that are already discovered by UEM. Rediscovery is necessary when the device was upgraded or downgraded (the device interface version (DIV) was modified).

Procedure:

1. Log on to the UEM client with an **upgrade** account.

   NOTICE: Use the same password as the default one for the **root** account.

2. Select **Administration** → **Upgrade Mode**.

   The **Upgrade Mode Configuration** window appears.

3. Select the **Disable Upgrade Mode** check box.
4. Optional: If you do **not** want UEM to start the rediscovery of all the managed devices, clear the **Rediscover remaining devices** check box.
5. Click **Apply**.

   The Upgrade Mode is disabled and the **Status: Disabled** notification is displayed.

6 Close the window.

Chapter 6

UEM Maintenance

Maintenance procedures help you backup and secure data on the Unified Event Manager (UEM) software application.

6.1 System Information Backup

Administrators can back up the data associated with Unified Event Manager (UEM) from the UEM administration menu. UEM data backups can take place without disabling the UEM server application.

UEM backs up:

- Managed resource inventory (Network Database) and customizations to this view
- Maps background images and other maps view customizations
- UEM groups and users
- SNMPv3 credentials (includes default, device, and NBI information)
- E-mail (paging) and alarm sound file configuration
- E-mail certificate
- Web Service credentials

NOTICE: The UEM data backups can take place without disabling the UEM server application.

6.2 System Information Restoration

Restoration procedures are performed to recover from any accidental loss of data, or if the entire server application and its data are lost. Unified Event Manager (UEM) validates the data being restored for consistency with the software installed during the restore process. If any discrepancies are detected, an error is reported.

The administrator must synchronize the SNMPv3 credentials after a system restore. It applies if the archive used for restoration is older than the last date/time the SNMPv3 credentials were modified. If the SNMPv3 configuration is not updated after the restore, UEM can be unable to communicate with one or more devices. Verify SNMPv3 credentials for the following interfaces:

MotoMaster
The SNMPv3 user who uses all communications from UEM to the devices.

MotoInformA or MotoInformB
The SNMPv3 user who uses all notifications (SNMP INFORM message) sent from devices to UEM.

MotoNorth and MotoNorthMotorola
The SNMPv3 credentials used by the North Bound Interface. Contact the Motorola Solutions Support Center (SSC) after the restoration process is complete. When the SNMPv3 configuration used for remote monitoring is enabled, they can verify it.

6.3
Enabling and Disabling UEM

Unified Event Manager (UEM) is enabled and disabled through the Administration menu on the UEM server application. For information on how to enable and disable all UEM applications, see the *Private Network Management Servers* manual and online help.

NOTICE: Fault management services, statistical collection, and reporting of events and alarms are not available when UEM is disabled.

6.4
Accessing and Retrieving Events Archives in UEM

Follow this procedure to access the events archive files when a Unified Event Manager (UEM) session is active. If no UEM sessions are active, you cannot access the events archive files. Only users with appropriate privileges can access event archives.

Procedure:

1. Log on to the UEM client with an account that has permissions to view event archives; you can change accounts in **Security Administration**.
2. From the main menu, select **Logging** → **Event Archive**.

   The browser window appears.
3. Select the **CSV Files List** tab.

   A list of available files is displayed.
4. Choose an appropriate file.

   Depending on your browser, the file opens in a browser window or is downloaded.
5. Select the contents and save the file to the local client PC. Repeat step 4 to save multiple event archive files.

The files are saved to the local client PC. Now, they can be saved to external media for long-term storage.

6.5
Accessing and Retrieving Performance Archives in UEM

You can access the performance archive files when a Unified Event Manager (UEM) session is active. If no UEM sessions are active, you cannot access the performance archive files. Only users with appropriate privileges can access event archives.

Procedure:

1. Log on to the UEM client with an account which has permissions to view performance archives; you can change accounts in **Security Administration**.
2. From the main menu, select **Logging** → **Performance Archives** or press CTRL + SHIFT + H.

   The browser window appears with the list of available files and catalogs.
3. Choose the appropriate file.

   Depending on your browser, the file opens in the browser window or is downloaded.
4. Select the contents and save to the local client PC. Repeat step 3 to save multiple event archive files.

NOTICE: After the files are saved to the local client PC, they can be saved to external media for long-term storage.

6.6

Accessing and Retrieving Server Logs in UEM

You can access the server logs when a Unified Event Manager (UEM) session is active. If no UEM sessions are active, you cannot access the server logs. Only users with appropriate privileges can access event archives.

Procedure:

1. Log on to the UEM client with an account which has permissions to view server logs; you can change accounts in **Security Administration**.
2. From the main menu, select **Logging** → **Server Logs**.

   The browser window appears with the list of available files and catalogs.
3. Navigate to the appropriate catalog, and select the appropriate file.

   The file opens in the browser window.
4. Select the contents and save to the local client PC. Repeat step 3 to save multiple event archive files.

   NOTICE: After the files are saved to the local client PC, they can be saved to external media for long-term storage.

6.7

Trap Overload Overview

In Unified Event Manager (UEM), the term *trap* is used to refer to SNMP trap, SNMP inform, and Web Service notifications. Traps are notifications sent to UEM by resources that UEM manages. UEM processes all traps it receives. In UEM, *processing* means converting traps into alarms and events and presenting them in this form in the UEM client. UEM can process a finite number of traps at a time. When the number of traps that UEM receives exceeds the capacity of UEM to process them, trap overload occurs, and the excessive traps are queued in the trap buffer for processing according to their priority.

Overload Buffer States

The trap buffer is a finite space in which UEM queues the excessive traps for processing. The trap buffer has different states that reflect the number of traps that are queued in the trap buffer. The buffer states are displayed in the overload buffer state bar in the lower right corner of the main UEM window.

The following buffer state definitions explain how UEM behaves depending on the number of traps queued for processing in the buffer.

Clear 

UEM operates normally. UEM processes all traps that are queued in the trap buffer. The queued traps take less than 5% of the trap buffer capacity.

Minor 

UEM receives more traps than it can process. The queued traps take between 5%–70% of the trap buffer capacity. When the overload buffer state changes to minor, based on trap statistics that are available on the UEM client web interface, you can verify if the managed resource that sends multiple traps works correctly, and undertake necessary actions.

Major Overload buffer state: Major

UEM receives more traps than it can process and cannot process the queued traps for a considerable amount of time. The queued traps take between 70%–95% of the trap buffer capacity. When the overload buffer state changes to major, based on trap statistics that are available on the UEM client web interface, you can verify if the managed resource that sends multiple traps works correctly, and undertake necessary actions, for example unmanage the resource or clear traps sent by the resource.

Critical Overload buffer state: Critical

The trap buffer is almost full. The queued traps take up to 95% of the trap buffer capacity. UEM automatically clears the buffer to exit the critical state. Based on the configured cleanup percentage, the overload buffer state changes to major, minor, or clear.

NOTICE: The hysteresis between the overload buffer states is 3%. As a result, the overload buffer state changes from, for example, major to minor when traps take 67% of the trap buffer capacity, though the threshold of the minor state is 70%. The hysteresis prevents frequent state changes when the capacity of the trap buffer is right between 2 states.

Trap Processing Order

When the overload buffer state is clear, UEM processes all traps in the order in which it receives the traps. When the overload buffer state is minor, major, or critical, UEM processes the queued traps depending on the trap type and managed resource type. UEM gives processing priority to:

- All types of traps that change the state of managed resources
- All types of managed resources whose synchronization takes long, that is Zone Controller (ZC), Site Controller (SC), and Remote Terminal Unit (RTU)

The RTU and ZC traps are of the highest processing priority, SC traps are of high processing priority, and transport managed resource traps are of normal processing priority. When traps are added to the trap buffer, UEM queues them for processing according to their priority.

Automatic Trap Cleanup

When the overload buffer state changes to critical, by default UEM clears 20% of traps queued in the buffer. You can modify the percentage of traps that UEM automatically clears when the overload buffer state changes to critical.

The order in which UEM automatically clears the trap buffer depends on the priority of traps:

- Traps of the lowest priority are cleared from the trap buffer as the first ones
- Traps generated by managed resources whose synchronization takes long are cleared from the trap buffer as the last ones

After UEM automatically clears the trap buffer, you are informed about it in a message. In the message, UEM asks you to recognize the fact that the automatic cleanup was performed by clicking **OK**. The message also contains information about the number of automatic cleanups performed since your last cleanup recognition, and about the date of the last cleanup.

This process explains how UEM behaves when the trap buffer reaches the critical state.

1. UEM initiates the process of removing a percentage of traps queued in the trap buffer.
2. UEM identifies the percentage of traps of the lowest priority for removal.
3. UEM removes all identified traps and schedules synchronization of the managed resources whose traps are removed.
4. Managed resources are synchronized and communicate with UEM. The amount of time synchronization takes depends among others on the amount of trap traffic that UEM receives, the

number of managed resources scheduled for synchronization. As a result of the synchronization, UEM receives up-to-date information from the managed resources.

5 Details about all traps that UEM removes form the trap buffer are collected in the `purgeEvents.log` file.

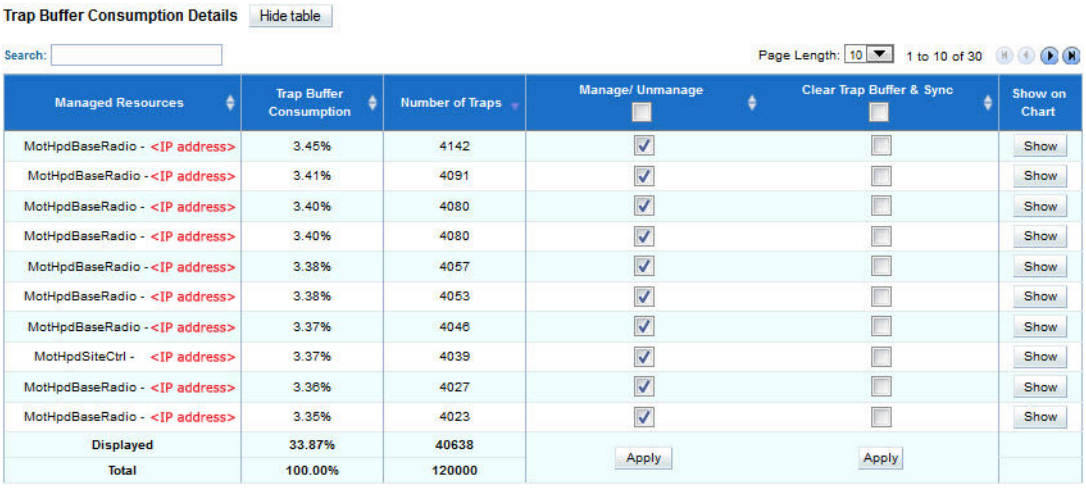
Trap Statistics

Trap statistics are displayed in the UEM client web interface. You can open the UEM client web interface by clicking the overload buffer state bar in the lower right corner of the main UEM window. Trap statistics are displayed in the form of charts and tables. The charts provide you with a visual representation of the trap buffer consumption and trap rate. The tables provide you with details about the trap buffer consumption and trap rate, and with trap management options.

Trap Buffer Consumption Details

In the **Trap Buffer Consumption Details** table, you can find information about the current trap buffer consumption.

Figure 55: Trap Buffer Consumption Details Table



The table consists of the following elements and options:

Managed Resources
Resources managed by UEM whose traps are currently queued in the trap buffer for processing.

Trap Buffer Consumption
Percentage of the current trap buffer capacity that is taken by traps queued in the trap buffer. The same information is presented graphically in the **Trap Buffer Consumption** chart.

Number of Traps
Number of traps currently queued in the trap buffer.

Manage/Unmanage
Option that enables you to manage or unmanage UEM resources. For example, you can unmanage resources that are broken so that they do not send many traps to the trap buffer and take a lot of the trap buffer capacity. After the resources are fixed, you can manage the fixed resources to enable UEM to receive traps from them.

Clean Trap Buffer & Sync
Option that enables you to clear the trap buffer of all traps UEM received from a managed resource. After the trap buffer is cleared, UEM schedules synchronization with managed resources whose traps you removed. As a result, UEM receives up-to-date information from the managed resources.

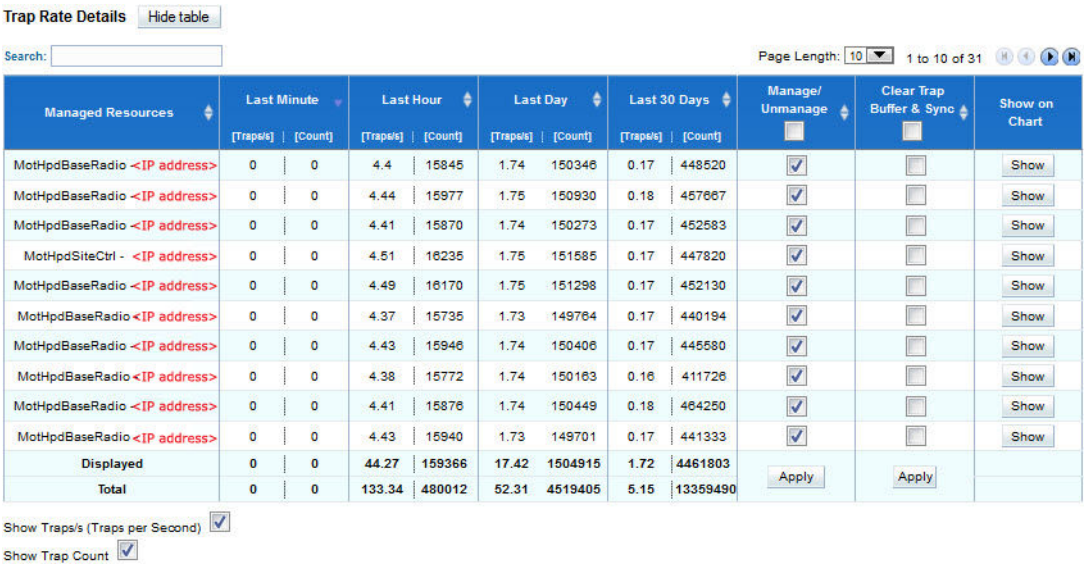
Show on Chart

Option that displays traps belonging to a managed resource on the **Trap Buffer Consumption** chart. With this option, you can display traps sent to UEM by a managed resource to see how much of the trap buffer capacity these traps take. Based on this information, you can decide to unmanage the managed resource to save some trap buffer capacity.

Trap Rate Details

In the **Trap Rate Details** table, you can find historical information about the trap buffer consumption.

Figure 56: Trap Rate Details Table



The table consists of the following elements and options:

Managed Resources

Resources managed by UEM whose traps were added to the trap buffer in the last minute, hour, day, or 30 days.

Traps/s

The number of traps added per second to the trap buffer in the last minute, hour, day, or 30 days. These values are displayed in the table by default. You can hide them by clearing the **Show Traps/s (Traps per Second)** check box.

Count

The number of traps added to the trap buffer within the last minute, hour, day, or 30 days. These values are displayed in the table by default. You can hide them by clearing the **Show Trap Count** check box.

Manage/Unmanage

Option that enables you to manage or unmanage UEM resources. For example, you can unmanage resources that are broken so that they do not send many traps to the trap buffer and take a lot of the trap buffer capacity. After the resources are fixed, you can manage the fixed resources to enable UEM to receive traps from them.

Clean Trap Buffer & Sync

Option that enables you to clear the trap buffer of all traps UEM received from a managed resource. After the trap buffer is cleared, UEM schedules synchronization with managed resources whose traps you removed. As a result, UEM receives up-to-date information from the managed resources.

Show on Chart

Option that displays traps belonging to a managed resource on the **Trap Rate** chart. With this option, you can display the rate of traps sent to UEM per second by one or more managed

resources of your choice. The traps rate value displayed on the chart is the same as the trap rate value displayed in the **Last Minute** column.

Related Links

Configuring E-mail Notifications for Alarm Filters on page 107
Configuring E-mail Notifications for Event Filters on page 114

6.7.1

Cleaning the Trap Buffer Manually

When the number of traps that UEM receives exceeds the capacity of UEM to process them, UEM queues the traps in the trap buffer for processing. From the UEM client web interface, you can manually clear the trap buffer, for example, of managed resources that send multiple traps to UEM. By manually clearing the trap buffer, you save the trap buffer space.

Procedure:

1. In the lower right corner of the main UEM window, click the overload buffer state bar.
2. In the UEM client web interface, go to the **Trap Buffer Consumption Details** or **Trap Rate Details** table and clear traps:

   NOTICE: The traps you remove from the trap buffer are not permanently deleted. The traps are stored in the `purgeEvents.log` file.

   - To clear all traps from the buffer, select the **Clear Trap Buffer & Sync** check box in the table heading. Click **Apply**.
   - To clear selected traps from the buffer, in the **Clear Trap Buffer & Sync** column, select check boxes for the traps you want to clear. Click **Apply**.

   The traps are deleted from the trap buffer. The deleted traps are collected in the `purgeEvents.log` file.
3. Optional: Access the `purgeEvents.log` file from the UEM client by selecting **Logging** → **Server Logs** from the main menu.

UEM schedules synchronization with managed resources whose traps you manually removed from the trap buffer. As a result, UEM receives up-to-date information from the managed resources.

6.7.2

Configuring Automatic Cleanup of the Trap Buffer

When the number of traps that Unified Event Manager (UEM) receives exceeds the capacity of UEM to process them, the excessive traps are queued in the trap buffer for processing. When the overload buffer state changes to critical, by default UEM clears 20% of traps queued in the buffer. You can modify the percentage of traps that UEM automatically clears when the overload buffer state changes to the critical state.

Procedure:

1. In the lower right corner of the main UEM window, click the overload buffer state bar.
2. In the UEM client web interface, go to the **Automatic Trap Buffer Cleanup** area.
3. In the **Automatically clear** field, enter the percentage of traps buffer that UEM clears automatically when the trap buffer reaches the critical state. Click **Submit**.

When the trap buffer reaches the critical state, UEM automatically removes from the trap buffer the percent of traps you set. UEM schedules synchronization with managed resources whose traps it automatically removed from the trap buffer. As a result, UEM receives up-to-date information from the

managed resources. Based on the configured cleanup percentage, the overload buffer state changes to major, minor, or clear.

6.7.3
Managing and Unmanaging Managed Resources From the Trap Buffer

When the number of traps that Unified Event Manager (UEM) receives exceeds the capacity of UEM to process them, the excessive traps are queued in the trap buffer for processing. From the UEM client web interface, you can manage and unmanage managed resources listed in the trap buffer that send many traps to UEM.

Procedure:

1. In the lower right corner of the main UEM window, click the overload buffer state bar.
2. In the UEM client web interface, go to the **Trap Buffer Consumption Details** or **Trap Rate Details** table and manage or unmanage managed resources:
   - To unmanage all managed resources, clear the **Manage/Unmanage** check box in the table heading. Click **Apply**.
   - To unmanage selected managed resources, in the **Clear Trap Buffer & Sync** column, clear check boxes for the managed resources you want to unmanage. Click **Apply**.
   - To manage all managed resources, select the **Manage/Unmanage** check box in the table heading. Click **Apply**.
   - To manage selected managed resources, in the **Clear Trap Buffer & Sync** column, select check boxes for the managed resources you want to manage. Click **Apply**.

UEM does not receive traps form the unmanaged resources and still receives traps from the managed resources.

6.8
Viewing Archived Events in UEM

You can access the events archive files when a Unified Event Manager (UEM) session is active. If no UEM sessions are active, you cannot access the events archive files. Only users with appropriate privileges can access event archives.

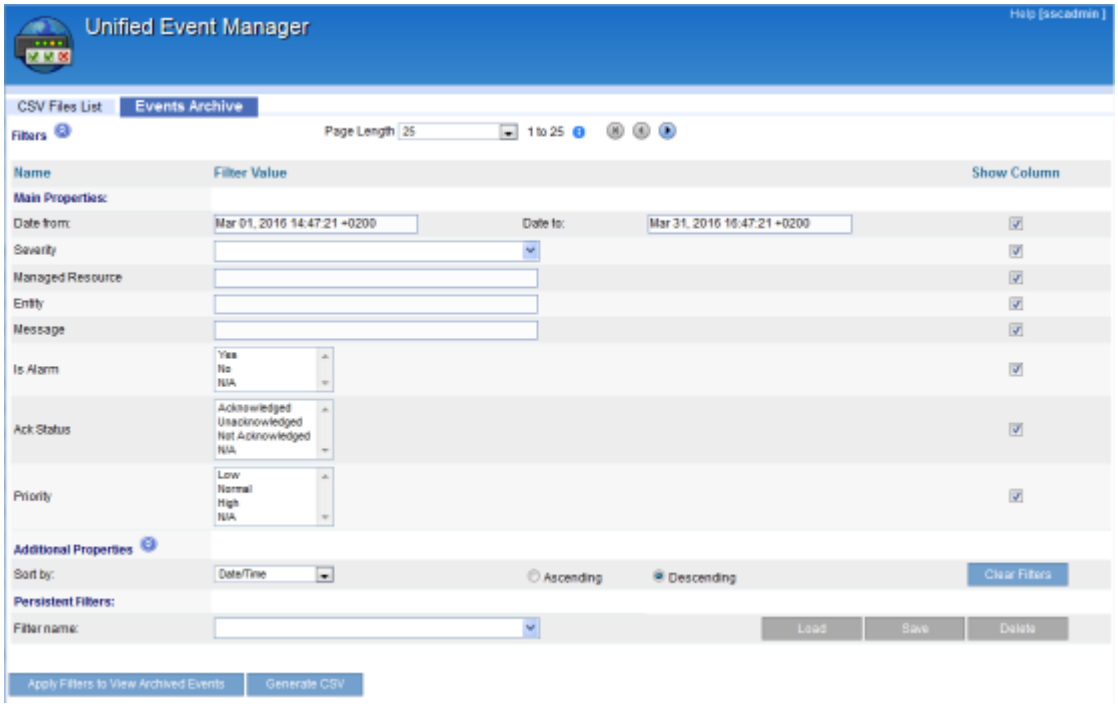
Procedure:

1. Log on to the UEM client with an account that has permissions to view event archives.

   You can change accounts by selecting **Administration** → **Security Administration** from the main menu.
2. From the main menu, select **Logging** → **Event Archive**.
3. In the online administration panel, select the **Events Archive** tab.
4. In the **Events Archive** tab specify the match criteria by which you want to filter the data. Click **Apply Filters to View Archived Events**.

   For information on wildcard characters, see Wildcard Characters for Filtering on page 133.

Figure 57: Events Archive – UEM Client Web Interface



A list of archived events is displayed.

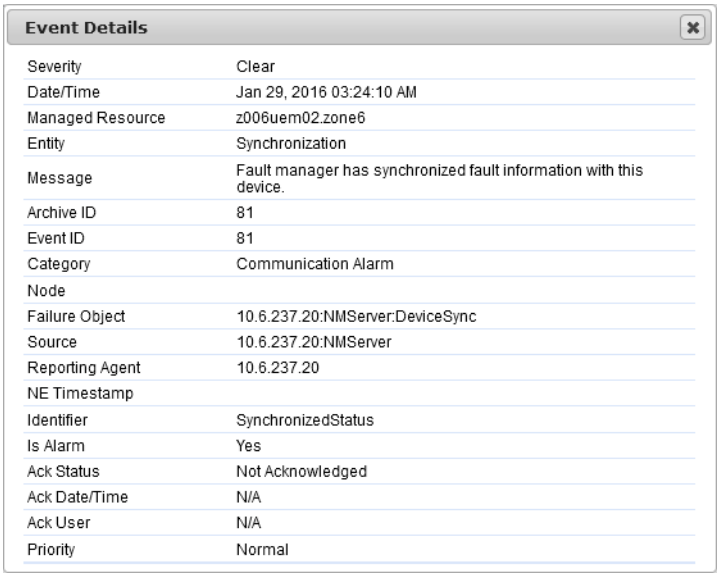
5 Optional: View specific event columns by selecting or clearing appropriate **Show Columns** check boxes.

You can hold down the CONTROL key to select or deselect multiple values for **Is Alarm**, **Ack Status** and **Priority**.

6 Save the specified search criteria by entering a value for **Filter name** and clicking **Save**.

7 Optional: View event details by double-clicking an event.

Figure 58: Event Details – UEM Client Web Interface



The **Event Details** dialog box appears.

8 Click **Generate CSV**.

A `.csv` file with filtered events is sent to the browser. You can open or save the file. The file contains all event properties.

Chapter 7

UEM Troubleshooting

Fault management and troubleshooting information related to Unified Event Manager (UEM) helps you react quickly in case you observe any issues.

7.1

Rediscovering Devices After Device Configuration Change

If you change the configuration of devices discovered in Unified Event Manager (UEM), for example, of objects that UEM displays as Logical Managed Resources (LMR), it is possible that UEM displays traps incorrectly.

For example, this scenario occurs often after you add sites to Zone Controller or configure new site channels and conventional channels for Conventional Channel Gateway (CCGW). Follow this procedure to ensure that UEM displays traps correctly.
Because UEM does not add LMRs automatically, for state transitioning traps that are sent to new objects, UEM determines the impacted managed resource.

Procedure:

Rediscover devices with changed configuration.

Devices are rediscovered and LMRs that reflect the current configuration of the devices are added.

Related Links

Discovering Network Elements on page 198
Discovering Groups of Network Elements on page 200

7.2

Deleting and Discovering Devices After Device Configuration Change

If you change the configuration of devices discovered in Unified Event Manager (UEM), for example, if you change the parameters that are used to identify Logical Managed Resources (LMR), it is possible that UEM displays incorrect reports about LMRs. For example, this scenario occurs usually after you change the site ID for all reporting sites of a device, that is for Zone Controller, Site Controllers, and Conventional Channel Gateway (CCGW). As a result, it is possible that UEM displays two sites: one with the old site ID and the other one with the new site ID, and ZoneWatch grays out site and zone options. Follow this procedure to ensure that after you reconfigure devices in Site Controller to contain a correct site ID, UEM displays correct reports about LMRs.

Procedure:

1. Delete the reconfigured devices.
2. Rediscover devices.

Devices are rediscovered, old LMRs are deleted, and new LMRs are added.

Related Links

Deleting Network Elements on page 187
Discovering Groups of Network Elements on page 200
Discovering Network Elements on page 198

7.3

The Most Common Device Reconfiguration Scenarios Requiring Additional User Actions

Specific types of devices discovered in Unified Event Manager (UEM) need additional actions (typically discovery or rediscovery) performed when their configuration is changed. The following table contains the most common devices and scenarios, for which those actions must be performed.

See Rediscovering Devices After Device Configuration Change on page 255, and Deleting and Discovering Devices After Device Configuration Change on page 255.

Table 61: Configuration change scenarios for the most common devices

Device	Scenario	Actions to perform
Conventional Channel Gateway (CCGW)	Conventional channels have been added, deleted, or reconfigured on the device.	Rediscovering the device.
	A conventional site ID has been changed on the device.	Deleting and discovering the device once again.
Moscad RTU	A new configuration from SDM3000 Builder has been loaded.	Rediscovering the device.
	An instance ID has been changed on the device for any reported network element.	Deleting and discovering the device once again.
	A site ID has been changed on the device for any reported network element.	
PTP	A site ID has been changed on the device.	Deleting and discovering the device once again.
Site Controller	A site ID has been changed on the device.	Deleting and discovering the device once again.
SmartX Site Converter	SmartX site channels have been added, deleted, or reconfigured on the device.	Rediscovering the device.
	A SmartX site ID has been changed on the device.	Deleting and discovering the device once again.
VMware vCenter Server	Virtual machines have been added, deleted, or reconfigured on the device.	Rediscovering the device.
Zone Controller	Sites have been added, deleted, or reconfigured on the device.	Rediscovering the device.
	Site channels have been added, deleted, or reconfigured on the device.	
	A site ID for any site has been changed on the device.	Deleting and discovering the device once again.

Table continued...

Device	Scenario	Actions to perform
	A zone ID has been changed on the device.	

NOTICE: If the configuration change has taken place for a device which is a part of a redundancy group, the specified actions should be performed for both devices in this group.

7.4
Verifying UEM Operation with Geographic Redundancy

Follow this procedure to ensure correct UEM operation for geo-redundant sites.

Procedure:

1. In the **Navigation View** panel, navigate to the site for which you configured geographic redundancy, and click on it.
2. In the **Site View** window, expand the site controller object group.
3. Verify that there are three site controllers:
   - one active – marked as **A**
   - two inactive – marked as **I**

7.5
Client Server Connection is Lost

Unified Event Manager (UEM) displays a message when it detects that the connection to the server is lost.

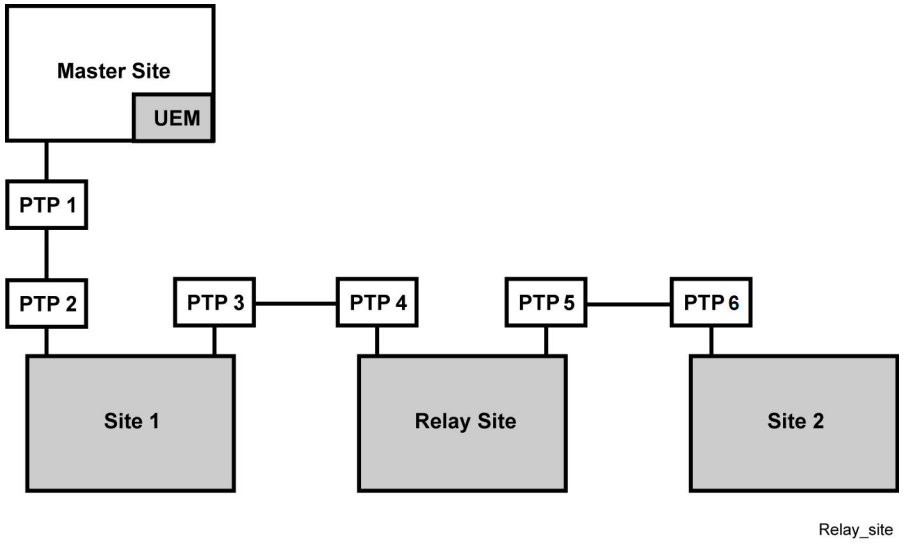
The application is terminated when you click **OK**. To resolve this issue, restart the UEM application.

7.6
Tracking the Status of PTP Devices

The loss of wireless link of a Point-To-Point (PTP) device may result in the loss of connectivity to a large portion of the network, especially if this single link of failure can cause the loss of connectivity (from zone core) to any site(s) that is dependent on this link (for example, ISR site(s) that is connected through a relay site).

For example, if the device marked PTP 1 in the figure shown below goes offline, all the devices in Site 1, Relay Site, and Site 2, as well as PTP devices 2 through 6, report a CommFailure. This means that UEM cannot communicate to these devices at this moment. However, it does not mean that all these resources malfunctioned. Whenever such a massive loss of connectivity occurs, consult your system architecture to identify which PTP device at the highest level (from zone core perspective) cannot be communicated by UEM. It is possible that bringing one PTP device back online can fix connectivity issues with a large portion of the network.

Figure 59: Relay Site – Example



To monitor the status of PTP devices, you can group them in a Custom View (see Custom View Operations on page 127). Try grouping PTP devices based on the “subSystemName” parameter. For example, filter on failures in PTP 2 and all devices in Site 2 (see the figure) using the phrase `*ptp1*,*ptp2*,*site1*`. An asterisk means “any string” and comma means “or”.

You can also find the subnet which the PTP device belongs to. Open the Managed Object Properties dialog box (see Viewing Managed Resource Properties on page 191) and select the **Others** tab. The parentNet field displays the IP address of the subnet in which this PTP device is located. Use the Physical Detail View to monitor the status of the subnet.

7.7 Login Errors

A login error occurs as a result of using an incorrect user ID and password. To resolve this issue, the end user can log on to the application only by specifying an active user ID and an appropriate authentication password.

7.8 Configuring Server Logging

If you want to access Server Logs, see Accessing and Retrieving Server Logs in UEM on page 247. Only Motorola Solutions Support Center (SSC) personnel can update or modify settings for the server log. There are multiple log levels within the server. They are:

- ALL
- DEBUG
- INFO
- WARN
- ERROR
- FATAL
- OFF

A log level can be assigned to a particular application module. For example, if the log level DEBUG is assigned to DISCOVERY, all logs related to DISCOVERY with a level greater or equal DEBUG are logged. The relationship between levels is as follows:

- ALL < DEBUG < INFO < WARN < ERROR < FATAL < OFF

where ALL means most of the information will be logged and OFF means none of the logging information will be published.

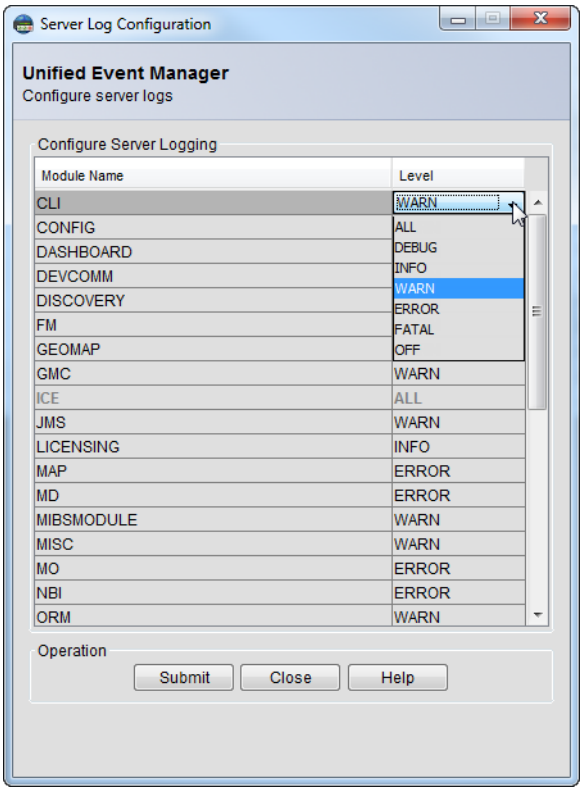
Procedure:

1 From the **Logging** menu, select **Server Logging Configuration**.

2 In the **Server Log Configuration** dialog box, select an appropriate logging level for a given application module.

The drop-down list appears when you click a cell in the **Level** column of the table. Some loggers may have a special meaning and are not manageable through the user interface. In such cases they remain grayed-out.

Figure 60: Server Log Configuration Dialog Box



3 Click **Submit**.

The log level change made to one or more modules of the application is updated on the server. The result of the operation appears at the bottom of the dialog box.

7.9 Configuring Client Logging

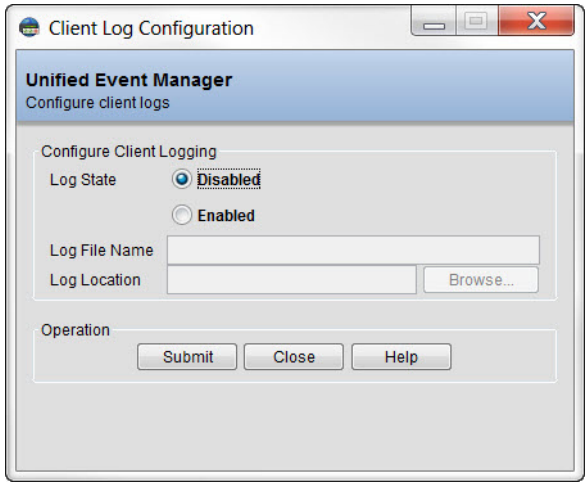
Client log files can be created only by the Motorola Solutions Support Center (SSC) personnel.

Prerequisites: Request SSC to create client log files for you.

Procedure:

1 From the **Logging** menu, select **Client Logging Configuration**.

Figure 61: Client Log Configuration Window



2 In the **Client Log Configuration** dialog box, for the **Log State** radio button, select **Enabled**.

The logging state is disabled by default.

The **Log File Name** and **Log Location** fields are enabled.

3 In the **Log File Name** field, type a valid file name.

The valid file name must not contain any of the following symbols:

- < (less than)
- > (greater than)
- : (colon)
- " (double quote)
- / (forward slash)
- \ (backslash)
- | (vertical bar or pipe)
- ? (question mark)
- * (asterisk)

The file name composed of dots only (one or more) is invalid.

4 Click **Browse** and locate the file in which you want to the save the logs. Click **Submit**.

The status of the operation is displayed at the bottom of the window.

All client logs are logged in the selected text file.

7.10 Command Operation Succeeds but Device Reports a Failure

Unified Event Manager (UEM) displays a message indicating that the command operation succeeded, but an alarm indicating a hardware failure or similar is reported against the device. This situation may occur if the hardware or service against which the command was sent is physically not present or has not been configured. In most cases, it may be necessary to update the configuration of the device to remove the component that is not present. Once the configuration is updated, it may also be necessary to invoke the synchronization operation on the impacted device.

NOTICE: The Zone Controller and Network Management Servers do not report hardware components. The ESXi reports hardware components in the form of transient notifications.

7.11

Discovering Subnets Results in Wrong Assignment of Node Types

During the discovery of subnets that include Virtual Management Server (VMS) and a Network Time Protocol (NTP) server, Unified Event Manager (UEM) sends a Simple Network Management Protocol (SNMP) request to the NTP server that is hosted by VMS.

Although the NTP server does not communicate over SNMP, VMS sends a response to UEM by using the NTP server interface. Follow this procedure when UEM reports the CommFailure alarm on the NTP server or on VMS due to the discovery of an incorrect node type. Possible discovery results are:

- UEM discovers a VMS object as the Generic Node node type
- UEM discovers an NTP server as the ESXi node type
- an NTP server discovered as the ESXi node type is in the CommFailure state

Procedure:

1. Delete all VMS and NTP objects from all affected UEM clients.
2. Discover all VMS objects on each UEM.
3. Verify that all VMS objects are discovered as the ESXi node type.
4. After at least five minutes, discover all NTP objects on each UEM.
5. Verify that all NTP objects are discovered as the Generic Node node type.

The NTP server is discovered as the Generic Node node type and VMS is discovered as the ESXi node type.

7.12

Hardware Troubleshooting

For Unified Event Manager (UEM) hardware troubleshooting, see the *Virtual Management Server Hardware* or *Virtual Management Server Software* manual.

7.13

Hardware Troubleshooting with UEM

The following devices report hardware problems to UEM:

- Archiving Interface Server
- Base Radios
- Comparators (GCM 8000)
- Switches
- Dispatch Consoles
- Generic Application Server
- MOSCAD NMF RTUs
- Network Management Server
- MCC 7500 IP Logging Recorder
- Packet Data Gateway
- Routers
- Site Controllers

- SmartX Site Converter
- Terminal Servers
- Voice Processor Module
- Site Link Relay Module
- ISSI.1 Gateway Module
- MPTT Gateway Module*
- Console Alias Manager Server

* The MPTT Gateway refers to the Public Safety Push To Talk (PTT) Gateway.

To determine the status of these devices, check the severity in the **Network Database** window. See Viewing Managed Resource Properties on page 191.

To view details about the status of the device, check the alarms and events for these hardware components. See Displaying Alarm or Event Details from the Network Database Window on page 153.

7.13.1
Hardware Troubleshooting in Network Database

Process:

1. In the **Network Database** window, select the relevant Generic Application Server and click **View → Events**.

   NOTICE: Hardware events are reported with a `Warning` severity.

2. To see which applications are affected by the hardware event reported by the Generic Application Server, open the **Network Database**. See Viewing Inventory from the Network Database View on page 194.

7.14
Sluggish Performance Monitoring

The Unified Event Manager client application may take a few seconds to become active after it is left running overnight. The same can occur after a few hours of inactivity. This behavior is normal, but if it shows signs of sluggishness, such as being slow to refresh or clicks taking unusually long to respond, it may indicate that application is overloaded.

Determine how many sessions are active on the UEM client (see Active Users Operations on page 135). Make sure that no more than ten sessions are active. If the number of open sessions exceeds ten, close enough sessions to drop to ten or below.

7.15
Performance Management Troubleshooting

If your graph displays any of the following messages, see the appropriate information in this section.

No data available

Reason: By default, automatic data collection starts 10 minutes after the UEM server application is started and the device is discovered. Also, data collection for a newly added statistic starts only after 10 minutes. The message `No data available` means that the data is not collected and there is a delay in the collection process.

NOTICE: For Counter type OIDs, the initial data collected is not stored. When data is collected for the second time, the difference between the two values is calculated and stored. Therefore, depending on the polling interval set, the data is collected again. An additional delay in plotting of data in a graph is possible in the case of Counter type OIDs.

Cannot plot [Data is String Type]

Reason: The collected data from the device is of string type, therefore the graph is not plotted.

Date Range Setting incorrect [From-Date is greater than To-Date]

Reason: The From date and To date that you set in Custom Date Range settings are incorrect. Check for the date/time values set and click **Plot Chart** again.

7.16
Removing Alarms for Deleted Entities

When a managed resource is removed from the Radio System, Unified Event Manager (UEM) can still report alarms against the resource. Follow this process, if the removal of the resource or entity is permanent or if you want to remove the alarms.

Process:

1. Ensure that the configuration of the device is modified to remove the deleted entity from that device using the applicable software (CSS, UNC Device Server, and so on). This changes the device settings to reflect the current configuration.
2. In UEM, go to the **Network Database** view and locate the managed resource (device).
3. Synchronize the device status with UEM (see Synchronizing Managed Resources on page 196). UEM performs a full synchronization on the device with the deleted entity.

   NOTICE: After the synchronization is complete, events from the deleted entity remain, but are only visible in the Network Events view. Alarms for the deleted entity are also removed.
4. Back up the UEM data. For more information, see System Information Backup on page 245.

7.17
Fault Management of Devices in CEN

When a Network Management Alliance (NMA) device with reliable communication can be installed on the ASTRO® system Radio Network Infrastructure (RNI) and Customer Enterprise Network (CEN), consider a few fault management scenarios.

Fault management of an NMA device depends on which network it is installed. The RNI and CEN environments involve using a firewall and the Network Address Translation (NAT) mechanism between the two of them. Because of these mechanisms it is possible that a device that is fully fault managed on RNI by the Unified Event Manager (UEM) server is not reported correctly if it is placed on CEN.

Possible scenarios of device discovery from CEN on UEM:

- A device installed on CEN is able to respond using SNMP to UEM that is installed on RNI. However, the IP address of the UEM server is not the same on CEN and on RNI. As a result UEM discovers the device, however, it is not able to synchronize the device. UEM reports the Communication Failure alarm against the synchronization entity of the device.
- The firewall between RNI and CEN blocks SNMP traffic. UEM can connect with a device only as a result of an Internet Control Message Protocol (ICMP) ping. As a result, UEM discovers the device as a generic node and reports the device as an IP managed device.

- The firewall between RNI and CEN blocks SNMP and ICMP traffic. The device is not accessible from RNI using SNMP and ICMP. As a result UEM does not discover the device because the IP address cannot be reached by using the SNMP or ICMP ping.

If UEM displays a CommFailure message for a managed resource, the potential reason is that the managed resource was re-configured and the maximum number of registered UEM managers was reached. To remanage the resource, reset the resource SNMPv3 data. For information about resetting the SNMPv3 data, see the *SNMPv3* manual.

When a device is discovered on RNI and moved to CEN with the same IP address, UEM displays the device status according to the following scenarios:

- The SNMP and ICMP traffic is not blocked between RNI and CEN. As a result, UEM displays device status as clear until synchronization is requested manually by the user or by the device itself. If synchronization is requested, UEM displays the communication failure alarm against the synchronization entity of the device.
- The SNMP or SNMP and ICMP traffic is blocked by the firewall between RNI and CEN. As a result UEM displays the communication failure alarm against the synchronization and communication entity of the device.

NOTICE:
The communication failure alarm against the Communication entity is displayed in up to two and a half (2.5) minutes.

The communication failure alarm against the Synchronization entity is displayed in up to ten (10) minutes.

7.18
SNMPv3 Devices Troubleshooting

Unified Event Manager (UEM) provides a method of testing the current configuration of SNMPv3 connection for a specified IP address. It provides a status of the connection and the reason for any failed connection attempts.

When credentials are updated and it is not reflected in the user interface, verify login details. For example, if you log on as MotorolaSSC, the default credentials of the Configure North Bound Interface are displayed. If the credentials are updated, verify these changes in the USM table.

Related Links

Groups of Network Elements Managed by UEM on page 42

7.18.1
Outbound SNMPv3 Configuration Tests

Testing for outbound Simple Network Management Protocol version 3 (SNMPv3) configuration ensures that the outbound SNMPv3 communication is working properly.

7.18.1.1
Pinging Network Elements

Use this procedure to verify the connection between UEM and a discovered device, and check for any packet loss or loss of connectivity along the overall path. The ping command sends a series of Internet Control Message Protocol (ICMP) echo request packets to a specified device to determine if a device is alive. If the device does not respond to ping, it will not respond to SNMP communication attempts either.

Procedure:

1 In the **Navigation View** panel, highlight the **Network Database** node.

2 Right-click a specific device in the list and select **Ping**.

The **Ping results** window opens.

3 Wait for the status information to appear.

7.18.1.2
Testing Any Device SNMPv3 Configuration

Procedure:

1 From the main menu, go to **Tools** → **Test Any Device SNMPv3 Configuration**.

2 In the **Test Any Device SNMPv3 Configuration** window, enter the IP address (or hostname) and port number of the network element you want to test. Click **Start**.

The status of the request is updated in the status bar.

7.18.1.3
Testing SNMPv3 Communication Between Network Elements and UEM

Procedure:

1 From the **Network Database**, right-click a managed resource and select **Test SNMPv3 Configuration**.

The **Test SNMPv3 Configuration** window appears. The IP address and the port number are populated automatically.

2 Click **Start**.

NOTICE: Alternatively, you can also test the outbound SNMPv3 communication between a network element and UEM by clicking **Tools** → **Test Any Device SNMPv3 Communication**. Enter the IP address and port number of the network element you want to test, and click **Start**. The status of the request is updated in the status bar.

The status of the request appears.

7.18.2
SNMPv3 Inbound Communication Tests

To test inbound SNMPv3 communication for devices capable of reliable communication, invoke synchronization. See Synchronizing Managed Resources on page 196. You can also determine if a device is capable of Reliable Communication. See Determining Reliable Communication Capability of a Managed Resource on page 192.

If Synchronization succeeds and no CommFailure alarm for it is generated, then the inbound communication is configured properly. If a CommFailure alarm is generated for synchronization, see “Synchronization Failure: Synchronization Cycles” section in SNMP Communication Alarms and Events on page 265. Testing inbound communication for devices incapable of Reliable Communication requires sending a trap from the device to UEM.

NOTICE: For detailed procedure on how to send traps from a device consult the specific device manual.

7.18.3
SNMP Communication Alarms and Events

The connection between devices and Unified Event Manager (UEM) is constantly monitored by the Supervision procedure. If any change in the connection state occurs it is reported in form of an alarm

for communication entity stating the nature of change as well as the reason for it. Additional events or alarms may be generated depending on the situation.

CommFailure Alarm on UEM

UEM displays a communication failure alarm message for one or more managed resources with the CommFailure severity (see Severity Definitions on page 65). This alarm indicates that UEM has lost its ability to communicate with the device. For IP managed devices it can occur if the device ceases to respond to ICMP queries. For devices communicating via SNMPv3, it can occur under any one of the following conditions:

- Loss of connectivity
- Unstable or noisy link
- SNMPv3 configuration mismatch
- SNMP interface errors
- Device out-of-synchronization with UEM (this situation may be related to many conditions)
- Failed Manager Registration on the device
- Device out-of-synchronization with the UEM (this situation may be related to many conditions)

NOTICE: For event details, see the “Alarms and Events” chapter in the *Unified Event Manager Online Help*.

CommFailure Alarm for Legacy Site Controller Managed Resources

UEM displays a communication failure message with the CommFailure severity for Site Controller managed resources if the following situation occurs:

- UEM communicates over SNMPv1 with a Site Controller managed resources
- the Site Controller is **not** enabled
- Site Controller managed resources do not work correctly

UEM displays the communication failure message with the CommFailure severity instead of indicating the real state of the managed resource because of SNMPv1 limitations.

The solution is to enable the Site Controller. Contact Motorola Solutions Support Center (SSC) to enable the Site Controller for you.

Synchronization Failure: Synchronization Cycles

Synchronization process can be started either by the user according to Synchronizing Managed Resources on page 196 or by the UEM after the supervision process, after discovery process or during a regular synchronization cycle for devices not capable of reliable communication. If UEM initiates the synchronization process it is not displayed as a separate job (see Viewing Job Status on page 141), as is the case when the user invokes it manually. Therefore a state change of a synchronization alarm may occur, though the user did not specifically request synchronization of a device.

Synchronization Failure: Misconfiguration of SNMP Credentials

If Synchronization fails due to a credential problem, then the SNMP credentials for the device are most likely not configured properly. Communication for devices managed by UEM is performed by two SNMP users: MotoMaster and MotoInform. MotoMaster is used by devices that are incapable of reliable communication, while MotoInform is used by those capable of Reliable Communication. To determine whether a device is capable of Reliable Communication see Reliable Communication on page 39.

Depending on the capability of reliable communication of the device verify that the credentials for the required SNMP user are set properly. To change them see Configuring Global SNMPv3 Credentials for the MotoMaster User on page 83 and Configuring Global SNMPv3 Inform Credentials on page 84.

Warnings (due to credentials mismatch)

Whenever UEM receives an inform which it is unable to process due to a mismatch in SNMP credentials for MotoInformA or MotoInformB account, a warning event is generated stating a credential failure.

7.19 Digital Notification Troubleshooting

This section provides guidelines for troubleshooting Digital Notification.

7.19.1 Testing E-mail Action Configuration

The Send Test E-mail functionality does not provide status of this operation. To check the status, see e-mail logs or check the e-mail client.

Process:

1. Configure E-mail action as described by the manuals or open an existing one.
2. Click **Send Test E-mail** to send an e-mail and confirm the operation.
3. Check the mail on the mail server using the client.
4. Check e-mail server logs. See Accessing and Retrieving Server Logs in UEM on page 247.
5. Check the latest entries and look for an e-mail with content described in Test E-mail Content on page 284.

7.19.2 Checking E-mail Action Operation Status

E-mail logs are available through the UEM client. The logs contain information about the status of each e-mail sending operation. See Accessing and Retrieving Server Logs in UEM on page 247.

The content of each log entry includes:

- Status of operation (Failed/Success and reason)
- E-mail recipient
- Alarm/Event ID
- Alarm/Event Source
- Alarm/Event Severity
- E-mail subject
- E-mail text

To check the status of an operation, open the log file and search for particular event or alarm details.

7.19.3
Checking If a Certificate Is in the `.der` Format

OpenSSL toolkit is an open source set of tools available at http://www.openssl.org. It can be used for a variety of tasks related to SSL certificates. Follow the link provided to learn the terms of use and installation procedures.

Procedure:

1. Copy the file to the system where OpenSSL is installed.
2. Issue command: `Openssl x509 –in-form DER –in <certificate_file_path> –text`.

   If the command succeeds, it prints out details of the certificate. If the command fails but the path is correct, the certificate is not in `.der` format. For more information, see http://www.openssl.org.

Example:
A failed OpenSSL check:

```
openssl x509 -in e-mail_cert.pem -inform DER -text
unable to load certificate
4472:error:0D0680A8:asn1 encoding routines:ASN1_CHECK_TLEN:wrong
tag:tasn_dec.c:
1282:
4472:error:0D07803A:asn1 encoding
routines:ASN1_ITEM_EX_D2I:nested asn1 error:ta
sn_dec.c:374:Type=X509
```

A successful OpenSSL check:

```
openssl x509 -in e-mail_cert.cer -inform DER -text

Certificate:
 Data:
 Version: 3 (0x2)
 Serial Number:
 15:cb:32:6a:00:01:00:00:00:09
 Signature Algorithm: sha1WithRSAEncryption
 Issuer: DC=com, DC=test, DC=uem, CN=test-uem
 Validity
 Not Before: Mar 11 02:38:33 2009 GMT
 Not After : Mar 11 02:48:33 2010 GMT
 Subject: CN=test.uem.com
 Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 RSA Public Key: (2048 bit)
 Modulus (2048 bit):
 <data>
 Exponent: 65537 (0x10001)
 X509v3 extensions:
 X509v3 Subject Key Identifier:

47:3B:74:F2:DB:6C:CE:03:12:D6:1E:57:00:C9:62:C2:9E:81:81:1C
 X509v3 Extended Key Usage:
 TLS Web Server Authentication
 X509v3 Key Usage: critical
 Digital Signature, Key Encipherment
 X509v3 Subject Alternative Name: critical
 DNS:test.uem.com
 X509v3 Authority Key Identifier:
```

```
keyid:1D:29:7E:D0:4B:57:93:E5:35:C9:DF:00:E6:E9:A2:9E:00:90:28:BD

X509v3 CRL Distribution Points:


Signature Algorithm: sha1WithRSAEncryption
7c:ed:5b:03:79:b1:aa:c4:b0:cf:ec:ad:e4:a5:33:ab:5b:82:
98:59:c4:9b:10:b3:a2:e1:8c:4b:24:44:d0:c4:97:9d:4c:86:
dd:96:81:44:4a:f4:8d:27:be:94:ad:e0:4d:23:ec:a4:ab:41:
0f:35:45:60:5b:5e:61:b2:46:84:39:49:dc:ce:69:66:0f:c4:
7c:9f:35:13:b4:bf:02:31:9d:f7:69:ef:7c:15:0e:c0:a5:09:
08:25:b4:4c:46:29:40:04:bb:76:51:af:96:be:d4:69:04:8c:
72:0f:2a:89:54:ce:6e:14:92:19:e6:7f:28:80:c1:bd:92:61:
85:e5:fd:48:89:33:fd:e9:a6:36:f3:83:ef:be:ce:73:d4:12:
00:59:30:bc:5a:76:71:e1:39:b4:bc:13:5c:e0:70:55:c1:e2:
68:27:10:5a:ee:32:9e:cd:a2:05:85:9b:da:e5:82:1a:b4:a5:
43:01:5d:52:df:71:92:c9:b0:4b:5d:e9:69:3d:2e:bc:6f:a2:
cc:02:8d:23:25:52:11:81:72:d4:7a:cd:4a:f0:8d:e9:a2:72:
d1:21:5f:33:42:12:e8:73:1b:68:8d:3c:67:6a:23:40:2b:fe:
3e:89:1f:56:82:ff:35:9d:fa:11:d7:a9:93:6b:1e:f8:41:2d:
ab:9f:61:e6
```

7.19.4
Certificate Details

The certificate contains several fields that allow checking who issued the certificate, and what the characteristics are. The user should verify the certificate before importing it to UEM.

The key parameters of the certificate are:

- Organization details for which the certificate has been issued
- Serial number
- Fingerprint (the name thumbprint is also used)
- Security parameters

The certificate details (selected items) are displayed to the user during the installation on UEM for verification and acceptance.

You can obtain certificate details using one of the following ways:

- Checking Certificate Details Using GUI Tools on page 270
- Use OpenSSL toolkit to print certificate details. For more information, see Checking If a Certificate Is in the .der Format on page 268.
- Checking Certificate Details Using Admin Menu on page 271

7.19.4.1

Checking Certificate Details Using GUI Tools

Operating systems usually provide tools – browsers that allow you to display certificate details. For example, Microsoft Windows provides a certificate viewer.

Figure 62: Certificate Viewer Details A

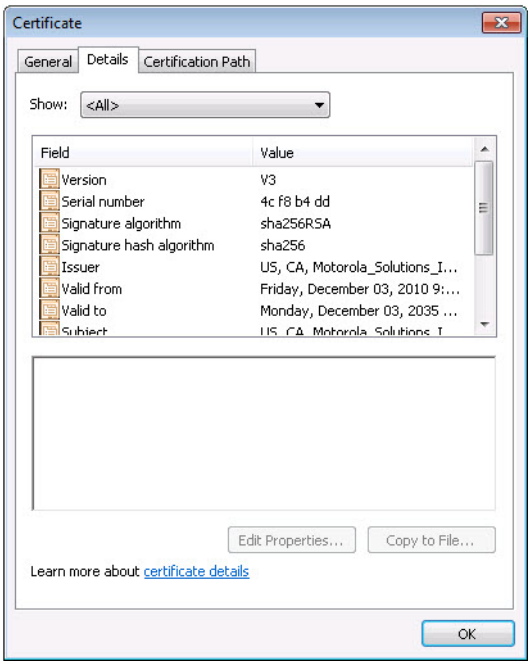
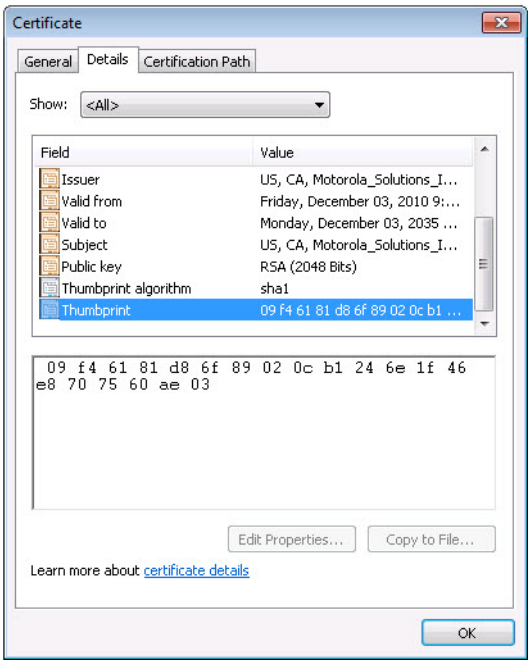


Figure 63: Certificate Viewer Details B



7.19.4.2

Checking Certificate Details Using Admin Menu

Log on as the server administrator and, from the admin menu, select **Unified Event Manager Administration → Mail Server SSL Certificate Management → Show installed certificate**.

Example:

```
 Mail Server SSL Certificate Management (* - Option not available)
**************************************
  1. Install SSL Certificate
  2. Display Installed SSL Certificate
  3. Remove SSL Certificate
  h. Help
  b. Back to Previous Menu
  q. Quit
Enter selection (1-3,h,b,q): 2
Installed certificate details:
---------------------------------
Alias: mailsslcertificatealias
[
[
  Version: V3
  Subject: CN=simulator, OU=Automatically-generated SSL key, O=AXIGEN Mail
Server
  Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

  Key:  Sun RSA public key, 1024 bits
  modulus: xxxxxxxxxxxxxxxx
  public exponent: xxxxx
  Validity: [From: Tue Mar 06 02:24:33 CST 2012,
              To: Wed Mar 06 02:24:33 CST 2013]
  Issuer: CN=simulator, OU=Automatically-generated SSL key, O=AXIGEN Mail
Server
  SerialNumber: [    xxxxxxxx xxxxxxxx]

Certificate Extensions: 1
[1]: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
   SSL server
]

]
  Algorithm: [SHA1withRSA]
  Signature:
0000: XX XX XX XX XX XX XX XX   XX XX XX XX XX XX XX XX  ................
0010: XX XX XX XX XX XX XX XX   XX XX XX XX XX XX XX XX  ................
0020: XX XX XX XX XX XX XX XX   XX XX XX XX XX XX XX XX  ................
0030: XX XX XX XX XX XX XX XX   XX XX XX XX XX XX XX XX  ................
0040: XX XX XX XX XX XX XX XX   XX XX XX XX XX XX XX XX  ................
0050: XX XX XX XX XX XX XX XX   XX XX XX XX XX XX XX XX  ................
0060: XX XX XX XX XX XX XX XX   XX XX XX XX XX XX XX XX  ................
0070: XX XX XX XX XX XX XX XX   XX XX XX XX XX XX XX XX  ................

]
```

7.19.5

Converting the Certificate to the `.der` Format with OpenSSL

In most cases, the mail server administrator can provide the certificate in the `.der` format. However, if the certificate is in a different format, but still compatible with the x509 standard, the user can convert the certificate using one of the many available commercial or open source tools. The OpenSSL toolkit

is an open source set of tools available at http://www.openssl.org. It can be used for a variety of tasks related to SSL certificates. Follow the link provided to learn the terms of use and installation procedures.

Procedure:

1. Copy the certificate file to the system with the OpenSSL tool (see OpenSSL tool details).
2. Determine the certificate format.
3. Convert the file format, as described in the documentation at http://www.openssl.org.

Example: PEM to `.der` format conversion:

```
openssl x509 –inform PEM –in original_certificate_file.cer
–outform DER –out converted_certificate_file.cer
```

7.19.6
Checking If Server Supports STARTTLS Using Telnet Session

By using a telnet client, you can check an e-mail server by connecting to the server port on which the server is listening for Simple Mail Transfer Protocol (SMTP) client connections. This procedure helps you debug problems with secure communication. To confirm server configuration and support STARTTLS, contact your mail server administrator.

Procedure:

1. Open the telnet client and connect to the server, specifying the address and port.
2. When the connection is made, issue the following command: `EHLO myhost`.

   The server responds with a list of extensions supported.
3. Check if STARTTLS is on the list. If the EHLO command is unsuccessful, repeat it.
4. Issue the command STARTTLS.

   If the server supports STARTTLS, a message about server readiness appears.

Example: Message informing you that a server supports STARTTLS:

```
220 moto-qn1j2o8dnk.uem.test.com ESMTP MAIL Service ready at Fri,
13 Mar 2009 01:56:38 -0700

EHLO uem-host
250-moto-qn1j2o8dnk.uem.test.com Hello [XXX.XX.XXX.XX]
250-SIZE 10485760
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-STARTTLS
250-AUTH LOGIN
250-8BITMIME
250-BINARYMIME
250 CHUNKING
STARTTLS
220 2.0.0 SMTP server ready
```

7.20

Troubleshooting CommFailure Caused by Wrong DDP Metadata

A Fault Management Toolkit device can display a CommFailure alarm which is cleared within two minutes, and displayed again within ten minutes. This behavior can be caused by an error in the Polling Properties in the Device Definition Package (DDP) describing the device type.

Prerequisites: FMToolkit 1.0 is installed on the PC.

When and where to use: Perform this process to verify the correctness of the metadata in the `.ddp` file describing the device type.

Process:

1. In the Fault Management Toolkit, load the `.ddp` file.

   See *Loading and Updating an Existing Device Definition Package* in the *Fault Management Toolkit Developer Guide*.

2. In the **Polling Definitions** panel, open every polling object from the **Polling List**.
3. In the **Polling Properties** tab, verify the varbinds are of the correct type by perform the following actions:

   a. In the **MIB browser**, after making sure appropriate MIBs are loaded, open the MIBs and verify the OIDs.

   b. Execute the following command:`/opt/Motorola/ca/bin/snmpwalk` ***`<device_SNMP_credentials><IP address>`*** `.1`

   Where ***`<device_SNMP_credentials>`*** are appropriate device SNMP credentials, and ***`<IP address>`*** is the physical IP address of the device.

   Step example:

```
# /opt/Motorola/ca/bin/snmpwalk -c public -u MotoInformA
44.114.9.10 .1
SNMPv2-MIB::sysDescr.0 = STRING: HP Sotrage Works P2000 G3 SAS
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.1000
SNMPv2-MIB::sysUpTime.0 = Timeticks: (101010) 0:16:50.10
SNMPv2-MIB::sysContact.0 = STRING: sysContact
SNMPv2-MIB::sysName.0 = STRING: DAS_HP_P2000_A7_13_0_1255
SNMPv2-MIB::sysLocation.0 = STRING: sysLocation
SNMPv2-MIB::sysServices.0 = INTEGER: 2147483647
RFC1213-MIB::ifNumber.0 = INTEGER: 1
```

4. Reload the `.ddp` file into the UEM database.

   See Loading DDPs on page 143.

This page intentionally left blank.

Appendix A

Digital Notification

This appendix provides additional information concerning the Digital Notification feature.

A.1
Digital Notification Introduction

In Unified Event Manager (UEM), Digital Notification is a service that allows sending an e-mail notification upon receiving an event or alarm matching user-defined criteria. The e-mails are sent to an external mail server by using Simple Mail Transfer Protocol (SMTP).Secure and non-secure e-mail communication is a licensed UEM service that is available only for users with a feature license for the e-mail notification service. For more information about licenses, see the *License Manager* manual.

Glossary

SMTP
Simple Mail Transfer Protocol

TLS
Transport Layer Security

SSL
Secure Socket Layer

MTA
Mail Transfer Agent

x509
Certificate encoding standard

RFC
Request For Comments standards documentation

DER
Distinguished Encoding Rules – Certificate encoding standard

PEM
Privacy Enhanced Mail – Certificate encoding standard

CEN
Customer Enterprise Network

STARTTLS
SMTP standard extension for secure mail communication

A.2
Digital Notification Concepts

This section provides an overview of the concepts related to Digital Notification.

A.2.1
Digital Notification Overview

The main purpose of the Digital Notification functionality is to provide the operator with the ability to receive digital notifications about fault events occurring in the ASTRO® 25 system. E-mail communication has been chosen as the mechanism for these digital notifications.

Some advantages of the e-mail technology are:

- common (well-known technology)
- simple to configure
- simple to use

An external mail server is required to receive digital notifications. The mail server is not included in the ASTRO® 25 system. It is assumed that your organization owns the mail server or delegates/outsources mail server or services management to an external organization.

Simple Mail Transfer Protocol (SMTP) has been chosen from many mail standards and protocols. It is a standardized and commonly used technology. Additional extensions to SMTP are supported, such as authentication and secure communication with SSL/TLS.

A.2.2
Architecture and Operation Concepts

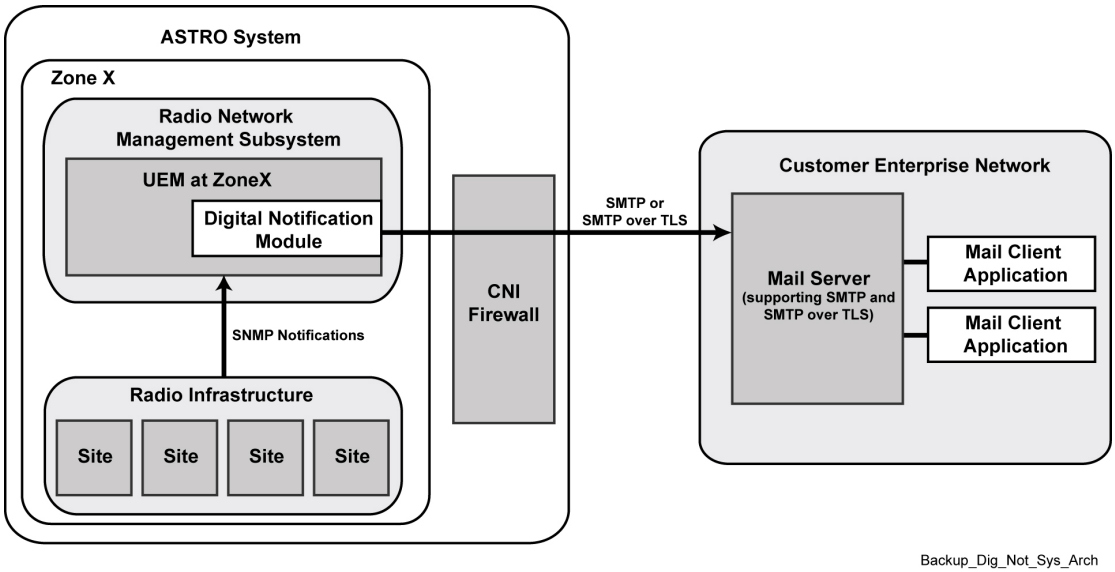
For each occurrence of a condition in the system, an event is created in Unified Event Manager (UEM) and presented to the user in the **Network Events** window. The event details allow the user to identify the source of the event and details of the problem. In some cases, if the event indicates a failure or Change in a state, it is elevated to an alarm and is presented in the **Alarms** window.

The operator can configure filters to select desired events or alarms and associate an action to be executed when the desired events/alarms occur. When the event/alarm occurs, UEM checks filters and if it finds a matching filter, then actions related to that filter are executed.

One of the possible action types is an e-mail action. The user may choose to send an e-mail notification to an external server. Based on configuration parameters entered by the user, UEM sends the e-mail to a specific mail server at a specific e-mail address with the content defined by the user. For each event or alarm, there is a separate e-mail message sent to the mail server. After sending an e-mail, UEM logs information about the operation status in a separate log.

The following figure shows typical architecture of the system configured to send digital notifications from UEM.

Figure 64: Digital Notification System Architecture



UEM is located in a specific Zone in the RNMS subsystem. UEM manages fault information from all discovered devices and creates Events and Alarms. The user can create an alarm or event filter to select specific information and assign an e-mail action to the filter to generate an e-mail each time the filter criteria are met. Based on the configuration of the e-mail action, UEM sends an e-mail to an external mail server using SMTP in clear or secure mode. The mail server is located outside of the ASTRO® 25 system in the Customer Enterprise Network and is managed by either the customer or another company. The connection between the ASTRO® 25 system and the CEN is realized by the Customer Network Interface.

A.2.3
Concepts and Standards

This section provides an overview of concepts and standards which apply to Unified Event Manager (UEM). It covers reporting, protocol support, and secure communication.

A.2.3.1
Zone-Level Events Reporting

The Unified Event Manager (UEM) application server reports fault status information from devices assigned to a particular zone where UEM operates. Similarly, e-mail notifications which are based on fault reporting from the devices are zone-specific.

A.2.3.2
Simple Mail Transfer Protocol (SMTP) Support

Unified Event Manager (UEM) supports Simple Mail Transfer Protocol (SMTP) and selected extensions. SMTP has been chosen as a widely used and standardized solution. The supported SMTP

standard is *RFC 821 - Simple Mail Transfer Protocol*. For more information, see Digital Notification Standards and References on page 287.

A.2.3.3
Simple Mail Transfer Protocol (SMTP) Service Extensions Support

Unified Event Manager (UEM) requires a mail server with support for an SMTP service extensions standard. The standard is *RFC 1869 SMTP Service Extension Support*. For more information, see Digital Notification Standards and References on page 287.

A.2.3.4
Simple Mail Transfer Protocol (SMTP) Authentication Extension Support

Unified Event Manager (UEM) supports the authentication extension to Simple Mail Transfer Protocol (SMTP). Details are described in the standard *RFC 2554 - SMTP Service Extension for Authentication*. For more information, see Digital Notification Standards and References on page 287.

A.2.3.5
Client Only Functionality

Unified Event Manager (UEM) server acts as an SMTP client. Therefore, it is capable only of sending e-mails.

A.2.3.6
Message Content Configuration

The content of messages sent from Unified Event Manager (UEM) can be dynamically populated with the content of the event/alarm which triggered the e-mail action.

A.2.3.7
Event and Alarms Filtering

E-mail actions are attached to event or alarm filters which are used to select specific types of events or alarms for which the e-mail actions are performed.

A.2.3.8
Secure Communication

Optionally, Unified Event Manager (UEM) supports secure e-mail communication using the SMTP over TLS protocol and the STARTTLS extension. Details are described in the *RFC 2487 - SMTP Service Extension for Secure SMTP over TLS*. For more information, see Digital Notification Standards and References on page 287.

A.2.3.9
Certificates Usage for Secure Communication

SSL certificates are used for secure e-mail communication. The certificate must conform the following standards: *RFC 3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* and *ITU standard x690 - Specification of Distinguished Encoding Rules (DER)*.

A.2.4
Digital Notifications

By default, e-mails are sent using Simple Mail Transfer Protocol (SMTP). The SMTP communication is not encrypted.

SMTP is supported by all major mail server vendors on the market.

The user has to provide authentication account and password parameters that are used on the mail server for authentication.

NOTICE: The whole communication takes place over an unencrypted link and thus your organization has to assume the message details are disclosed to external parties.

A.2.5
Secure Digital Notifications

Secure communication is an optional feature. The secure communication requires special configuration steps and a mail server that supports secure communication standards described in this section. Secure communication is accomplished by using STARTLS to initiate secure connection and the TLS protocol which provides a secure channel for SMTP communication.

STARTTLS allows the mail client to negotiate a secure connection with a mail server, if it is supported. First of all, the non-secure connection is upgraded to a secure connection with the use of the SSLv3/ TLSv1 protocol. A valid SSL certificate is necessary to establish a secure channel between the client and the server. When a connection is successfully upgraded to a secure connection, SMTP communication continues and uses optional authentication. All data is sent over an encrypted link.

IMPORTANT: If the server does not support the STARTLS, the connection fails. Other security standards are not supported (for example “SMTP over SSL”).

A.3
Digital Notification Configuration

This section provides an overview of Digital Notification configuration.

A.3.1
Basic Configuration

Basic configuration steps include:

- Creating an alarm/event or editing an existing one.
- Creating an E-mail Action or editing/choosing an existing one.
- Optionally testing configuration.
- Saving new configuration.

For more information about configuration parameters, see Alarm Filters Configuration on page 105 and Event Filters Configuration on page 112.

A.3.2
Secure Mode Configuration

In the secure e-mail mode, an additional step of configuring the SSL certificate is required.

The following configuration is recommended:

- Import the SSL certificate, and disable and re-enable the Unified Event Manager (UEM) application server.
- Create an alarm/event or edit an existing one.
- Create an E-mail Action or edit/choose an existing one and set the secure mode.
- Optionally, test the configuration.
- Save the new configuration.

For more information about configuration parameters, see Alarm Filters Configuration on page 105 and Event Filters Configuration on page 112.

For information about installing the certificate configuration, see the *Private Network Management Servers* manual.

A.3.3
Configuration Input

Basic Parameters

- Server address
- E-mail address of the recipient
- E-mail address of the sender
- Message subject
- Message content

To successfully send e-mail messages, valid server address and e-mail address of the recipient are required.

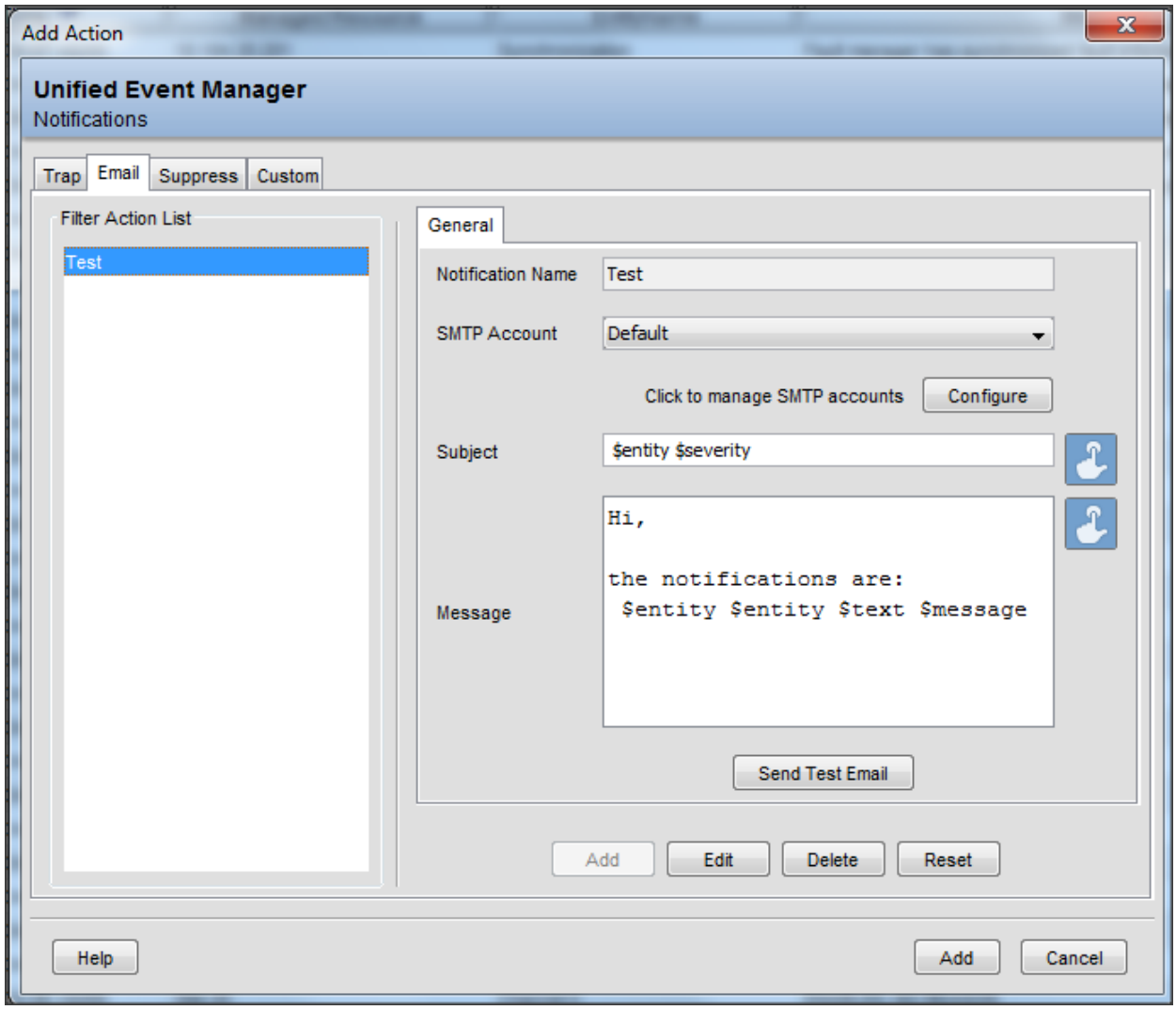
NOTICE: The mail server must be configured to properly handle the e-mail received. Store the e-mail in the mailbox if it is locally managed or relay the e-mail to the correct server if the mailbox is on a different server.

If the user chooses to respond to the e-mail received from Unified Event Manager (UEM), the e-mail address of the sender is used.

NOTICE: UEM provides SMTP client functionality only. It is not capable of receiving e-mail. This field is intended to identify the source of the e-mail notification (for example, uem@z001uem01.zone1) or redirect the reply to a valid address (for example, support@motorola.com).

The message subject and content contain details on an event or alarm that has occurred in the system. The content of these fields can be populated with the content of a particular event or alarm and/or custom text.

Figure 65: Add Action Window – E-mail Message



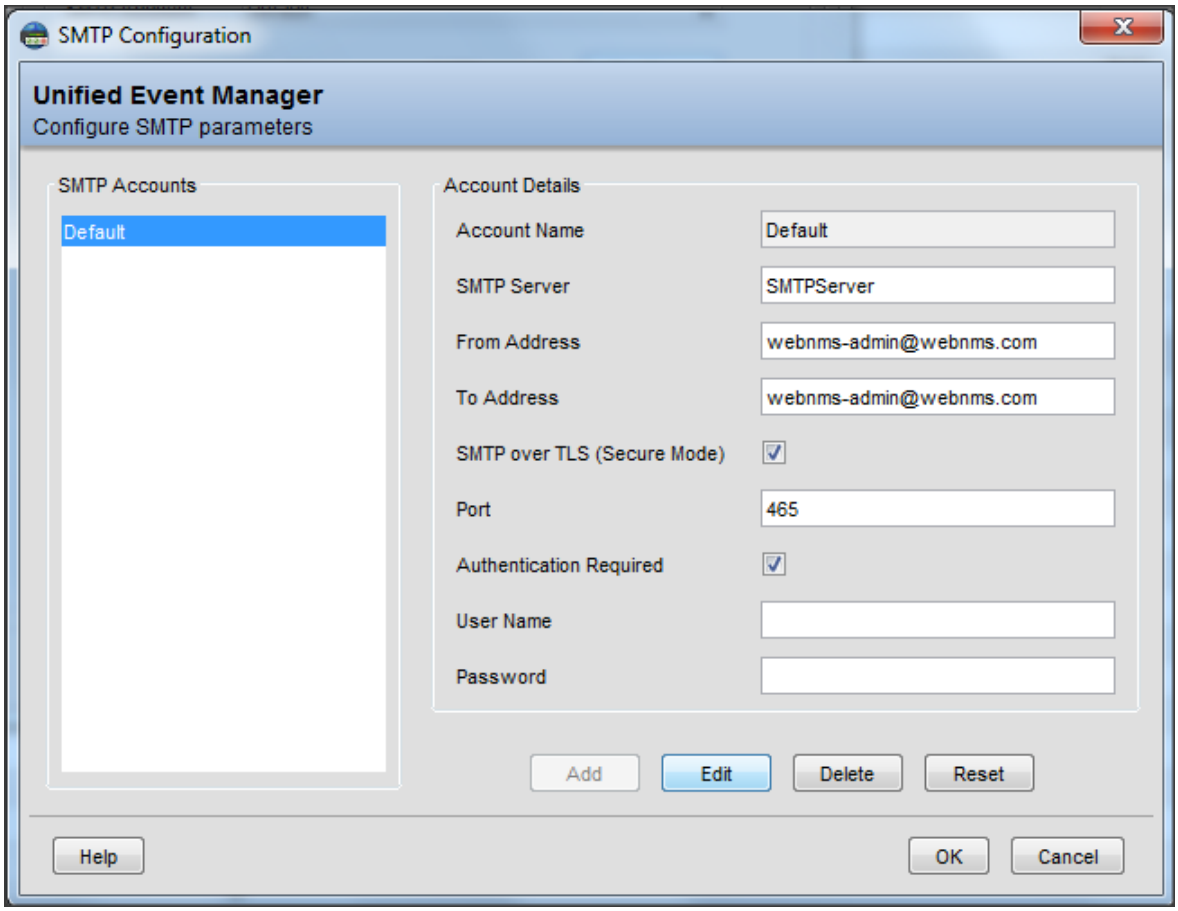
E-mail Account Configuration

In UEM, a communication mode and Simple Mail Transfer Protocol (SMTP) port are used globally in all e-mail actions. SMTP communicates in two modes: non-secure and secure. The non-secure SMTP communication mode is the default mode set in UEM. The default port value set for non-secure SMTP communication is 25. The secure SMTP communication mode uses the Transport Layer Security (TLS) protocol. The default port value set for secure SMTP communication is 465.

Typically, mail servers support secure communication on port 465 or port 587. However, mail server administrators can configure devices to use other ports. Contact your mail server administrator to verify the port settings.

NOTICE: By default, the Radio Network Infrastructure (RNI) firewall allows communication on the following SMTP ports: 25, 465, and 587. If your mail server configuration uses a custom port, before using Digital Notification, contact the Solution Support Center (SSC) to ensure that this custom port is unblocked on the RNI firewall.

Figure 66: SMTP Configuration



A.3.3.1
Filter Criteria

For each filter, a set of match criteria can be configured by user. By default, the criteria are empty, which means that all events and alarms match them.

It is recommended to narrow down the match criteria, especially for event filters. Using the defaults can cause too many e-mails to be sent to the mail server.

For more information about configuration parameters, see Alarm Filters Configuration on page 105 and Event Filters Configuration on page 112.

A.3.3.2
Message Content

The message subject and text can be dynamically populated with certain details from event or alarm messages. To include these dynamic values, select them from the list available in the e-mail action dialog.

NOTICE: A dynamic value is a word or phrase between $ at the beginning and a whitespace at the end separating this value from the other selected values. If a dynamic value that you selected does not exist in an event or alarm, no information regarding this property will be provided in the e-mail.

$category
The category of the event or alarm.

$entity
The failure object or entity which has the problem indicated by this event or alarm. The Entity and the Failure Object refer to the same property.

$text $message
A descriptive text message about the event or alarm.

$severity
The severity of the event or alarm.

$stringseverity
The severity of the event or alarm as text.

$source
The ManagedObject to which the event or alarm corresponds.

$managedResourceDisplayName
The user-friendly name of the managed object which the event or alarm corresponds to.

$reportingAgent
The IP Address of the device (agent) sending the alarm.

$neTimeStamp
The time at which the Event was generated on the device.

$identifier
This attribute is an internal attribute that uniquely identifies a particular event and can be used by a northbound manager to determine if the event is a duplicate without relying on the event text.

Additional dynamic variables can be used. See documentation sections listed at the end of this section.

For more details on configuration parameters, see Alarm Filters Configuration on page 105 and Event Filters Configuration on page 112.

A.3.4
SSL Certificate

SSL certificates are used to provide secure connection between the Unified Event Manager (UEM) server and the mail server.

The certificates are provided by the mail server administrator. If the certificate format is other than `.der`, the file has to be converted to the `.der` format. Usually the administrator can generate certificates in a specific format. For more information, see UEM Troubleshooting on page 255.

IMPORTANT: Only one certificate can be installed at a given time, which implies that only one secure server can be used at a given time.

SSL certificates are managed from the Unified Event Manager Administration Menu. To access the Mail Server SSL Certificate Management Menu, perform the following actions:

1. Log on as the UEM server administrator and provide the valid password.
2. Run `admin_menu`.
3. Select `OS Administration`.
4. Select `Security Provisioning`.
5. Select `Mail Server SSL Certificate Management`.

The `Mail Server SSL Certificate Management` menu is as follows:

```
Mail Server SSL Certificate Management
**************************************
1. Install SSL Certificate
2. Display Installed SSL Certificate
3. Remove SSL Certificate
```

```
h. Help
b. Back to Previous Menu
q. Quit
Enter selection (1–3,h,b,q):
```

The following options are available:

Install SSL Certificate
Installs the certificate from the file provided by the mail server administrator.

Display Installed SSL Certificate
Checks if the certificate is installed. If the certificate is installed, the certificate details are displayed.

Remove SSL Certificate
Allows removing the installed certificate.

NOTICE: To apply changes after installing or removing the certificate, UEM server has to be disabled and re-enabled.

The following is an example of an SSL certificate being installed from a CD.

```
Mail Server SSL Certificate Management (* - Option not available)
*************************************
  1. Install SSL Certificate
  2. Display Installed SSL Certificate
  3. Remove SSL Certificate
  h. Help
  b. Back to Previous Menu
  q. Quit
Enter selection (1-3,h,b,q): 1
Enter path to certificate file:
/cdrom/cdrom0/axigen.cer
Enter alias for certificate:
axigen_cert
Owner: CN=AXIGEN, OU=Automatically-generated SSL key, O=AXIGEN Mail Server
Issuer: CN=AXIGEN, OU=Automatically-generated SSL key, O=AXIGEN Mail Server
Serial number: XXXXXXXXXXXX
Valid from: Wed Mar 11 17:33:54 UTC 2010 until: Thu Mar 11 17:33:54 UTC 2011
Certificate fingerprints:
MD5: XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX
SHA1: XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX

Do you want to import the certificate (y/n):
y
Certificate was added to keystore
---------------------------------
Certificate Successfully Installed.
Please disable and re-enable the UEM to start using the new certificate.
```

To change or install a new certificate, the previous one has to be removed and the new or updated certificate installed. It is best to do both operations with the UEM server disabled.

For more details on configuration parameters, see Alarm Filters Configuration on page 105 and Event Filters Configuration on page 112.

For information on how to install the certificate, see the *Private Network Management Servers* manual.

A.3.5
Test E-mail Content

The **Send Test E-mail** functionality available from e-mail action configuration windows is intended to send test message using the destination and connection parameters specified in the action.

The following parameters are used to send the test e-mail:

- Server address

- To e-mail ID
- From e-mail ID
- Authentication settings: user and password
- Connection parameters: mode and port

The test e-mail content is:

- Subject: “Test E-mail”
- Content:

```
TIME: <Timestamp>
This is test E-mail
```

- Example of timestamp: `Mon Mar 30 12:08:00 UTC 2009`

A.3.6
Mail Server Compatibility

Digital notifications in clear mode should be compatible with any mail server that supports Simple Mail Transfer Protocol (SMTP) implemented according to the RFC 821 standard.

Digital notifications in secure mode are compatible with mail servers supporting secure mail standard RFC 2487. Especially STARTTLS must be supported and configured on the mail server.

The following servers had been tested with secure mail functionality:

- Microsoft Exchange Server 2007
- IBM Lotus Domino version 8.5
- Sendmail version 8.14.3
- Axigen Mail Server version 6.2.2

IMPORTANT: Motorola Solutions does not provide the mail server. Provide the mail server and ensure that the server is configured according to the standards described in this document. Especially:

- Ensure the server supports STARTLS and all mentioned standards.
- Ensure the server is configured to use STARTLS on a particular port. For more information, see UEM Troubleshooting on page 255.
- Ensure the user can get the SSL certificate from the mail server administrator.

A.3.7
Installing and Configuring PageGate Server

Follow this procedure to install and configure the third-party PageGate server. Page Gate provides capability to translate SMTP e-mail messages to dialup pages. It allows you to configure the UEM to receive paging notifications, instead of e-mails, for alarm and event filters. PageGate runs as a Windows service and can be installed either inside or outside the Motorola Solutions Radio Network.

For more information, see http://www.notepage.net/pagegate.htm

NOTICE: There are other software solutions and services that may be used for e-mail to pager integration.

Procedure:

1. Download the PageGate Server setup file.
2. Navigate to the download directory and double-click `setup.exe`.
3. Select **Install PageGate Server**.

4 Follow the on-screen instructions to complete the installation.

5 When the installation completes, from the Windows **Start** menu, run the PageGate admin application.

6 In the **PageGate Setup** window, perform the following actions:

   a Leave default directory values.

   b Select the **Scheduler** check box.

   c Select the **GetMail** check box.

   d Select the **Connector1** check box.

   e Click **Apply**.

7 When prompted to create database, log, and archive directories, click **Yes**.

8 When prompted, restart the application.

9 From the PageGate explorer window, select **Registration**.

10 In the **Registration Information** window, enter software registration information and key. Click **Apply**.

   The **Version** and other information in the upper right corner populate once the registration and key information is applied.

11 From the PageGate explorer window, select **Program** → **Settings**, and perform the following actions:

   a In the **Run PageGate As** section, select **Window Service**.

   b Select the **Scheduler** check box.

   c Select the **GetMail** check box.

   d Select the **Connector1** check box.

   e Click **Apply**.

12 In the **NT Service Login Information** window, leave the fields blank and click **Apply**.

13 From the PageGate explorer window, select **Interfaces** → **GetMail** → **Settings** and perform the following actions:

   a Select the **Enable** check box.

   b In the **Local Domain** field, enter a name for the local domain.

   c Click **Apply**.

   d When prompted whether to enable the interface for all existing recipients and groups, click **Yes**.

14 From the PageGate explorer window, select **Connectors** → **Connector1** → **Settings**, and perform the following actions:

   a From the **Initial String** drop-down list, select **(auto)**.

   b In the **Dialing Prefix** window, add any dialing prefixes required for this line.

   c From the **Dedicated Carrier** drop-down list, select **(none)**.

   d From the **Serial Port** drop-down list, select a serial port number that corresponds to the modem and connected telephone line.

15 In the PageGate explorer window, right-click the **Carrier** member, select **Add**, and performing the following actions:

   a In the **Carrier** field, enter a name for the paging service being added.

   b In the **Protocol** field, select the appropriate dial-out protocol.

c In the **Phone Number** field, enter the access number to the paging service.

d Based on the requirements of the service provider, select the modem configuration.

e Click **Apply**.

16 In the PageGate explorer window, add pager recipients by performing the following actions:

a Right-click the **Recipients** member and select **Add**

b Optional: In the **Recipient** field, enter a custom recipient name.

c Under **Enabled Services**, make sure only **Get Mail** check box is selected.

d Enter the pager information for the recipient.

e Click **Apply**.

f Repeat step 16 to add more recipients.

17 In the PageGate explorer window, configure groups of recipients by performing the following actions:

a Right-click the **Groups** member and select **Add**.

b In the **Description** field, enter a group description.

c In the **Group** field, enter a group name.

d Select the **GetMail** check box.

e Click **Apply**.

A.4 Digital Notification Standards and References

This section provides reference materials concerning Digital Notification.

A.4.1 Simple Mail Transfer Protocol (SMTP)

RFC 821 - Simple Mail Transfer Protocol: http://tools.ietf.org/html/rfc821

A.4.2 Simple Mail Transfer Protocol (SMTP) Extensions

RFC 1869 - SMTP Service Extensions: http://tools.ietf.org/html/rfc1869

Abstract: *"This memo defines a framework for extending the SMTP service by defining a means whereby a server SMTP can inform a client SMTP as to the service extensions it supports. Extensions to the SMTP service are registered with the IANA. This framework does not require modification of existing SMTP clients or servers unless the features of the service extensions are to be requested or provided."*

RFC 2554 - SMTP Service Extension for Authentication: http://tools.ietf.org/html/rfc2554

Abstract: *"This document defines an SMTP service extension [ESMTP] whereby an SMTP client may indicate an authentication mechanism to the server, perform an authentication protocol exchange, and optionally negotiate a security layer for subsequent protocol interactions. This extension is a profile of the Simple Authentication and Security Layer [SASL]."*

A.4.3 Simple Mail Transfer Protocol (SMTP) over TLS and STARTLS

RFC 2487 - SMTP Service Extension for Secure SMTP over TLS

http://tools.ietf.org/html/rfc2487

Abstract:

"This document describes an extension to the SMTP (Simple Mail Transfer Protocol) service that allows an SMTP server and client to use TLS (Transport Layer Security) to provide private, authenticated communication over the Internet. This gives SMTP agents the ability to protect some or all of their communications from eavesdroppers and attackers."

A.4.4
Certificate Standards

RFC 3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (applicable sections only): http://tools.ietf.org/html/rfc3280

Abstract: *"This memo profiles the X.509 v3 certificate and X.509 v2 Certificate Revocation List (CRL) for use in the Internet. An overview of this approach and model are provided as an introduction. The X.509 v3 certificate format is described in detail, with additional information regarding the format and semantics of Internet name forms. Standard certificate extensions are described and two Internet-specific extensions are defined. A set of required certificate extensions is specified. The X.509 v2 CRL format is described in detail, and required extensions are defined. An algorithm for X.509 certification path validation is described. An ASN.1 module and examples are provided in the appendices."*

ITU standard x690 - Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER):

https://www.itu.int/rec/T-REC-X.690-201508-I/en

A.4.5
Unified Event Manager Online Help

The *Unified Event Manager Online Help* is accessible from the Unified Event Manager (UEM) client application from the main menu.

A.4.6
Unified Event Manager Manual

The *Unified Event Manager* manual is available as part of the ASTRO® 25 documentation.

A.4.7
Private Network Management Servers Manual

The *Private Network Management Servers* manual is available as part of the ASTRO® 25 documentation.

Appendix B

Terminal Session Software Installation

The following procedures describe the installation of software necessary to launch terminal sessions for Motorola Base Radio - CS (MOSCAD), Motorola Receiver - ATAC 3000, or TeNSr/IMACS Channel Bank network elements managed on Unified Event Manager (UEM) through SDM3000 SCADA. Installation of the following software must be performed by an administrator.

Related Links

Launching Remote Connector Terminal Sessions on page 185

B.1
Installing Serial/IP

Serial/IP is used for launching terminal sessions for Motorola Base Radio - CS (MOSCAD) and Motorola Receiver - ATAC 3000 on systems with Windows 7.

Installation of this tool is not required on Windows 10.

Procedure:

1. Insert the *SDM Builder* media into the optical drive.
2. Using Windows Explorer, navigate to the ***<D:>***`\Install\Serial-IP Version 4.9.2\Native\` directory, and double-click `SerialIP.msi`.

   Where ***<D>*** is the letter corresponding to your optical drive.
3. In the **Welcome** dialog box, click **Next**.
4. In the **License Agreement** dialog box, select **I accept the license agreement** , and click **Next**.
5. In the **User Information** window, perform the following actions:
   a. In the **Full name** field, enter an appropriate user name.
   b. In the **Organization** field, enter the organization name.
   c. In the **License key** field, type the license key you received with the installation CD.
   d. Click **Next**.
6. Follow the on-screen instructions to complete the installation.

   If this is first installation of the Serial/IP Redirector on this computer, the Select Port dialog box appears. Otherwise, the Serial/IP Control Panel dialog box appears.

   NOTICE: If no dialog box appears, open the **Serial/IP Control Panel** dialog box by opening the **Start** menu and selecting**Programs** → **Serial-IP** → **ControlPanel**.
7. If COM4 port is not present, click **Select Ports…**, and in the **Select Port** dialog box, select **COM4** and click **OK**

Postrequisites: Verify that Serial/IP appears in the list of installed programs in the Microsoft Windows Control Panel.

B.2
Installing Motorola Radio Service Software

Motorola Radio Service Software (RSS) is used for launching terminal sessions for Motorola Base Radio - CS (MOSCAD) and Motorola Receiver - ATAC 3000 on systems with Windows 7.

Installation of this tool is not required on Windows 10.

Procedure:

1. From Motorola Online https://businessonline.motorolasolutions.com/, download the Motorola Radio Service Software setup file.
2. Using Windows Explorer, navigate to your download directory and double-click the installation file.
3. Follow the on-screen instructions to complete the installation.

B.3
Installing HyperACCESS

HyperACCESS is a tool for launching terminal sessions for TeNSr/IMACS Channel Bank on systems with Windows 7 and 10.

Procedure:

1. Insert the *SDM Builder* media into the optical drive.
2. Using Windows Explorer, navigate to ***<D:>***`\Install\HyperACCESS- v9.0\Native` directory, and double-click `h32setup.exe`.

   Where ***<D>*** is the letter corresponding to your optical drive.
3. In the **HyperACCESS Setup** dialog box, click the **Install HyperACCESS** button.
4. Follow the on-screen instructions to complete the installation.
5. When the installation process completes, in the **User Information** window, perform the following actions:
   a. In the **Name** field, enter an appropriate user name.
   b. In the **Company** field, enter the company name.
   c. In the **Serial Number** field, enter a valid product serial number.
   d. Click **Next**.
6. In the **Select a Connection** dialog box, select **Choose from among the existing connections** and click **Next**.
7. In the **Existing Connections** dialog box, Select **WinSock (TCP/IP)** and click **Next**.

   The **Transfer Folders** dialog box appears
8. Follow the on-screen instructions to complete the setup.
9. In the **Hilgraeve Product Registration** dialog box, perform the following actions:
   a. Clear the **Inform me of product news and updates via e-mail** option.
   b. Select the **Remind me to register later** option.
   c. Click **Finish**.
   d. When prompted by the **Please Register** dialog box, click **OK**.
10. In the **HyperACCESS** dialog box, click **Yes**.

11 In the **Default Telnet Application** dialog box, select the check box next to the **Stop asking me this question** option, and click **No**.

12 Open HyperACCESS by clicking the Start button. In the search box, type: `HyperACCESS`

13 In the dialog box, allow other users to run HyperACCESS by clicking **Yes**.

Postrequisites: Verify that HyperACCESS appears in the list of installed programs in the Microsoft Windows Control Panel.

B.4

Installing Remote Connector

Remote Connector is used for launching terminal sessions on systems with Windows 7 and 10.

Procedure:

1 Depending on your system, perform one of the following actions:

- If you are using an L/M core system, insert the *PRNM Suite* media into the optical drive.
- If you are using a K core system, insert the *UEM Client Conf* media into the optical drive.

2 Using Windows Explorer, navigate to the optical drive and double-click `RemoteConnector.msi`.

The setup window appears.

3 Wait for the installation to complete and click **Finish** to exit the installer.

This page intentionally left blank.