System Release 7.18
ASTRO® 25

INTEGRATED VOICE AND DATA

SNMPv3
Feature Guide

MAY 2022

MN005414A01-J

Intellectual Property and Regulatory Notices

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.

No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission of Motorola Solutions, Inc.

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.

License Rights

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.

Open Source Content

This product may contain Open Source software used under license. Refer to the product installation media for full Open Source Legal Notices and Attribution content.

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

The European Union's WEEE directive and the UK's WEEE regulation require that products sold into EU countries and the UK must have the crossed-out wheelie bin label on the product (or the package in some cases). As defined by the WEEE directive, this crossed-out wheelie bin label means that customers and end-users in EU and UK countries should not dispose of electronic and electrical equipment or accessories in household waste.

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

Disclaimer

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

Contact Us

The Centralized Managed Support Operations (CMSO) is the primary contact for technical support included in your organization's service agreement with Motorola Solutions.

Service agreement customers should be sure to call the Centralized Managed Support Operations (CMSO) in all situations listed under Customer Responsibilities in their agreement, such as:

- Before reloading software
- To confirm troubleshooting results and analysis before taking action

Your organization received support phone numbers and other contact information appropriate for your geographic region and service agreement. Use that contact information for the most efficient response. However, if needed, you can also find general support contact information on the Motorola Solutions website, by following these steps:

1. Enter motorolasolutions.com in your browser.
2. Ensure that your organization's country or region is displayed on the page. Clicking or tapping the name of the region provides a way to change it.
3. Select "Support" on the motorolasolutions.com page.

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 or title of the section with the error
- A description of the error

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

Document History

Version	Description	Date
MN005414A01-A	Original release of the *SNMPv3 Feature Guide*.	September 2018
MN005414A01-B	In the following sections, added information on the need for restoring SNMP service on non-certified hardware after some Windows 10 upgrades: • Installing the Configuration Utility for Windows on page 39 • Installing the SNMPv3 Common Agent Software on page 41	October 2019
MN005414A01-C	Added content for Gen10 support and ESXi 6.5 with new user interfaces. Updated section: Configuring the License Manager for SNMPv3 on page 137.	January 2020
MN005414A01-D01	Updated section: Changing SNMPv3 User Security Level on page 113	May 2020
MN005414A01-E	Sections added: • SLC Series Terminal Servers Configuration for SNMPv3 on page 124 • Configuring the Lantronix Terminal Server for the noAuth/noPriv Mode on page 124 • Configuring the Lantronix Terminal Server for the Auth/noPriv Mode on page 124 • Configuring the Lantronix Terminal Server for the Auth/Priv Mode on page 125 Sections updated: • Device Configuration for SNMPv3 on page 52 • Local Configuration on page 45 • LX Series Terminal Servers Configuration for SNMPv3 on page 120 • Logging On to a LX Series Terminal Server on page 120 • Configuring a LX Series Terminal Server for the noAuthNoPriv Mode on page 121 • Changing a LX Series Terminal Server From noAuthNoPriv Mode to AuthNoPriv Mode on page 122 • Changing a LX Series Terminal Server From noAuthNoPriv Mode to AuthPriv Mode on page 122	October 2020

Version	Description	Date
	• Changing a LX Series Terminal Server From AuthNoPriv Mode to AuthPriv Mode on page 122 • Changing a LX Series Terminal Server From AuthNoPriv Mode to noAuthNoPriv Mode on page 123 • Changing a LX Series Terminal Server From AuthPriv Mode to noAuthNoPriv Mode on page 123	
MN005414A01-F	New sections: • Configuring SNMPv3 Passphrases on DSC 8000 for MotoAdmin Account on page 72 • Configuring SNMPv3 Passphrases on DSC 8000 for Other USM Accounts on page 73 • Resetting SNMPv3 Passphrases to Default on DSC 8000 on page 153 Sections updated: • SNMPv3 Deployment Scope on page 21 • Required USM User Accounts on page 30 • Local Configuration of Site Elements on page 51 • SNMPv3 Communication Matrix on page 53	June 2021
MN005414A01-G	Sections updated: • Device Configuration for SNMPv3 on page 52 • Configuring Console Site Elements, Dynamic Transcoders, and Group Data Gateways for SNMPv3 on page 66	July 2021
MN005414A01-H	Sections updated: • Resetting SNMPv3 Passphrases to Default on DSC 8000 on page 153 • Logon Information on page 153	February 2022
MN005414A01-J	Sections updated: • Configuring the Lantronix Terminal Server for the noAuth/noPriv Mode on page 124 • Configuring the Lantronix Terminal Server for the Auth/noPriv Mode on page 124 • Configuring the Lantronix Terminal Server for the Auth/Priv Mode on page 125	May 2022

Contents

List of Figures

List of Tables

List of Processes

List of Procedures

About SNMPv3 Feature Guide

The Simple Network Management Protocol (SNMP) is a set of protocols used for managing complex networks. The SNMP application layer protocol facilitates the exchange of management information between network devices. It is built on the User Datagram Protocol (UDP). SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

SNMP version 3 (SNMPv3) is a secured protocol for delivering network management traffic between a manager and agents.

This manual provides information relating to the implementation and management of the SNMPv3 protocol in an ASTRO® 25 system.

Related Information

Refer to the following documents for associated information about the radio system:

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 R56 manual. This document may be purchased by contacting the Centralized Managed Support Operations (CMSO).
Overview and Recovery for Systems with Juniper SRX Routers Reference Guide	Provides an overview of the new system features, technical illustrations, and system-level disaster recovery that support the ASTRO® 25 radio communication system with Juniper SRX routers.
Enterprise OS Software Reference Guide	Provides detailed information about commands and syntax for all Enterprise OS (EOS) software service parameters.
Enterprise OS Software User Guide	Provides information on how to use Enterprise OS (EOS) software to operate and configure system routers and gateways.
Motorola GGM 8000 Hardware User Guide	Includes hardware installation, basic software configuration, and cabling instructions for the Motorola GGM 8000 gateway. Available on Motorola Online: https://businessonline.motorolasolutions.com To access the manuals, select **Resource Center→ Product Information→ Manuals→ Network Infrastructure→ Routers and Gateways**.

Related Information	Purpose
Motorola Network Router (MNR) S2500 Hardware User Guide	Includes hardware installation, basic software configuration, and cabling instructions for Motorola Network Router (MNR) S2500 routers. Available on Motorola Online: https://businessonline.motorolasolutions.com To access the manuals, select **Resource Center**→ **Product Information**→ **Manuals**→ **Network Infrastructure**→ **Routers and Gateways**.
Motorola Network Router (MNR) S6000 Hardware User Guide	Includes hardware installation, basic software configuration, and cabling instructions for Motorola Network Router (MNR) S6000 routers. Available on Motorola Online: https://businessonline.motorolasolutions.com To access the manuals, select **Resource Center**→ **Product Information**→ **Manuals**→ **Network Infrastructure**→ **Routers and Gateways**.

Chapter 1

SNMP Description

Simple Network Management Protocol version 3 (SNMPv3) is the security protocol used in the ASTRO® 25 system.

1.1 What Is SNMP?

The Simple Network Management Protocol (SNMP) is a set of rules that various end points in a network use when they communicate. 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) and User Datagram Protocol/Internet Protocol (UDP/IP) suites.

SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

Reliable fault information is also a part of SNMP. In an ASTRO® 25 system, the fault information involves utilizing INFORM requests as a mechanism to deliver some critical fault traps from devices to the Unified Event Manager (UEM).

1.1.1 SNMP Versions

SNMP currently has the following versions:

Version 1

(SNMPv1) is the original simple request-response protocol and framework of SNMP. The Network Management system issues a request, and the managed devices return responses. Four protocol operations are used in an SNMPv1 framework: GET, GETNEXT, SET, and TRAP.

Version 2

(SNMPv2) improves upon SNMPv1 protocols and adds two new protocol operations: GETBULK and INFORM.

GETBULK is an operation used on both the agent and manager side of the communications. The manager uses this operation to retrieve statistics for performance management.

Version 3

(SNMPv3) offers improved security through support for authentication with or without encryption and provides a Management Information Base (MIB) access control scheme. SNMPv3 supports the User-Based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. The View-based Access Control Model (VACM) is the SNMPv3 approach for MIB access control.

1.1.2 SNMPv3 Security Features

SNMP offers protection against threats such as:

Modification of Information

SNMP prevents an unauthorized entity from altering messages or values generated by an authorized entity in the system.

Masquerade
SNMP prevents an unauthorized entity from assuming the identity of an authorized entity in order to perform management operations.

Message Stream Modification
SNMP prevents the malicious reordering, delaying, or replaying of messages that result in the disruption of normal sub-network service operation. This disruption could cause unauthorized management operations.

Disclosure
SNMP prevents eavesdropping on the exchanges between SNMP engines.

1.2 SNMPv3 in the ASTRO 25 IVD System

The use of SNMPv3 is the solution chosen to resolve known security issues of SNMPv1 and SNMPv2.

ASTRO® 25 system components can operate in the following modes:

- Some components always use SNMPv3 only, for example: Ethernet switch in both the High Performance Data (HPD) site, and Integrated Voice and Data (IV&D) site.
- Some components must support SNMPv3 and previous SNMP versions at the same time, for example: InfoVista, Configuration/Service Software (CSS), Software Download Manager (SWDL), and (at a subsystem level) the Radio Network Management subsystem.
- Some components must support both SNMPv3 and previous SNMP versions, but not at the same time. That is, they use only one or the other SNMP version at a time, depending on the context or application.

1.2.1 SNMPv3 Deployment Scope

The following are some of the many possible variants of SNMPv3 deployment in the ASTRO® 25 system:

- Devices enabled for SNMPv3, for example: Zone Controller
- Devices not enabled for any version of SNMP or IP fault management, for example: Firewall Management Server (FMS)
- Devices with limited SNMPv3 support (not fault managed by UEM), for example: GMC

NOTE:
By limited default SNMPv3 support, it is understood that the device runs on Windows Server 2012 and is not fault managed by UEM but has the Windows SNMPv3 Common Agent installed and configured for fault management. For details, see "SNMPv3 Common Agent Installation" and "Configuring the SNMPv3 Agents" in the *SNMPv3 Feature Guide*.

For details of SNMPv3 deployment and information on the type of fault management of particular devices, refer to the configuration section specific to that device. See "Device Configuration for SNMPv3" in the *SNMPv3 Feature Guide*.

Table 1: SNMPv3 Deployment in ASTRO 25 Systems

Subsystem/Site	Device	SNMPv3 Deployment Scope
Fault Management	SDM3000 RTU	**Enabled for SNMPv3** The SDM3000 RTU is fault managed as an agent by the fault manager using SNMPv3.

Subsystem/Site	Device	SNMPv3 Deployment Scope
		An SDM3000 RTU operating in the SNMPv3 mode is allowed to use SNMPv1 to communicate as a manager with third-party devices at a site supporting SNMPv1 (as long as the site forwards this traffic using SNMPv3). This applies only to third-party devices. **NOTE:** The Generic MIB (Management Information Base) feature only supports SNMPv3 between the SDM3000 RTU and a third-party fault manager. However, SNMPv2 are still supported between the SDM3000 RTU and the downstream devices.
High Performance Data (HPD) Site	**Enabled for SNMPv3:** • Configuration/Service Software (CSS) • GCP 8000 Site Controller (HPD SC) • GTR 8000 Base Radio (HPD BR) • Repeater (ISR) Sites • Simulcast Sites • Software Download Manager (SWDL)	
Network Transport Subsystem (note that at Analog Conventional Sites, this includes the Conventional Channel Interface, if enabled)	**Enabled for SNMPv3:** • Conventional Channel Interface • Ethernet LAN switches • Fortinet firewalls • MNR routers and GGM 8000 gateways • Terminal Servers • Juniper SRX **Exceptions (not enabled for SNMPv3):** • The Simulcast Site Reference (SSR) and Network Time Protocol Server (NTPS) are IP managed by the fault manager without using SNMP. The Simulcast Site Reference (SSR) and Network Time Protocol Server (NTPS) are IP managed by the fault manager without using SNMP.	
Network Transport Management Subsystem	**Enabled for SNMPv3:** • GCP 8000 Site Controller (SC) • InfoVista server as manager for routers • IV&D Conventional PDG • Packet Data Gateway (PDG)	
	Exception (not enabled for SNMPv3):	
	As a manager for other devices, InfoVista uses SNMPv1 and SNMPv2 only.	
Zone Controller Subsystem	**Enabled for SNMPv3:** Zone Controller (ZC)	
Data Subsystem	**Enabled for SNMPv3:** Packet Data Gateway (PDG) and IV&D Conventional PDG, in both IV&D and HPD systems.	

Subsystem/Site	Device	SNMPv3 Deployment Scope
	Exception (not enabled for SNMPv3):	
	The PDG is restricted to SNMPv1 access for the Zone Database Server (ZDS).	
System Traffic Monitoring Subsystem (STM)	**Enabled for SNMPv3:** Air Traffic Router (ATR)	
Private Network Management (PNM) Subsystem	**Enabled for SNMPv3:** • License Manager (LM) • Software Download Manager (SWDL) • System Statistics Server (SSS) • Unified Event Manager (UEM) Server • Unified Network Configurator (UNC) • Unified Network Configurator Device Server (UNCDS) • User Configuration Server (UCS) • Zone Database Server (ZDS) • Zone Statistics Server (ZSS) **NOTE:** For devices managed by the UEM and Unified Network Configurator (UNC) only: • Only SNMPv3 is used for all SNMP-based communications with devices designated in this table as being enabled for SNMPv3. • For all other SNMP communication, only SNMPv1 and SNMPv2 are used.	
Repeater (ASR) Sites	**Enabled for SNMPv3:** • Configuration/Service Software (CSS) • GCP 8000 Site Controller (Private SC) • GTR 8000 Base Radio (Site Repeater BR) • Software Download Manager (SWDL)	
Simulcast Sites	**Enabled for SNMPv3:** • Configuration/Service Software • DSC8000 • GCP 8000 Site Controller (Simulcast SC) • GCM 8000 Comparator • GPB 8000 Reference Distribution Module (RDM) • GTR 8000 Multisite Base Radio (MsBR) • GPW 8000 Voting Receiver • Software Download Manager	
Logging Subsystem	**Enabled for SNMPv3:** • The MCC 7500 IP Logging Recorder is fault managed using SNMPv3 by the UEM. • The Replay system is IP managed.	

Subsystem/Site	Device	SNMPv3 Deployment Scope
Dispatch Console Subsystem	**Enabled for SNMPv3:** • Archiving Interface Server (AIS) • Configuration/Service Software (CSS) • MCC 7500 VPM Dispatch Console • MCC 7500E Dispatch Console • PRX 7000 Console Proxy • MKM 7000 Console Alias Manager (CAM) • Voice Processor Module (VPM)	
Conventional Fixed Radio Subsystem	**Enabled for SNMPv3:** • Configuration/Service Software (CSS) • DCG 9000 Gateway • GCM 8000 Conventional Comparator • GRV 8000 Conventional Comparator • GCP 8000 Site Controller (Conventional SC) • GPW 8000 Receiver • GTR 8000 Base Radio (Conventional BR) • Software Download Manager (SWDL)	
Telephone Interconnect Subsystem	**Enabled for SNMPv3:** • Configuration/Service Software (CSS) • Cisco Console Telephony Media Gateway • Telephone Media Gateway (TMG)	
	Exceptions (not enabled for SNMPv3):	
	The following devices are IP managed by the fault manager (without using SNMP): • NEC IP PBX Server • NEC Media Gateways • NEC Console Telephony Gateway • NEC/AudioCodes Console Telephony Media Gateway	
Information Security and Management Subsystem	**Exceptions (not enabled for SNMPv3):**	
	The following devices are IP managed by the fault manager (without using SNMP): • Firewall Management applications, if deployed • Firewall Management Server, if deployed	
IP Services Subsystem	**Enabled for SNMPv3:** • Backup and Restore Server (BAR) • Domain Controllers/Authentication Servers • IP Packet Capture	
	Not enabled for SNMPv3 (IP managed by the fault manager):	

Subsystem/Site	Device	SNMPv3 Deployment Scope
	• Centralized Event Logging Server • Firewall Management Server (FMS)	
	Limited SNMPv3: • Core Security Management Server (CSMS) • InfoVista	
ISSI.1 Network Gateway	**Enabled for SNMPv3:** • ISSI.1 Gateway Module • Site Link Relay Module	
Inter-System Gateway Subsystem	**Enabled for SNMPv3:** Inter-System Gateway (ISGW)	
Key Management	**Enabled for SNMPv3:** Authentication Center (AuC)	
Time and Frequency Reference Subsystem	**Enabled for SNMPv3:** • Backhaul Switch • PTP devices • TRAK devices	
Server Virtualization Subsystem	**Enabled for SNMPv3:** Direct Attached Storage (DAS) Management Controller	
Dynamic Transcoder Subsystem	**Enabled for SNMPv3:** Dynamic Transcoder	
Group Data Gateway Subsystem	**Enabled for SNMPv3:** Group Data Gateway (GDG)	
Data Applications Subsystem	**Enabled for SNMPv3:** Personnel Accountability Server	

Chapter 2

SNMPv3 Theory of Operations

Simple Network Management Protocol Version 3 (SNMPv3) supports several security mechanisms.

2.1 SNMPv3 Security Levels

There are three SNMPv3 security levels.

Without authentication and without privacy (noAuthNoPriv)
SNMPv3 traffic does not require authentication by the receiving side, and the message is not encrypted. This is the default operational scenario for SNMPv3 (also known as *clear mode*).

With authentication but without privacy (AuthNoPriv)
SNMPv3 traffic requires authentication by the receiving side, and the message is not encrypted.

With authentication and with privacy (AuthPriv)
SNMPv3 traffic requires authentication by the receiving side, and the message is encrypted.

Table 2: SNMPv3 Security Levels for Network Elements

Security Level	Security Level Definition	AuthProtocol and AuthPassword	PrivProtocol and PrivPassword
AuthPriv	SNMP messages are sent with authentication and with privacy	Yes	Yes
noAuthNoPriv	SNMP messages are sent without authentication and without privacy	No	No
AuthNoPriv	SNMP messages are sent with authentication but without privacy	Yes	No

2.1.1 SNMPv3 and Secure Communication

Secure operation means SNMPv3 authentication is enabled, with or without encryption. Therefore, an attempt to break into the system (as indicated in the following list) is unsuccessful.

A system configured with the required information enables SNMPv3 secure communication between relevant system devices.

The security afforded by SNMPv3 only protects the system against certain intrusions. Other types of intrusions are prevented by other security features in the system.

The types of intrusions that are successfully prevented are:

- Interception of SNMP messages by eavesdroppers and attempts to decode them.
- Interception and modification of the content of SNMP messages. (Encryption of the messages prevents the contents from being understood and modified.)
- Attempts to initiate SNMP commands by unauthorized users.

- Replaying of SNMP messages transmitted earlier.

NOTE: The system cannot prevent an authorized user from executing SNMP commands with malicious intent.

2.1.2 SNMPv3 and Non-Secure Communication

The system configured in clear mode (no authentication and no encryption) provides normal services without adverse effects from the use of SNMPv3, such as degradation to call setup and audio delay.

This is a simpler configuration, because no passphrases are required, and key updates are not necessary. This is also the default SNMPv3 configuration (no authentication and no encryption) when the system is initially installed.

2.2 SHA Authentication

For SNMPv3 authentication, the system uses the Hashed Message Authentication Code function (HMAC-SHA-96), according to the RFC3414 document. A hash function takes an input message of arbitrary length and outputs fixed-length code. The fixed-length output is called the hash, or the message digest, of the original input message.

2.3 AES Encryption

For SNMPv3 encryption, the system uses the Advanced Encryption Standard (AES) encryption algorithm, with a 128-bit CFB Mode key, according to the RFC3826 document.

AES is the mandated encryption algorithm for the current ASTRO® 25 system release. AES encryption is not part of the core SNMPv3 standards, but SNMPv3 User-based Security Model (USM) is extensible to support additional encryption algorithms. RFC3826 was designed to extend the USM to support AES encryption. The use of any other algorithm is not a supported configuration and is not allowed.

2.4 SNMPv3 in the User-Based Security Model

SNMPv3 support for authentication with or without encryption is specified in the User-based Security Model (USM).

In SNMPv3, the USM user is the entity on whose behalf an operation is being performed (for example, a GET, SET, TRAP, or INFORM request). The system defines the exact User Policy (that is, what a user means in the context of a particular system). A set of configuration parameters associated with a user account allows SNMP traffic to be encrypted or authenticated. The SNMPv3 user account policy used in ASTRO® 25 systems depends on the manager and/or agent architecture of the system. The user account policy allows logical subsets of devices in the system to have independent encryption and/or authentication settings and keys.

A user may be a logical entity, such as an application or a set of applications that are enabled for SNMPv3, acting on behalf of an individual or a role, or set of individuals or roles, including combinations.

ASTRO® 25 system is pre-poplulated with USM user accounts needed to perform system administration and fault management. Tools are provided to modify the security level and passphrases of these accounts.

The configuration of USM includes the following information for each SNMPv3 user:

User name/security name and associated passphrase

The system owner is responsible for secure storage of passphrases. The passphrase is used to generate the necessary authentication and encryption keys for this user account.

Security level settings

The settings are used to indicate if authentication and encryption are used or not (in SNMPv3, you can opt to use neither, just authentication, or both authentication and encryption).

Security algorithms used for authentication and encryption

For authentication, SNMPv3 defines both SHA and MD5, but SHA support is recommended. MD5 is supported but it is no longer secure. For encryption, SNMPv3 standards define DES standards, but the USM can be extended to support 128-bit AES encryption.

2.4.1 USM Users for SNMPv3

User-based Security Model (USM) authenticates the users who want to log on to the system. The following lists types of USM user accounts, together with their definitions:

MotoAdmin

An administrative user account which has a secure default configuration with both authentication and privacy enabled. This user account is created in Site Elements, MNR routers and GGM 8000 gateways, SDM3000 Network Translator (SNT), and SDM3000 RTU. This USM user identity is used for the following operations:

- Performing all the passphrase changes for all USM user accounts, including itself.
- Changing the security level of other USM user accounts.

MotoMaster

Applicable for all traffic between the agent and managers except where other USM user accounts are defined in this table. That is, for GET/GETNEXT/GETBULK/SET and TRAPS between agents and Radio/Transport Network Management subsystem.

MotoMaster is an account used by the UNC, UEM, InfoVista, and ZSS to communicate with any managed devices that are enabled for SNMPv3. The account is installed in clear mode by default but can be configured to be secure.

MotoInformA

One of the two USM user accounts (along with MotoInformB) which are used for all notification traffic between all SNMPv3 agents and managers (that is, for INFORM requests, and INFORM responses). For subsystems that support the reliable communication feature, MotoInformA is the default active user account. Initially, it is used for all INFORM traffic between the manager and agents.

MotoInformB

One of the two USM user accounts (along with MotoInformA) which are used for all notification traffic between all SNMPv3 agents and managers (that is, for INFORM requests, and INFORM responses). For subsystems that support the reliable communication feature, MotoInformA is the default active user account. Initially, it is used for all INFORM traffic between the manager and agents.

MotoCSS

Used for all SNMPv3 traffic, including traps, between an agent and CSS (a transient manager).

This user account is used for CSS to perform the manager registration request to site elements and to receive traps.

MotoRTU

Used for all SNMPv3 traffic, including traps, between an agent and an SDM3000 RTU (a permanent manager).

This user account is used for SDM3000 RTU, as a permanent manager to site elements, to perform manager registration requests to the site elements, and to receive traps.

MotoNFM
Used for communication between SDM3000 RTUs and SDM3000 Network Translator (SNT).

MotoSWDL
Used for all SNMPv3 traffic, including traps, between an agent and SWDL (a transient manager). This user account is used for SWDL to perform the manager registration request to site elements and to receive traps.

MotoNorthMotorola
Used for all SNMPv3 traffic forwarded from a Motorola Solutions manager to any higher level Motorola Solutions manager-of-managers, within or outside the ASTRO® 25 system. For example, for traffic forwarded to the Centralized Managed Support Operations (CMSO).

MotoNorth
Used for all SNMPv3 traffic forwarded from a Motorola Solutions manager to any higher level Motorola Solutions manager-of-managers, within or outside the ASTRO® 25 system. For example, for traffic forwarded to the Centralized Managed Support Operations (CMSO). Available only on UEM.

MotoNM
Used for all SNMPv3 traffic within the Radio Network Management Subsystem. This user account is also used between the Radio Network Management Subsystem and the System Traffic Monitoring Subsystem.

MotoDynamicReport
Used for SNMPv3 GET, GETNEXT, and GETBULK operations between the Dynamic Reports application and the ATR. Unlike MotoNM, the MotoDynamicReport user credentials must be provided every time the Dynamic Reports application is launched.

MotoAuc
Used for providing the Zone Controller (ZC) with the Infrastructure Key (Ki) for radio authentication.

MotoZSS
Used to support data transfer between SC and ZSS.

MotoSDM_MIB
Used for secure communication between the SDM3000 RTU and a third-party SNMPv3-capable fault manager, if a license for Generic MIB (Management Information Base) was provided for the SDM. This user is configurable only if the Generic MIB feature was enabled in the **Project Properties** dialog box.

NOTE: The Generic MIB feature is available for the following ASTRO® 25 architectural configurations:

- K core systems
- Express Trunking Standalone Site
- Conventional Only - Standalone RF Site

2.4.2 USM User Strategy

SNMPv3 requires a User-based Security Model (USM) user strategy to support its implementation.

The use of other strategies or methodologies is not supported and might not guarantee the correct operational communications. Motorola Solutions recommends that you use the supported strategy to ensure communications.

Part of this requirement includes the usage details of MotoInformA and MotoInformB:

MotoInformA
One of the two USM user accounts (along with MotoInformB) which are used for all notification traffic between all SNMPv3 agents and managers (that is, for INFORM requests, and INFORM

responses). For subsystems that support the reliable communication feature, MotoInformA is the default active user account. Initially, it is used for all INFORM traffic between the manager and agents.

MotoInformB

One of the two USM user accounts (along with MotoInformA) which are used for all notification traffic between all SNMPv3 agents and managers (that is, for INFORM requests, and INFORM responses). For subsystems that support the reliable communication feature, MotoInformA is the default active user account. Initially, it is used for all INFORM traffic between the manager and agents.

Some USM user accounts, such as **MotoMaster**, are common across managers, so coordination is required for passphrase updates. For example, when credentials are changed for the MotoMaster user account on a router, then the same credential changes must be made for the MotoMaster user account on every manager that manages that router, including the Unified Event Manager (UEM) and InfoVista servers. The credentials for the user account on the device must match the credentials for the same user account on the managers that manage that device.

The **MotoCSS** and **MotoSWDL** user accounts are intended for transient manager traffic. These USM user accounts can be present on multiple PCs like those running the CSS application which uses MotoCSS. Assigning separate USM user accounts for the transient manager traffic ensures that none of these USM user accounts compromise other SNMPv3 traffic. (Traffic still applies to both MotoInformA and MotoInformB, but the ability to SET and, to a lesser extent, GET is the most significant risk.)

2.4.3 Required USM User Accounts

Not all user accounts listed in USM Users for SNMPv3 on page 28 are required.

The term *agent* refers to devices managed for SNMPv3 by other devices, which are known as managers.

Table 3: Required USM User Accounts

Device	USM User Name	Usage
SDM3000 RTU (Remote Terminal Unit)	MotoMaster	• Processes GET/SET/GETNEXT requests from Unified Event Manager (UEM). • Sends traps to UEM.
	MotoInformA or MotoInformB	Sends the INFORM request to UEM and processes INFORM responses.
	MotoRTU	Acts as a permanent manager for GET/SET to each of Site Controller (SC)/Base Radio (BR)/Comparators/GPB 8000 RDM.
	MotoAdmin	Administrative user account
SDM3000 Network Translator (SNT)	MotoMaster	• Processes GET/SET/GETNEXT requests from Unified Event Manager (UEM). • Sends traps to UEM.
	MotoInformA or MotoInformB	Sends the INFORM request to UEM and processes INFORM responses.
	MotoAdmin	Administrative user account
DCG 9000 gateway	MotoAdmin	Administrative user account

Device	USM User Name	Usage
	MotoInformA and MotoInformB	Sends the INFORM request to UEM and processes INFORM response (if Conventional Channel Interface is enabled). Only one MotoInform account is present at any time.
	MotoMaster	• Processes GET/SET/GETNEXT/GETBULK requests from UEM/UNC/InfoVista. • Sends traps to UEM.
MNR routers and GGM 8000 gateways (including the Conventional Channel Interface, if enabled)	MotoAdmin	Administrative user account
	MotoInformA or MotoInformB	Sends the INFORM request to UEM and processes INFORM response (if Conventional Channel Interface is enabled). Only one MotoInform account is present at any time.
	MotoMaster	• Processes GET/SET/GETNEXT/GETBULK requests from UEM/UNC/InfoVista. • Sends traps to UEM.
Ethernet LAN switch	MotoMaster	• Processes GET/SET/GETNEXT/GETBULK requests from UEM/UNC/InfoVista. • Sends traps to UEM.
Terminal Servers	MotoMaster	• Processes GET/SET/GETNEXT/GETBULK requests from UEM/UNC. • Sends traps to UEM.
InfoVista Server	MotoMaster	Sends GET/GETBULK requests to all managed SNMPv3 agents.
Zone Controller	MotoMaster	• Processes GET/SET/GETNEXT requests from UEM. • Sends traps to UEM.
	MotoInformA or MotoInformB	Sends the INFORM request to a registered manager and process the INFORM response.
	MotoAdmin	Administrative user account
	MotoNorthMotorola	Reserved for Centralized Managed Support Operations (CMSO).
	MotoAuc	Used for Ki provisioning.
Packet Data Gateway (PDG)	MotoMaster	• Processes GET/SET/GETNEXT requests from UEM. • Sends traps to UEM.
	MotoInformA or MotoInformB	Sends the INFORM request to the registered manager and processes the INFORM response. The MotoInformA account is used for non-secure operation, and MotoInformB for secure operation. Only one MotoInform account is present at any time.
	MotoAdmin	Administrative user account
Unified Network Configurator (UNC)	MotoMaster	• Sends GET/SET/GETNEXT requests to all managed SNMPv3 agents. • Receives notification from managed SNMPv3 agents.
	MotoInformA and MotoInformB	Receives the INFORM request from INFORM SNMPv3 agents and send the INFORM response back.

Device	USM User Name	Usage
	MotoAdmin	Administrative user account
	MotoNM	Sends/processes GET/SET requests within the Radio Network Management Subsystem.
UNCDS	MotoMaster	• Sends GET/SET/GETNEXT requests to all managed SNMPv3 agents. • Receives notification from managed SNMPv3 agents.
	MotoInformA and MotoInformB	Receives the INFORM request from INFORM SNMPv3 agents and send the INFORM response back.
	MotoAdmin	Administrative user account
	MotoNM	Sends/processes GET/SET requests within the Radio Network Management Subsystem.
Unified Event Manager (UEM)	MotoMaster (as manager)	• Sends GET/SET/GETNEXT requests to all managed SNMPv3 agents. • Receives notifications from managed SNMPv3 agents.
	MotoInformA or MotoInformB	Receives the INFORM request from INFORM SNMPv3 agents and sends the INFORM response back.
	MotoNorthMotorola	Reserved for Centralized Managed Support Operations (CMSO). Only for UEM.
	MotoNorth	Reserved for Centralized Managed Support Operations (CMSO).
	MotoMaster (as agent)	• Processes GET/SET/GETNEXT requests from UEM. • Sends traps to UEM.
	MotoAdmin	Administrative user account
	MotoNM	Sends/processes GET/SET requests within the Radio Network Management Subsystem.
Private Network Management (PNM) server applications: User Configuration Server (UCS), System Statistics Server (SSS), Zone Database Server (ZDS), Zone Statistics Server (ZSS)	MotoNM	Sends/processes GET/SET requests within the Radio Network Management Subsystem.
	MotoInformA or MotoInformB	Sends the INFORM request to the registered manager and processes the INFORM response.
	MotoAdmin	Administrative user account
	MotoMaster	• Processes GET/SET/GETNEXT requests from UEM. • Sends traps to UEM.
Air Traffic Router (ATR)	MotoNM	Sends/processes GET/SET requests within the Radio Network Management and System Traffic Monitoring Subsystems.
	MotoInformA or MotoInformB	Sends the INFORM request to the registered manager and processes the INFORM response.
	MotoAdmin	Administrative user account.

Device	USM User Name	Usage
	MotoDynamicReport	Processes GET requests from the Dynamic Report application.
	MotoMaster	• Processes GET/SET/GETNEXT requests from UEM. • Sends traps to UEM.
Console Site Elements: MCC 7500 VPM Dispatch Consoles, MCC 7500E Dispatch Consoles, Archiving Interface Server (AIS), Voice Processor Module (VPM), Conventional Site Controller (CSC), MCC 7500 Aux I/O Server, PRX 7000 Console Proxy	MotoAdmin	Administrative user account
	MotoInformA	Sends the INFORM Request for Reliable Communication to the registered manager and processes the INFORM response.
	MotoInformB	Sends the INFORM Request for Reliable Communication to the registered manager and processes the INFORM response.
	MotoCSS (CSC)	• Processes GET/SET requests from the Configuration/Service Software (CSS). • Sends messages to CSS.
	MotoMaster	• Processes GET/SET/GETNEXT requests from UEM. • Sends traps to UEM.
	MotoRTU (for CSC only)	• Processes GET/SET requests from SDM3000 RTU (Permanent Manager). • Sends traps to SDM3000 RTU (Permanent manager).
	MotoSWDL (for CSC and VPM only)	• Processes GET/SET requests from SWDL. • Sends traps to SWDL. • Acts as transient manager.
MCC 7500 IP Logging Recorder	MotoMaster	• Processes GET/SET/GETNEXT/GETBULK requests from UNC, Unified Event Manager (UEM), and InfoVista. • Sends the change-flag trap to UNC and traps to UEM.
MKM 7000 Console Alias Manager (CAM)	MotoMaster	• Processes GET/SET/GETNEXT requests from UEM. • Sends traps to UEM.
	MotoAdmin	Administrative user account
RF Site Elements: Site Controller, Base Radio, Comparator, GPB 8000 Reference Distribution Module (RDM), DSC 8000	MotoMaster	• Processes GET/SET/GETNEXT requests from UEM. • Sends traps to UEM.
	MotoInformA or MotoInformB	Sends the INFORM request to UEM and processes the INFORM response.
	MotoRTU **NOTE:** Not present on DSC 8000.	• Processes GET/SET requests from SDM3000 RTU (Permanent Manager). • Sends traps to SDM3000 RTU (Permanent manager).
	MotoCSS **NOTE:** Not present on DSC 8000.	• Processes GET/SET requests from CSS. • Sends traps to CSS. • Acts as transient manager.

Device	USM User Name	Usage
		• Orchestrate GTR 8000 subsite SWDL upgrades when a DSC 8000 Virtualized Prime Site is present.
	MotoSWDL	• Processes GET/SET requests from SWDL. • Sends traps to SWDL. • Acts as transient manager.
	MotoAdmin	Administrative user account
	MotoZSS (for Repeater and Simulcast SCs only, also not present on DSC 8000.)	Supports data transfer between SC and ZSS.
Software Download Manager (SWDL)	MotoSWDL	• Sends GET/SET requests to Site Controller (SC)/Base Radio (BR)/Comparators/GPB 8000 RDM. • Receives traps from Site Controller (SC)/Base Radio (BR)/Comparator/GPB 8000 RDM. • Communicates with the Voice Processor Module (VPM).
Configuration/ Service Software (CSS)	MotoAdmin	Can locally change the security level and passphrases of a user account in a site element.
	MotoCSS	Communicates with RF site and VPM devices.
Telephone Media Gateway (TMG)	MotoMaster	• Processes GET/SET/GETNEXT requests from Unified Event Manager (UEM). • Sends NMA messages to UEM. • Processes GET/SET requests from SWDL (UNC).
	MotoInformA and MotoInformB	Sends the INFORM request to the registered manager and processes the INFORM response.
	MotoCSS	• Processes GET/SET requests from CSS. • Sends NMA messages to CSS.
	MotoAdmin	Locally changes the security level and passphrases of a user account in a site element.
Cisco Console Telephony Media Gateway	MotoMaster	Processes GET/SET requests from SWDL (UNC).
Inter-System Gateway (ISGW)	MotoMaster	• Processes GET/SET/GETNEXT requests from UEM. • Sends traps to UEM.
	MotoInformA and MotoInformB	Sends the INFORM request to a registered manager and processes the INFORM response.
	MotoAdmin	Administrative user account
ISSI.1 Network Gateway/Site Link Relay Module	MotoMaster	Processes GET/SET/GETNEXT requests from UEM.
	MotoInformA and MotoInformB	Sends the INFORM request to the registered manager and processes the INFORM response.

Device	USM User Name	Usage
	MotoAdmin	Administrative user account
ISSI.1 Network Gateway/ISSI.1 Gateway Module	MotoMaster	Processes GET/SET/GETNEXT requests from UEM.
	MotoInformA and MotoInformB	Sends the INFORM request to the registered manager and processes the INFORM response.
	MotoAdmin	Administrative user account
Authentication Center (AuC)	MotoMaster	• Processes GET/SET/GETNEXT requests from UEM. • Sends traps to UEM.
	MotoInformA or MotoInformB	Sends the INFORM request to the registered manager and processes the INFORM response. Both MotoInformA and MotoInformB accounts are used for secure operations. Only one MotoInform account is present at any time.
	MotoAdmin	Administrative user account
PTP	MotoMaster	Processes GET/SET/GETNEXT requests from UEM.
		Sends traps to UEM.
TRAK	MotoMaster	Processes GET/SET/GETNEXT requests from UEM.
		Sends traps to UEM.
Domain Controller	MotoMaster	• Processes GET/SET/GETNEXT requests from UEM. • Sends traps to UEM.
	MotoAdmin	Administrative user account
	MotoInformA and MotoInformB	Sends the INFORM request to the registered manager and processes the INFORM response.
Core Security Management Server (CSMS)	MotoMaster	• Processes GET/SET/GETNEXT requests from UEM. • Sends traps to UEM.
	MotoAdmin	Administrative user account
	MotoInformA and MotoInformB	Sends the INFORM request to the registered manager and processes the INFORM response.
Backup and Restore Server (BAR)	MotoMaster	• Processes GET/SET/GETNEXT requests from UEM. • Sends traps to UEM.
	MotoInformA and MotoInformB	Sends the INFORM request to the registered manager and processes the INFORM response.
	MotoAdmin	Administrative user account
Direct Attached Storage (DAS) Management Controller	MotoMaster	• Processes GET/SET/GETNEXT requests from UEM. • Sends traps to UEM.
Fortinet firewalls	MotoMaster	• Processes GET/SET/GETNEXT requests from UEM. • Sends traps to UEM.
License Manager	MotoMaster	• Processes GET/SET/GETNEXT requests from UEM.

Device	USM User Name	Usage
		• Sends traps to UEM.
	MotoInformA and MotoInformB	Sends the INFORM request to a registered manager and processes the INFORM response.
IP Packet Capture	MotoMaster	• Processes GET/SET/GETNEXT requests from UEM. • Sends traps to UEM.
	MotoInformA and MotoInformB	Sends the INFORM request to a registered manager and processes the INFORM response.
	MotoAdmin	Administrative user account
Dynamic Transcoder	MotoMaster	• Processes GET/SET/GETNEXT requests from UEM. • Sends traps to UEM.
	MotoInformA and MotoInformB	Sends the INFORM request to the registered manager and processes the INFORM response.
	MotoAdmin	Administrative user account
Group Data Gateway	MotoMaster	• Processes GET/SET/GETNEXT requests from UEM. • Sends traps to UEM.
	MotoInformA and MotoInformB	Sends the INFORM request to the registered manager and processes the INFORM response.
	MotoAdmin	Administrative user account
Personnel Accountability Server	MotoMaster	• Processes GET/SET/GETNEXT requests from UEM. • Sends traps to UEM.

NOTE: MotoInformA and MotoInformB accounts are present on each device. However, only one account is used to send INFORMs to the UEM at a time. Each time there is a credential change for the INFORM user, the user is switched from MotoInformA to MotoInfomB, or from MotoInformB to MotoInformA, depending on which user was active before the credential change.

2.4.3.1 SNMP INFORM Requests

INFORM requests are a reliable mechanism for an agent to asynchronously send information to a manager.

The underlying mechanism is User Datagram Protocol (UDP), but the agent retries a limited number of times if no response to the INFORM is received from the manager.

2.5 View-Based Access Control Model

View-based Access Control Model (VACM) is used to implement access control on USM user accounts. This requirement does not restrict read access. For example, USM users can read MIB information to determine where other USM users exist.

The MotoAdmin user account is not required to add, modify, or delete the non-administrator SNMPv3 user accounts in the following subsystems:

- Private Network Management Subsystem
- Transport Network Management Subsystem
- Ethernet LAN switch in the Transport Network Subsystem
- MCC 7500 IP Logging Recorder
- Terminal Server

Access Control

The access control subsystem implements VACM to apply access restrictions to the USM user accounts listed in USM Users for SNMPv3 on page 28.

These user accounts cannot be used to change credentials of other USM user accounts (for example, one user's identity cannot be used to modify another user's key information). This includes actions like addition or deletion of other user accounts, except for an indicated administrative USM user account (MotoAdmin) which can change to, and add/delete, other USM user accounts. These are used to modify MotoMaster's key information in its managed SNMPv3 devices.

Although the application does not grant full access to every Management Information Base (MIB) to all USM users, VACM provides management and control of these user accounts, as described in system requirements. This does not restrict read access; for example, USM users can read MIB information to determine where other USM users exist.

Chapter 3

SNMPv3 Installation

Installing a system utilizing Simple Network Management Protocol Version 3 (SNMPv3) encryption and/or authentication capabilities requires the installer to have access to the system's USM policy and the specific SNMPv3 configuration parameters for each user account. All devices install SNMPv3 configuration as part of normal system software installation. After all devices that are enabled for SNMPv3 are installed, initial SNMPv3 communication is configured as clear mode, with No Authentication and No Encryption. Have the UEM discover these SNMPv3 devices using clear mode first, before the security is enabled on SNMPv3 communication.

3.1 SNMPv3 Configuration Utility for Unix

The SNMPv3 configuration utility for Unix operating systems (Solaris and Linux), also known as the Common Credentials User Interface, applies to the following devices:

- Devices using the **Solaris** operating system:
  - Generic Application Server
  - ISSI.1 Network Gateway site devices:
    - ISSI.1 Gateway Module
    - Site Link Relay Module
- Devices using the **Linux** operating system:
  - Air Traffic Router (ATR)
  - Backup and Restore Server (BAR)
  - Intersystem Gateway (ISGW)
  - License Manager (LM)
  - Packet Data Gateway (PDG)
  - System Statistics Server (SSS)
  - Unified Event Manager (UEM)
  - Unified Network Configurator (UNC)
  - Unified Network Configurator Device Server (UNCDS)
  - User Configuration Server (UCS)
  - Virtual Management Server
  - Zone Controller (ZC)
  - Zone Database Server (ZDS)
  - Zone Statistics Server (ZSS)

The configuration utility for Unix is installed automatically during installation of software for these devices, so there is no installation procedure for the utility.

3.2 SNMPv3 Configuration Utility for Windows

The SNMPv3 configuration utility for the Windows operating system applies to the following devices:

- Authentication Center (AuC)
- Core Security Management Server (CSMS)
- Domain Controller (DC)
- Dynamic Transcoder
- Group Data Gateway (GDG)
- InfoVista Server
- MCC 7500 VPM Dispatch Console
- MCC 7500E Dispatch Console
- MCC 7500 Archiving Interface Server (AIS)
- PRX 7000 Console Proxy
- MKM 7000 Console Alias Manager (CAM)

Installation files are distributed on the *Windows Supplemental* media for the ASTRO® 25 system. For details, see the *Windows Supplemental Configuration Setup Guide*.

Although the Common Agent is automatically installed with the MKM 7000 Console Alias Manager (CAM) software, the Common Credentials User Interface for SNMPv3 Credentials must be installed separately. See Installing the Configuration Utility for Windows on page 39.

3.2.1

Installing the Configuration Utility for Windows

Perform this procedure to install the Common Credentials User Interface for Windows.

NOTE: Do **not** perform this procedure on the following devices:

- Core Security Management Server (CSMS)
- Domain Controller
- InfoVista

For the following devices, Configuration Utility for Windows is already installed as part of the software installation. Continue with Configuring Console Site Elements, Dynamic Transcoders, and Group Data Gateways for SNMPv3 on page 66:

- MCC 7500E Dispatch Console
- MCC 7500 VPM-based Dispatch Console and 7500 AIS
- PRX 7000 Console Proxy
- Dynamic Transcoder
- Group Data Gateway (GDG)

NOTE: If you use non-certified hardware running Windows 10 OS either installed by yourself or provided together with the hardware by a 3rd party vendor, updates of the OS (for example version 1809) may not have SNMP service components. In such cases, prior to further processing, access the SNMP components and install them according to Microsoft Windows Features on Demand procedure, either on your own or with the support of the vendor. Motorola recommends offline installation. You **cannot** use *Motorola Windows Client* and *Motorola Windows Box Profile* media on hardware that is not certified by Motorola Solutions.

Prerequisites: Obtain the *Windows Supplemental* media. For more information, see the *Windows Supplemental Configuration Setup Guide*.

Procedure:

1 Insert the *Windows Supplemental* media into the CD/DVD drive.

2 Open the Windows command prompt.

3 In the command prompt, navigate to the `WIF` directory on the media.

4 Enter:

```
WindowsInstallFramework.exe /e /i "Motorola SNMPv3-Credentials-WSUI.xml"
```

If the **User Account Control** dialog box appears, click **Allow** or type in the administrator password for the account displayed, depending on the prompt command, and then click **Yes**.

5 In the installation finished message, click **OK**.

6 Reboot the device.

3.3

SNMPv3 Common Agent Installation

The installation of SNMPv3 Common Agent for Windows-based devices introduces advanced fault state management features, including supervision process determining device availability (up, down) and fault information synchronization status (synchronized, out of sync, synchronizing) with a single SNMP GET.

3.3.1

Installing the SNMPv3 Services Software

Perform this procedure only on Windows Server 2012 devices.

NOTE: Do **not** perform this procedure on the Domain Controller (DC) and InfoVista.

Prerequisites: Ensure that Windows Server 2012 is installed.

Procedure:

1 Log on to the Windows-based device using a valid domain account or local Windows administrator account.

If you log on to Windows with a local account, use the Windows administrator account (the account name set up by Motorola Solutions is `motosec` for Windows Server 2012-based devices).

2 Open the PowerShell command prompt as administrator:

a From **Start**, click **Search**.

b In the search field, type in: `powershell`

c Right-click **Windows PowerShell**, and select **Run as administrator**.

3 Enter:

```
Add-WindowsFeature -name SNMP-Service
```

If the **User Account Control** dialog box appears, click **Yes** or **Continue**, depending on the prompt you see.

The SNMPv3 Services software is installed.

3.3.2 Installing the SNMPv3 Common Agent Software

Perform this procedure to install the SNMPv3 Common Agent software on Windows-based devices.

NOTE: Do **not** perform this procedure on the Domain Controller, CSMS, InfoVista, and MKM 7000 Console Alias Manager (CAM).

NOTE: If you use non-certified hardware running Windows 10 OS either installed by yourself or provided together with the hardware by a 3rd party vendor, updates of the OS (for example version 1809) may not have SNMP service components. In such cases, prior to further processing, access the SNMP components and install them according to Microsoft Windows Features on Demand procedure, either on your own or with the support of the vendor. Motorola recommends offline installation. You **cannot** use *Motorola Windows Client* and *Motorola Windows Box Profile* media on hardware that is not certified by Motorola Solutions.

Prerequisites: Obtain the *Windows Supplemental* media. For more information, see the *Windows Supplemental Configuration Setup Guide*.

NOTE: OpenSSL does not need to be installed separately as it is installed as part of this procedure. For more information on OpenSSL, see the *Windows Supplemental Configuration Setup Guide*.

Procedure:

1. Log on to the Windows-based device by using a valid domain account or a local Windows administrator account.

   If you log on to Windows with a local account, use the Windows administrator account (the account name set up by Motorola Solutions is `motosec` for Windows Server 2012-based devices and `secmoto` for Windows 7 and Windows 10-based devices).

2. Insert the *Windows Supplemental* media into the CD/DVD drive.

   If the **User Account Control** dialog box appears, click **Continue**.

3. Navigate to the `WIF` folder on the media.

4. Enter:

   ```
   WindowsInstallFramework.exe /e /i "Motorola Common Agent.xml"
   ```

   If the **User Account Control** dialog box appears, click **Allow** or type in the administrator password for the account displayed, depending on the prompt command, and then click **Yes**.

5. In the installation finished message, click **OK**.

6. Reboot the device.

Postrequisites: To configure SNMPv3 agents, see Configuring the SNMPv3 Agents on page 51.

Chapter 4

SNMPv3 Configuration

There are various configuration procedures relating to Simple Network Management Protocol Version 3 (SNMPv3). The security configuration needs to be performed in a sequence.

4.1 Initial Configuration

Initial configuration is performed automatically during software installation. The initial configuration is clear (noAuthNoPriv), except for the MotoAdmin user account, which are always configured as secure (AuthPriv).

After initial installation, you need to configure three USM (User-based Security Model) SNMPv3 user accounts:

MotoAdmin
This user account is like the Unix superuser (root). The MotoAdmin user account's security level is AuthPriv (Authentication and Privacy), and it is never allowed to be changed.

MotoMaster
This user account has a security level of noAuthNoPriv (No Authentication, No Privacy). This can be changed by the MotoAdmin user.

MotoNorthMotorola
This user account has a security level of AuthPriv (Authentication, Privacy). This can be changed by the MotoAdmin user.

4.2 SNMPv3 Credentials Reconfiguration

Changing a device IP address requires a reconfiguration of SNMPv3 credentials as the device's local engine ID changes when the IP address is changed. For example, if a specific SNMPv3 user was set to AuthPriv, it will be changed back to noAuthNoPriv.

In addition, an extra step must be executed before reconfiguring the SNMPv3 user credentials for the following devices:

- GCP 8000 Site Controller
- GTR 8000 Base Radio
- GCM 8000 Comparators
- GRV 8000 Comparators
- GPB 8000 Reference Distribution Module (RDM)
- GPW 8000 Receiver
- Voice Processor Module (VPM)
- Telephone Media Gateway (TMG)
- Packet Data Gateway (PDG)
- SDM3000 RTU

Due to a limitation on the number of users these devices support, the SNMPv3 users must be reset to their factory default values before they are reconfigured.

For details, see procedures respective to each device.

4.3 Security Policies and SNMPv3 Configuration

Implementation of SNMPv3 encryption and authentication capabilities requires administrative access to your system USM policy and the specific SNMPv3 configuration parameters for each user account. (For details, contact your system administrator).

Configure the parameters and verify whether the system is operating with the necessary level of security. If only some devices in the system are enabled for SNMPv3, then the system administrator must be aware of which devices need SNMPv3 configuration.

When authentication or encryption are used, the USM passphrases must be unique to a particular system and follow good security practices. For example:

- Different passphrases for authentication and encryption for a USM user account.
- Minimum length of at least 15 characters.
- Maximum passphrase length of 64 characters.
- Strong passphrases that incorporate mixed-case English alphanumeric characters and selected punctuation characters.
- No repetitive patterns.

NOTE: Avoid the use of repetitive characters in a passphrase when setting up SNMPv3 devices, as it may increase passphrase vulnerability. For example, avoid using `aaaaaaaa` or `ASDFASDF`. For details about your system passphrase policies, contact your system administrator.

4.4 Secure Default Administrative Configuration

The initial default SNMPv3 configuration is secure (set to AuthPriv) for the administrative USM user account, MotoAdmin, which performs the following functions:

- Change security levels for other USM user accounts.
- Change or reset the passphrases of other USM user accounts.

This ensures that the user account initially defaults to a secure configuration (with both authentication and encryption) in order to protect the integrity of the SNMPv3 settings.

The default AuthPriv security level for the MotoAdmin user account cannot be changed. No USM user has permissions to change the MotoAdmin security level.

4.5 User Account Creation for SNMPv3

USM user accounts are created automatically when the software is installed, except MotoInform user accounts on some devices. Interaction from any operation and maintenance user is not required.

Except for MotoAdmin with security enabled, all USM user accounts, including MotoInformA, are created in clear mode (set to noAuthNoPriv).

For system expansion, the MotoMaster user account in the added device must be changed to the same credentials as those of the MotoMaster defined in the UEM. This allows the device to accept registration requests from the UEM.

NOTE: All USM user accounts are created automatically when the software is installed, except for MotoInform user for some devices. The user may need to run UEM Discovery on the device to create the MotoInformA user account. Based on your security policies, if SNMPv3 credentials are required, this should be executed after device installation but before you configure SNMPv3 credentials using AuthPriv. Therefore, have UEM discover these SNMPv3 devices using clear mode first, before the security is enabled on SNMPv3 communication.

4.5.1 Secure and Non-Secure SNMPv3 Configuration

The system allows either secure or non-secure configurations of SNMPv3.

Secure SNMPv3 configuration
Secure means that SNMPv3 is using both authentication and/or privacy (encryption).

Non-Secure SNMPv3 configuration
Non-Secure means no authentication and no privacy (encryption) in SNMPv3.

NOTE: Motorola Solutions-built devices are provided with the non-secure default configuration. Third-party equipment used in the system may require manual configuration to set them up in the non-secure mode.

4.6 User Configuration Scenarios

NOTE: For procedures to configure the MotoInformA or MotoInformB user account, see UEM Configuration for SNMPv3 on page 58.

4.6.1 MotoAdmin User Account Reset

To reset credentials, use the configuration utility for the operating system used by the device for which credentials require reset.

- For Unix (Solaris or Linux) devices, see Configuring USM User Security with the Unix Configuration Utility on page 47.
- For Windows devices, see Configuring USM User Security with the Windows Configuration Utility on page 47.

4.6.2 Creation of MotoInformA (noAuthNoPriv by Default)

When there is no MotoInformA or MotoInformB account on the system and a trap needs to be sent out (because of an existing registration or a manual registration), the MotoInformA account is automatically created with **noAuthNoPriv**. However, MotoInformA can be also set to **AuthPriv** (for example, when MotoInformB credentials are changed).

NOTE: This can also happen when the MotoInformA account is deleted and also when, after this deletion, a trap is sent and the account is created again.

4.6.3
Creation of MotoInformB (AuthPriv)

Whenever the MotoInformB account is created with **AuthPriv**, the credentials must be changed in order for the management station to be able to decode the INFORM information. When this is done, the MotoInformA account can be deleted and the MotoInformB account will be used for the (encrypted and authenticated) traps.

NOTE:
The user can change the security level for the MotoInformB account.

Both MotoInformA and MotoInformB always belong to the **notify_grp VACM** group. This cannot be changed.

4.6.4
MotoMaster Privilege Level Change

To change the privilege level for the MotoMaster account using the SNMPv3 configuration utilities, see Local Configuration of SNMPv3 Security Level for USM User Accounts on page 46.

4.7
Local Configuration

The system allows only authorized users to locally change the SNMPv3 configuration.

These changes include the security level configured for SNMPv3 (AuthPriv, AuthNoPriv, or noAuthNoPriv) and updating or resetting key information. An authorized user holds the credentials (login and password) required to access SNMPv3 configuration.

NOTE: Authorized users can also access the SNMPv3 information remotely through SSH, if SSH is supported on this device, and if the authorized user has valid SSH credentials to access this device.

The following devices do not require the MotoAdmin user account:

- Ethernet LAN switches
- Terminal Server LX and SLC Series
- InfoVista Server
- Console site elements: MCC 7500 IP Logging Recorder
- PTP devices
- TRAK devices

4.7.1
Local Configuration of SNMPv3 Key Information

The subsystem can be locally configured with new SNMPv3 key information for any USM user account. In such cases, the USM user must have a new passphrase information and the administrator must have appropriate privileges.

You need to be able to initially configure, and later update, the SNMPv3 USM authentication and encryption key information for the user account.

The local key change mechanism is the only method to perform key changes for all user accounts, including MotoMaster.

Local key change operation in the UNC, UEM, InfoVista, MCC 7500 IP Logging Recorder, Terminal Server, Ethernet LAN switches, TRAK and PTP devices does **not** check MotoAdmin user credentials because these applications have their own mechanisms to perform the key change operation. All devices that support the local user account key change mechanism have a matched new localized key. Any key change does not shut down SNMPv3 communication. All devices follow RFC3414 to generate the new localized keys.

The MotoAdmin user can make passphrase changes. Therefore, *appropriate privilege* means the user executing the change must provide the MotoAdmin USM user account credentials (passphrases), in addition to satisfying any other existing authorization schemes to access the passphrase change functionality.

Operation is expected to continue normally during and after the key change procedure, without any local disruption of operations.

Key information is updated in each pertinent device of the subsystem. This means an engine ID must be explicitly provided (for example, agents sending INFORM requests need the engine ID of the manager) or implicitly known. For example, an agent's own engine ID is used in some cases. In other cases, a manager uses discovery to learn the appropriate agent's engine ID, based on a non-localized key (storing a non-localized key is not allowed on managed devices).

Local configuration includes configuration performed through the site LAN, such as the way CSS behaves while configuring site devices like the Site Controller (SC) and Base Radio (BR). Local configuration is not meant to include configuration across a WAN link.

IMPORTANT: Procedures to configure local SNMPv3 keys are specific to each device that is enabled for SNMPv3. For local key configuration procedures for a device, refer to the section of this chapter specific to each device. See Device Configuration for SNMPv3 on page 52.

4.7.2 Local Configuration of SNMPv3 Security Level for USM User Accounts

Devices can be configured locally to use one of the three supported SNMPv3 security levels (AuthPriv, AuthNoPriv, and noAuthNoPriv) for USM user accounts.

An administrator can choose one of the available security levels for SNMPv3 because they have to configure their initial security stance and may change their original decision. This applies where SNMPv3 is enabled. The configuration is done per USM user account (so all USM user accounts require the same settings to get a consistent security stance). This activity involves the deletion and recreation of the user account.

Successful SNMPv3 communication requires (among other criteria) that the configured security levels match among devices that communicate to each other using SNMPv3.

Local configuration is the only way to perform the security level change function, that is, no centralized mechanism is available.

Local security level changes in CSS, SWDL, Router User Interfaces, and SDM3000 RTU User Interfaces require a valid MotoAdmin user's credentials. Implementation of this request also requires deleting the target user account, and cloning from the MotoAdmin user account.

Local security level changes in the UNC, UEM, InfoVista, Terminal Server LX Series, MCC 7500 IP Logging Recorder, and Ethernet LAN switches do **not** require valid MotoAdmin user credentials because these are third-party applications that do not require a MotoAdmin user account. These applications have their own mechanism to perform security level changes.

To change the security level on MotoInformA or MotoInformB user accounts in CSS, Router User Interfaces, and SDM3000 RTU User Interfaces, operations and maintenance users must provide these User Interfaces with the UEM’s Fully Qualified Domain Name (FQDN). The User Interface translates the Fully Qualified Domain Name to UEMs snmpEngineID hexadecimal value to calculate the new key values. User Interface must produce UEM’s snmpEngineID.

4.7.2.1 Configuring USM User Security with the Unix Configuration Utility

Configuring USM user security with the Unix configuration utility applies to devices running on either the Solaris or the Linux operating system.

Procedures for devices using Unix operating systems are specific to each device:

- For Zone Controllers, see Zone Controller Configuration for SNMPv3 on page 78.
- For the Packet Data Gateway, see PDG Configuration for SNMPv3 on page 76.
- For the PNM Servers, see PNM Servers and ATR Configuration for SNMPv3 on page 82.
- For ISGW, see ISGW Configuration for SNMPv3 on page 80
- For ISSI.1, see Configuring ISSI.1 Network Gateway for SNMPv3 on page 126
- For BAR, see BAR Configuration for SNMPv3 on page 133.
- For the License Manager, see Configuring the License Manager for SNMPv3 on page 137.
- For IP Packet Capture, see IP Packet Capture Configuration for SNMPv3 on page 140.

4.7.2.2 Configuring USM User Security with the Windows Configuration Utility

Perform this procedure to configure User-based Security Model (USM) with the Windows configuration utility on the following devices:

- Authentication Center (AuC)
- Core Security Management Server (CSMS)
- Domain Controller
- Dynamic Transcoder
- Group Data Gateway (GDG)
- InfoVista Server
- PRX 7000 Console Proxy
- MCC 7500 VPM-based Dispatch Console and MCC 7500 Archiving Interface Server (AIS)
- MCC 7500E Dispatch Console
- MKM 7000 Console Alias Manager (CAM)

Prerequisites: Install the configuration utility for Windows. See Installing the Configuration Utility for Windows on page 50.

Procedure:

1 Open the SNMP basic user credential maintenance utility by locating and running the `CA_UserCredentials.exe` file as administrator.

Depending on the device, the default location is:

Table 4: Location of the SNMPv3 file

Device	Path
• MCC 7500 VPM Dispatch Console • MCC 7500E Dispatch Console • MCC 7500 AIS	`C:\Program Files (x86)\Motorola\Motorola SNMPv3-Credentials-WSUI`

Device	Path
• AuC • Domain Controller • CSMS • InfoVista • GMC • CAM • MCC 7500 VPM Dispatch Console (Windows 7 and Windows 10) • MCC 7500E Dispatch Console (Windows 10 only) • AIS (Windows 7 and Windows 10) • Dynamic Transcoder • GDG • PRX 7000 Console Proxy	• **For 64bit:**`C:\Program Files\Motorola\Motorola SNMPv3-Credentials-WSUI` • **For 32bit:**`C:\Program Files (x86)\Motorola\Motorola SNMPv3-Credentials-WSUI`

To reset the MotoAdmin account, the user has to belong to the group with authority to perform the operations in this procedure (see the *Authentication Services Feature Guide* and contact your Active Directory administrator) and launch `CA_UserCredentials.exe` in one of the following ways:

- From an elevated Windows command line. For information how to run the elevated Windows command line, see “Starting the Windows Command Line as Administrator” in the *Authentication Services Feature Guide*.
- By right-clicking the file and selecting **Run as administrator**.

The **MotoAdmin Credentials Validation** dialog box appears. The dialog box requires input of valid credentials for the MotoAdmin user account. For security, characters in passphrase inputs are replaced by asterisks (*) on the screen.

2 In the **MotoAdmin Authentication Passphrase** field, enter the authentication passphrase.

3 In the **MotoAdmin Privacy Passphrase** field, enter the privacy passphrase.

4 In the **Agent Port** field, enter a valid port number for the device for which you want to set authentication. Use the default port for each device.

5 Click **OK**.

MotoAdmin credentials are validated and the **SNMPv3 User Credential Maintenance** window appears, showing the security name and security level for each user.

6 If applicable, perform one of the following actions:

If…	Then…
If MotoAdmin credentials cannot be validated,	the following error message appears: `SNMPv3 Administration cannot be performed. Contact the system administrator.` To return to the **MotoAdmin Credentials Validation** dialog box, click **OK**.

If…	Then…
If MotoAdmin credentials are lost,	perform the following actions: **a** Click **Reset MotoAdmin Account Validation** in the MotoAdmin Credentials. **b** Click **OK** in the **Warning** dialog box. **c** At the prompts, enter new passphrases for MotoAdmin. Credentials are overwritten and the utility closes. The following message appears: `MotoAdmin account successfully reset`.
If you attempt to reset the MotoAdmin account from a user account other than the Windows administrative account,	the following error message appears: `This action is allowed only for admin user account`.

7 Select the user account for which you want to set SNMPv3 credentials:

   a Locate the user in the lists of users. For a list of INFORM users, select the **SNMPv3 Inform Users** tab. For a list of all other users, select the **SNMPv3 Users** tab.

   b Click the table row for the selected user account. (To release selection, click an empty row.)

8 To set the security level for the selected user account, click **Set Security Level**.

   For the MotoAdmin user account, this option is disabled because the security level of MotoAdmin cannot be changed.

9 In the **Select New Security Level** dialog box, select the desired security level from the list. Click **OK**.

   The dialog box lists security levels other than the previously configured security level. For example, if a user account previously was configured with a security level of noAuthNoPriv, the dialog box displays two options: **AuthNoPriv** and **AuthPriv**.

10 In the **User Validation** dialog box, set passphrases for the selected user account:

If…	Then…
If the selected user account has a security level of noAuthNoPriv,	perform the following actions: **a** In the **New Authentication Passphrase** dialog box, type the new passphrase in the appropriate fields. **b** In the warning dialog box, click **OK**, and then **Yes**. The **SNMPv3 User Credential Maintenance** window returns.
If the selected user account has a security level of AuthNoPriv,	perform the following actions: **a** In the **Enter Authentication Passphrase** field, type the current authentication passphrase. Click **OK**. **b** In the **New Authentication Passphrase** dialog box, type the new passphrase in the appropriate fields. **c** In the warning dialog box, click **OK**, and then **Yes**. The **SNMPv3 User Credential Maintenance** window returns.

If…	Then…
If the selected user account has a security level of AuthPriv,	perform the following actions: **a** Type the current authentication and privacy passphrases in the appropriate fields, then type the current authentication and privacy passphrases in the appropriate fields. Click **OK**. **b** In the **New Authentication Passphrase** dialog box, type the new authentication passphrase in the appropriate fields and click **OK**. **c** In the **New Privacy Passphrase** dialog box, type the new privacy passphrase in the appropriate fields and click **OK**. **d** In the warning dialog box, click **Yes**. The **SNMPv3 User Credential Maintenance** window returns.
If user credentials cannot be validated,	the following error message appears: `SNMPv3 Administration cannot be performed. Contact the system administrator.` To return to the **User Validation** dialog box, click **OK**.
If two text entries for the same passphrase do not match,	the following error message appears: `New and Verified passphrases do not match.` To return to the passphrase entry screen, click **OK**.
If the passphrase is too long or too short, or the passphrase contains any invalid characters,	an error message displaying password requirements appears. To return to the passphrase entry screen, click **OK**.

11 To exit the configuration utility, click **Exit**.

The utility window closes.

4.7.2.2.1 Installing the Configuration Utility for Windows

Perform this procedure to install the Common Credentials User Interface for Windows.

NOTE: Do **not** perform this procedure on the following devices:

- Core Security Management Server (CSMS)
- Domain Controller
- InfoVista

For the following devices, Configuration Utility for Windows is already installed as part of the software installation:

- MCC 7500E Dispatch Console
- MCC 7500 VPM-based Dispatch Console and 7500 AIS
- PRX 7000 Console Proxy
- Dynamic Transcoder
- Group Data Gateway (GDG)

Prerequisites: Obtain the *Windows Supplemental* media. For more information, see the *Windows Supplemental Configuration Setup Guide*.

Procedure:

1. Insert the *Windows Supplemental* media into the CD/DVD drive.
2. Open the Windows command prompt.
3. In the command prompt, navigate to the `WIF` directory on the media.
4. Enter:

   ```
   WindowsInstallFramework.exe /e /i "Motorola SNMPv3-Credentials-WSUI.xml"
   ```

   If the **User Account Control** dialog box appears, click **Allow** or type in the administrator password for the account displayed, depending on the prompt command, and then click **Yes**.
5. In the installation finished message, click **OK**.
6. Reboot the device.

4.7.2.3
Configuring USM User Security with ESU Launchpad

The Enhanced Software Update (ESU) Launchpad is an application used for DCG 9000 configuration.

For more information on configuring SNMPv3 for DCG 9000, see section "Changing DCG 9000 SNMPv3 Credentials" in the *DCG 9000 Feature Guide*.

4.7.3
Local SNMPv3 Information Reset Mechanism

Reset of local SNMPv3 configuration information to its default state is specific to each device that is enabled for SNMPv3. For local reset instructions, refer to the section of this chapter that describes SNMPv3 configuration for the device requiring local reset. See Device Configuration for SNMPv3 on page 52.

4.7.4
Local Configuration of Site Elements

Local configuration of site elements only applies to G-Series RF Site equipment and VPM-based devices. To configure parameters related to SNMPv3 user accounts, you must have MotoAdmin user rights and be connected to the SNMPv3-capable device. Configuration/Service Software (CSS) allows the user to configure SNMPv3 users on the Site Controller/Base Radio/Comparator/GPB 8000 RDM/VPM/TMG devices. With CSS, the user can update passwords, security level, EngineID (for MotoInforms only), and create or delete any user account (excluding MotoAdmin).

4.8
Configuring the SNMPv3 Agents

Perform this procedure to configure the SNMPv3 agents by using the *Windows Supplemental* media on Windows Server 2012-based devices.

IMPORTANT: Do **not** perform this procedure on the Domain Controller, InfoVista, and MKM 7000 Console Alias Manager (CAM).

Prerequisites: Obtain the *Windows Supplemental* media and the Windows administrator account name. For more information, see the *Windows Supplemental Configuration Setup Guide*.

Procedure:

1. Log on to the Windows-based device by using a valid domain account or local Windows administrator account.

If you log on to Windows with a local account, use the Windows administrator account (the account name set up by Motorola Solutions is `motosec` for Windows Server 2012-based devices).

2. Insert the *Windows Supplemental* media into the CD/DVD drive.
3. In the Command Prompt, navigate to the `WIF` folder on the media.
4. Enter:

   ```
   WindowsInstallFramework.exe /e /i "Motorola Common Agent
   Configuration.xml"
   ```

   If the **User Account Control** dialog box appears, click **Allow** or type in the administrator password for the account displayed, depending on the prompt command, and then click **Yes**.
5. In the installation finished message, click **OK**.
6. Enter:

   ```
   WindowsInstallFramework.exe /e /i "Motorola Initial SNMPv3 Credential
   Extractor Default Configuration.xml"
   ```
7. Click **OK**.
8. Reboot the device.

4.9 Device Configuration for SNMPv3

Configuration procedures are available for the following devices and applications in the ASTRO® 25 system:

- Air Traffic Router (ATR)
- Authentication Center (AuC)
- Backup and Restore Server (BAR)
- Configuration/Service Software (CSS)
- Console site elements: MCC 7500 VPM Dispatch Consoles, MCC 7500E Dispatch Consoles, Archiving Interface Server (AIS), Conventional Site Controller, Console Aux I/O Server (SDM3000), and MKM 7000 Console Alias Manager (CAM), Group Data Gateway (GDG), PRX 7000 Console Proxy
- Core Security Management Server (CSMS)
- Domain Controller (DC)
- Dynamic Transcoder
- Ethernet LAN switches
- Fortinet firewalls
- InfoVista Server
- IP Packet Capture
- Intersystem Gateway (ISGW)
- ISSI.1 Network Gateway
- License Manager (LM)
- MCC 7500 IP Logging Recorder
- MNR routers and GGM 8000 gateways
- Fault Management devices
- Packet Data Gateway (PDG)

- Private Network Management (PNM) servers: User Configuration Server (UCS), System Statistics Server (SSS), Zone Database Server (ZDS), and Zone Statistics Server (ZSS)
- PTP devices
- RF site devices
- Software Download Manager (SWDL)
- Telephone Media Gateway (TMG)
- Terminal Servers LX Series (Model T) and SLC Series (Lantronix SLC 8000)
- TRAK devices
- Unified Event Manager (UEM)
- Unified Network Configurator (UNC)
- Unified Network Configurator Device Server (UNCDS)
- Voice Processor Module (VPM)
- Zone Controllers

If a device or application is not listed here, see the device-specific manual.

4.9.1 SNMPv3 Communication Matrix

The SNMPv3 communication matrix shows the relationships between devices (also known as agents) and their managers, as well as the SNMPv3 user types used by the managers to manage those devices, and the functions performed by those devices when managed for SNMPv3.

NOTE:
The table does not include the MotoAdmin user account because MotoAdmin is used strictly for SNMPv3 administration.

No MotoAuc VACM parameter is accessible unless MotoAuc is at the authPriv security level. MotoAuc for ZC must be set to authPriv before KI transfer is enabled.

Table 5: SNMPv3 Communication Matrix

Device	Manager	SNMPv3 User	Functions
ATR	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
	SSS	MotoNM	Network Management
	ZSS		
	Dynamic Report application	MotoDynamicReport	Dynamic reports
	UNC	MotoMaster	Discovery, Configuration, Trap reporting
Authentication Center (AuC)	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
	ZC	MotoAuc	Reliable transfer of Ki between AuC and ZC
Backup and Restore Server (BAR)	UEM	MotoMaster	Supervision, Discovery, Trap reporting

Device	Manager	SNMPv3 User	Functions
		MotoInformA and MotoInformB	Reliable Communication
Console Telephony Media Gateway	UNC	MotoMaster	Configuration, Software Download, Transient Manager
Core Security Management Server (CSMS)	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
Direct Attached Storage (DAS) Management Controller	UEM	MotoMaster	Supervision, Discovery, Trap reporting
Domain Controller	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
Dynamic Transcoder	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
Ethernet LAN Switches	UEM	MotoMaster	Supervision, Discovery, Trap reporting
	UNC		Configuration
	InfoVista		Statistics collection
Fortinet firewalls	UEM, UNC	MotoMaster	Processes GET/SET/GETNEXT/GETBULK requests from UEM/UNC. Sends traps to UEM.
GCM 8000/GRV 8000 Comparators	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
	CSS	MotoCSS	Configuration, Transient Manager
	SWDL	MotoSWDL	Software Download
	UNC	MotoMaster	Configuration
	SDM3000 RTU	MotoRTU	Permanent manager polling RF site elements
GCP 8000 Site Controller (PSC, Centralized Managed Support Operations (CMSO), HPDSC, CSC)	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
	CSS	MotoCSS	Configuration, Transient Manager
	SWDL	MotoSWDL	Software Download
	UNC	MotoMaster	Configuration
	SDM3000 RTU	MotoRTU	Permanent manager polling RF site elements
	InfoVista	MotoMaster	Statistics collection

Device	Manager	SNMPv3 User	Functions
	ZSS	MotoZSS **NOTE:** This account is only created on Repeater and Simulcast SCs.	Statistics collection
DSC 8000	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
	SWDL	MotoSWDL	Software Download
	UNC	MotoMaster	Configuration
Group Data Gateway (GDG)	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
GPB 8000 Reference Distribution Module (RDM)	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
	CSS	MotoCSS	Configuration, Transient Manager
	SWDL	MotoSWDL	Software Download
	UNC	MotoMaster	Configuration
	SDM3000 RTU	MotoRTU	Permanent manager polling RF site elements
	InfoVista	MotoMaster	Statistics collection
GTR 8000 Base Radio (BR) GPW 8000 Receiver	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
	CSS	MotoCSS	Configuration, Transient Manager
	SWDL	MotoSWDL	Software Download
	UNC	MotoMaster	Configuration
	SDM3000 RTU	MotoRTU	Permanent manager polling RF site elements
IP Packet Capture	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
ISGW	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
	UNC	MotoMaster	Discovery, Configuration, Trap reporting
ISSI.1 Network Gateway:	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication

Device	Manager	SNMPv3 User	Functions
Site Link Relay Module and ISSI.1 Gateway Module			
License Manager	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
MCC 7500 VPM Dispatch Console and AIS	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
	CSS	MotoCSS	Configuration, Transient Manager
	SWDL	MotoSWDL	Software Download
MCC 7500E Dispatch Console (only inside the RNI)	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
MCC 7500 IP Logging Recorder	UEM	MotoMaster	Supervision, Discovery, Trap reporting
MKM 7000 Console Alias Manager (CAM)	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
	CSS	MotoCSS	Configuration, Transient Manager
MNR routers and GGM 8000 gateways	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
	UNC	MotoMaster	Configuration
	InfoVista		Statistics collection
PDG	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
	InfoVista	MotoMaster	Statistics collection
	UNC	MotoMaster	Discovery, Configuration, Trap reporting
PRX 7000 Console Proxy	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
PTP devices	UEM	MotoMaster	Supervision, Discovery, Trap reporting
SDM3000 RTU	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
	SDM3000 Network Translator (SNT)	MotoNFM	Supervision, Notification reporting

Device	Manager	SNMPv3 User	Functions
	Third-party fault manager supported by Generic MIB (Management Information Base)	MotoSDM_MIB	Monitoring, Trap reporting, Communication
SSS	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
	SSS	MotoNM	Network Management
	UNC	MotoMaster	Discovery, Configuration, Trap reporting
Terminal Server	UEM	MotoMaster	Supervision, Discovery, Trap reporting
	UNC	MotoMaster	Discovery, Configuration, Trap reporting
TMG	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
	UNC	MotoMaster	Configuration, Software Download, Transient Manager
	CSS	MotoCSS	Configuration, Transient Manager
	SWDL	MotoSWDL	Software Download
TRAK devices	UEM	MotoMaster	Supervision, Discovery, Trap reporting
UCS	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
	UCS	MotoNM	Network Management
	UNC		
	SSS		
	ZDS		
UEM	UEM	MotoNM	Network Management
		MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
UNC	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
	UNC	MotoNM	Network Management
	UCS		
	UNCDS		

Device	Manager	SNMPv3 User	Functions
UNCDS	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
	UNCDS	MotoNM	Network Management
Voice Processor Module	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
	UNC	MotoMaster	Configuration, Software Download, Transient Manager
	CSS	MotoCSS	Configuration, Transient Manager
	SWDL	MotoSWDL	Software Download
ZDS	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
	ZDS	MotoNM	Network Management
Zone Controllers	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
	AuC	MotoAuc	Reliable transfer of Ki between AuC and ZC
	UNC	MotoMaster	Discovery, Configuration, Trap reporting
ZSS	UEM	MotoMaster	Supervision, Discovery, Trap reporting
		MotoInformA and MotoInformB	Reliable Communication
	ZSS	MotoNM	Network Management
	UNC	MotoMaster	Discovery, Configuration, Trap reporting
	Site Controllers	MotoZSS	Statistics gathering

4.9.2 UEM Configuration for SNMPv3

The Generic MIB feature is available for the following ASTRO® 25 architectural configurations:

- K core systems
- Express Trunking Standalone Site
- Conventional Only – Standalone RF Site

The Unified Event Manager (UEM) is a fault management application designed to handle the following critical fault management functions:

- Discovering devices
- Handling faults
- Detecting and reporting loss of communication and synchronization

For a detailed list of devices fault managed by UEM and their location in the ASTRO® 25 system, see "Groups of Devices Managed by UEM" in the *Unified Event Manager User Guide*.

The default credentials vary, based on the user login:

- If the user has logged on as MotoCSS, then the default credentials of NBI configuration are displayed.
- If the user has logged on as Admin or Security Admin, then the credentials of any user that is a member of the MotoCSS, Admin for the SecurityAdmin group are displayed.

Use the same procedure to configure either MotoMaster, MotoInformA, or MotoInformB.

CAUTION: The normal sequence for changing credentials for an INFORM user is to change credentials in the Unified Event Manager (UEM) first, then on the UEM-managed device, and then verify the key change event on the UEM. It is important to follow the normal sequence, in order to prevent consequences that could include a zone-wide failure in the reporting of reliable faults. For more information, see Troubleshooting Reliable Communication Failure on page 147.

4.9.2.1

SNMPv3 Credentials Configuration on UEM

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

Table 6: SNMPv3 Interfaces on UEM

UEM is configured with default SNMPv3 credentials for the following interfaces. By default, UEM restricts configuration of those SNMPv3 credentials to specific groups.

Function	SNMPv3 Interface	Groups with Configuration Rights
Outbound and inbound communication between UEM and devices	MotoMaster	SuperUser, SecurityAdmin
Inbound communication from devices to UEM	MotoInformaA, MotoInformB	SuperUser, SecurityAdmin
Communication with NMS through North Bound Interface (NBI)	MotoNorth	SuperUser, SecurityAdmin
	MotoNorthMotorola	MotorolaSSC

Table 7: SNMPv3 Security Levels for Network Elements

Security Level	Security Level Definition	AuthProtocol and AuthPassword	PrivProtocol and PrivPassword
AuthPriv	SNMP messages are sent with authentication and with privacy	Yes	Yes
noAuthNoPriv	SNMP messages are sent without authentication and without privacy	No	No

Security Level	Security Level Definition	AuthProtocol and AuthPassword	PrivProtocol and PrivPassword
AuthNoPriv	SNMP messages are sent with authentication but without privacy	Yes	No

IMPORTANT:
On UEM restart, if no Manager of Managers (MoM) is registered for an NBI user (MotoNorthMotorola for MotorolaSSC group and MotoNorth for all others), the security level is reset from NoAuthNoPriv and AuthNoPriv to AuthPriv with a new random Authentication Passphrase and new random Privacy Passphrase.

Service Name is the term used in the UEM interface for Fully Qualified Domain Name (FQDN). Service names are case sensitive, so be careful when entering or referencing service names in UEM.

Configuration Types

There are three types of SNMPv3 credentials configuration:

- Global SNMPv3 credentials configuration. See:
  - Configuring Global SNMPv3 Credentials for the MotoMaster User on page 60
  - Configuring Global SNMPv3 Inform Credentials on page 61
- Network element SNMPv3 credentials configuration. See:
  - Updating the Network Element SNMPv3 Credentials on page 62

  NOTE: You can configure network element SNMPv3 credentials only after the network element/device has been successfully discovered. If credentials for the discovery job were not configured, network elements are discovered with Global MotoMaster SNMPv3 credentials.
- Discovery session SNMPv3 credentials configuration. See:
  - Configuring Discovery Job Credentials on page 63

4.9.2.2

Configuring Global SNMPv3 Credentials for the MotoMaster User

Configure the global SNMPv3 credentials for outbound 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.

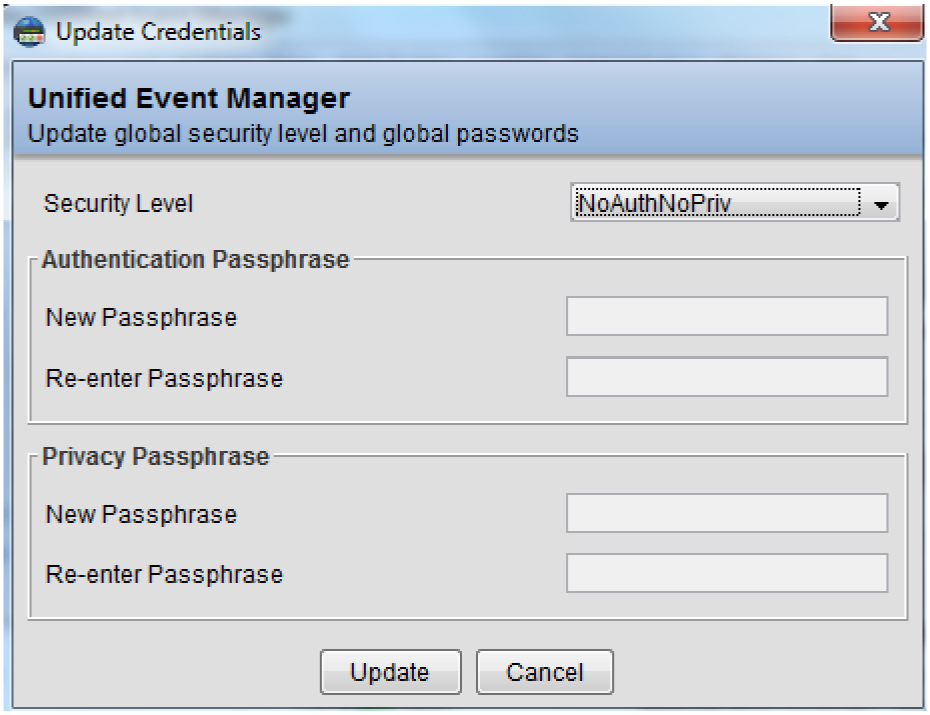
Procedure:

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 1: Update Credentials Dialog Box



Update Credentials

Unified Event Manager

Update global security level and global passwords

Security Level: NoAuthNoPriv

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

> **NOTE:** 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.

4.9.2.3 Configuring Global SNMPv3 Inform Credentials

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

Procedure:

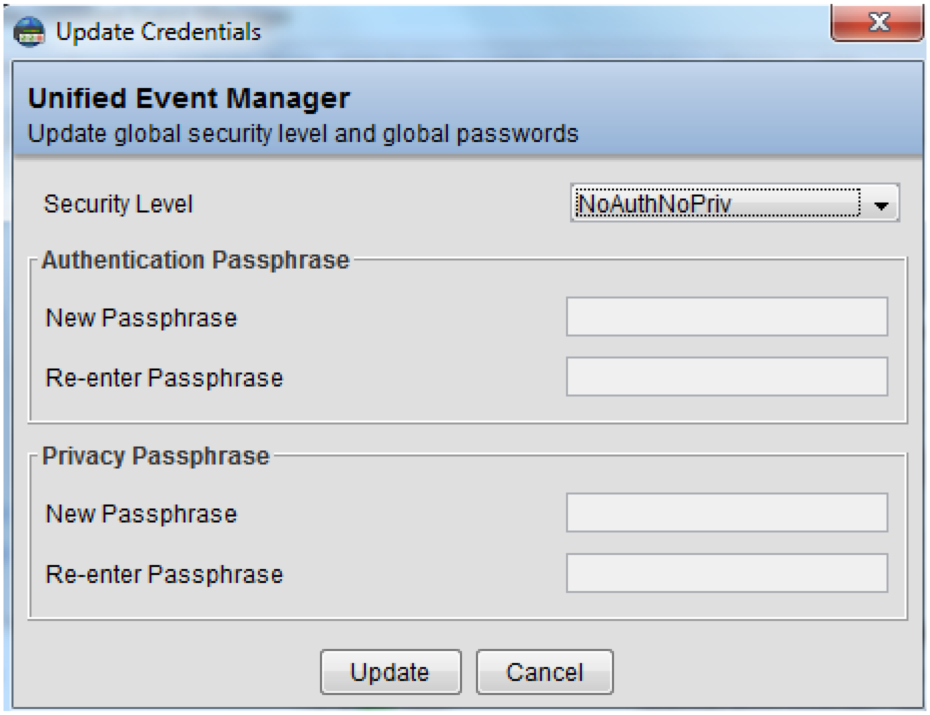
1 Log on to UEM as admin, security admin or any user who can change credentials.

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 2: Update Credentials Dialog Box



Update Credentials

Unified Event Manager

Update global security level and global passwords

Security Level: NoAuthNoPriv

Authentication Passphrase

New Passphrase:

Re-enter Passphrase:

Privacy Passphrase

New Passphrase:

Re-enter Passphrase:

The **Update Credentials** dialog box appears.

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

NOTE: 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.

4.9.2.4 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.

4.9.2.5 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.

4.9.2.6

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.

4.9.2.7

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.

4.9.3

UNC Configuration for SNMPv3

- To configure the Radio System 1 credential, see Configuring SNMPv3 Radio System Credentials in EMC Smarts on page 64.
- To use the new credential, see Applying an SNMPv3 Credential to a Device in EMC Smarts on page 65.
- To create a credential, see Creating SNMPv3 Credentials in EMC Smarts on page 65.

IMPORTANT: Changing the credentials in the UEM and UNC requires the account to be changed in the managed devices too.

4.9.3.1

Configuring SNMPv3 Radio System Credentials in EMC Smarts

Radio System 1 is a pre-defined SNMPv3 credential provided. Perform this procedure to configure the **Radio System 1** credential.

NOTE: An optional part of SNMPv3 is to use Authentication and Encryption. This procedure needs to be coordinated with procedures that modify the devices. To switch over Unified Network Configurator to use SNMPv3 with Authentication and Encryption, an SNMPv3 credential must be defined and then the credential must be assigned to a set of devices.

Prerequisites: Obtain access to EMC® Smarts®.

Procedure:

1. Launch the **System Administration** window by pressing F4.
2. To open the list of credentials, select **Global→Credentials Manager→Credentials**.
3. Select the **Radio System 1** credential and click **Edit**.

   The **Edit Shared Credential** window appears.
4. On the **Security** tab, in the **User Name** field, enter the USM user name.

   Typically, it is `MotoMaster`.
5. Select the security level:
   - For authentication only, select **auth_nopriv**.
   - For authentication and encryption, select **auth_priv**.
6. Set the authentication protocol to **HMACSHA** and enter the authentication passphrases in the required fields.
7. If **auth_priv** is the selected security level, set the **Privacy Protocol** to **AES128** and enter the privacy passphrases in the required fields.

   NOTE: Privacy passphrases should be different for **auth** and for **priv**.

4.9.3.2

Applying an SNMPv3 Credential to a Device in EMC Smarts

Prerequisites: Obtain access to EMC® Smarts®.

Procedure:

1. From any of the device collections in Unified Network Configurator (UNC), select one or more devices.

   These device collections are either the network, sites in the network, or view in the network.
2. Right-click **Edit Device**, and select **Update Credentials**.

   The **Update Credentials** window appears.
3. On the **In-Band** tab, set SNMP Credentials to the new credential created (the default SNMPv3 User) and select **Active**.
4. Click **Save only**.
5. Once the device has been updated through loading new software and/or new configuration, validate SNMP communication to the device by right-clicking the device and selecting **Test Credentials**.

4.9.3.3

Creating SNMPv3 Credentials in EMC Smarts

Prerequisites: Obtain access to EMC® Smarts®.

Procedure:

1. Launch the **System Administration** window by pressing F4.
2. To open the list of credentials, select **Global→Credentials Manager→Credentials**.
3. Select the SNMPv3 credential that is currently used by the devices (such as the default **Radio System 1** credential) and click **Copy**.

4. Enter the new credential name.
5. In the **Security** tab, enter the new authentication and privacy passphrases in the required fields.

4.9.4 Configuring Console Site Elements, Dynamic Transcoders, and Group Data Gateways for SNMPv3

Perform this process to configure the following devices for SNMPv3:

- MCC 7500E Dispatch Console
- MCC 7500 VPM Dispatch Console
- MCC 7500 Archiving Interface Server (AIS)
- MKM 7000 Console Alias Manager (CAM)
- PRX 7000 Console Proxy
- Voice Processor Module (VPM)
- Dynamic Transcoder
- Group Data Gateway (GDG)

NOTE:
For details about the SNMPv3 Configuration Utility for Windows devices, see Configuring USM User Security with the Windows Configuration Utility on page 47. For details on VPM configuration, see Configuring RF Site and VPM-Based Devices for SNMPv3 on page 69.

The Conventional Site Controller is configured using the Configuration/Service Software (CSS) and Software Download Manager (SWDL) applications. For more information, see Configuring RF Site and VPM-Based Devices for SNMPv3 on page 69.

SNMPv3 functionality for the CAM server does not apply to the K core configurations. For details, see the *MKM 7000 Console Alias Manager Online Help*.

Prerequisites:

- Install the Configuration Utility for Windows. See Installing the Configuration Utility for Windows on page 39.

  NOTE: Do **not** install the Configuration Utility for Windows for MCC 7500 VPM and MCC 7500E Dispatch Consoles, MCC 7500 AIS, Dynamic Transcoder, PRX 7000 Console Proxy, and GDG. For those devices, the utility is already installed as part of the software installation.

- Configure SNMPv3 credentials on UEM. See UEM Configuration for SNMPv3 on page 58.
- Obtain MotoAdmin passphrases. Use the default passphrase on initial configuration.

Process:

1. To open the utility for SNMP user credential maintenance:

If…	Then…
If your OS is Windows 7,	From **Start**, select **All Programs→Motorola→Motorola SNMPv3-Credentials-WSUI→CA User Credentials**.
If your OS is Windows 10,	From **Start**, select **All apps**. From the list, select **Motorola→CA User Credentials**.

The **MotoAdmin Credentials Validation** dialog box appears. The dialog box requires input of valid credentials for the MotoAdmin user account.

2 Optional: Perform initial SNMPv3 configuration of the MotoAdmin user:

  a Click **Reset MotoAdmin account**.

  b Set new credentials for MotoAdmin and click **OK**.

  c In the **Warning** window that appears, click **Yes**.

  d In the **System** window that appears, click **OK**.

  To reset the MotoAdmin account, the user has to belong to the group with authority to perform the operations in this procedure (see the *Authentication Services Feature Guide* and contact your Active Directory administrator) and launch `CA_UserCredentials.exe` in one of the following ways:

  - From an elevated Windows command line. For information how to run the elevated Windows command line, see “Starting the Windows Command Line as Administrator” in the *Authentication Services Feature Guide*.
  - By right-clicking the file and selecting **Run as administrator**.

3 Log on to the utility as the MotoAdmin user:

  a In the appropriate fields, enter the authentication and privacy passphrases.

  b In the **Agent Port** field, enter a valid port number for the utility. The default port is `161`.

  c Click **OK**.

  MotoAdmin credentials are validated, and the **SNMPv3 User Credential Maintenance** window appears, showing the security name and security level for each user.

4 Perform Changing the Passphrases for the MotoAdmin User Account to Configure Console Site Elements, Dynamic Transcoders, and Group Data Gateways for SNMPv3 on page 67.

5 Perform Setting the Security Level of the MotoMaster User Account to Configure Console Site Elements, Dynamic Transcoders, and Group Data Gateways for SNMPv3 on page 68.

6 Optional: For VPM, perform Setting or Resetting Credentials for VPM on page 68.

7 To set the security level of the MotoInformA and MotoInformB user accounts as configured on the UEM, click **Change to Opposite**.

8 To exit the configuration utility, click **Exit**.

4.9.4.1

Changing the Passphrases for the MotoAdmin User Account to Configure Console Site Elements, Dynamic Transcoders, and Group Data Gateways for SNMPv3

Prerequisites: See Configuring Console Site Elements, Dynamic Transcoders, and Group Data Gateways for SNMPv3 on page 66.

Procedure:

1 From the list of users on the **SNMPv3 Users** tab, select **MotoAdmin**.

2 Click **Set Passphrase**.

3 In the **User Validation** dialog box, type the current passphrases for the MotoMaster user account. Click **OK**.

4 In the **New Authentication Passphrase** dialog box, type the new authentication passphrase for the MotoAdmin user account. Click **OK**.

5 In the **New Privacy Passphrase** dialog box, type the new privacy passphrase for the MotoAdmin user account. Click **OK**.

6 In the confirmation dialog box, click **Yes**.

NOTE: The security level of the MotoAdmin user account cannot be changed.

4.9.4.2 Setting the Security Level of the MotoMaster User Account to Configure Console Site Elements, Dynamic Transcoders, and Group Data Gateways for SNMPv3

Prerequisites: See Configuring Console Site Elements, Dynamic Transcoders, and Group Data Gateways for SNMPv3 on page 66.

Procedure:

1 From the list of user accounts on the **SNMPv3 Users** tab, select **MotoMaster**.

2 Click **Set Security Level**.

3 In the **Select New Security Level** dialog box, select an option which matches the security level of MotoMaster as configured on the UEM:

- **AuthNoPriv**
- **AuthPriv**

4 Click **OK**.

5 In the **New Authentication Passphrase** dialog box, type the new authentication passphrase for MotoMaster. Click **OK**.

6 If the security level is **AuthPriv**, in the **New Privacy Passphrase** dialog box, type the new privacy passphrase for MotoMaster. Click **OK**.

7 In the **User Validation** dialog box, type the current passphrases for the MotoMaster user account. Click **OK**.

8 In the confirmation dialog box, click **Yes**.

4.9.4.3 Setting or Resetting Credentials for VPM

This procedure is optional. SNMPv3 protocol can be enabled to secure the communication between the Console Software Download Manager (Console SWDL) and the Voice Processor Module (VPM). This requires entering user credentials into the VPM through the Unified Network Configurator, as well as entering local credentials on the Console. For more information on Console SWDL, see the *Software Download Manager Online Help*.

Prerequisites: See Configuring Console Site Elements, Dynamic Transcoders, and Group Data Gateways for SNMPv3 on page 66.

Procedure:

1 Log on as an administrator.

2 Navigate to `C:\Program Files (x86)\Motorola MCC 7500\bin\`.

3 Execute the `SctVPM.exe` file.

4 In the **SNMPv3 Credential Tool for VPM** window, enter authentication and encryption passphrases for the VPM.

Credentials must match credentials which the CSS/UNC pushed to the VPM.

5 Click **Set**.

If user credentials for SNMPv3 are forgotten, clear them and revert SNMPv3 to clear-mode by clicking **Reset**.

4.9.5 MCC 7500 IP Logging Recorder Configuration for SNMPv3

Configuration of the MCC 7500 IP Logging Recorder is described in the documentation supplied with the device.

NOTE: For additional or replacement copies of MCC 7500 IP Logging Recorder documentation, contact your Motorola Solutions representative.

4.9.6 Configuring RF Site and VPM-Based Devices for SNMPv3

Perform this procedure to configure devices at RF sites for SNMPv3 by using the Configuration/Service Software (CSS) application. This procedure applies to the following devices:
RF site devices:

- GTR 8000 Base Radio
- GCM 8000 Comparators
- GRV 8000 Comparators
- GPB 8000 Reference Distribution Module (RDM)
- GCP 8000 Site Controller
- GPW 8000 Receiver

Voice Processor Module (VPM) devices:

- Voice Processor Module (VPM)
- Telephone Media Gateway (TMG)

Prerequisites: Install the latest version of CSS.

Procedure:

1. Launch the CSS application and connect to the device.
2. In the CSS main window, select **SNMPv3 Configuration→Configure SNMPv3 Users (Ethernet)**.

   The **SNMPv3 Login/Connection Screen** dialog box appears, showing MotoAdmin as the selected SNMPv3 user. The dialog box displays the following message: `An Ethernet connection must be established with the SNMPv3 capable device on behalf of MotoAdmin user before this operation can be selected.`
3. Click **OK**.
4. In the **SNMPv3 Password Prompt**, enter the passphrases and the device IP address:

If…	Then…
If you are connecting to a device through a front panel Ethernet connection, before making any other selections or entries,	click **Front Panel Ethernet**.
If you know the IP address or the Fully Qualified Domain Name (FQDN) for the device,	enter that value in the **Device IP Address** field.

If…	Then…
If you do not know the IP address for the device,	perform the following actions: **a** Click **Fetch DNS**. **b** Enter the Zone, Site, Subsite (if active), and Device ID. **c** From the **Device** drop-down list, select the device you are trying to connect to. **d** Click **OK**.

5 Click **OK**.

A connection is made with the selected device, the MotoAdmin passphrases are authenticated, and the **Configure SNMPv3 Users** screen appears.

6 From the list of users, select the name of the user account that you want to configure.

The **User Status** screen appears. Depending on the user selection, some fields on this screen become read-only or disabled (grayed-out).

NOTE:
Ensure that you have the required SNMPv3 credentials information (Authentication passphrase, Encryption passphrase, and Authoritative Engine ID) to configure the device before proceeding. The user credentials information includes both the current and new credentials. Without the current credentials, you cannot access the device and cannot change the user credentials.

Changing to the incorrect user credentials may disable access to the device from the UNC or prevent the device from sending alarms to the Unified Event Manager (for fault management).

7 Perform one the following actions:

If…	Then…
If the status is: • `Active` • `Not in service` • `Not ready`	the user is configured on the device, and the **Update** and **Delete** options are enabled. Perform one of the following actions: • To update a user account, go to step 8 • To delete a user account, click **Delete**, and go to step 12
If the status is `Not present`**,**	the user account is not present on the device, and the **Create** option is enabled. Perform the following actions: **a** From the drop-down list, select a **Username** that is not present on the device. **b** Select a Security Level. See step 8. **c** Complete all required fields for the Security Level and user type selected. See step 9 through step 11. **d** Click **Create**. **e** Go to step 12.

8 From the drop-down list, select a Security Level. For security level description, see Table 1.

9 Change the authentication password for user accounts with a security level of AuthNoPriv or AuthPriv:

   a Enter the current authentication password.

   b Enter the current password. If you do not know the password, select the **I do not remember old password** check box.

   c In the **New Password** and **Confirm New Password** fields, enter a new password.

   NOTE: Passwords must be between 8 and 64 characters in length and consist of upper- or lowercase alphanumeric characters, excluding @ # $ ^ or _.

   d Click **Update**.

   The authentication password is changed.

10 Change the encryption password for user accounts with a security level of AuthPriv:

   a Enter the current encryption password.

   b Enter the current password. If you do not know the password, select the **I do not remember old password** check box.

   c In the **New Password** and **Confirm New Password** fields, enter a new password.

   NOTE: Passwords must be between 8 and 64 characters in length and consist of upper- or lowercase alphanumeric characters, excluding @ # $ ^ or _.

   d Click **Update**.

   The encryption password is changed.

11 Change the Authoritative Engine ID for INFORM user accounts (MotoInformA or MotoInformB):

   a From the drop-down list, select **Current Engine ID**.

   b In the text field, enter a new Engine ID.

   NOTE: Engine IDs must be between 1 and 27 lowercase characters in length, must comply with Domain Name syntax, and must be the fault manager's DNS FQDN. For the DNS FQDN, contact your System Administrator.

   c Click **Update**.

   The Authoritative Engine ID is changed.

12 In the **Confirmation** dialog box, click **Yes**.

   The status of the configuration operations appears. Successful operations are marked with a green mark, while failed operations are marked with a red mark.

13 Repeat step 6 through step 12 for each SNMPv3 user account.

14 In the **Configure SNMPv3 Users** dialog box, click **Cancel**.

   The dialog box closes and the CSS main window appears.

15 Close the CSS application.

16 **NOTE:** You can only perform step 16 and step 17 if all the sites are already configured.

   Configure SNMPv3 manager passphrases for sites. See Configuring SNMPv3 Manager Passphrases for Sites on page 85.

17 Verify SNMPv3 configuration status for sites. See Verifying SNMPv3 Configuration Status for Sites on page 89.

4.9.6.1 MotoZSS Passphrase Rotation From UNC

You can change the MotoZSS user account passphrases for Site Controllers from the Unified Network Configurator (UNC) by using the
`Rotate SNMPv3 Passphrase for Site Controller Statistical user`
saved command. For sites with Summit-based equipment and using SNMPv3, this command creates the MotoZSS user account on the Site Controller, if it does not already exist. See “UNC Saved Commands” and “Accessing and Executing Existing Saved Commands” in the *Unified Network Configurator User Guide*.

NOTE: From the UNC, you can only change MotoZSS user account passphrases on Site Controllers and not on the Zone Statistics Server (ZSS). Ensure that the MotoZSS passphrases configured on the Site Controllers are the same as the ones on the ZSS.

4.9.7 Configuring SNMPv3 Passphrases on DSC 8000 for MotoAdmin Account

Prerequisites:
Ensure that credentials for MotoAdmin account are added in the Unified Network Configurator (UNC). See "Adding Global Credentials in the VMware Smart Assurance Network Configuration Manager" in the *Unified Network Configurator User Guide*.

Procedure:

Changing the current SNMPv3 credentials for MotoAdmin account

1. Log on to the EMC Smarts Network Configuration Manager.
2. In the left navigation pane of the EMC Smarts Network Configuration Manager dashboard, select **Networks→Astro 25 Radio Network→Devices**.
3. Right-click the DSC8000 NM Agent device on the right side of the window and select **Properies**.
4. In the **Device Properties** window, select the **Communication** tab.
5. Click **Update Credentials**.
6. In the **Update Credentials** window, select **In-Band** tab.
7. In the **SNMPv3** section, select the current MotoAdmin SNMPv3 credential.
8. For the new MotoAdmin SNMPv3 credential, check the **Active** box.
9. Click **Save only**.
10. Right-click the DSC8000 NM Agent device on the right side of the window and select **Properies**.
11. In the **Device Properties** window, select the **Communication** tab.
12. Click **Update Credentials**.
13. In the **Update Credentials** window, select **In-Band** tab.
14. In the **SNMPv3** section, select the new MotoAdmin SNMPv3 credential.
15. For the new MotoAdmin SNMPv3 credential, check the **Active** box.
16. Click **Schedule**.

    The **Schedule Push Job** window appears.

17. Type the job name and schedule the job.
18. Click **Approve & Submit**.

Clicking **Approve & Submit** closes the Schedule Job window and the job status can be viewed by using Schedule Manager available from the **Tools** menu on the VMware Smart Assurance Network Configuration Manager main window.

Restoring MotoMaster account credentials in UNC

19 Right-click the DSC8000 NM Agent device on the right side of the window and select **Properies**.

20 In the **Device Properties** window, select the **Communication** tab.

21 Click **Update Credentials**.

22 In the **Update Credentials** window, select **In-Band** tab.

23 In the **SNMPv3** section, select the current MotoMaster SNMPv3 credential.

24 For the new MotoMaster SNMPv3 credential, check the **Active** box.

25 Click **Save only**.

26 Right-click the DSC8000 NM Agent device on the right side of the window and select **Test Credentials**.

27 In the **Schedule Push Job** window, click **Approve & Submit**.

28 Verify that the scheduled job completed successfully:

- **a** Open the schedule manager by pressing F7.
- **b** Sort the list by ascending job ID by clicking **Job ID** until an upward-pointing arrow appears.
- **c** Verify that the job is the top job on the list, select the job and verify that the target device is listed in the task list.
- **d** Verify the job completes without an error. The schedule manager will need to be refreshed manually by hitting F5 periodically.

  You need to refresh the schedule manager manually by hitting F5 periodically.

4.9.8 Configuring SNMPv3 Passphrases on DSC 8000 for Other USM Accounts

You can use this procedure to change current SNMPv3 credentials to new SNMPv3 AuthPriv credentials. Rolling credentials to NoAuthNoPriv or AuthNoPriv are not supported.

You can reset SNMP credentials to NoAuthNoPriv by performing Resetting SNMPv3 Passphrases to Default on DSC 8000 on page 153.

Procedure:

1. Log on to the EMC Smarts Network Configuration Manager.
2. In the left navigation pane of the EMC Smarts Network Configuration Manager dashboard, select **Networks→Astro 25 Radio Network→Devices**.
3. Right-click the DSC8000 NM Agent device on the right side of the window and select **Saved Commands**.

   The **Select Item** dialog box appears.
4. Click the folder icon at the top of the dialog box, to the right of the **Look In** field. Continue to click this icon until the `System` folder displays on the list of folders, in the **Select Item** dialog box.
5. In the **Select Item** dialog box, go to **System→Motorola→SNMPv3**.

   A list of saved commands displays in the **Select Item** dialog box.
6. Select **Change SNMPv3 Users From Clear to AuthPriv**.

7 In the **Template Variable Substitution** dialog box, perform the following actions:

   a Enter new newAuthPass and newPrivPass.

   b Enter current adminAuthPass and currentAuthPass.

   c Select the desired **targetInformUser**.

   d Click **OK**.

   When successful, MotoMaster, MotoSWDL and selected Inform user accounts use new credentials.

8 Right-click the DSC8000 NM Agent device on the right side of the window and select **Properies**.

9 In the **Device Properties** window, select the **Communication** tab.

10 Click **Update Credentials**.

11 In the **Update Credentials** window, select **In-Band** tab.

12 In the **SNMPv3** section, select the current MotoMaster SNMPv3 credential.

13 For the new MotoMaster SNMPv3 credential, check the **Active** box.

14 Click **Save only**.

15 Right-click the DSC8000 NM Agent device on the right side of the window and select **Test Credentials**.

16 In the **Schedule Push Job** window, click **Approve & Submit**.

4.9.9 PTP Devices and E4G Backhaul Switches SNMPv3 Configuration

Fault management of the Point-to-Point (PTP) devices uses the SNMPv3 protocol with AES for privacy and SHA1 for authentication. The E4G backhaul switches also support SNMP.

NOTE:
For detailed formation on how to configure a PTP device for SNMP, see the appropriate *Cambium Networks PTP User Guide*.

The PTP management agent is compatible with SNMP for various Management Information Bases (MIBs). For a detailed list, see the appropriate *Cambium Networks PTP User Guide*.

When SNMPv3 is enabled, whenever a PTP Event occurs, a trap is sent to the SNMP trap receiver(s) configured in the PTP. In an ASTRO® 25 system, UEM receives the trap information from the PTP devices.

PTP devices support web pages for configuring SNMPv3 security. Web-based management of SNMPv3 security allows for two security roles:

- Read Only
- System Administrator

NOTE: Both UEM and PTP use the System Administrator role through MotoMaster to process all SNMP Get/GetNext/Set requests and trap processing. For details, see SNMP User Accounts Configuration on page 75.

PTP Bootstrapping involves setting up a PTP device locally before accessing the PTP device through an NM Client. During this process, setting up the PTP License Key establishes the AES algorithm required for SNMPv3 (and HTTPS) support. A link is provided in the appropriate Cambium Networks PTP User Guide to access the PTP License Key Generator, if necessary.

To simplify PTP replacement, the user should always select IP address as SNMP Engine ID Format. The security level and passphrase setting of the underlying SNMP user account in the PTP configuration should match the UEM settings.

Table 8: SNMP Configuration Values for PTP Devices

This table provides basic SNMP configuration values for PTP devices. For more information, see the appropriate *Cambium Networks PTP User Guide*.

Attributes	Value
SNMP State	Enabled
SNMP Version	v3
SNMP Security Mode	Web-based
SNMP Engine ID Format	IP Address
SNMP Port Number	161

Table 9: SNMP User Policy Configuration Values for PTP Devices

This table provides SNMP User Policy Configuration values for PTP devices. For details, see the appropriate *Cambium Networks PTP User Guide*.

Attributes	Value
System Admin Policy Security Level	AuthPriv
System Admin Policy Authentication Protocol	SHA-1
System Admin Policy Privacy Protocol	AES (Rijndael)
Read Only Policy Security Level	AuthPriv
Read Only Policy Authentication Protocol	SHA-1
Read Only Policy Privacy Protocol	AES (Rijndael)

4.9.9.1 SNMP User Accounts Configuration

When configuring SNMP User Accounts for Point-to-Point (PTP) devices, configure the following entries:

- Name = MotoMaster
- Role = System Administrator

NOTE: All other user entries are disabled.

4.9.9.2 SNMP Trap Configuration

When configuring SNMP Traps for Point-to-Point (PTP) devices, set the following values:

- SNMP Trap IP Address = 10.Zone.233.20 (Trap Destination 1 Configuration)
- SNMP Trap User Account = User 1: MotoMaster

NOTE: Trap Destination 2 Configuration entries are left to default values. For details, see the appropriate *Cambium Networks PTP User Guide*. Trap Destination 2 is configured for DSR where a PTP can send traps to two UEMs for each zone.

The PTP web-based interface may be used to enable or disable generation of each supported SNMP notification or diagnostic alarm.

IMPORTANT: All Traps (Notifications) should be enabled.

4.9.9.3

E4G Devices Configuration for SNMPv3

For information on how to configure E4G devices for SNMP, see the following documents, or contact an Extreme Networks or Cambium Networks field representative.

- System Planner for PTP-based backhaul networks
- Extreme Networks E4G mobile backhaul documentation

4.9.10

TRAK Devices Configuration for SNMPv3

SNMPv3 configuration of the following TRAK models is described in the documentation supplied with the device:

- 9100
- 8835

For more information, see the *RF Site Technician Reference Guide*, *RF Site Technician Guide* and *Network Time Protocol Server Feature Guide*.

4.9.11

PDG Configuration for SNMPv3

You can configure USM user security for the Packet Data Gateway (PDG), as well as modify user passphrases and security levels.

4.9.11.1

Configuring USM User Security for the PDG

Prerequisites: Ensure that the device is joined to an Active Directory domain. Obtain your Active Directory credentials. For information about setting up Active Directory users so that they can perform specific administration menu procedures, see “Appendix B” in the *Authentication Services Feature Guide* and contact your Active Directory administrator.

Procedure:

1. Log on to the PDG console with your Active Directory account credentials.
2. At the user prompt, enter: `admin_menu`
3. In the main PDG administration menu, select **OS Administration**.
4. In the **OS Administration** menu, select **Security Provisioning**.
5. In the **Security Provisioning** menu, select **Manage SNMP Passphrases**.
6. In the **Manage SNMP Passphrases** menu, select **Configure SNMPv3 Agent**.

   The **SNMP Configuration Utility** appears.

7. At the MotoAdmin Authentication Passphrase prompt, enter the MotoAdmin Authentication Passphrase.

8 At the MotoAdmin Privacy Passphrase prompt, enter the MotoAdmin Privacy Passphrase.

SNMP Administration options appear.

9 Select the type of user account to configure:

- If you want to modify credentials for an INFORM user account, select **Modify SNMP Inform Configuration**. The system displays the currently active INFORM user account (either MotoInformA or MotoInformB) and indicates that user account's security level.
- If you want to modify credentials for any other user account, select **Modify SNMP User Configuration**. The system displays a list of user accounts currently available for configuration if you are logged on as MotoAdmin, including MotoMaster. The list shows the security levels of the user accounts listed.

10 From the **Select User to Modify** menu, select a user:

- If you select the MotoAdmin user account, which always has a security level of AuthPriv, so only its passphrases can be changed, change the passphrases. See Modifying User Passphrases for the PDG on page 77.
- If you select a user account with a security level of noAuthNoPriv, which means that no passphrases are configured for that user account, change the security level. See Modifying User Security Levels for the PDG on page 77.
- If you select a user account other than MotoAdmin with a security level of AuthPriv or you select a user account with a security level of AuthNoPriv, in the **Select Modification** menu, change the passphrases. See Modifying User Passphrases for the PDG on page 77. Then, change the security level. See Modifying User Security Levels for the PDG on page 77.

11 To exit the menu and return to the user prompt, type `q`. Press ENTER.

4.9.11.2
Modifying User Passphrases for the PDG

Prerequisites: See Configuring USM User Security for the PDG on page 76.

Procedure:

1 From the **Select Modification** menu, select **Update Passphrases**.

The system prompts for the authentication passphrase for the selected user account.

NOTE: For the MotoAdmin user, the **Select Modification** menu does not appear.

2 Enter and confirm the authentication passphrase.

If the selected user account has a security level of AuthNoPriv, the passphrases are updated, and the **Select User to Modify** menu returns.
If the selected user account has a security level of AuthPriv, the system prompts for the privacy passphrase for the selected user account. Continue to step 3.

3 Enter and confirm the privacy passphrase.

The passphrases are updated, and the **Select User to Modify** menu returns.

4.9.11.3
Modifying User Security Levels for the PDG

Prerequisites: See Configuring USM User Security for the PDG on page 76.

Procedure:

1. From the **Select Modification** menu, select **Update Security Level**.

   The system displays the name and current security level of the selected user account, along with a list of allowable security levels for that user account.

   NOTE: For user accounts with a security level of noAuthNoPriv, the **Select Modification** menu does not appear.

2. Select the desired security level from the list.

   The security level is updated, and the **Select User to Modify** menu returns.

Postrequisites: If you need to recover passphrases for the MotoAdmin user account for the PDG, see Recovering MotoAdmin Passphrases on page 149.

4.9.12

Zone Controller Configuration for SNMPv3

You can configure USM user security, modify user passphrases, and set or modify user security levels for a Zone Controller (ZC).

4.9.12.1

Configuring USM User Security for Zone Controllers

Perform this procedure to configure USM user security for the active and standby Zone Controllers.

Prerequisites: Obtain Active Directory account credentials. For information about setting up Active Directory users so that they can perform specific administration menu procedures, see “Appendix B” in the *Authentication Services Feature Guide* and contact your Active Directory administrator.

Procedure:

1. Log on to the Zone Controller with your Active Directory account credentials.
2. At the user prompt, enter: `admin_menu`
3. In the main Zone Controller administration menu, select **OS Administration**.
4. In the **OS Administration** menu, select **Security Provisioning**.
5. In the **Security Provisioning** menu, select **Manage SNMP Passphrases**.
6. In the **Manage SNMP Passphrases** menu, select **Configure SNMPv3 Agent**.

   The SNMP Configuration Utility appears. You are prompted for the MotoAdmin Authentication Passphrase.

7. At the MotoAdmin Authentication Passphrase prompt, enter the MotoAdmin Authentication Passphrase.
8. At the MotoAdmin Encryption Passphrase prompt, enter the MotoAdmin Encryption Passphrase.

   SNMP Administration options appear.

9. Select the type of user account to configure:
   - If you want to modify credentials for an INFORM user account, select **Modify SNMP Inform Configuration**. The system displays the currently active INFORM user account (either MotoInformA or MotoInformB) and indicates that user account's security level.
   - If you want to modify credentials for any other user account, select **Modify SNMP User Configuration**. The system displays a list of user accounts currently available for

configuration if you are logged in as MotoAdmin, including MotoMaster. The list shows the security levels of the user accounts listed.

10 From the **Select User to Modify** menu, select a user:

- If you select the MotoAdmin user, which always has a security level of AuthPriv, so only its passphrases can be changed, change the passphrases. See Modifying User Passphrases for Zone Controllers on page 79.
- If you select a user with a security level of noAuthNoPriv, which means that no passphrases are configured for that user, set the security level. See Setting User Security Levels for Zone Controllers on page 79.
- If you select a user other than MotoAdmin with a security level of AuthPriv, or you select a user with a security level of AuthNoPriv, in the **Select Modification** menu, change the passphrases. See Modifying User Passphrases for Zone Controllers on page 79. Then, change the security level. See Setting User Security Levels for Zone Controllers on page 79.

11 Enter: `q`

Repeat the sequence until the Common Credentials User Interface closes.

4.9.12.2
Modifying User Passphrases for Zone Controllers

Prerequisites: See Configuring USM User Security for Zone Controllers on page 78.

Procedure:

1 From the **Select Modification** menu, select **Update Passphrases**.

The system prompts for the authentication passphrase for the selected user account.

NOTE: For the MotoAdmin user account, the **Select Modification** menu does not appear.

2 Enter and confirm the authentication passphrase.

If the selected user account has a security level of AuthNoPriv, the passphrases are updated, and the **Select User to Modify** menu returns.
If the selected user account has a security level of AuthPriv, the system prompts for the privacy passphrase for the selected user account.

3 Enter and confirm the privacy passphrase.

The passphrases are updated, and the **Select User to Modify** menu returns.

4.9.12.3
Setting User Security Levels for Zone Controllers

Prerequisites: See Configuring USM User Security for Zone Controllers on page 78.

Procedure:

1 From the **Enter New Security Level** menu, select the option for the new security level of the user.

Prompts for new passphrases appear, followed by prompts for MotoAdmin passphrases.

2. Enter the appropriate passphrases. Press Enter.

   The security level of the selected user is updated and the **Select User to Modify** menu appears.

4.9.12.4
Modifying User Security Levels for Zone Controllers

Prerequisites: See Configuring USM User Security for Zone Controllers on page 78.

Procedure:

1. From the **Select Modification** menu, select **Change Security Level**.

   The **Enter New Security Level** menu appears, displaying the name and current security level of the selected user account, and a list of allowed security levels for that user account.

2. From the list, select the desired security level.

   Depending on the security level selected, prompts for new passphrases appear, followed by prompts for MotoAdmins passphrases.

3. Enter the appropriate passphrases. Press Enter.

   The security level of the selected user is updated and the **Select User to Modify** menu appears.

Postrequisites: If you need to recover passphrases for the MotoAdmin user account for a Zone Controller, see Recovering MotoAdmin Passphrases on page 149.

4.9.13
ISGW Configuration for SNMPv3

You can configure USM user security, modify user passphrases, and set or modify user security levels for ISGW.

4.9.13.1
Configuring USM User Security for ISGW

Perform this procedure to configure USM user security for the active and standby ISGW.

Prerequisites: Obtain the Active Directory account credentials. For information about setting up Active Directory users so that they can perform specific administration menu procedures, see the *Authentication Services Feature Guide* and contact your Active Directory administrator.

Procedure:

1. Log on to the ISGW with your Active Directory account credentials.
2. At the user prompt, enter: `admin_menu`
3. In the main ISGW administration menu, select **OS Administration**.
4. In the **OS Administration** menu, select **Security Provisioning**.
5. In the **Security Provisioning** menu, select **Manage SNMP Passphrases**.
6. In the **Manage SNMP Passphrases** menu, select **Configure SNMPv3 Agent**.

   The SNMP Configuration Utility appears.

7. At the MotoAdmin Authentication Passphrase prompt, enter the MotoAdmin Authentication Passphrase.

8 At the MotoAdmin Encryption Passphrase prompt, enter the MotoAdmin Encryption Passphrase.

The SNMP Administration options appear.

9 Select the type of user account to configure:

- If you want to modify credentials for an INFORM user account, select **Modify SNMP Inform Configuration**. The system displays the currently active INFORM user account (either MotoInformA or MotoInformB) and indicates that user account's security level.
- If you want to modify credentials for any other user account, select **Modify SNMP User Configuration**. The system displays a list of user accounts currently available for configuration if you are logged in as MotoAdmin, including MotoMaster. The list shows the security levels of the user accounts listed.

10 From the **Select User to Modify** menu, select a user:

If…	Then…
If you select the MotoAdmin user, which always has a security level of AuthPriv, so only its passphrases can be changed,	change the passphrases. See Modifying User Passphrases for ISGW on page 81.
If you select a user with a security level of noAuthNoPriv, which means that no passphrases are configured for that user,	set the security level. See Setting User Security Levels for ISGW on page 82.
If you select a user other than MotoAdmin with a security level of AuthPriv, or you select a user with a security level of AuthNoPriv,	perform the following actions: **a** In the **Select Modification** menu, change the passphrases. See Modifying User Passphrases for ISGW on page 81. **b** Change the security level. See Setting User Security Levels for ISGW on page 82.

11 Enter `q`. Repeat the sequence until the Common Credentials User Interface closes.

4.9.13.2
Modifying User Passphrases for ISGW

Prerequisites: See Configuring USM User Security for ISGW on page 80.

Procedure:

1 From the **Select Modification** menu, select **Update Passphrases**.

The system prompts for the authentication passphrase for the selected user account.

NOTE: For the MotoAdmin user account, the **Select Modification** menu does not appear.

2 Enter and confirm the authentication passphrase.

If the selected user account has a security level of AuthNoPriv, the passphrases are updated, and the **Select User to Modify** menu returns.
If the selected user account has a security level of AuthPriv, the system prompts for the privacy passphrase for the selected user account.

3 Enter and confirm the privacy passphrase.

The passphrases are updated, and the **Select User to Modify** menu returns.

4.9.13.3

Setting User Security Levels for ISGW

Prerequisites: See Configuring USM User Security for ISGW on page 80.

Procedure:

1 From the **Enter New Security Level** menu, select the option for the new security level of the user.

Prompts for new passphrases appear, followed by prompts for MotoAdmin passphrases.

2 Enter the appropriate passphrases, based on the display prompts. Press ENTER.

The security level of the selected user is updated and the **Select User to Modify** menu appears.

4.9.13.4

Modifying User Security Levels for ISGW

Prerequisites: Security levels for the ISGW have already been configured. See Configuring USM User Security for ISGW on page 80.

Procedure:

1 From the **Select Modification** menu, select **Change Security Level**.

The **Enter New Security Level** menu appears, displaying the name and current security level of the selected user account, and a list of allowed security levels for that user account.

2 Select the desired security level from the list.

Depending on the security level selected, prompts for new passphrases appear, followed by prompts for MotoAdmins passphrases.

3 Enter the appropriate passphrases, based on the display prompts. Press ENTER.

The security level of the selected user is updated and the **Select User to Modify** menu appears.

Postrequisites: If you need to recover passphrases for the MotoAdmin user account for ISGW, see Recovering MotoAdmin Passphrases on page 149.

4.9.14

PNM Servers and ATR Configuration for SNMPv3

You can configure SNMPv3 for the following devices:

- User Configuration Server (UCS)
- System Statistics Server (SSS)
- Zone Database Server (ZDS)
- Zone Statistics Server (ZSS)
- Unified Event Manager (UEM) Server
- Unified Network Configurator (UNC)
- Unified Network Configurator Device Server (UNCDS)
- Air Traffic Router (ATR), unless otherwise noted

For a complete list of manager/agent relationships, see SNMPv3 Communication Matrix on page 53.

The PNM Servers define two types of SNMPv3 user accounts:

- Manager's side (for devices that manage other devices)
- Agent's side (for devices managed by the managers)

An ATR defines SNMPv3 agent as the only type of a user account.

Each of the devices is an SNMPv3 agent, but there are only a few SNMPv3 managers. For example, ZSS is configured as an agent for the UEM, the UEM being the manager.

Correct communication between PNM servers including backup, restore, and synchronization of databases requires correct configuration of both managers and agents.

4.9.14.1

Configuring PNM Servers and ATRs for SNMPv3

The order in which the devices are configured is arbitrary, as long as SNMPv3 agents are configured first. For a complete list of manager/agent relationships, see SNMPv3 Communication Matrix on page 53.

Process:

1. For every PNM Server and ATR, configure the SNMPv3 agent. See Configuring the Agent's SNMPv3 Credentials for PNM Servers or ATRs on page 86.
2. For every PNM Server, configure the SNMPv3 manager. See Configuring SNMPv3 Manager Credentials on page 83.
3. For every ZSS Server, configure the SNMPv3 manager for Sites. See Configuring SNMPv3 Manager Passphrases for Sites on page 85.
4. Repeat the procedure for every zone in the system, including primary and backup DSR core.

   IMPORTANT: While configuring the SNMPv3 manager, it is possible to set different passwords for each agent. For example, UCS is a manager for UCS, but also UNC and SSS. If different passwords are set on each of the three agents (UCS, UNC, SSS), three different paths need to be configured with three different passwords for each.

SNMPv3 agent and manager is configured in all zones.

4.9.14.2

Configuring SNMPv3 Manager Credentials

Perform this procedure to configure the manager's SNMPv3 credentials for a PNM server (**not** for an ATR).

Prerequisites: Obtain Active Directory credentials. For information about setting up Active Directory users so that they can perform specific administration menu procedures, see “Appendix B” in the *Authentication Services Feature Guide* and contact your Active Directory administrator.

Procedure:

1. Log on to the server application:

If…	Then…
If the server application you are logging on to is joined to an Active Directory domain, and a domain controller is available to the server on the network,	log on to the server using your Active Directory account credentials.

If…	Then…
	A command prompt appears, including information on the hostname, domainname, and timezone.
If the server application you are logging on to is not joined to an Active Directory domain, or a domain controller is not available to the server on the network,	use the VMware vSphere Client to access the server and log on with the root account. See “Logging On to the VMware vSphere Client” in the *Virtual Management Server Software User Guide*.

2. At the command prompt, enter: `admin_menu`
3. In the server administration menu, select **OS Administration**. Press ENTER.
4. In the **OS Administration** menu, select **Security Provisioning**. Press ENTER.
5. In the **Security Provisioning** menu, select **Manage SNMP Passphrases**. Press ENTER.
6. In the **Manage SNMP Passphrases** menu, select **Configure SNMPv3 Manager**. Press ENTER.

   The system prompts for passphrases for the MotoAdmin user account.
7. Enter valid passphrases for the MotoAdmin user account.
8. In the **SNMP Administration** menu, select **Change MotoNM Security Level**.

   The system displays a list of devices that might be configured, as well as the status of communication between the current device and the remote device. Server applications are present on the list only if they are reachable from the server.
9. Select the device to configure.
10. At the new security level prompt, select the desired security level for the device.
11. At the new passphrases prompt, enter new manager passphrases for the device.
12. In the **SNMPv3 Configuration** menu, to exit the configuration utility, enter: `q`.

    The Common Credentials User Interface closes.

4.9.14.3 Configuring SNMPv3 Manager Passphrases

Perform this procedure to configure the manager's SNMPv3 passphrases for a PNM server (**not** for an ATR).

Prerequisites: Obtain Active Directory account credentials. For information about setting up Active Directory users so that they can perform specific administration menu procedures, see “Appendix B” in the *Authentication Services Feature Guide* and contact your Active Directory administrator.

Procedure:

1. Log on to the server application:

If…	Then…
If the server application you are logging on to is joined to an Active Directory domain, and a domain controller is available to the server on the network,	log on to the server using your Active Directory account credentials. A command prompt appears, including information on the hostname, domainname, and timezone.

If…	Then…
If the server application you are logging on to is not joined to an Active Directory domain, or a domain controller is not available to the server on the network,	use the VMware vSphere Client to access the server and log on with the root account. See “Logging On to the VMware vSphere Client” in the *Virtual Management Server Software User Guide*.

2. At the command prompt, enter: `admin_menu`
3. In the main administration menu, select **OS Administration**. Press ENTER.
4. In the **OS Administration** menu, select **Security Provisioning**. Press ENTER.
5. In the **Security Provisioning** menu, select **Manage SNMP Passphrases**. Press ENTER.
6. In the **Manage SNMP Passphrases** menu, select **Configure SNMPv3 Manager**. Press ENTER.

   The system prompts for passphrases for the MotoAdmin user account.

7. Enter valid passphrases for the MotoAdmin user account.
8. In the **SNMPv3 Manager Configuration** menu, select **Change MotoNM Passphrases**.

   The system displays a list of devices that might be configured, as well as the status of communication between the current device and the remote device.

   NOTE: If the MotoNM user account's security level is set to noAuthNoPriv, then this option is unavailable and you can skip this step.

9. Select the device to configure.

   The system prompts for new manager passphrases for the device.

10. Enter new manager passphrases for the device.

    The operation succeeded message appears. The **Select User to Modify** menu returns.

4.9.14.4
Configuring SNMPv3 Manager Passphrases for Sites

Perform this procedure to configure the ZSS Server with the MotoZSS SNMPv3 manager passphrases that were previously configured into each Site Controller. This procedure is applicable only if Inbound RF Quality Metrics Collection is enabled on your system.

NOTE:
The MotoZSS passphrases need to be the same as the ones configured on the Site Controllers.

The security level for the MotoZSS user account is always AuthPriv.

Prerequisites:
Obtain Active Directory credentials. For information about setting up Active Directory users so that they can perform specific administration menu procedures, see “Appendix B” in the *Authentication Services Feature Guide* and contact your Active Directory administrator.

Ensure that all the sites are already configured.

Procedure:

1. Log on to the ZSS server application:

If…	Then…
If the server application you are logging on to is joined to an Active Directory domain, and a domain controller is available to the server on the network,	log on to the server using your Active Directory account credentials. A command prompt appears, including information on the hostname, domainname, and timezone.
If the server application you are logging on to is not joined to an Active Directory domain, or a domain controller is not available to the server on the network,	use the VMware vSphere Client to access the server and log on with the root account. See “Logging On to the VMware vSphere Client” in the *Virtual Management Server Software User Guide*.

2 At the command prompt, enter: `admin_menu`

3 In the server administration menu, select **OS Administration**. Press ENTER.

4 In the **OS Administration** menu, select **Security Provisioning**. Press ENTER.

5 In the **Security Provisioning** menu, select **Manage SNMP Passphrases**. Press ENTER.

6 In the **Manage SNMP Passphrases** menu, select **Configure SNMPv3 Managers for Sites**. Press ENTER.

7 At the prompt, enter valid passphrases for the MotoAdmin user account.

8 In the **Configure SNMPv3 Managers for Sites** menu, select **Change MotoZSS Passphrases**.

The system displays a list of Site Controllers that may be configured.

NOTE: Ensure that the sites are already configured on the UNC. Otherwise, a message that there are no sites to configure appears.

9 Select the device or all devices to configure.

10 At the prompt, enter new manager passphrases for the device or all devices.

A message that the passphrases have been changed successfully appears.

11 To return to the **Change MotoZSS Passphrases** menu, press ENTER.

12 To close the main administration menu, in the **Change MotoZSS Passphrases** menu, enter: `q`

4.9.14.5
Configuring the Agent's SNMPv3 Credentials for PNM Servers or ATRs

Prerequisites: Active Directory account credentials. For information about setting up Active Directory users so that they can perform specific administration menu procedures, see “Appendix B” in the *Authentication Services Feature Guide* and contact your Active Directory administrator.

Procedure:

1 Log on to the server application:

If…	Then…
If the server application you are logging on to is joined to an Active Directory domain, and a domain controller is available to the server on the network,	log on to the server using your Active Directory account credentials. A command prompt appears, including information on the hostname, domainname, and timezone.

If…	Then…
If the server application you are logging on to is not joined to an Active Directory domain, or a domain controller is not available to the server on the network,	use the VMware vSphere Client to access the server and log on with the root account. See “Logging On to the VMware vSphere Client” in the *Virtual Management Server Software User Guide*.

2 At the root prompt, enter: `admin_menu`

The server application administration menu and the menu prompt appear. There is a slight delay for the server to display the menu system.

3 In the administration menu, select **OS Administration**. Press Enter.

4 In the **OS Administration** menu, select **Security Provisioning**. Press Enter.

5 In the **Security Provisioning** menu, select **Manage SNMP Passphrases**. Press Enter.

6 In the **Manage SNMP Passphrases** menu, select **Configure SNMPv3 Agent**. Press Enter.

The system prompts for passphrases for the MotoAdmin user account.

7 Enter valid passphrases for the MotoAdmin user account.

The **SNMPv3 Agent Configuration** menu appears.

8 Select the type of user account to configure:

- If you want to modify credentials for an INFORM user account, select **Modify SNMP Inform Configuration**. The system displays the currently active INFORM user account (either MotoInformA or MotoInformB) and indicates that user account's security level.
- If you want to modify credentials for any other user account, select **Modify SNMP User Configuration**. The system displays a list of user accounts currently available for configuration if you are logged on as MotoAdmin, including MotoMaster. The list shows the security levels of the user accounts listed.

9 From the **Select User to Modify** menu, select a user:

If…	Then…
If you select the MotoAdmin user account, which always has a security level of AuthPriv, so only its passphrases can be changed,	change the passphrases. See Configuring the Agent's SNMPv3 Passphrases for PNM Servers or an ATR on page 88.
If you select a user account with a security level of NoAuthNoPriv, which means that no passphrases are configured for that user account,	change the security level. See Configuring the Agent's Security Level for PNM Servers or an ATR on page 88.
If you select a user other than MotoAdmin with a security level of AuthPriv, or you select a user with a security level of AuthNoPriv,	in the **Select Modification** menu, perform the following actions: **a** Change the passphrases. See Configuring the Agent's SNMPv3 Passphrases for PNM Servers or an ATR on page 88. **b** Change the security level. See Configuring the Agent's Security Level for PNM Servers or an ATR on page 88.

10 Enter: `q`. Repeat this step until you exit the configuration utility.

The Common Credentials User Interface closes.

4.9.14.5.1
Configuring the Agent's SNMPv3 Passphrases for PNM Servers or an ATR

Prerequisites: See Configuring the Agent's SNMPv3 Credentials for PNM Servers or ATRs on page 86.

Procedure:

1 From the **Select Modification** menu, select **Update Passphrases**.

The system prompts for the authentication passphrase for the selected user account.

NOTE: For the MotoAdmin user account, the **Select Modification** menu does not appear.

2 In case of AuthPriv or AuthNoPriv, enter the authentication passphrase.

The system prompts for confirmation of the passphrase.

3 Re-enter the authentication passphrase.

If the selected user account has a security level of AuthNoPriv, the passphrases are updated, and the **Select User to Modify** menu returns.
If the selected user account has a security level of AuthPriv, the system prompts for the privacy passphrase for the selected user account.

4 In case of AuthPriv, enter the privacy passphrase.

5 For accounts other than MotoAdmin, enter the MotoAdmin authentication and privacy passphrases

The passphrases are updated, and the **Select User to Modify** menu returns.

4.9.14.5.2
Configuring the Agent's Security Level for PNM Servers or an ATR

Prerequisites: See Configuring the Agent's SNMPv3 Credentials for PNM Servers or ATRs on page 86.

Procedure:

1 From the **Select Modification** menu, select **Update Security Level**.

NOTE: For user accounts with a security level of noAuthNoPriv, the **Select Modification** menu does not appear.

The system displays the name and current security level of the selected user account, along with a list of allowable security levels for that user account.

2 From the list, select the desired security level.

3 If requested, enter the appropriate passphrase.

The security level is updated, and the **Select User to Modify** menu returns.

4.9.14.5.3

Verifying SNMPv3 Configuration Status

Perform this procedure to display configuration status for a PNM server (**not** for an ATR).

Prerequisites: Obtain Active Directory account credentials. For information about setting up Active Directory users so that they can perform specific administration menu procedures, see “Appendix B” in the *Authentication Services Feature Guide* and contact your Active Directory administrator.

Procedure:

1 Log on to the server application:

If…	Then…
If the server application you are logging on to is joined to an Active Directory domain, and a domain controller is available to the server on the network,	log on to the server using your Active Directory account credentials. A command prompt appears, including information on the hostname, domainname, and timezone.
If the server application you are logging on to is not joined to an Active Directory domain, or a domain controller is not available to the server on the network,	use the VMware vSphere Client to access the server and log on with the root account. See “Logging On to the VMware vSphere Client” in the *Virtual Management Server Software User Guide*.

2 At the command prompt, enter: `admin_menu`

3 In the main administration menu, select **OS Administration**. Press ENTER.

4 In the **OS Administration** menu, select **Security Provisioning**. Press ENTER.

5 In the **Security Provisioning** menu, select **Manage SNMP Passphrases**. Press ENTER.

6 In the **Manage SNMP Passphrases** menu, select **Configure SNMPv3 Manager**. Press ENTER.

The system prompts for passphrases for the MotoAdmin user account.

7 Enter valid passphrases for the MotoAdmin user account.

8 In the **SNMPv3 Manager Configuration** menu, select **Display SNMPv3 Configuration Status**.

The system displays a list of devices currently configured, as well as the status of communication between the current device and the remote device.

9 Select **Return to Main Menu**.

The **SNMPv3 Configuration** menu returns.

Postrequisites: If you need to recover passphrases for the MotoAdmin user account for a PNM Server, see Recovering MotoAdmin Passphrases on page 149.

4.9.14.5.4

Verifying SNMPv3 Configuration Status for Sites

Perform this procedure to verify the configuration status for a ZSS server only, and only if Inbound RF Quality Metrics Collection is enabled on your system.

Prerequisites: Obtain Active Directory credentials. For information about setting up Active Directory users so that they can perform specific administration menu procedures, see “Appendix B” in the *Authentication Services Feature Guide* and contact your Active Directory administrator.

Procedure:

1 Log on to the ZSS server application:

If…	Then…
If the server application you are logging on to is joined to an Active Directory domain, and a domain controller is available to the server on the network,	log on to the server using your Active Directory account credentials. A command prompt appears, including information on the hostname, domainname, and timezone.
If the server application you are logging on to is not joined to an Active Directory domain, or a domain controller is not available to the server on the network,	use the VMware vSphere Client to access the server and log on with the root account. See “Logging On to the VMware vSphere Client” in the *Virtual Management Server Software User Guide*.

2 At the command prompt, enter: `admin_menu`

3 In the main administration menu, select **OS Administration**. Press ENTER.

4 In the **OS Administration** menu, select **Security Provisioning**. Press ENTER.

5 In the **Security Provisioning** menu, select **Manage SNMP Passphrases**. Press ENTER.

6 In the **Manage SNMP Passphrases** menu, select **Configure SNMPv3 Managers for Sites**. Press ENTER.

7 At the prompt, enter valid passphrases for the MotoAdmin user account.

8 In the **Configure SNMPv3 Managers for Sites** menu, select **Display SNMPv3 Configuration Status**.

The system displays a list of devices currently configured, as well as the status of communication between the current device and the remote device.

NOTE: The following statuses are possible:

- `OK`: SNMPv3 is correctly configured
- `Misconfigured`: SNMPv3 is misconfigured
- `Unreachable`: No connection to the device

9 To return to the main administration menu, enter: `q`

4.9.14.6 MotoMaster User Account Credentials for the ZSS

You can discover the Zone Statistics Server (ZSS) by using the UNCW Discovery Wizard. See “Performing Device Discovery with the UNCW Discovery Wizard” in the *Unified Network Configurator User Guide*.

To change the MotoMaster user account credentials after discovery, see UNC Configuration for SNMPv3 on page 64.

4.9.15 Configuring InfoVista for SNMPv3

Prerequisites: Ensure that the device is joined to an Active Directory domain and that Active Directory account credentials are obtained.

NOTE: When using Active Directory credentials, ensure that the Active Directory domain is selected in the **Log on to** field. If your Active Directory account fails, enter the credentials for a Windows user account that is maintained locally on this Windows-based device, and ensure that the local hostname is selected in the **Log on to** field.

Procedure:

1 Log on using your Active Directory account that is a member of the group with authority to perform the operations in this procedure.

See the *Authentication Services Feature Guide* and contact your Active Directory administrator.

2 On the desktop, double-click the **IV-Report** icon.

3 In the **Login** window, perform the following actions:

a In the **User name** field, type the appropriate username.

b In the **Password** field, type the appropriate password.

c Leave the **Server IP** field blank.

d Click **OK**.

4 In the **InfoVista IV-Report** window, select the **General** tab.

5 Select and expand the Library for the device for which you want to modify the security configuration.

Step example: Select **Libraries**→**Motorola**→**Motorola Network Router**→**Vistas**→**Motorola Network Router**→**Instances**.

6 Click the device.

7 In the list of parameters, double-click the SNMPv3 parameter that you want to change.

A dialog box appears.

8 In the **Value** field, type the appropriate parameter and click **OK**.

9 Repeat step 7 and step 8 for each parameter that you want to change for a device.

10 Repeat step 5 through step 8 for each device for which you want to change SNMPv3 parameters.

11 From the **File** menu, select **Exit**.

4.9.15.1 InfoVista and SNMPv3

InfoVista is a customizable performance management application that operates on the InfoVista server. InfoVista interfaces with, and gathers data from, multiple network devices supporting Simple Network Management Protocol (SNMP), including master site routers, Ethernet LAN switches, and Cooperative WAN Routing (CWR). This data includes CPU utilization, memory utilization, buffer utilization, port characteristics, and traffic analysis.

InfoVista uses SNMPv3 to gather statistics from routers, Ethernet LAN switches, the GCP 8000 Site Controller, and the Packet Data Gateway (PDG). In particular, InfoVista performs the following tasks:

- Collects Management Information Base (MIB) data at the specified time intervals.
- Reports and graphs MIB data for single or multiple devices, spanning daily, weekly, monthly, and yearly time periods.
- Provides customized reports using pre-configured report templates for network transport devices in your Motorola Solutions radio system.

The InfoVista client application is used to access server software and perform administrative tasks, such as starting and stopping existing reports, adding an instance, or creating a report.

4.9.16 Fault Management Configuration for SNMPv3

In the fault management system, the SDM3000 Builder software is used to set up and configure SDM3000 RTU. The SDM3000 Builder is a software application that facilitates easy planning of the sites and gateways. Using this application, you can build the system level configuration and install it in the SDM3000 RTU.

IMPORTANT:
If SDM3000 RTU IP address is changed, re-apply the MotoMaster setting. See Configuring the Protocols for SDM3000 RTU on page 95.

4.9.16.1 Configuring SDM3000 RTU for SNMPv3

Prerequisites: Install the SDM3000 Builder application.

IMPORTANT: To verify the link between the SDM3000 RTU and the RF site elements, see “Verifying Operability” in the *SDM3000 RTU Owner's Manual*.

Process:

1. Define the settings for SNMP communication. See Defining SNMP Communication Settings for SDM3000 RTU on page 93.
2. Change the SNMPv3 passphrases. See Changing the SNMPv3 Passphrases for SDM3000 RTU on page 94.
3. Configure the SNMPv3 security for Fault Management. See Configuring the Protocols for SDM3000 RTU on page 95.

4.9.16.2 SNMP Communication Settings and SDM3000 RTU

The SDM3000 RTU can communicate using the SNMPv3 protocol.

For secure communication between the SDM3000 RTU the devices in the site and the manager using the SNMPv3, the same user and the same security level are required.

NOTE: The Generic MIB (Management Information Base) feature only supports SNMPv3 between the SDM3000 RTU and a third-party fault manager. However, SNMPv2 is still supported between the SDM3000 RTU and the downstream devices.

For a description of the possible security levels, see SNMPv3 Security Levels on page 26.

Authentication enables verification of the message sender and whether the message has been altered. When privacy is used, the data portion of an SNMP message is encrypted.

The available user accounts are:

MotoAdmin

Administrator level, used for managing other user accounts. Security level of AuthPriv cannot be changed.

MotoInformA or MotoInformB

Used for sending SNMP INFORM messages to the Unified Event Manager (UEM).

NOTE: Generally, only one of these user accounts is active. They coexist only during the system key update, until all elements in the system are synchronized with the same passphrase. Until then, one user uses the old passphrase and the other user uses the new passphrase, in order to allow secure communication with elements in the system that already have the new passphrase, as well as elements that were not updated yet. After system key update, the whole system uses the INFORM user account that was set to be active next.

MotoMaster

Used for communication with the UEM for all SNMP commands, except for INFORM requests.

MotoRTU

Used for communication with devices in the site. Not relevant for SNT.

MotoNFM

Used for connection between the SNT unit and the SDM3000 RTU.

MotoSDM_MIB

Used for secure communication between the SDM3000 RTU and a third-party SNMPv3-capable fault manager, if a license for Generic MIB (Management Information Base) was provided for the SDM. This user is configurable only if the Generic MIB feature was enabled in the **Project Properties** dialog box.

NOTE: The Generic MIB feature is available for the following ASTRO® 25 architectural configurations:

- K core systems
- Express Trunking Standalone Site
- Conventional Only - Standalone RF Site

4.9.16.3 Defining SNMP Communication Settings for SDM3000 RTU

Perform this procedure to define the security level for each user account.

Prerequisites: Install SDM3000 RTU and SDM3000 Builder application.

Procedure:

1 Open the SDM3000 Builder application.

2 Select the desired project.

A list of sites appears in the **Main** pane.

3 In the **Project** pane, click the tree root of the project.

A list of Zones appears in the **Main** pane.

4 In the **Edit Zone** window, select the **SNMP Settings** tab.

5 From the drop-down list, select the desired Authorization/Privacy setting for each user account.

The passphrase for each USM user account is set in a different dialog box. See Changing the SNMPv3 Passphrases for SDM3000 RTU on page 94.

6 To add a manager, click **Add**.

If an illegal name is entered, a cross mark appears. Check the tool tip for details. Additional managers should be added if the domain name of the manager defined in the system is different from the default, or if there is more than one manager defined in the zone. (This configuration is not expected.)

7 To remove an entry from the list, click the entry and select **Remove**.

8 To save the changes, click **OK**.

If security levels set are different for the MotoInform, MotoMaster, and MotoNFM user accounts, a warning appears. To accept, click **OK**. To make changes, **Cancel**.

9 Repeat step 4 through step 8 for each zone.

4.9.16.4

Changing the SNMPv3 Passphrases for SDM3000 RTU

Perform this procedure to change the SNMPv3 passphrases for each USM user account. The SNMPv3 passphrases can be set before starting the installation. When SNMPv1 is used, these settings do not need to be configured.

NOTE:
For each USM user account, an SNMPv3 passphrase is defined to enable secure communication:

- Between the SDM3000 RTU and the devices
- Between the SDM3000 RTU or and the manager synchronized for the specific user account throughout the entire system

For all user accounts with a security level that supports authentication (can also support privacy), these SNMPv3 passphrases should be changed periodically. The time period between passphrase changes is determined by system policy, so contact your system administrator for guidance.

Procedure:

1 In the SDM3000 Builder application, open a project. In the **Project** pane, select a zone.

A list of sites appears in the **Main** pane.

2 In the **Main** pane, select a site.

3 From the **Tools** menu, select **SNMPv3→Passphrases**.

4 In the **SNMPv3 Passphrases** window, select the account you want to change the passphrases for:

- If you want to change passphrases for MotoInformA or MotoinformB, the passphrase should be changed for the user account that will be active next. In the **Select user** drop-down list, select the MotoInform user account that is active next, and proceed with step 5.
- If you want to change other user accounts, proceed with step 5.

5 Enter the current and new passphrases and confirm the passphrases for authentication with or without privacy.

Each passphrase may be between 8 and 64 alphanumeric characters and may include up to 19 additional special characters. The security level cannot be changed in this screen. To change the security level, see Defining SNMP Communication Settings for SDM3000 RTU on page 93.

If an illegal passphrase is entered, a cross mark appears. Check the tool tip for details.

6 Click **OK**.

7 Repeat step 1 through step 6 for each zone.

4.9.16.5 Configuring the Protocols for SDM3000 RTU

Configuration of the SNMPv3 protocol must be performed after installing the SDM3000 Builder project, or during installation. The SDM3000 RTU's IP address is required to configure the SNMPv3 settings. Certain devices in a site have an SNMP version as well. These are set by default to either SNMPv1 or SNMPv3, based on the device type. Some of these defaults may be changed. When only SNMPv1 is used, the SNMPv3 protocol for the SDM3000 RTU does not need to be configured.

NOTE: The Generic MIB (Management Information Base) feature only supports SNMPv3 between the SDM3000 RTU and a third-party fault manager. However, SNMPv1 and SNMPv2 are still supported between the SDM3000 RTU and the downstream devices.

Perform this procedure to configure SNMPv3 security settings (that is, user account passphrases and security levels) for SDM3000 RTU.

Procedure:

1 From the **Tools** menu, select **Operational Settings→SDM3000 RTU**.

The **Select Operation** dialog box appears.

2 Select **SNMPv3 Settings**, and then **Configure**. Click **Next**.

3 **IMPORTANT:**
For maximum security, the initial installation of operational settings (passphrases, keys, and other relevant elements) should be done to the SDM3000 RTU through the Console Port. This ensures that the SDM3000 Builder is communicating with the actual SDM3000 RTU, and not with some other entity impersonating the RTU.

The exception to this rule is when the SDM3000 RTU was previously configured to use Secure or both Clear and Secure Protocols. In that case, SSH encrypts the SNMPv3 credentials and you can use a different port than the console port for installation.

In the **Target Select** dialog box, select the operation that you want to perform:

If…	Then…
If you want to install the settings to the current site,	perform the following actions: **a** Select **Current Site** or **Current SNT**. **b** Click **Next**.
If you want to install the settings to the current site, if the SDM3000 RTU was previously configured to use Secure or both Clear and Secure Protocols, and you do no want to use the console port,	perform the following actions: **a** Select **Current Site** or **Current SNT**. **b** Select **To Network IP Address** and enter the IP address. **c** Click **Next**.
If you want to install the settings to all sites,	perform the following actions: **a** Select **All Sites** or **All SNTs**. **b** Click **Next**.
If you want to install the settings to selected sites,	perform the following actions: **a** Select **Select Sites** or **Select SNTs**. **b** Click **Next**. **c** Select the sites and click **Next**.

4 **NOTE:**
It is not possible to change the passphrases and set security level for the same user account at the same time. Repeat this step as necessary.

Each passphrase can be between 8 and 64 alphanumeric characters, and can include up to 19 additional special characters.

In the **Select SNMPv3 Users** dialog box, select the user account for which you want to modify configuration:

If…	Then…
If you want to change passphrases for the MotoAdmin user account (whose security level cannot be changed because it is always AuthPriv),	perform the following actions: **a** Select **MotoAdmin**, and then **Change Passphrases**. **b** Follow the instructions on the screen, and then enter the required passphrases when prompted.
If you want to change passphrases of any user account except MotoAdmin,	perform the following actions: **a** From the list, select the user account, and click **Change Passphrases**. **b** Follow the instructions on the screen, and then enter the required passphrases when prompted.
If you want to change the security level of any user account except MotoAdmin,	perform the following actions: **a** From the list, select the user account, and click **Set Security Level**. **IMPORTANT:** If SDM3000 RTU IP address is changed, reapply the SNMPv3 MotoMaster setting and select the MotoMaster user. **b** Follow the instructions on the screen, and select the security level when prompted.

The **Summary** dialog box appears.

5 To install the SNMPv3 configuration settings to the SDM3000 RTU, click **Install**.

The first time that the user initiates an installation to a site after launching SDM3000 Builder and opening an existing project or creating a new project, a dialog box appears, requesting a user name and password to connect to the site. This pop-up appears if a password is already entered during this session, but the password is invalid for the current site. If the previously entered password is valid for the current site, no pop-up appears and the installation to the site continues normally. If the SDM3000 RTU's host key is not known to the SDM3000 Builder, a prompt appears to confirm the connection. If the connection is with the RTU (for example, through the Console port or on the site) and you trust the host or if the RTU keys are regenerated, click **OK** to add the RTU to the list of known hosts in the SDM3000 Builder. If the installation is completed successfully, the **Installation Complete** window appears. If the installation is not completed successfully, the **Installation Failed** window appears. Check the Installation log file for details on the failure.

4.9.16.6
Resetting SNMPv3 Configuration for SDM3000 RTU

Prerequisites: Ensure that the SDM3000 RTU is installed.

Procedure:

1 From the **Tools** menu, select **Operational Settings**. Click **SDM3000 RTU**.

2 In the **Select Operation** dialog box, select **SNMPv3 Settings**, and click **Reset**.

3 **IMPORTANT:**
For maximum security, the initial installation of operational settings (passphrases, keys, and so on) should be done to the RTU through the Console Port. This ensures that the SDM3000 Builder is communicating with the actual SDM3000 RTU and not with some other entity impersonating the RTU.

The exception to this rule is when the SDM3000 RTU was previously configured to use Secure or both Clear and Secure Protocols. In that case, SSH encrypts the SNMPv3 credentials and you can use a different port than the console port for installation.

In the **Target Select** dialog box, select the operation that you want to perform.

4 Perform one of the following actions:

If…	Then…
If you want to install the settings to the current site,	perform the following actions: **a** Click **Current Site** or **Current SNT**. **b** Click **Next**. The **Reset SNMPv3** dialog box appears.
If you want to install the settings to the current site, if the SDM3000 RTU was previously configured to use Secure or both Clear and Secure Protocols, and you do no want to use the console port,	perform the following actions: **a** Click **Current Site** or **Current SNT**. **b** Click **To Network IP Address** and enter the IP address. **c** Click **Next**. The **Select SNMPv3 Users** dialog box appears.
If you want to install the settings to all sites,	perform the following actions: **a** Click **All Sites** or **All SNTs**. **b** Click **Next**. The **Reset SNMPv3** dialog box appears.
If you want to install the settings to the selected sites,	perform the following actions: **a** Click **Select Sites** or **Select SNTs**. **b** Click **Next**. **c** In the **Select Sites** dialog box, select the sites and click **Next**. The **Reset SNMPv3** dialog box appears.

5 In the **Reset SNMPv3 Configuration** dialog box, select the operation that you want to perform:

If…	Then…
If you want to change the authentication and/or privacy (encryption) passphrases for the MotoAdmin user account only,	perform the following actions: **a** Click **Override Passphrases of MotoAdmin**. **b** In the appropriate fields, enter the passphrases.

If…	Then…
	c Click **Next**. **NOTE:** If an illegal passphrase is entered, a cross mark appears. Each passphrase must be between 8 and 64 alphanumeric characters in length and include up to 19 additional special characters.
If you want to reset all SNMPv3 settings (including passphrases and USM user account security levels) to the factory defaults,	click **Reset SNMPv3 Settings** and then click **Next**. **NOTE:** If an illegal passphrase is entered, a cross mark appears.

The **Summary** dialog box appears.

6 To install the SNMPv3 configuration settings to the SDM3000 RTU, click **Install**.

The first time that the user initiates an installation to a site after launching SDM3000 Builder and opening an existing project or creating a new project, a dialog box appears, requesting a user name and password to connect to the site. This pop-up appears if a password is already entered during this session, but the password is invalid for the current site. If the previously entered password is valid for the current site, no pop-up appears and the installation to the site continues normally. If the SDM3000 RTU's (SNT) host key is not known to the SDM3000 Builder, a prompt appears to confirm the connection. If the connection is definitely with the RTU or SNT (for example, through the Console port or on the site) and you trust the host or if the RTU/SNT keys are regenerated, click **OK** to add the RTU/SNT to the list of known hosts in the SDM3000 Builder. If the installation is completed successfully, the **Installation Complete** window appears. If the installation is not completed successfully, the **Installation Failed** window appears. Check the Installation log file for details on the failure.

4.9.17

Configuring CSS for SNMPv3

NOTE: CSS recognizes the SNMP version when connecting to the devices.

Prerequisites: Ensure that the latest version of the Configuration/Service Software (CSS) application is installed.

Procedure:

1 Perform one of the following actions:

- If you are trying to connect to the devices using SNMPv3, click **Connect**.
- If you are the MotoCSS user, enter the appropriate credentials and security levels.

2 From the drop-down list, select a security level. For security level description, see SNMPv3 Security Levels on page 26.

4.9.18

Configuring Software Download for SNMPv3

Prerequisites: Install the Software Download Manager (SWDL).

Procedure:

1. **NOTE:** SWDL recognizes SNMP version when connecting to the devices.

   Perform one of the following actions:

   - If you are trying to connect to the devices using SNMPv3, click **Connect**.
   - If you are the MotoSWDL user, enter appropriate credentials and security levels.

   For additional instructions, see the *Software Download Manager Online Help*.
2. From the drop-down list, select a security level. For security level description, see SNMPv3 Security Levels on page 26.

4.9.19

MNR Routers and GGM 8000 Gateways Configuration for SNMPv3

MNR routers (S2500 and S6000) and GGM 8000 gateways are configured for SNMPv3 management through dynamic registration from the configured managers. See SNMPv3 Communication Matrix on page 53. For more information, see the *S6000 and S2500 Routers Feature Guide* and the *GGM 8000 System Gateway Feature Guide*.

IMPORTANT: To configure SNMPv3 USM user accounts on MNR routers and GGM 8000 gateways, use the MNR routers' or GGM 8000 gateways' local console or Secure Shell (SSH) mechanism to access the MNR routers' and GGM 8000 gateways' CLI. For devices with no local console, use SSH.

For important reference information, including how to reset SNMPv3 data for MNR routers and GGM 8000 gateways, see Reference Information for MNR Routers and GGM 8000 Gateways SNMPv3 Configuration on page 110.

4.9.19.1

Accessing the User Manager Menu for MNR Routers and GGM 8000 Gateways with Administrative Privileges

Prerequisites: Set the SNMP control to V3 by entering: `SETDefault -SNMP CONTrol = V3`

Procedure:

1. Log on to the MNR router or GGM 8000 gateway by using the local router console or the Secure Shell (SSH) mechanism.

   For more information on SSH, see the *Securing Protocols with SSH Feature Guide*.

   The command prompt for the MNR router or GGM 8000 gateway appears.
2. At the command prompt, enter: `UserManage`
3. From the menu, select **SNMP V3 User Manager Menu**.
4. **NOTE:** If you attempt to log on as a non-MotoAdmin user or enter the incorrect passphrases, the system returns an error message.

   At the `USM User` prompt, enter: `MotoAdmin`
5. At the prompt, enter the authentication passphrase for the MotoAdmin user account.

6 At the prompt, enter the encryption passphrase for the MotoAdmin user account.

The User Manager menu appears.

NOTE: When you log on as the MotoAdmin user, the MNR routers and GGM 8000 gateways generate an audlCfgChg trap similar to the following: `EOS USM user MotoAdmin with engineID 800000a1010a01fd36 Authentication passphrase changed`. This trap is generated because the router and gateway software sends an `snmpChangeAuthPassphrase` command to the Common Agent as part of the passphrase validation process. The trap is expected and does not require any action.

4.9.19.2

Maintenance of Predefined SNMPv3 USM Users on MNR Routers and GGM 8000 Gateways

MNR S2500 and MNR S6000 routers and GGM 8000 gateways support the following pre-defined USM user accounts:

MotoAdmin

Can issue any command from the **SNMPv3 User Manager** menu. The MotoAdmin user account is associated with the **admin_grp** VACM group.

MotoMaster

Can only change its own authentication and encryption passphrases. The MotoMaster user account is associated with one of the following VACM groups:

- **MotoMaster_grp_authpriv**
- **MotoMaster_grp_authnopriv**
- **MotoMaster_grp_noauthnopriv**

By default, the MotoMaster user account is associated with the **MotoMaster_grp_noauthnopriv** VACM group and is not secured through either authentication or encryption.

In addition, MNR routers and GGM 8000 gateways support inform users, which are used solely for the inform traffic supported by the NMA reliable communication feature. Each agent always uses the inform user account (MotoInformA/B) to send SNMPv3 inform events to the manager. An inform user is created automatically in the USM table in clear mode when the Common Agent receives a multiple manager request (MMR) for reliable communication from a permanent manager. Unless they are being used as conventional channel interfaces, MNR routers and GGM 8000 gateways support up to eight permanent managers (and correspondingly eight inform user accounts). MNR S2500 routers or GGM 8000 gateways used as conventional channel interfaces support only up to four permanent managers (and correspondingly four inform user accounts). Inform users are identified by their name (MotoInformA/B) and the engine ID of the manager that sent the MMR. For further details about managing the inform user accounts, see Overview of Maintaining the MotoInform Users for MNR

Routers and GGM 8000 Gateways on page 103. For details about the predefined VACM groups, see VACM Groups Used in MNR Routers and GGM 8000 Gateways SNMPv3 Configuration on page 111.

IMPORTANT:
If you do not know the FQDN or Engine ID value that is currently assigned to the USM user account you are managing, enter **6** from the SNMP V3 User Manager menu to select **List All Accounts** and record the value currently assigned to the user account. You need this value to complete the management procedures. For details about FQDN and Engine ID values, see FQDN and Engine ID Values for MNR Routers and GGM 8000 Gateways on page 112.

If you load a configuration file that changes the system IP address on an MNR router or a GGM 8000 gateway, the SNMPv3 credentials must be re-established with that MNR router and GGM 8000 gateway. Therefore, if SNMPv3 users were configured on the MNR router or GGM 8000 gateway before the system IP address change, you must issue the `ResetV3` command to reset the SNMPv3 data, then re-configure the SNMPv3 users with the appropriate privilege levels.

4.9.19.2.1
Maintaining the MotoAdmin User for MNR Routers and GGM 8000 Gateways

Perform this procedure to change the passphrases for the MotoAdmin user for MNR routers or GGM 8000 gateways.

NOTE: The security level for the MotoAdmin user account cannot be changed, and the MotoAdmin user account cannot be deleted.

Process:

1. Access the **SNMP V3 User Manager** menu. See Accessing the User Manager Menu for MNR Routers and GGM 8000 Gateways with Administrative Privileges on page 99.
2. Change the authentication passphrase. See Changing the Authentication Passphrase for MNR Routers and GGM 8000 Gateways on page 101.
3. Change the encryption passphrase. See Changing the Encryption Passphrase for MNR Routers and GGM 8000 Gateways on page 102.

4.9.19.2.2
Changing the Authentication Passphrase for MNR Routers and GGM 8000 Gateways

Prerequisites: See Maintaining the MotoAdmin User for MNR Routers and GGM 8000 Gateways on page 101.

Procedure:

1. Select **Change Non-Inform User Authentication PassPhrase**.
2. At the USM User prompt, enter: `MotoAdmin`

   The default engine ID is the local MNR router or GGM 8000 gateway. If this is the engine ID assigned to the MotoAdmin user account, at the Engine ID prompt, press ENTER.
3. At the Engine ID prompt, enter the engine ID number of the SNMP engine assigned to the MotoAdmin user account.
4. At the appropriate prompts, enter the required passphrases.

   The MotoAdmin authentication passphrase is changed, and the **SNMP V3 User Manager** menu returns.

4.9.19.2.3 Changing the Encryption Passphrase for MNR Routers and GGM 8000 Gateways

Prerequisites: See Maintaining the MotoAdmin User for MNR Routers and GGM 8000 Gateways on page 101.

Procedure:

1. Select **Change Non-Inform User Encryption PassPhrase**.
2. At the USM User prompt, enter: `MotoAdmin`
3. At the Engine ID prompt, enter the engine ID number of the SNMP engine assigned to the MotoAdmin user account.

   The default engine ID is the local MNR router or GGM 8000 gateway. If this is the engine ID assigned to the MotoAdmin user account, at the Engine ID prompt, press ENTER.
4. At the Current Authentication PassPhrase prompt, enter the current authentication passphrase for the MotoAdmin user account. This is the new authentication passphrase that you assigned to the MotoAdmin user account in Changing the Authentication Passphrase for MNR Routers and GGM 8000 Gateways on page 101.
5. At the appropriate prompts, enter the required passphrases.

   The MotoAdmin encryption passphrase is changed, and the **SNMP V3 User Manager** menu returns.

4.9.19.2.4 Maintaining the MotoMaster User for MNR Routers and GGM 8000 Gateways

Prerequisites: Ensure that by default the MotoMaster user account is associated with the **MotoMaster_grp_noauthnopriv** VACM group and is not secured through either authentication or encryption (noAuthNoPriv security level).

Procedure:

1. Access the **SNMP V3 User Manager** menu. See Accessing the User Manager Menu for MNR Routers and GGM 8000 Gateways with Administrative Privileges on page 99.
2. Delete the MotoMaster user account:
   a. Select **Delete USM User**.
   b. At the USM User prompt, enter: `MotoMaster`
   c. At the Engine ID prompt, enter the engine ID number of the SNMP engine assigned to the MotoMaster user account.

   The default engine ID is the local MNR router or GGM 8000 gateway. If this is the engine ID assigned to the MotoMaster user account, at the Engine ID prompt, press ENTER.

   The MotoMaster user account is deleted, and the **SNMP V3 User Manager** menu returns.
3. Recreate the MotoMaster user account with the desired privilege level:
   a. Select **Create USM User**.
   b. At the USM User prompt, enter: `MotoMaster`
   c. At the Engine ID prompt, enter the engine ID number of the SNMP engine you want to assign to the MotoMaster user account.

      The default engine ID is the local MNR router or GGM 8000 gateway. To use the default value, at the Engine ID prompt, press ENTER.

- **d** At the Security Level prompt, select **AuthPriv** for authentication and privacy (encryption), or **AuthNoPriv** for authentication but no privacy (encryption).

The MotoMaster user account is created, and the **SNMP V3 User Manager** menu returns.

4 Change the authentication passphrase for the MotoMaster user account:

- **a** Select **Change Non-Inform User Authentication PassPhrase**.
- **b** At the USM User prompt, enter: `MotoMaster`
- **c** At the Engine ID prompt, enter the engine ID number of the SNMP engine assigned to the MotoMaster user account.

  The default engine ID is the local MNR router or GGM 8000 gateway. If this is the engine ID assigned to the MotoMaster user account, at the Engine ID prompt, press ENTER.
- **d** At the Current Authentication PassPhrase prompt, enter the current authentication passphrase for the MotoAdmin user account.

  If you assigned the MotoMaster user account security level 1 (AuthPriv), the Current Encryption Passphrase prompt appears. Enter the current encryption passphrase for the MotoAdmin user account. If you assigned the MotoMaster user account security level 2 (AuthNoPriv), you are not prompted for the current encryption passphrase.
- **e** At the appropriate prompts, enter the required passphrases.

The MotoMaster authentication passphrase is changed, and the **SNMP V3 User Manager** menu returns.

5 **NOTE:** This step is required only if you assigned the MotoMaster a user account security level of AuthPriv.

Change the encryption passphrase for the MotoMaster user account:

- **a** Select **Change Non-Inform User Encryption PassPhrase**.
- **b** At the USM User prompt, enter: `MotoMaster`
- **c** At the Engine ID prompt, enter the engine ID number of the SNMP engine assigned to the MotoMaster user account.

  The default engine ID is the local MNR router or GGM 8000 gateway. If this is the engine ID assigned to the MotoMaster user account, at the Engine ID prompt, press ENTER.
- **d** At the Current Authentication PassPhrase prompt, enter the current authentication passphrase for the MotoMaster user account. This is the New Authentication PassPhrase you entered for the MotoMaster user account in step 4.
- **e** At the appropriate prompts, enter the required passphrases.

The MotoMaster encryption passphrase is changed, and the **SNMP V3 User Manager** menu returns.

4.9.19.2.5
Overview of Maintaining the MotoInform Users for MNR Routers and GGM 8000 Gateways

MNR routers (S2500 and S6000) and GGM 8000 gateways support an inform user account (**MotoInformA or B**) that send trap (INFORM) requests to registered managers in support of reliable communication. Unless they are used as conventional channel interfaces, MNR routers and GGM 8000 gateways support up to eight permanent managers (and, correspondingly, eight inform user accounts).

MNR S2500 routers or GGM 8000 gateways used as conventional channel interfaces support only up to four permanent managers (and correspondingly four inform user accounts).

Inform users are identified by their name (MotoInformA/B) and the engine ID of the manager that sent the MMR.

The **MotoInformA** user account is initially created in one of two ways:

- Manually, by the SNMP V3 User Manager Menu. For details how to manually create the **MotoInformA** user account with NoAuthNoPriv privileges (clear mode), see Creating the Initial MotoInformA (NoAuthNoPriv) User for MNR Routers and GGM 8000 Gateways Manually on page 104.
- Automatically, when there is no MotoInform user account on the MNR router or GGM 8000 gateway, and the MNR router or GGM 8000 gateway needs to send out a trap (due to an existing or manual registration). In this case the **MotoInformA** account is created with NoAuthNoPriv privileges (clear mode). The **MotoInformA** account is also automatically created with NoAuthNoPriv privileges if the **MotoInform** user account is deleted and a trap needs to be sent after the deletion.

Each **MotoInformA** user account has a corresponding **MotoInformB** user account associated with the same engine ID. Only one of these accounts (either **MotoInformA** or **MotoInformB**) is active on the router or a gateway at a time. The active inform user account is referred to as the current/used inform user account. The non-active inform user account is referred to as the target/unused inform user account.

You cannot change the credentials (security level and passphrases) for a current/used inform user account. Instead, activate the target/unused user account and assign the desired privileges and passphrases to that user account by using the **Change Inform User Credentials** option from the **SNMP V3 User Manager** menu. When you complete Changing the Credentials for the MotoInformA/B User for MNR Routers and GGM 8000 Gateways on page 105, the MNR router and GGM 8000 gateway software activates the target/unused user account, which then becomes the current/used user account, and deletes the current/used user account, which then becomes the target/unused user account.

For example, if you need to assign AuthPriv or AuthNoPriv privilege levels to a **MotoInformA** user account that has been automatically created by an MMR for reliable communication, then use the **Change Inform User Credentials** option from the **SNMP V3 User Manager** menu to create and activate the corresponding **MotoInformB** user account and assign it the appropriate security level and passphrases. As a result, the initial **MotoInformA** user account is deleted and the router uses the **MotoInformB** user account. The **MotoInformA** or **MotoInformB** account always belongs to the **notify_grp** VACM group.

To create the **MotoInformA** user account if no inform user account has been previously created on the MNR routers and GGM 8000 gateways, see Creating the Initial MotoInformA (NoAuthNoPriv) User for MNR Routers and GGM 8000 Gateways Manually on page 104. You can use option **6** (**List All Accounts**) from the **SNMP V3 User Manager** menu to check for the existence of an inform user account on the MNR routers and GGM 8000 gateways.

IMPORTANT: If you maintain the **MotoInform** user account for the Unified Event Manager (UEM), enter the **Service Name** from the UEM interface when prompted for the FQDN in Creating the Initial MotoInformA (NoAuthNoPriv) User for MNR Routers and GGM 8000 Gateways Manually on page 104. The **Service Name** is case-sensitive.

4.9.19.2.6 Creating the Initial MotoInformA (NoAuthNoPriv) User for MNR Routers and GGM 8000 Gateways Manually

Perform this procedure to create the **MotoInformA** user account if no inform user account has been previously created on the MNR routers and GGM 8000 gateways. If you need to assign AuthPriv or AuthNoPriv privilege levels to the MotoInform account, then use the **Change Inform User Credentials** option from the **SNMP V3 User Manager** menu to create and activate the MotoInformB user account and assign it the appropriate security level and passphrases. When you have completed this procedure successfully, the initial MotoInformA account is deleted and the MNR router or GGM 8000 gateway uses the MotoInformB account. For details on how to change the security level and passphrases for the MotoInform user account, see Changing the Credentials for the MotoInformA/B User for MNR Routers and GGM 8000 Gateways on page 105.

Procedure:

1. Access the **SNMP V3 User Manager** menu. See Accessing the User Manager Menu for MNR Routers and GGM 8000 Gateways with Administrative Privileges on page 99.
2. From the **SNMP V3 User Manager** menu, select **Create USM User**.
3. At the USM User Name prompt, enter: **MotoInformA**
4. At the FQDN/Engine ID prompt, select **FQDN Format**, and enter the FQDN of the SNMP engine you want to assign to the MotoInformA user account.

   The FQDN (fully qualified domain name) is the complete domain name of the authorized manager involved in the SNMPv3 message exchange. The authorized manager is the manager that registers with the SNMPv3 engine on the MNR routers or GGM 8000 gateways. The FQDN consists of two parts: the hostname and the domain name.

   Step example: To identify host z001uem01 within the domain zone01 as the authorized manager involved in the SNMPv3 message exchange, enter: `Z001uem01.zone 1`
5. At the Security Level prompt, select **NoAuthNoPriv**.

   The **SNMPV3 User Manager** menu returns.

4.9.19.2.7

Changing the Credentials for the MotoInformA/B User for MNR Routers and GGM 8000 Gateways

Perform this procedure to change the security level and passphrases for the MotoInform user account.

Procedure:

1. Access the **SNMP V3 User Manager** menu. See Accessing the User Manager Menu for MNR Routers and GGM 8000 Gateways with Administrative Privileges on page 99.
2. Determine the name (MotoInformA or MotoInformB) of the INFORM user for which you want to change the credentials. From the **SNMP V3 User Manager** menu, select **List All Accounts**.

   Account information appears.
3. If two accounts are listed for the same FQDN (one with Status `Active` and one with Status `Not in Service`), delete the `Not in Service` account. To delete the account, from the **SNMP V3 User Manager** menu, select **2 (Delete USM User)**.
4. From the **SNMP V3 User Manager** menu, select **Change Inform User Credentials**.
5. At the USM User to Activate prompt, enter the name of the target/unused INFORM user account (`MotoInformA` or `MotoInformB`).

   This is the name of the MotoInformA/B user account that is not listed in step 2.

   NOTE: You cannot change the credentials of a current/used INFORM user account. If you enter the name of the current/used INFORM user account, an error message appears.

   Step example: To change the credentials for INFORM user MotoInformA with FQDN z001uem01.zone1, enter: `MotoInformB`

6 At the FQDN/Engine ID prompt, select **FQDN Format**, and enter the FQDN of the INFORM user account you want to activate.

The FQDN is the same for the current/used MotoInformA/B user account and its corresponding target/unused MotoInformA/B user account.

Step example: Enter: `z001uem01.zone1`

7 At the Security Level prompt, enter the number corresponding to the security level that you want to assign to the MotoInformA/B user account.

If you specify security level 1 (AuthPriv) or 2 (AuthNoPriv), the `Current Authentication PassPhrase` prompt appears.
If you specify security level 3 (noAuthnoPriv), you are not prompted for passphrases. Skip to step 13.

8 At the Current Authentication PassPhrase prompt, enter the current authentication passphrase for the MotoAdmin user account.

NOTE: When the target/unused INFORM user account is activated, it is cloned from the MotoAdmin user account. Therefore, the current authentication passphrase is that of the MotoAdmin user account, **not** the current/used INFORM user account.

9 At the Current Encryption PassPhrase prompt, enter the current encryption passphrase for the MotoAdmin user account.

NOTE: When the target/unused INFORM user account is activated, it is cloned from the MotoAdmin user account. Therefore, the current encryption passphrase is that of the MotoAdmin user account **not** the current/ used INFORM user account.

10 At the New Authentication PassPhrase prompt, enter the new authentication passphrase for the MotoInformA/B user account.

11 At the Retype New Authentication PassPhrase prompt, re-enter the new authentication passphrase for verification.

NOTE: If authentication passphrases do not match, an error message appears, a `Not in Service` INFORM user is created, and the target/unused INFORM user is not activated. Delete the `Not in Service` user by selecting **2 (Delete USM User)** from the **SNMP V3 User Manager** menu, and then change the INFORM user credentials. This also applies when you are entering the encryption passphrase for an INFORM user with security level 1 (AuthPriv).

If you assigned the MotoInformA/B user account security level 1 (AuthPriv), the New Encryption PassPhrase prompt appears. Enter the new encryption passphrase for the MotoInformA/B user account and re-type the new encryption passphrase at the prompt for verification.
If you assigned the MotoInformA/B user account security level 2 (AuthNoPriv), you are not prompted for a new encryption passphrase.

The current/used INORM user account is deleted and becomes the target/unused INFORM user account. The target/unused INFORM user account becomes the current/used INFORM user account, and the **SNMP V3 User Manager** menu returns.

12 For the INFORM user for which you changed the credentials, verify that the target/unused INFORM user is now the current/used INFORM user. From the **SNMP V3 User Manager** menu, select **List All Accounts**.

Account information appears. The USM name for the INFORM user corresponding to FQDN z001uem01.zone1 is now `MotoInformB`.

13 If you assigned the MotoInformA/B user account AuthPriv or AuthNoPriv privileges, verify that authorized and encrypted (AuthPriv) or authorized (AuthNoPriv) INFORMs can be received and read by the Unified Event Manager (UEM).

The newly-activated MotoInformA/B account is now used for encrypted and authenticated (AuthPriv) or authenticated (AuthNoPriv) traps.

4.9.19.3
Management of General SNMPv3 USM Users on MNR Routers and GGM 8000 Gateways

When you add a new user account to the USM database, it is cloned from the MotoAdmin user account and assigned to a VACM group based on the security level that you specify (AuthPriv, AuthNoPriv, or NoAuthNoPriv). The new user account also inherits the MotoAdmin user accounts passphrases:

- If you assign the new user account the AuthPriv security level, the user account inherits the MotoAdmin user accounts current authentication and encryption passphrases. Change these passphrases after the user account is created.
- If you assign the new user account the AuthNoPriv security level, the user account inherits the MotoAdmin user accounts current authentication passphrase. Change the authentication passphrase after the user account is created.
- If you assign the new user account the NoAuthNoPriv security level, it does not have passphrases.

IMPORTANT: If you do not know the Engine ID value that is currently assigned to the USM user account you are managing, select **List All Accounts** from the **SNMP V3 User Manager** menu and record the Engine ID value currently assigned to the user account. You need this value to complete the management procedures. For details about FQDN and Engine ID values, see FQDN and Engine ID Values for MNR Routers and GGM 8000 Gateways on page 112.

4.9.19.3.1
Adding an SNMPv3 USM User for MNR Routers and GGM 8000 Gateways

Procedure:

1 Access the **SNMP V3 User Manager** menu. See Accessing the User Manager Menu for MNR Routers and GGM 8000 Gateways with Administrative Privileges on page 99.

2 Create the user account for the user that you want to add:

  a Select **Create USM User**.

  b At the USM User prompt, enter a name of up to 31 characters.

  c At the Engine ID prompt, enter the engine ID number of the SNMP engine you want to assign to the user account.

  The default engine ID is the local MNR router or GGM 8000 gateway. To use the default value, at the Engine ID prompt, press Enter.

  d At the Security Level prompt, select the security level for the new user account.

The user account is created, and the **SNMP V3 User Manager** menu returns.

3 For user accounts with a security level of AuthPriv or AuthNoPriv, change the authentication passphrase. See Changing an SNMPv3 USM User Authentication Passphrase for MNR Routers and GGM 8000 Gateways on page 108.

The authentication passphrase is changed, and the **SNMP V3 User Manager** menu returns.

4. For user accounts with a security level of AuthPriv, change the privacy (encryption) passphrase. See Changing an SNMPv3 USM User Encryption Passphrase for MNR Routers and GGM 8000 Gateways on page 109.

   The encryption passphrase is changed, and the **SNMP V3 User Manager** menu returns.

4.9.19.3.2 Deleting an SNMPv3 USM User for MNR Routers and GGM 8000 Gateways

Procedure:

1. Access the **SNMP V3 User Manager** menu. See Accessing the User Manager Menu for MNR Routers and GGM 8000 Gateways with Administrative Privileges on page 99.
2. Select **Delete USM User**.
3. At the USM User prompt, enter the name of the user account you want to delete.
4. At the Engine ID prompt, enter the engine ID number of the SNMP engine assigned to the user account.

   The default engine ID is the local MNR router or GGM 8000 gateway. If this is the engine ID assigned to the user account, at the Engine ID prompt, press ENTER.

   The user account is deleted, and the **SNMP V3 User Manager** menu returns.

4.9.19.3.3 Changing an SNMPv3 USM User Authentication Passphrase for MNR Routers and GGM 8000 Gateways

NOTE:
This procedure applies only to user accounts assigned security level 1 (AuthPriv) or security level 2 (AuthNoPriv); user accounts assigned security level 3 (NoAuthNoPriv) are not associated with authentication or encryption passphrases.

This procedure applies only to non-INFORM USM user accounts. To change the authentication passphrase for the MotoInformA/B user account, see Changing the Credentials for the MotoInformA/B User for MNR Routers and GGM 8000 Gateways on page 105.

Procedure:

1. Access the **SNMP V3 User Manager** menu. See Accessing the User Manager Menu for MNR Routers and GGM 8000 Gateways with Administrative Privileges on page 99.
2. To change the authentication passphrase, select **Change Non-Inform User Authentication PassPhrase**.

   For passphrase requirements, see SNMPv3 Passphrase Restrictions for MNR Routers and GGM 8000 Gateways on page 111.
3. At the USM User prompt, enter the user account name.

   NOTE: If you enter the user name of a USM user account with security level 3 (NoAuthNoPriv), an error message appears.
4. At the Engine ID prompt, enter the engine ID number of the SNMP engine assigned to the user account.

   The default engine ID is the local MNR router or GGM 8000 gateway. If this is the engine ID assigned to the user account, at the Engine ID prompt, press ENTER.
5. At the Current Authentication PassPhrase prompt, enter the current authentication passphrase for the user account:

- If you just created the user account and have not changed the authentication/encryption passphrase, the current passphrase is the passphrase for the MotoAdmin user account.
- If you assigned the MotoMaster user account security level 1 (AuthPriv), at the `Current Encryption Passphrase` prompt, enter the current encryption passphrase for the user account.
- If you assigned the MotoMaster user account security level 2 (AuthNoPriv), you are not prompted for the current encryption passphrase.

6 Enter and re-enter the new authentication passphrase for the user account.

The user accounts authentication passphrase is changed, and the **SNMP V3 User Manager** menu returns.

4.9.19.3.4

Changing an SNMPv3 USM User Encryption Passphrase for MNR Routers and GGM 8000 Gateways

NOTE:
This procedure applies only to users assigned security level 1 (AuthPriv). Users assigned security level 2 (AuthNoPriv) or security level 3 (NoAuthNoPriv) are not associated with encryption passphrases.

This procedure applies only to non-INFORM USM users. To change the authentication passphrase for the MotoInformA/B user, see Changing the Credentials for the MotoInformA/B User for MNR Routers and GGM 8000 Gateways on page 105.

Procedure:

1 Access the **SNMP V3 User Manager** menu. See Accessing the User Manager Menu for MNR Routers and GGM 8000 Gateways with Administrative Privileges on page 99.

2 To change the encryption passphrase, select **Change Non-Inform User Encryption PassPhrase**.

For passphrase requirements, see SNMPv3 Passphrase Restrictions for MNR Routers and GGM 8000 Gateways on page 111.

3 At the USM User prompt, enter the user name.

If you enter the user name of a USM user with security level 2 (AuthNoPriv) or security level 3 (NoAuthNoPriv), an error message appears.

4 At the Engine ID prompt, enter the engine ID number of the SNMP engine assigned to the user.

The default engine ID is the local MNR router or GGM 8000 gateway. If this is the engine ID assigned to the user, at the Engine ID prompt, press ENTER.

5 At the Current Authentication PassPhrase prompt, enter the current authentication passphrase for the user.

If you only created the user and have not changed the authentication passphrase, the current authentication passphrase is the authentication passphrase for the MotoAdmin user.

6 At the Current Encryption Passphrase prompt, enter the current encryption passphrase for the user.

If you only created the user and have not changed the encryption passphrase, the current authentication passphrase is the authentication passphrase for the MotoAdmin user.

7 At the New Encryption PassPhrase prompt, enter the new encryption passphrase for the user.

8. At the Retype New Encryption PassPhrase prompt, re-enter the new encryption passphrase for verification.

   The users encryption passphrase is changed, and the **SNMP V3 User Manager** menu returns.

4.9.19.3.5 Viewing SNMPv3 USM Users for MNR Routers and GGM 8000 Gateways

Process:

1. Access the **SNMP V3 User Manager** menu. See Accessing the User Manager Menu for MNR Routers and GGM 8000 Gateways with Administrative Privileges on page 99.
2. To display information for the specified USM user, select **List All Accounts**. See SNMPv3 USM Users for MNR Routers and GGM 8000 Gateways List on page 110.

4.9.19.3.6 SNMPv3 USM Users for MNR Routers and GGM 8000 Gateways List

The following accounts provide information for the specified USM user:

USM Name
The user name of the user.

Security Level
The security privilege level for the user, based on the VACM group to which the user is assigned:

- **AuthPriv**: the user is secured with authentication and privacy (encryption)
- **AuthNoPriv**: the user is secured with authentication but not with encryption
- **noAuthNoPriv**: the user is not secured with authentication or encryption (clear SNMPv3)

Engine ID
The SNMP engine ID assigned to the user. If the engine ID was assigned as an FQDN, the FQDN is translated into an engine ID value.

FQDN
(Displayed for MotoInformA/B users only.) The fully-qualified domain name of the SNMP engine assigned to the inform user account.

Status
The status of the USM user:

- `Active`: the user is created and ready to be used
- `Not in service`: operations on the user have been suspended
- `Not Ready`: the user is created but not ready to be used
- `Create and go`: the user is being created and will be active as soon as it is created
- `Create and wait`: the user is being created but is not ready to be used
- `Destroy`: the user is being or should be deleted

4.9.19.4 Reference Information for MNR Routers and GGM 8000 Gateways SNMPv3 Configuration

Additional information about passphrase restrictions, predefined VACM groups, and the FQDN/Engine ID values is used in SNMPv3 configuration procedures for MNR routers (S2500 and S6000) and GGM 8000 gateways.

4.9.19.4.1 Resetting SNMPv3 Data on MNR Routers and GGM 8000 Gateways

You can use the `ResetV3` command to reset the following data:

- SNMPv3 information saved in memory
- SNMPv3 information written to the persistence file
- Information retained by the SNMP Common Agent

⚠ **CAUTION:** Consult a Motorola Solutions field service engineer before using the `ResetV3` command. This command was developed primarily for use in certain controlled situations and is not intended to be performed as a part of normal system operation. Incorrect use of the `ResetV3` command can potentially result in SNMPv3 protocol authentication failure, which causes the device to become unmanageable from the UNC.

Procedure:

From a router console or SSH mechanism, enter: `ResetV3`

Changes take effect after you restart the MNR routers and GGM 8000 gateways.

Postrequisites: Clear the USM cache. See “Accessing and Executing Existing Saved Commands” in the *Unified Network Configurator User Guide*.

4.9.19.4.2 SNMPv3 Passphrase Restrictions for MNR Routers and GGM 8000 Gateways

The SNMPv3 user authentication or encryption passphrase must be 8-64 characters long and may contain uppercase and lowercase alphabetic characters (A-Z) and (a-z), numeric characters (0-9), and any of the allowed special characters (! % & ( ) * + , - . / : ; < = > ?).

4.9.19.4.3 VACM Groups Used in MNR Routers and GGM 8000 Gateways SNMPv3 Configuration

MNR routers and GGM 8000 gateways support the following predefined VACM groups:

MotoMaster_grp_authpriv
For MotoMaster users only; can change its own authentication and encryption passphrases and is allowed access to the entire SNMP-USER-BASED-SM-MIB tree.

MotoMaster_grp_authnopriv
For MotoMaster users only; can change its own authentication and passphrase but not its own encryption passphrase and encryption passphrases and is allowed access to the entire SNMP-USERBASED- SM-MIB tree.

MotoMaster_grp_noauthnopriv
For MotoMaster users only; cannot change its authentication or encryption passphrases and is allowed access to the entire SNMP-USER-BASED-SM-MIB tree.

notify_grp
Cannot change its authentication or encryption passphrases and is allowed only to receive notifications. Users in this group have no read/write access to the SNMP-USER-BASEDSM-MIB tree.

admin_grp
Can change the authentication and encryption passphrases for any USM user and is allowed access to all MIB trees.

4.9.19.4.4 FQDN and Engine ID Values for MNR Routers and GGM 8000 Gateways

An SNMP entity consists of an SNMP engine and one or more associated applications. Applications use the services of the engine for sending and receiving messages, authenticating and encrypting messages, and controlling access to managed objects.

To protect against the message replay, delay and redirection, one of the SNMP engines involved in each communication is designated to be the **authoritative** SNMP engine.

- If an SNMP message contains a payload that **expects** a response, then the **receiver** of such messages is authoritative.
- If an SNMP message contains a payload that **does not expect** a response, then the **sender** of such a message is authoritative.

The FQDN/Engine ID value in MNR router and GGM 8000 gateway SNMPv3 configuration identifies the authoritative SNMP engine. That is, the SNMP engine ID of the authorized manager involved in the SNMPv3 message exchange. The authorized manager is the manager that registers with the SNMPv3 engine on the router or gateway.

IMPORTANT: *Service Name* is the term used in the Unified Event Manager (UEM) interface for FQDN. Service names are case-sensitive, so be careful when entering or referencing service names in UEM.

The authoritative engine may be the destination for a message that expects a response (for example a GET, GETNEXT, GETBULK, SET, or INFORM request). In this case, the remote manager (for example, the UEM) does the registration, and the user specifies a remote engine ID when you create a USM user. You can enter the remote engine ID as either an FQDN or an engine ID (32-byte hexadecimal digit). If you enter the value as an FQDN, MNR router and GGM 8000 gateway software converts the FQDN to an engine ID which is decoded to a prefix plus an FQDN. For example, `800000A1047A30303175656D30312E7A6F6E6531` is decoded to `800000A104(prefix) + z001uem01.zone1`.

The authoritative engine may be the source for a message that does not expect a response (for example a trap, response, or report). In this case, the MNR router and GGM 8000 gateway software does the registration, the engine ID is local, and you are not required to specify it when you create a USM user. Press ENTER in response to either the FQDN or Engine ID prompt to direct the MNR routers or GGM 8000 gateways to use the local engine ID. The router and gateway software decodes the local engine ID to the prefix plus the routers system IP address, for example, `800000A (prefix) + 10.1.253.51`.

When the router or gateway is first booted, the router or gateway system IP address is automatically assigned as the FQDN or Engine ID value for the predefined USM users (MotoAdmin, MotoMaster, and MotoInform). You can change this value if you delete and recreate the predefined user.

For non-predefined USM users, you assign the FQDN or Engine ID value when you create the user account as described in Adding an SNMPv3 USM User for MNR Routers and GGM 8000 Gateways on page 107.

If you do not know the FQDN/Engine ID value assigned to a USM user, and you need to enter the value in order to modify the user, you can select **List All Accounts** from the **SNMP V3 User Manager** menu to view the currently assigned values for all configured USM users.

4.9.20 Juniper SRX Router Configuration

The Juniper SRX series routers are used in various network locations within the ASTRO® 25 system.

SNMP configuration for Juniper routers is contained in automatically generated `.cfg` configuration file, which is loaded during installation. See section "Configuring Juniper SRX Routers" in the *Juniper SRX Routers and Firewalls Feature Guide*.

For manual configuration of user-requested changes, see Changing SNMPv3 User Security Level on page 113.

4.9.20.1 Changing SNMPv3 User Security Level

Use this procedure to manually configure the password authentication and encryption for each SNMP user.

Procedure:

1. Log on to the Juniper SRX router with Secure Shell (SSH).
2. Verify SNMP configuration by entering: `show snmp v3 users`
3. Launch configuration mode by entering: `configure`
4. Configure authentication settings:
   - For MD5 authentication, enter:
     `set snmp v3 usm local-engine user` ***`<user name>`*** `authentication-md5 authentication-password` ***`<password>`***
   - For SHA authentication, enter:
     `set snmp v3 usm local-engine user` ***`<user name>`*** `authentication-sha authentication-password` ***`<password>`***

   where:

   `<user name>` is the name of the user account you want to configure

   `<password>` is the password of that user account
5. Configure privacy settings:
   - For DES privacy, enter:
     `set snmp v3 usm local-engine user` ***`<user name>`*** `privacy-des privacy-password` ***`<password>`***
   - For 3DES privacy, enter:
     `set snmp v3 usm local-engine user` ***`<user name>`*** `privacy-3des privacy-password` ***`<password>`***
   - For AES128 privacy, enter:
     `set snmp v3 usm local-engine user` ***`<user name>`*** `privacy-aes128 privacy-password` ***`<password>`***

   where:

   `<user name>` is the name of the user account you want to configure

   `<password>` is the password of that user account
6. Set the security level of an access group for a used security-name to privacy by entering:
   `set snmp v3 vacm access group RO default-context-prefix security-model usm security-level privacy read-view FULL-VIEW`
7. Delete the previous security-level which must be set to none by entering:
   `delete snmp v3 vacm access group RO default-context-prefix security-model usm security-level none read-view FULL-VIEW`
8. Change the security level of target parameters to privacy by entering:
   `set snmp v3 target-parameters SNMP_V3_PARM parameters security-level privacy`
9. Verify if authentication has been changed on correct groups by entering: `Show | compare`
10. Commit changes and exit configuration mode by entering: `commit and-quit`

11 Verify if authentication and privacy is enabled by entering: `show snmp v3 users`

4.9.21 Ethernet LAN Switches Configuration for SNMPv3

For guidance about which procedures to use, contact your system administrator.

NOTE: Hewlett-Packard 2600, 3500, 3800, and Aruba 2930F Series Ethernet LAN switches are initially pre-configured with SNMPv3 in the following way:

- User name: MotoMaster
- Authentication: none
- Privacy: none

4.9.21.1 Performing Initial Clear Configuration for Ethernet LAN Switches

Prerequisites: Obtain logon credentials.

Procedure:

1. From the Configuration command prompt, log on to the switch as a manager-level user.

   The `<SYSNAME>#` command prompt for manager-level users appears, where `<SYSNAME>` is the host name of the switch.

2. From the privilege mode, enter: `configure`

   The configuration command prompt appears.

   NOTE: Run all the configuration commands from the configuration command prompt.

3. Enter: `snmpv3 enable`
4. Enter: `snmpv3 only`
5. Enter: `snmpv3 user "initial"`
6. Enter: `snmpv3 user "MotoMaster"`
7. Enter: `snmpv3 group OperatorNoAuth user "MotoMaster" sec-model ver3`
8. Enter: `snmpv3 notify "notify1" tagvalue "tag1"`
9. Enter:

   ```
   snmpv3 targetaddress "address1" params "param1"
   <IPAddressOfTrapReceiver>filter All taglist "tag1"
   ```

10. Enter:

    ```
    snmpv3 params "param1" user "MotoMaster" sec-model ver3 message-
    processing ver3 noauth
    ```

    The switch is configured.

11. Enter: `logout`

    The command prompt window closes.

4.9.21.2 Changing a Switch from Clear (noAuthNoPriv) to AuthNoPriv Mode

Prerequisites: Obtain logon credentials.

Procedure:

1. From the Configuration command prompt, log on to the switch as a manager-level user.

   The ***<SYSNAME>***`#` command prompt for manager-level users appears, where ***<SYSNAME>*** is the host name of the switch.

2. From the privilege mode, enter: `configure`

   The configuration command prompt appears.

   NOTE: Run all the configuration commands from the configuration command prompt.

3. Enter: `no snmpv3 group operatorNoAuth user "MotoMaster" sec-model ver3`
4. Enter: `snmpv3 group ManagerAuth user "MotoMaster" sec-model ver3`
5. Enter:
   ```
   snmpv3 params "param1" user "MotoMaster" sec-model ver3 message-processing ver3 auth
   ```
6. Enter: `snmpv3 user MotoMaster auth sha <authPassPhrase>`
7. Enter: `wr mem`

   The switch is configured.

8. Enter: `logout`

   The command prompt window closes.

4.9.21.3 Changing a Switch from Clear (noAuthNoPriv) to AuthPriv Mode

Prerequisites: Obtain logon credentials.

Procedure:

1. From the Configuration command prompt, log on to the switch as a manager-level user.

   The ***<SYSNAME>***`#` command prompt for manager-level users appears, where ***<SYSNAME>*** is the host name of the switch.

2. From the privilege mode, enter: `configure`

   The configuration command prompt appears.

   NOTE: Run all the configuration commands from the configuration command prompt.

3. Enter: `no snmpv3 group operatorNoAuth user "MotoMaster" sec-model ver3`
4. Enter: `snmpv3 group ManagerPriv user "MotoMaster" sec-model ver3`
5. Enter:
   ```
   snmpv3 params "param1" user "MotoMaster" sec-model ver3 message-processing ver3 priv
   ```

6. Enter:
   `snmpv3 user MotoMaster auth sha <authPassPhrase>priv aes <privPassPhrase>`
7. Enter: `wr mem`

   The switch is configured.
8. Enter: `logout`

   The command prompt window closes.

4.9.21.4

Changing a Switch from AuthNoPriv to AuthPriv Mode

Prerequisites: Obtain logon credentials.

Procedure:

1. From the Configuration command prompt, log on to the switch as a manager-level user.

   The ***<SYSNAME>***`#` command prompt for manager-level users appears, where ***<SYSNAME>*** is the host name of the switch.
2. From the privilege mode, enter: `configure`

   The configuration command prompt appears.

   NOTE: Run all the configuration commands from the configuration command prompt.
3. Enter: `no snmpv3 group managerauth user "MotoMaster" sec-model ver3`
4. Enter: `snmpv3 group ManagerPriv user "MotoMaster" sec-model ver3`
5. Enter:
   `snmpv3 params "param1" user "MotoMaster" sec-model ver3 message-processing ver3 priv`
6. Enter:
   `snmpv3 user MotoMaster auth sha <authPassPhrase>priv aes <privPassPhrase>`
7. Enter: `wr mem`

   The switch is configured.
8. Enter: `logout`

   The command prompt window closes.

4.9.21.5

Changing a Switch from AuthNoPriv to Clear (noAuthNoPriv) Mode

Prerequisites: Obtain logon credentials.

Procedure:

1. From the Configuration command prompt, log on to the switch as a manager-level user.

   The ***<SYSNAME>***`#` command prompt for manager-level users appears, where ***<SYSNAME>*** is the host name of the switch.

2 From the privilege mode, enter: `configure`

The configuration command prompt appears.

NOTE: Run all the configuration commands from the configuration command prompt.

3 Enter: `no snmpv3 group managerauth user "MotoMaster" sec-model ver3`

4 Enter: `no snmpv3 user MotoMaster`

5 Enter: `no snmpv3 params "param1"`

6 Enter: `snmpv3 user MotoMaster`

7 Enter:
```
snmpv3 params "param1" user "MotoMaster" sec-model ver3 message-processing ver3 noauth
```

8 Enter: `snmpv3 group operatorNoAuth user "MotoMaster" sec-model ver3`

9 Enter: `wr mem`

The switch is configured.

10 Enter: `logout`

The command prompt window closes.

4.9.21.6 Changing a Switch from AuthPriv to AuthNoPriv Mode

Prerequisites: Obtain logon credentials.

Procedure:

1 From the Configuration command prompt, log on to the switch as a manager-level user.

The ***<SYSNAME>***`#` command prompt for manager-level users appears, where ***<SYSNAME>*** is the host name of the switch.

2 From the privilege mode, enter: `configure`

The configuration command prompt appears.

NOTE: Run all the configuration commands from the configuration command prompt.

3 Enter: `no snmpv3 group managerpriv user "MotoMaster" sec-model ver3`

4 Enter: `snmpv3 group ManagerAuth user "MotoMaster" sec-model ver3`

5 Enter:
```
snmpv3 params "param1" user "MotoMaster" sec-model ver3 message-processing ver3 auth
```

6 Enter: `snmpv3 user MotoMaster auth sha <authPassPhrase>`

7 Enter: `wr mem`

The switch is configured.

8 Enter: `logout`

The command prompt window closes.

4.9.21.7

Changing a Switch from AuthPriv to Clear (noAuthNoPriv) Mode

Prerequisites: Obtain logon credentials.

Procedure:

1. From the Configuration command prompt, log on to the switch as a manager-level user.

   The ***<SYSNAME>***`#` command prompt for manager-level users appears, where ***<SYSNAME>*** is the host name of the switch.

2. From the privilege mode, enter: `configure`

   The configuration command prompt appears.

   NOTE: Run all the configuration commands from the configuration command prompt.

3. Enter: `no snmpv3 group managerpriv user "MotoMaster" sec-model ver3`
4. Enter: `no snmpv3 user MotoMaster`
5. Enter: `no snmpv3 params "param1"`
6. Enter: `snmpv3 user MotoMaster`
7. Enter:
   ```
   snmpv3 params "param1" user "MotoMaster" sec-model ver3 message-processing ver3 noauth
   ```
8. Enter: `snmpv3 group operatorNoAuth user "MotoMaster" sec-model ver3`
9. Enter: `wr mem`

   The switch is configured.

10. Enter: `logout`

    The command prompt window closes.

4.9.21.8

Changing the Switch Passphrase for AuthNoPriv

Prerequisites: Obtain logon credentials.

Procedure:

1. From the Configuration command prompt, log on to the switch as a manager-level user.

   The ***<SYSNAME>***`#` command prompt for manager-level users appears, where ***<SYSNAME>*** is the host name of the switch.

2. From the privilege mode, enter: `configure`

   The configuration command prompt appears.

   NOTE: Run all the configuration commands from the configuration command prompt.

3. Enter: `snmpv3 user MotoMaster auth sha <authPassPhrase>`

4 Enter: `wr mem`

The switch is configured.

5 Enter: `logout`

The command prompt window closes.

4.9.21.9 Changing the Switch Passphrase for AuthPriv

Prerequisites: Obtain logon credentials.

Procedure:

1 From the Configuration command prompt, log on to the switch as a manager-level user.

The ***<SYSNAME>***`#` command prompt for manager-level users appears, where ***<SYSNAME>*** is the host name of the switch.

2 From the privilege mode, enter: `configure`

The configuration command prompt appears.

NOTE: Run all the configuration commands from the configuration command prompt.

3 Enter:

```
snmpv3 user MotoMaster auth sha <authPassPhrase>priv aes
<privPassPhrase>
```

4 Enter: `wr mem`

The switch is configured.

5 Enter: `logout`

The command prompt window closes.

4.9.21.10 Defining the Trap Parameters

Perform this procedure to define the following trap parameters:

- SNMP trap receivers
- Authentication Failure trap

Prerequisites: Contact your system administrator for the IP address of the current zone fault management server.

Procedure:

1 To define switch SNMP trap receivers, enter: `snmp-server host` ***<name><IP_address>*** `all`

where:

<name> is the SNMP community name

<IP_address> is the IP address of the current zone fault management server. For example, `snmp-server host D 11.1.111.11 all` defines 11.1.111.11 as the trap-receiver for all traps with a community name of D.

The switch SNMP trap receivers are set. The following prompt appears: `<Hostname_text_string>)#`

2 To define the Authentication Failure trap, enter: `snmp-server enable traps authentication`

The Authentication Failure Trap is defined. The following prompt appears: `<Hostname_text_string>)#`

3 At the switch prompt, enter: `write memory`.

4.9.22 LX Series Terminal Servers Configuration for SNMPv3

If the system uses InReach LX Series terminal server, only models LX-4048, LX-4016, and LX-4008 are supported in the ASTRO® 25 system.

4.9.22.1 Logging On to a LX Series Terminal Server

Prerequisites: Obtain:

- DB-9 Modular adapter
- RJ45 cable
- Ethernet crossover cable

Procedure:

1 Connect the terminal sever to a laptop through serial connection by using the DB-9 Modular adapter and RJ45 cable or telnet to the IP address of the server.

A logon prompt appears.

2 Provide the Ethernet connection by using the Ethernet crossover cable.

3 Assign an IP address to the laptop in the same subnet as terminal server.

4 From the laptop, launch a terminal emulator, such as HyperTerminal or ProComm. Configure the following settings:

- data rate: `9600`
- data bits: `8`
- stop bits: `1`
- flow control: `Xon/Xoff`

The terminal emulator opens.

5 Log on to the terminal server:

a At the logon prompt, type the user name. Press ENTER.

b At the password prompt, type the password. Press ENTER.

6 At the InReach> user prompt, type `enable`. Press ENTER.

7 At the enable password prompt, type the appropriate enable password. Press Enter.

The InReach>> enable prompt appears.

4.9.22.2
Configuring a LX Series Terminal Server for the noAuthNoPriv Mode

Prerequisites: Obtain the IP address information from the system-specific configuration documentation provided by Motorola Solutions:

- `Client 0` ***`<zZZZuem01_IP>`*** is the `10.`***`<ZoneNumber>`***`.233.20`
- `Client 1` ***`<zZZZuem02_dsrIP>`*** is the `10.`***`<ZoneNumber>`***`.237.20`
- `Client 2` ***`<zZZZuem01_IP>`*** is the `10.`***`<Reciprocationg_dsr_zoneNumber>`***`.233.20`
- `Client 3` ***`<zZZZuem02_dsrIP>`*** is the `10.`***`<Reciprocationg_dsr_zoneNumber>`***`.237.20`

Procedure:

1. Log on to the terminal server.

   See Logging On to a LX Series Terminal Server on page 120.
2. At the enable prompt, enter: `Config int 1 address xxx.xxx.xxx.xxx mask xxx.xxx.xxx.xxx`
3. Enter: `config snmp enable`
4. Enter: `config snmp v3 user 0 name <SNMPv3_username>`
5. Enter: `config snmp v3 group 0 user <SNMPv3_username>`
6. Enter: `config snmp v3 group 0 group groupall`
7. Enter: `config snmp v3 access 0 name groupall`
8. Enter: `config snmp v3 access 0 readview viewall`
9. Enter: `config snmp v3 access 0 writeview viewall`
10. Enter: `config snmp v3 view 0 name viewall`
11. Enter: `config snmp v3 view 0 subtree 1.3.6.1`
12. Enter: `config snmp trap client 0 <zZZZuem01_IP>`
13. Enter: `config snmp trap client 0 ver v3`
14. Enter: `config snmp trap client 1 <zZZZuem02_dsrIP>`
15. Enter: `config snmp trap client 1 ver v3`
16. Enter: `config snmp trap client 2 <zZZZuem01_IP>`
17. Enter: `config snmp trap client 2 ver v3`
18. Enter: `config snmp trap client 3 <zZZZuem02_dsrIP>`
19. Enter: `config snmp trap client 3 ver v3`
20. To save the configuration on the terminal server, enter: `save configuration flash`

    The configuration is saved, and the enable prompt returns.

4.9.22.3 Changing a LX Series Terminal Server From noAuthNoPriv Mode to AuthNoPriv Mode

Prerequisites: Obtain the IP address information from the system-specific configuration documentation provided by Motorola Solutions.

Procedure:

1. Log on to the terminal server.

   See Logging On to a LX Series Terminal Server on page 120.
2. At the enable prompt, enter: `config snmp v3 access 0 seclevel AuthNoPriv`
3. Enter: `config snmp v3 user 0 authproto sha`
4. Enter: `config snmp v3 user 0 authpass <Press_enter>`
5. At the password prompt, enter the password.
6. To save the configuration on the terminal server, enter: `save configuration flash`

   The configuration is saved, and the enable prompt returns.

4.9.22.4 Changing a LX Series Terminal Server From noAuthNoPriv Mode to AuthPriv Mode

Prerequisites: Obtain IP address information from the system-specific configuration documentation provided by Motorola Solutions.

Procedure:

1. Log on to the terminal server.

   See Logging On to a LX Series Terminal Server on page 120.
2. At the enable prompt, enter: `config snmp v3 access 0 seclevel authAndPriv`
3. Enter: `config snmp v3 user 0 authproto sha`
4. Enter: `config snmp v3 user 0 authpass`
5. At the password prompt, enter the password.
6. At the enable prompt, enter: `config snmp v3 user 0 privproto aes`
7. Enter: `config snmp v3 user 0 privpass`
8. At the password prompt, enter the password.
9. To save the configuration on the terminal server, enter: `save configuration flash`

   The configuration is saved, and the enable prompt returns.

4.9.22.5 Changing a LX Series Terminal Server From AuthNoPriv Mode to AuthPriv Mode

Prerequisites: Obtain IP address information from the system-specific configuration documentation provided by Motorola Solutions.

Procedure:

1. Log on to the terminal server.

   See Logging On to a LX Series Terminal Server on page 120.
2. At the enable prompt, enter: `config snmp v3 access 0 seclevel authAndPriv`
3. Enter: `config snmp v3 user 0 authproto sha`
4. Enter: `config snmp v3 user 0 authpass`
5. At the password prompt, enter the password.
6. At the enable prompt, enter: `config snmp v3 user 0 privproto aes`
7. Enter: `config snmp v3 user 0 privpass`
8. At the password prompt, enter the password.
9. To save the configuration on the terminal server, enter: `save configuration flash`

   The configuration is saved, and the enable prompt returns.

4.9.22.6 Changing a LX Series Terminal Server From AuthNoPriv Mode to noAuthNoPriv Mode

Prerequisites: Obtain IP address information from the system-specific configuration documentation provided by Motorola Solutions.

Procedure:

1. Log on to the terminal server.

   See Logging On to a LX Series Terminal Server on page 120.
2. At the enable prompt, enter: `config snmp v3 access 0 seclevel noAuthNoPriv`
3. Enter: `config snmp v3 user 0 authproto none`
4. To save the configuration on the terminal server, enter: `save configuration flash`

   The configuration is saved, and the enable prompt returns.

4.9.22.7 Changing a LX Series Terminal Server From AuthPriv Mode to noAuthNoPriv Mode

Prerequisites: Obtain IP address information from the system-specific configuration documentation provided by Motorola Solutions.

Procedure:

1. Log on to the terminal server.

   See Logging On to a LX Series Terminal Server on page 120.
2. At the enable prompt, enter: `config snmp v3 access 0 seclevel noAuthNoPriv`
3. Enter: `config snmp v3 user 0 authproto none`
4. Enter: `config snmp v3 user 0 privproto none`
5. To save the configuration on the terminal server, enter: `save configuration flash`

   The configuration is saved, and the enable prompt returns.

4.9.23 SLC Series Terminal Servers Configuration for SNMPv3

If the system uses Lantronix SLC series terminal server, only model SLC80162201S with one or three FRRJ451601 (16 Device Port RJ45 I/O Module) modules is supported in the ASTRO® 25 system.

4.9.23.1 Configuring the Lantronix Terminal Server for the noAuth/noPriv Mode

Perform this procedure to configure the SLC series Terminal Server for the noAuth/noPriv Mode.

Prerequisites: Ensure that the service laptop and Lantronix SLC8000 device are connected.
Obtain the following:

- IP address and correct credentials to log on to the Lantronix Terminal Server.
- SNMP users and password/passphrases.

Procedure:

1. Log on to the Lantronix Terminal Server.
2. Configure SNMPv3 as NoAuth/NoPriv by entering: `set snmp v3security noauth`
3. Copy configuration to the second bank by entering: `admin config copy current`

4.9.23.2 Configuring the Lantronix Terminal Server for the Auth/noPriv Mode

Perform this procedure to configure the SLC series Terminal Server for the Auth/noPriv mode.

Prerequisites: Ensure that the service laptop and Lantronix SLC8000 device are connected.
Obtain the following:

- IP address and correct credentials to log on to the Lantronix Terminal Server.
- SNMP users and password/passphrases.

Procedure:

1. Log on to the Lantronix Terminal Server.
2. Configure SNMPv3 as Auth/NoPriv by entering: `set snmp v3security auth`
3. Configure the authentication method by entering: `set snmp v3auth sha`

   NOTE: You can choose md5, sha2_224, sha2_256, sha2_384 or sha2_512 as an alternative authentication method.

4. Configure authentication passwords by performing the following actions:
   a. Enter: `set snmp v3password`
   b. Enter SNMPv3 password and re-enter it when prompted.
   c. Enter: `set snmp v3rwpassword`
   d. Enter the password used in step 4b and re-enter it when prompted.
   e. Enter: `set snmp v3trappassword`
   f. Enter the password used in step 4b and re-enter it when prompted.

   NOTE: All three passwords should match.

5. Copy configuration to the second bank by entering: `admin config copy current`

4.9.23.3 Configuring the Lantronix Terminal Server for the Auth/Priv Mode

Perform this procedure to configure the SLC series Terminal Server for the Auth/Priv mode.

Prerequisites: Ensure that the service laptop and Lantronix SLC8000 device are connected. Obtain the following:

- IP address and correct credentials to log on to the Lantronix Terminal Server.
- SNMP users and password/passphrases.

Procedure:

1. Log on to the Lantronix Terminal Server.
2. Configure SNMPv3 as Auth/Priv by entering: `set snmp v3security authencrypt`
3. Configure the authentication method by entering: `set snmp v3auth sha`

   NOTE: You can choose md5, sha2_224, sha2_256, sha2_384 or sha2_512 as an alternative authentication method.
4. Configure the encryption method by entering: `set snmp v3encrypt aes`

   NOTE: You can choose `des` as an alternative encryption method.
5. Configure authentication passwords by performing the following actions:
   - **a** Enter: `set snmp v3password`
   - **b** Enter SNMPv3 password and re-enter it when prompted.
   - **c** Enter: `set snmp v3rwpassword`
   - **d** Enter the password used in step 5b and re-enter it when prompted.
   - **e** Enter: `set snmp v3trappassword`
   - **f** Enter the password used in step 5b and re-enter it when prompted.

   NOTE: All three passwords should match.
6. Configure encryption passphrases by performing the following actions:
   - **a** Enter: `set snmp v3phrase`
   - **b** Enter SNMPv3 password and re-enter it when prompted.
   - **c** Enter: `set snmp v3rwphrase`
   - **d** Enter the password used in step 6b and re-enter it when prompted.
   - **e** Enter: `set snmp v3trapphrase`
   - **f** Enter the password used in step 6b and re-enter it when prompted.

   NOTE: Each passphrase is set by default to be the same as previously typed RO, RW and Trap password, if not specified otherwise.
7. Copy configuration to the second bank by entering: `admin config copy current`

4.9.24 Configuring ISSI.1 Network Gateway for SNMPv3

Perform this procedure to set up the SNMPv3 credentials so that the Site Link Relay Module and ISSI.1 Gateway Module can communicate with UEM.

Prerequisites:
Obtain the Active Directory account credentials. For information about setting up Active Directory users so that they can perform specific administration menu procedures, see “Appendix B” in the *Authentication Services Feature Guide* and contact your Active Directory administrator.

Obtain MotoAdmin passphrases.

Procedure:

1. Log on to the Site Link Relay Module or ISSI.1 Network Gateway by using your Active Directory account credentials. See “Logging On to the ISSI.1 Network Gateway” in the *ISSI.1 Network Gateway Feature Guide*.
2. Enter: `admin_menu`
3. From the server application main menu, select **OS Administration**. Press ENTER.
4. From the **OS Administration** menu, select **Security Provisioning**. Press ENTER.
5. From the **Security Provisioning** menu, select **Manage SNMP Passphrases**. Press ENTER.
6. From the **Manage SNMP Passphrases** menu, select **SNMPv3 USM Administration**. Press ENTER.
7. At the prompt, enter the MotoAdmin Authentication Passphrase. Press ENTER.
8. At the prompt, enter the MotoAdmin Encryption Passphrase. Press ENTER.
9. From the **SNMP Administration** menu, select **Modify SNMP User Configuration**. Press ENTER.
10. From the **Select User to Modify** menu, select the user you want to change. Press ENTER.
11. **NOTE:** You cannot change the security level for the MotoAdmin user. You can only change the passphrase.

    From the **Enter New Security Level** menu, select the security level you want for the user. Press ENTER.
12. At the Enter MotoMaster Authentication Passphrase prompt, type a passphrase. Press ENTER.
13. At the Confirm MotoMaster Authentication Passphrase prompt, retype the passphrase. Press ENTER.
14. **NOTE:** This step applies only if AuthPriv is chosen as the security level. The AuthNoPriv setting does not require a privacy password.

    At the Enter MotoMaster Privacy Passphrase prompt, type a passphrase. Press ENTER.
15. **NOTE:** This step applies only if AuthPriv is chosen as the security level. The AuthNoPriv setting does not require a privacy password.

    At the Confirm MotoMaster Privacy Passphrase prompt, retype the passphrase. Press ENTER.
16. At the Enter MotoAdmin Authentication Passphrase prompt, type a passphrase. Press ENTER.
17. At the Enter MotoAdmin Privacy Passphrase prompt, type a passphrase. Press ENTER.
18. From the **Select User to the Modify** menu, select MotoAdmin. Press ENTER.
19. From the **Select Modification** menu, select **Update Passphrases**. Press ENTER.
20. At the Enter current MotoAdmin Authentication Passphrase prompt, type a passphrase. Press ENTER.

21 At the Enter current MotoAdmin Privacy Passphrase prompt, type a passphrase. Press ENTER.

22 At the Enter MotoAdmin Authentication Passphrase prompt, type a passphrase. Press ENTER.

23 At the Confirm MotoAdmin Authentication Passphrase prompt, retype the passphrase. Press ENTER.

24 At the Enter MotoAdmin Privacy Passphrase prompt, type a passphrase. Press ENTER.

25 At the Confirm MotoAdmin Privacy Passphrase prompt, retype the passphrase. Press ENTER.

26 In the **Select User to Modify** menu, type **q**. Press ENTER.

27 Perform one of the following actions:

- If you do not need to set the SNMP Inform Configuration, then skip to step 31.
- If you want to set the SNMP Inform Configuration, from the **SNMP Administration** menu, select **Modify SNMP Inform Configuration**. Press ENTER. This setting is optional, based on the desired security level from your security plan.

28 From the **Select Inform User to Modify** menu, select the user you want to modify. Press ENTER.

29 From the **Select Security Level** menu, select the security level you want to set for the selected user. Press ENTER.

30 In the **Select Inform User to Modify** menu, type **q**. Press ENTER.

NOTE: When changing the MotoInform user, it flips between MotoInformA and MotoInformB. You might need to repeat step 27 through step 30 to change the MotoInformA/B user that you want.

31 Log out of the Site Link Relay Module or the ISSI.1 Gateway Module and exit the SSH application:

a In the **SNMP Administration** menu, type `q`. Press ENTER.

b At the command prompt, enter: `exit`

The SSH connection is closed.

Postrequisites: Repeat the procedure for the other ISSI.1 Network Gateway application.

4.9.25 Cisco Console Telephony Media Gateways Configuration for SNMPv3

NEC BX800 and MP118 Console Telephony Media Gateways are initially pre-configured with SNMPv3 with the following settings:

- User name: MotoMaster
- Authentication: none
- Privacy: none

For guidance about which procedures to use, contact your system administrator.

4.9.25.1 Performing Initial Clear Configuration for Cisco Console Telephony Media Gateways

Prerequisites: Obtain logon credentials.

Procedure:

1 From the Configuration command prompt, log on to the Cisco Console Telephony Media Gateway as a manager-level user.

The ***<SYSNAME>***# command prompt for manager-level users appears, where ***<SYSNAME>*** is the host name of the Cisco Console Telephony Media Gateway.

2 From the privilege mode, enter: `configure Terminal`

The configuration command prompt appears.

NOTE: Run all the configuration commands from the configuration command prompt.

3 Enter: `snmp-server community D RO`

4 Enter: `snmp-server community M RW`

5 Enter: `snmp-server location` ***<location of the Console Telephony Media Gateway>***

6 Enter:
`snmp-server contact` ***<contact name of the Console Telephony Media Gateway>***

7 Enter: `snmp-server group OperatorNoAuth v3 noauth`

8 Enter: `snmp-server user MotoMaster OperatorNoAuth v3`

9 Enter: `exit`

10 Enter: `Wr mem`

The Cisco Console Telephony Media Gateway is configured.

11 Enter: `logout`

The command prompt window closes.

4.9.25.2
Changing a Console Telephony Media Gateway from Clear (noAuthNoPriv) to AuthNoPriv Mode

Prerequisites: Obtain logon credentials.

Procedure:

1 From the Configuration command prompt, log on to the Console Telephony Media Gateway as a manager-level user.

The ***<SYSNAME>***# command prompt for manager-level users appears, where ***<SYSNAME>*** is the hostname of the Console Telephony Media Gateway.

2 From the privilege mode, enter: `configure Terminal`

The configuration command prompt appears.

NOTE: Run all the configuration commands from the configuration command prompt.

3 Enter: `no snmp-server user MotoMaster OperatorNoAuth v3`

4 Enter: `no snmp-server group OperatorNoAuth v3 noauth`

5. Enter: `snmp-server group ManagerAuth v3 auth`
6. Enter: `snmp-server user MotoMaster ManagerAuth v3 auth sha` ***<authPassPhrase>***
7. Enter: `exit`
8. Enter: `wr mem`

   The Console Telephony Media Gateway is configured.

9. Enter: `logout`

   The command prompt window closes.

4.9.25.3 Changing a Console Telephony Media Gateway from Clear (noAuthNoPriv) to AuthPriv Mode

Prerequisites: Obtain logon credentials.

Procedure:

1. From the Configuration command prompt, log on to the Console Telephony Media Gateway as a manager-level user.

   The ***<SYSNAME>***# command prompt for manager-level users appears, where ***<SYSNAME>*** is the hostname of the Console Telephony Media Gateway.

2. From the privilege mode, enter: `configure Terminal`

   The configuration command prompt appears.

   NOTE: Run all the configuration commands from the configuration command prompt.

3. Enter: `no snmp-server user MotoMaster OperatorNoAuth v3`
4. Enter: `no snmp-server group OperatorNoAuth v3 noauth`
5. Enter: `snmp-server group ManagerPriv v3 priv`
6. Enter:
   `snmp-server user MotoMaster ManagerPriv v3 auth sha` ***<authPassPhrase>*** `priv aes 128` ***<privPassPhrase>***
7. Enter: `exit`
8. Enter: `wr mem`

   The Console Telephony Media Gateway is configured.

9. Enter: `logout`

   The command prompt window closes.

4.9.25.4 Changing a Console Telephony Media Gateway from AuthNoPriv to AuthPriv Mode

Prerequisites: Obtain logon credentials.

Procedure:

1. From the Configuration command prompt, log on to the Console Telephony Media Gateway as a manager-level user.

   The ***<SYSNAME>***# command prompt for manager-level users appears, where ***<SYSNAME>*** is the hostname of the Console Telephony Media Gateway.

2. From the privilege mode, enter: `configure Terminal`

   The configuration command prompt appears.

   NOTE: Run all the configuration commands from the configuration command prompt.

3. Enter: `no snmp-server user MotoMaster ManagerAuth v3`
4. Enter: `no snmp-server group ManagerAuth v3 auth`
5. Enter: `snmp-server group ManagerPriv v3 priv`
6. Enter:
   `snmp-server user MotoMaster ManagerPriv v3 auth sha` ***<authPassPhrase>*** `priv aes 128` ***<privPassPhrase>***
7. Enter: `exit`
8. Enter: `wr mem`

   The Console Telephony Media Gateway is configured.

9. Enter: `logout`

   The command prompt window closes.

4.9.25.5

Changing a Console Telephony Media Gateway from AuthNoPriv to Clear (noAuthNoPriv) Mode

Prerequisites: Obtain logon credentials.

Procedure:

1. From the Configuration command prompt, log on to the Console Telephony Media Gateway as a manager-level user.

   The ***<SYSNAME>***# command prompt for manager-level users appears, where ***<SYSNAME>*** is the hostname of the Console Telephony Media Gateway.

2. From the privilege mode, enter: `configure Terminal`

   The configuration command prompt appears.

   NOTE: Run all the configuration commands from the configuration command prompt.

3. Enter: `no snmp-server user MotoMaster ManagerAuth v3`
4. Enter: `no snmp-server group ManagerAuth v3 auth`
5. Enter: `snmp-server group OperatorNoAuth v3 noauth`
6. Enter: `snmp-server user MotoMaster OperatorNoAuth v3`
7. Enter: `exit`

8 Enter: `wr mem`

The Console Telephony Media Gateway is configured.

9 Enter: `logout`

The command prompt window closes.

4.9.25.6

Changing a Console Telephony Media Gateway from AuthPriv to AuthNoPriv Mode

Prerequisites: Obtain logon credentials.

Procedure:

1 From the Configuration command prompt, log on to the Console Telephony Media Gateway as a manager-level user.

The ***<SYSNAME>***# command prompt for manager-level users appears, where ***<SYSNAME>*** is the hostname of the Console Telephony Media Gateway.

2 From the privilege mode, enter: `configure Terminal`

The configuration command prompt appears.

NOTE: Run all the configuration commands from the configuration command prompt.

3 Enter: `no snmp-server user MotoMaster ManagerPriv v3`

4 Enter: `no snmp-server group ManagerPriv v3 priv`

5 Enter: `snmp-server group ManagerAuth v3 auth`

6 Enter: `snmp-server user MotoMaster ManagerAuth v3 auth sha` ***<authPassPhrase>***

7 Enter: `exit`

8 Enter: `wr mem`

The Console Telephony Media Gateway is configured.

9 Enter: `logout`

The command prompt window closes.

4.9.25.7

Changing a Console Telephony Media Gateway from AuthPriv to Clear (noAuthNoPriv) Mode

Prerequisites: Obtain logon credentials.

Procedure:

1 From the Configuration command prompt, log on to the Console Telephony Media Gateway as a manager-level user.

The ***<SYSNAME>***# command prompt for manager-level users appears, where ***<SYSNAME>*** is the hostname of the Console Telephony Media Gateway.

2 From the privilege mode, enter: `configure Terminal`

The configuration command prompt appears.

NOTE: Run all the configuration commands from the configuration command prompt.

3 Enter: `no snmp-server user MotoMaster ManagerPriv v3`

4 Enter: `no snmp-server group ManagerPriv v3 priv`

5 Enter: `snmp-server group OperatorNoAuth v3 noauth`

6 Enter: `snmp-server user MotoMaster OperatorNoAuth v3`

7 Enter: `exit`

8 Enter: `wr mem`

The Console Telephony Media Gateway is configured.

9 Enter: `logout`

The command prompt window closes.

4.9.25.8

Changing the Console Telephony Media Gateway Passphrase for AuthNoPriv

Prerequisites: Obtain logon credentials.

Procedure:

1 From the Configuration command prompt, log on to the Console Telephony Media Gateway as a manager-level user.

The ***<SYSNAME>***# command prompt for manager-level users appears, where ***<SYSNAME>*** is the hostname of the Console Telephony Media Gateway.

2 From the privilege mode, enter: `configure Terminal`

The configuration command prompt appears.

NOTE: Run all the configuration commands from the configuration command prompt.

3 Enter: `snmp-server user MotoMaster ManagerAuth v3 auth sha` ***<authPassPhrase>***

4 Enter: `exit`

5 Enter: `wr mem`

The Console Telephony Media Gateway is configured.

6 Enter: `logout`

The command prompt window closes.

4.9.25.9 Changing the Console Telephony Media Gateway Passphrase for AuthPriv

Prerequisites: Obtain logon credentials.

Procedure:

1. From the Configuration command prompt, log on to the Console Telephony Media Gateway as a manager-level user.

   The ***<SYSNAME>***# command prompt for manager-level users appears, where ***<SYSNAME>*** is the hostname of the Console Telephony Media Gateway.

2. From the privilege mode, enter: `configure Terminal`

   The configuration command prompt appears.

   NOTE: Run all the configuration commands from the configuration command prompt.

3. Enter:
   `snmp-server user MotoMaster ManagerPriv v3 auth sha <authPassPhrase> priv aes 128 <privPassPhrase>`

4. Enter: `exit`

5. Enter: `wr mem`

   The Console Telephony Media Gateway is configured.

6. Enter: `logout`

   The command prompt window closes.

4.9.26 BAR Configuration for SNMPv3

You can configure USM user security, modify user passphrases, and set or modify user security levels for a Backup and Restore (BAR) Server.

4.9.26.1 Configuring USM User Security for BAR

Perform this procedure to configure USM user security for the Backup and Restore (BAR) Server.

Prerequisites: Obtain Active Directory account credentials. For information about setting up Active Directory users so that they can perform specific administration menu procedures, see “Appendix B” in the *Authentication Services Feature Guide* and contact your Active Directory administrator.

Procedure:

1. Log on to the BAR Server with your Active Directory account credentials.
2. At the user prompt, enter: `admin_menu`
3. In the main BAR administration menu, select **OS Administration**.
4. In the **OS Administration** menu, select **Security Provisioning**.
5. In the **Security Provisioning**, select **Manage SNMP Passphrases**.

6 In the **Manage SNMP Passphrases** menu, select **Configure SNMPv3 Agent**.

The SNMP Configuration Utility appears.

7 At the MotoAdmin Authentication Passphrase prompt, enter the MotoAdmin Authentication Passphrase.

8 At the MotoAdmin Encryption Passphrase prompt, enter the MotoAdmin Encryption Passphrase.

SNMP Administration options are displayed.

9 Select the type of user account to configure:

If…	Then…
If you want to modify credentials for an INFORM user account,	select **Modify SNMP Inform Configuration**. The system displays the currently active INFORM user account (either MotoInformA or MotoInformB) and indicates that user account's security level.
If you want to modify credentials for any other user account,	select **Modify SNMP User Configuration**. The system displays a list of user accounts currently available for configuration if you are logged on as MotoAdmin, including MotoMaster. The list shows the security levels of the user accounts listed.

10 From the **Select User to Modify** menu, select a user:

If…	Then…
If you select the MotoAdmin user, which always has a security level of AuthPriv, so only its passphrases can be changed,	change the passphrases. See Modifying User Passphrases for BAR on page 134.
If you select a user with a security level of noAuthNoPriv, which means that no passphrases are configured for that user,	set the security level. See Setting User Security Levels for BAR on page 135.
If you select a user other than MotoAdmin with a security level of AuthPriv, or you select a user with a security level of AuthNoPriv,	perform one of the following actions: • For user passphrases, at the **Select Modification** menu, change the passphrases. See Modifying User Passphrases for BAR on page 134. • For user security levels, change the security level. See Modifying User Security Levels for BAR on page 135.

11 Enter: `q`

Repeat the sequence until the **Common Credentials User Interface** closes.

4.9.26.2 Modifying User Passphrases for BAR

Prerequisites: See Configuring USM User Security for BAR on page 133.

Procedure:

1. From the **Select Modification** menu, select **Update Passphrases**.

   For the MotoAdmin user account, the **Select Modification** menu does not appear.

   You are prompted for the authentication passphrase for the selected user account.

2. Enter the current authentication and privacy passphrases for the selected user account.

   You are prompted for the new authentication passphrase for the selected user account.

   NOTE: For the AuthNoPriv security level, you only need to provide current authentication passphrase.

3. Enter and confirm the authentication passphrase.

   - If the selected user account has a security level of AuthNoPriv, the passphrases are updated, and the **Select User to Modify** menu returns. End the procedure.
   - If the selected user account has a security level of AuthPriv, you are prompted for the privacy passphrase for the selected user account.

4. Enter and confirm the privacy passphrase.

   The passphrases are updated, and the **Select User to Modify** menu returns.

4.9.26.3 Setting User Security Levels for BAR

Prerequisites: See Configuring USM User Security for BAR on page 133.

Procedure:

1. From the **Enter New Security Level** menu, select the option for the new security level of the user.

   Prompts for new passphrases appear, followed by prompts for MotoAdmin passphrases.

2. Enter the appropriate passphrases. Press ENTER.

   The security level of the selected user is updated and the **Select User to Modify** menu appears.

4.9.26.4 Modifying User Security Levels for BAR

Prerequisites: See Configuring USM User Security for BAR on page 133.

Procedure:

1. From the **Select Modification** menu, select **Change Security Level**.
2. In the **Enter New Security Level** menu, select the security level.

   Depending on the security level selected, prompts for new passphrases may appear, followed by prompts for MotoAdmin passphrases.

3. Enter the appropriate passphrases.

   The security level of the selected user is updated and the **Select User to Modify** menu appears.

Postrequisites: To recover passphrases for the MotoAdmin user account for BAR, see Recovering MotoAdmin Passphrases on page 149.

4.9.27 Fortinet Firewall Configuration for SNMPv3

All Fortinet firewalls in the ASTRO® 25 system are initially pre-configured for SNMPv3 with one of the following settings:

- noauth/nopriv:
  - User name: MotoMaster
  - Authentication: none
  - Privacy: none
- auth/priv:
  - User name: MotoMaster
  - Authentication: true
  - Privacy: true

For guidance, contact your system administrator.

4.9.27.1 Configuring Fortinet Firewall SNMPv3 Security Level and Passphrase for Authentication and Private Algorithm

Procedure:

1. Open a WebUI connection and log on to the Fortinet firewall:
   - **a** Log on to the Network Management (NM) client using the Windows administrator account.
   - **b** From the NM client, launch a web browser.
   - **c** In the web browser URL field, enter: `https://`***`<IP address of the firewall>`***
   - **d** In the **Login Disclaimer** window, click **Accept**.
   - **e** Enter the user name and password for the firewall's administrator account, and click **Login**.
2. In the left pane of the firewall WebUI home page, select **Config→SNMP**.
3. In the middle pane of the WebUI under SNMPv3, click **MotoMaster**, and then click **Edit**.
4. In the **Edit SNMPv3 User** window, select the security level.
5. Perform one of the following actions:

If…	Then…
If you selected No Authentication, No Private,	Finish the configuration for NoAuthNoPriv security level by clicking **OK**.
If you selected Authentication, No Private,	perform the following actions: **a** In the **Authentication Algorithm** field, select **SHA1**. **b** In the **Password** field, enter the passphrase for authentication. **c** Click **OK**.

If…	Then…
If you selected Authentication, Private,	perform the following actions: **a** In the **Authentication Algorithm** field, select **SHA1**. **b** In the **Private Algorithm** field, select **AES**. **c** In the **Password** field corresponding to **Authentication Algorithm**, enter the passphrase for authentication. **d** In the **Password** field corresponding to **Private Algorithm**, enter the passphrase for private. **e** Click **OK**.

4.9.28

Configuring the License Manager for SNMPv3

The License Manager reports faults to the Unified Event Manager (UEM), which displays alarms for such events as capacity non-compliance, forced release of a session license, or application failure. Perform this procedure to configure communication between the License Manager and the UEM using Simple Network Management Protocol version 3 (SNMPv3).

Gen10: Configuring the License Manager for SNMPv3

Procedure:

1. Log on to the VMware ESXi Embedded Host Client by performing the following actions:
   - **a** Launch the web browser.
   - **b** In the address bar, enter the IP address of the VMS host.
   - **c** If a certificate warning appears, continue to the page.

     The form of the warning and steps to ignore it depend on the web browser.
   - **d** In the **User name** field, enter: `root`
   - **e** In the **Password** field, enter the password.
   - **f** Click **Log in**.
2. In the **Navigator** pane, click **Virtual Machines**.
3. In the **Virtual Machines** pane, right-click a VM and select **Console→Launch remote console**.
4. Click in the **Console** window and log on to the virtual machine as `root`.
5. At the command prompt, enter: `admin_menu`

   The administrative menu appears. To select a menu item, enter the number corresponding to that menu item, then press ENTER.
6. Select **OS Administration**.
7. Select **Security Provisioning**.
8. Select **Manage SNMP Passphrases**.
9. Select **Configure Agent SNMPv3**.
10. At the prompt, enter the authentication passphrase for the MotoAdmin user account.
11. At the prompt, enter the privilege passphrase for the MotoAdmin user account.
12. Select **Modify SNMP User Configuration**.
13. Select **MotoMaster**.

14 Select the security level for the MotoMaster user account.

- If you select **AuthNoPriv**, perform the following actions at the corresponding prompts:
  1. Enter the authentication passphrase for the MotoMaster user account.
  2. To confirm, re-enter the authentication passphrase.
  3. Enter the authentication passphrase for the MotoAdmin user account.
  4. Enter the privilege passphrase for the MotoAdmin user account.
- If you select **AuthPriv**, perform the following actions at the corresponding prompts:
  1. Enter the authentication passphrase for the new MotoMaster user account.
  2. To confirm, re-enter the authentication passphrase.
  3. Enter the privilege passphrase for the MotoMaster user account.
  4. To confirm, re-enter the privilege passphrase.
  5. Enter the authentication passphrase for the MotoAdmin user account.
  6. Enter the privilege passphrase for the MotoAdmin user account.

A message that the security level has been changed successfully appears. A list of user accounts available for configuration appears.

15 To return to the previous menu, enter: `q`

16 From the administrative menu, select **Modify SNMP Inform Configuration**.

17 For each MotoInform user account to be configured for SNMPv3 communication, select the security level.

- If you select **NoAuthNoPriv**, perform the following actions at the corresponding prompts:
  1. Enter the authentication passphrase for the MotoAdmin user account.
  2. Enter the privilege passphrase for the MotoAdmin user account.
- If you select **AuthNoPriv**, perform the following actions at the corresponding prompts:
  1. Enter the authentication passphrase for the MotoInform user account.
  2. To confirm, re-enter the authentication passphrase for the MotoInform user account.
  3. Enter the authentication passphrase for the MotoAdmin user account.
  4. At the prompt, type the appropriate MotoAdmin privacy passphrase. Press ENTER.
- If you select **AuthPriv**, perform the following actions at the corresponding prompts:
  1. Enter the authentication passphrase for the MotoInform user account.
  2. To confirm, re-enter the authentication passphrase for the MotoInform user account.
  3. Enter the privilege passphrase for the MotoAdmin user account.
  4. To confirm, re-enter the privilege passphrase for the MotoInform user account.
  5. Enter the authentication passphrase for the MotoAdmin user account.
  6. Enter the privilege passphrase for the MotoAdmin user account.

A message indicates that the security level has been changed successfully. A list of user accounts available for configuration appears.

18 To return to the previous menu, enter: `q`

19 To return to the previous menu, enter: `q`

20 To exit the administrative menu, enter: `q`

21 At the command prompt, enter: `exit`

Gen9 and Gen8: Configuring the License Manager for SNMPv3

Procedure:

1 From a Windows-based device, launch the VMware vSphere Client.

2 Log on to the VMS as the root user:

   a In the **IP address / Name** field, enter the IP address of the VMS host.

   b In the **User name** field, enter: `root`

   c In the **Password** field, enter the password for the root user account.

   The **vSphere Client Inventory** window appears.

3 In the left pane of the **vSphere Client Inventory** window, select the License Manager virtual machine.

4 In the right pane, select the **Console** tab.

5 In the License Manager console, click in the right pane and log on to the virtual machine as `root`.

6 At the command prompt, enter: `admin_menu`

   The administrative menu appears. To select a menu item, enter the number corresponding to that menu item, then press ENTER.

7 Select **OS Administration**.

8 Select **Security Provisioning**.

9 Select **Manage SNMP Passphrases**.

10 Select **Configure Agent SNMPv3**.

11 At the prompt, enter the authentication passphrase for the MotoAdmin user account.

12 At the prompt, enter the privilege passphrase for the MotoAdmin user account.

13 Select **Modify SNMP User Configuration**.

14 Select **MotoMaster**.

15 Select the security level for the MotoMaster user account.

- If you select **AuthNoPriv**, perform the following actions at the corresponding prompts:

  1 Enter the authentication passphrase for the MotoMaster user account.

  2 To confirm, re-enter the authentication passphrase.

  3 Enter the authentication passphrase for the MotoAdmin user account.

  4 Enter the privilege passphrase for the MotoAdmin user account.

- If you select **AuthPriv**, perform the following actions at the corresponding prompts:

  1 Enter the authentication passphrase for the new MotoMaster user account.

  2 To confirm, re-enter the authentication passphrase.

  3 Enter the privilege passphrase for the MotoMaster user account.

  4 To confirm, re-enter the privilege passphrase.

  5 Enter the authentication passphrase for the MotoAdmin user account.

6. Enter the privilege passphrase for the MotoAdmin user account.

A message that the security level has been changed successfully appears. A list of user accounts available for configuration appears.

16. To return to the previous menu, enter: `q`
17. From the administrative menu, select **Modify SNMP Inform Configuration**.
18. For each MotoInform user account to be configured for SNMPv3 communication, select the security level.
    - If you select **NoAuthNoPriv**, perform the following actions at the corresponding prompts:
      1. Enter the authentication passphrase for the MotoAdmin user account.
      2. Enter the privilege passphrase for the MotoAdmin user account.
    - If you select **AuthNoPriv**, perform the following actions at the corresponding prompts:
      1. Enter the authentication passphrase for the MotoInform user account.
      2. To confirm, re-enter the authentication passphrase for the MotoInform user account.
      3. Enter the authentication passphrase for the MotoAdmin user account.
      4. At the prompt, type the appropriate MotoAdmin privacy passphrase. Press ENTER.
    - If you select **AuthPriv**, perform the following actions at the corresponding prompts:
      1. Enter the authentication passphrase for the MotoInform user account.
      2. To confirm, re-enter the authentication passphrase for the MotoInform user account.
      3. Enter the privilege passphrase for the MotoAdmin user account.
      4. To confirm, re-enter the privilege passphrase for the MotoInform user account.
      5. Enter the authentication passphrase for the MotoAdmin user account.
      6. Enter the privilege passphrase for the MotoAdmin user account.

    A message indicates that the security level has been changed successfully. A list of user accounts available for configuration appears.
19. To return to the previous menu, enter: `q`
20. To return to the previous menu, enter: `q`
21. To exit the administrative menu, enter: `q`
22. At the command prompt, enter: `exit`

4.9.29
IP Packet Capture Configuration for SNMPv3

IP Packet Capture reports operational states and faults to the Unified Event Manager (UEM). UEM displays alarms and events for IP Packet Capture, such as errors related to packet captures or hypervisor definitions. The SNMPv3 protocol is used for secure communication between IP Packet Capture and UEM.

4.9.29.1
Configuring USM User Security for IP Packet Capture

By using the SNMP Configuration Utility, you can configure the security levels and passphrases for user accounts in the User-based Security Model (USM) for SNMPv3. The USM contains a list of users and their attributes, including SNMPv3 support for authentication with or without encryption. You can access the SNMP Configuration Utility from the main administration menu of the IP Packet Capture virtual machine.

Prerequisites: For L and M core systems, obtain Active Directory account credentials. For information about setting up Active Directory users so that they can perform specific administration menu procedures, see "Appendix B" in the *Authentication Services Feature Guide* and contact your Active Directory administrator.

Procedure:

1. Log on to the IP Packet Capture server:
   - For L and M core systems, log on with your Active Directory account credentials.
   - For K core systems, log on with local administrator root account credentials.
2. At the user prompt, enter: `admin_menu`
3. In the main IP Packet Capture administration menu, select **OS Administration**.
4. In the **OS Administration** menu, select **Security Provisioning**.
5. In the **Security Provisioning** menu, select **Manage SNMP Passphrases**.
6. In the **Manage SNMP Passphrases** menu, select **Configure SNMPv3 Agent**.

   The SNMP Configuration Utility appears.
7. At the MotoAdmin authentication passphrase prompt, enter the MotoAdmin authentication passphrase.
8. At the MotoAdmin Privacy passphrase prompt, enter the MotoAdmin Privacy passphrase.
9. In the **SNMP Administration** menu, select the type of user account to configure:

If…	Then…
If you want to modify credentials for an INFORM user account,	select **Modify SNMP Inform Configuration**. The system displays the currently active INFORM user account (MotoInformA or MotoInformB) and indicates the security level of that user account.
If you want to modify credentials for any other user account,	select **Modify SNMP User Configuration**. The system displays a list of user accounts currently available for configuration if you are logged on as MotoAdmin, including MotoMaster. The list shows the security levels of the user accounts listed.

10. From the **Select User to Modify** menu, select a user:

If…	Then…
If you select the MotoAdmin user, which always has a security level of AuthPriv, so only its passphrases can be changed,	change the passphrases. See Modifying User Passphrases for IP Packet Capture on page 142.
If you select a user with a security level of noAuthNoPriv, which means that no passphrases are configured for that user,	set the security level. See Setting User Security Levels for IP Packet Capture on page 143.
If you select a user other than MotoAdmin with a security level of Auth-	in the **Select Modification** menu, perform one of the following actions:

If…	Then…
Priv, or you select a user with a security level of AuthNoPriv,	• Change the passphrases. See Modifying User Passphrases for IP Packet Capture on page 142. • Change the security level. See Modifying User Security Levels for IP Packet Capture on page 143.

11 Enter: `q`

Repeat the sequence until the **Common Credentials User Interface** closes.

4.9.29.2
Modifying User Passphrases for IP Packet Capture

The SNMP Configuration Utility provides the option to modify the authentication and privacy passphrases for users with the AuthPriv and AuthNoPriv security levels. You can access the SNMP Configuration Utility from the main administration menu of the IP Packet Capture virtual machine.

Prerequisites: Perform Configuring USM User Security for IP Packet Capture on page 140.

Procedure:

1 After selecting a user account from the **Select User to Modify** menu, perform one of the following actions:

If…	Then…
If the selected user account has the AuthPriv security level,	perform the following actions: **a** From the **Select Modification** menu, select **Update Passphrases**. **NOTE:** The change of passphrases is the only modification available for the MotoAdmin user account. For the MotoAdmin user account, the **Select Modification** menu does not appear. **b** Enter the current authentication and privacy passphrases for the selected user account. **c** Enter and confirm the new authentication passphrase. **d** Enter and confirm the new privacy passphrase.
If the selected user account has the AuthNoPriv security level,	perform the following actions: **a** From the **Select Modification** menu, select **Update Passphrases**. **b** Enter the current authentication passphrase for the selected user account. **c** Enter and confirm the new authentication passphrase.

The passphrases are updated and the **Select User to Modify** menu appears.

4.9.29.3
Setting User Security Levels for IP Packet Capture

The SNMP Configuration Utility provides the option to set user security levels for users with the NoAuthNoPriv security level. You can access the SNMP Configuration Utility from the main administration menu of the IP Packet Capture virtual machine.

Prerequisites: Perform Configuring USM User Security for IP Packet Capture on page 140.

Procedure:

1. After selecting a user to modify, from the **Enter New Security Level** menu, select the option for the new security level of the user.
2. At the prompts for the new passphrases, enter the appropriate passphrases.
3. At the prompts for the MotoAdmin passphrases, enter the appropriate passphrases.

   The security level of the selected user is updated and the **Select User to Modify** menu appears.

4.9.29.4
Modifying User Security Levels for IP Packet Capture

The SNMP Configuration Utility provides the option to modify user security levels for users other than MotoAdmin with the AuthPriv security level and users with the AuthNoPriv security level. You can access the SNMP Configuration Utility from the main administration menu of the IP Packet Capture virtual machine.

Prerequisites: Perform Configuring USM User Security for IP Packet Capture on page 140.

Procedure:

1. After selecting a user account to modify, from the **Select Modification** menu, select **Change Security Level**.

   The **Enter New Security Level** menu appears, displaying the name and current security level of the selected user account, and a list of allowed security levels for that user account.

2. From the **Enter New Security Level** menu, select the desired security level.

   Depending on the security level selected, prompts for new passphrases may appear, followed by prompts for MotoAdmin passphrases.

3. At each prompt, enter the appropriate passphrase.

   The security level of the selected user is updated and the **Select User to Modify** menu appears.

4.9.30
Personnel Accountability Server Configuration for SNMPv3

The Personnel Accountability Server can be added to the Unified Event Manager (UEM) for fault management using Device Definition Package (DDP) files created in the Fault Management Toolkit.See "Loading DDPs" in the *Unified Event Manager User Guide*.

4.10
Tsub Configuration for SNMPv3

In the ASTRO® 25 system with the Edge Availability with Wireline Console feature implemented, the Trunking Subsystem (Tsub) prime site is equipped with the following devices that utilize SNMPv3. These devices all reside on the same Gen9/Gen10 Common Server Architecture (Virtual Management Server which is also fault managed through SNMPv3):

- Tsub Zone Controller (Tsub ZC)
- Tsub IP Packet Capture
- Tsub Domain Controller
- Tsub Transcoder (optional)

Tsubs also include existing site devices that are managed through SNMPv3. Regardless of whether these devices are deployed in a Tsub or non-Tsub, they are configured for SNMPv3 using the same procedures. This also applies to the devices deployed on the Tsub prime site server. For example, to configure the Tsub ZC for SNMPv3, perform Zone Controller Configuration for SNMPv3 on page 78.

Chapter 5

SNMPv3 Maintenance

NOTE: If you modify SNMPv3 credentials after the most recent backup to the UNC and UEM, then you must update credentials manually after any restore from backup. Each time you change credentials, perform a backup to UNC and UEM to prevent the need for the manual restores.

5.1

Backup of Credentials for Console Site Devices, AIS, Dynamic Transcoders, and Group Data Gateways

SNMPv3 credentials for the following devices require periodic local backup because these devices are not supported by the Backup and Restore (BAR) service on the Backup and Recovery (BAR) server.

After configuring the SNMPv3 credentials on the following devices, back up the credential file and store it at a secure location.

- MCC 7500 VPM Dispatch Console
- MCC 7500E Dispatch Console
- MCC 7500 Archiving Interface Server (AIS)
- PRX 7000 Console Proxy
- Dynamic Transcoder
- Group Data Gateway (GDG)

This allows the credential configuration to be restored in a system rebuild.

For consoles, the following file location is used:

```
c:\programdata\Motorola\Motorola Common Agent\persist\snmpd.conf
```

NOTE: MKM 7000 Console Alias Manager is supported by the Backup and Restore (BAR) service on the Backup and Recovery (BAR) server and does not require periodic local backup. See “Backing Up MKM 7000 CAM Unit IDs, Aliases, Mappings, and Configuration Data” in the *MKM 7000 Console Alias Manager Online Help*.

Chapter 6

SNMPv3 Troubleshooting

Fault management and troubleshooting information helps you react quickly in case of a failure. Choose the section that applies to your scenario.

6.1 Fault Management Tools for SNMPv3

There are two types of logs:

- Centralized Event Logs
- Local logs

6.1.1 Centralized Event Logs

The subsystem logs any SNMPv3 errors associated with a potential incorrect configuration due to inbound authentication or decryption failure by using a Centralized Event Log. *Inbound* refers to an SNMPv3 message received by an element within the subsystem from any other element.

IMPORTANT: These problems can be due to attempts to hack into the subsystem, and must be treated with greater importance than other problems more likely associated with incorrect configuration.

SNMPv3 devices log any SNMPv3 user account configuration change after the initial user creation is completed. For example, v3 user creation, passphrase change, security level change, or v3 user deletion.

For more information, see the *Centralized Event Logging Feature Guide*.

6.1.2 Local Logs

The subsystem locally logs any SNMPv3 errors associated with a potential SNMPv3 incorrect configuration. This reporting allows administrators to diagnose and troubleshoot SNMPv3 configuration problems. All relevant event specifics are included in the log entry. Administrators can remotely retrieve the log files from the device so that offline processing is possible.

The following SNMPv3 errors can result from incorrect configuration and trigger log event entries:

- Unknown engine ID
- Unsupported security level
- Unknown security name
- Encryption failure
- Authentication failure
- Decryption failure
- Insufficient access privilege

NOTE: The Transport Network router existing local log is for debugging purposes only.

6.2 Troubleshooting Reliable Communication Failure

Prerequisites: Reliable communication between the device and UEM is functioning normally.

Procedure:

1 Make the INFORM user's credential change at the UEM side.

  You need to know the current active INFORM user for reliable communication between this device and UEM, that is, MotoInformA or MotoInformB. Assuming that it is MotoInformA, ensure the credentials for the inactive one (MotoInformB in this case) are set to the desired ones. It is understood that MotoInformA is still active and receiving reliable communication INFORM messages from devices using MotoInformA.

2 Make the same change on the INFORM user's credential at the device side.

  See the procedures for routers (using router UI), RF site elements (using CSS), SDM3000 RTU, ZC, NM servers, ATR, PDG, MCC 7500 VPM Dispatch Console and AIS, MCC 7500E Dispatch Console, Dynamic Transcoder, Group Data Gateway (GDG), PRX 7000 Console Proxy or Conventional Site Controller.

  The Unix configuration utility is used for the ZC, NM servers, ATR, and PDG.

  The Windows configuration utility is used for MCC 7500 VPM Dispatch Console, MCC 7500E Dispatch Console, MCC 7500 AIS, Dynamic Transcoder, PRX 7000 Console Proxy, and GDG; CSS is used for the Conventional Site Controller.

  The goal at the device side is to make MotoInformB with the same credentials as the one set in UEM.

  The device sends a key change event to the UEM indicating the success of the key change at the device side. This event is seen at the UEM side to indicate that the reliable communication session between UEM and this device is using the new credential. All other devices are still using MotoInformA for their reliable communication sessions to the UEM.

  NOTE:
  When you set a new credential for MotoInformB at UEM and the same change is made at the device side for MotoInformB, but credentials mismatch on MotoInformB, the device attempts to send a key change event to the UEM, but the UEM discards it because the credentials are mismatched. You detect this mismatch because UEM does not receive the key change event.

  Instead of making MotoInformB a desired credential in UEM, you can modify the existing active MotoInformA credentials without changing the device side. In this case, UEM discards all reliable communication messages from all devices using MotoInformA, with no indication and no error logged. You would assume that the process is successful because no fault is reported in UEM.

Postrequisites: After any credential change for any INFORM user, verify that reliable communication is restored to normal by monitoring the following state/cause event. The normal sequence of maintaining the INFORM user's credentials must be followed, or inability to report reliable faults throughout a zone will occur.

6.3 Security Level Change Failure and/or Passphrase/Key Change Failure

During the update of a USM passphrase, the update procedure call fails. This may be due to mismatch in the user or passphrase information, or due to reset/reboot of the device which might result in the device getting into an unknown state.

The administrator can retrieve enough information from the system to understand the nature of the failure and initiates recovery. The following options are available:

- The administrator can continue the update.
- Roll back to the default passphrase and then set the appropriate passphrase.
- Delete or recreate the same user with the expected passphrase.

The administrator must know the user ID and passphrases. Typically, administrators keep control of the passphrases and store them in a secure place.

6.4 Fault Display

The handler needs the fault display to be an accurate reflection of the health of the system so that faulty equipment can be quickly recognized.

6.4.1 INFORM User Key Change Notification by Agent

The Agent notifies all registered managers upon successful SNMPv3 key change or security level change.

This provides an automatically initiated mechanism to support verification of communications after a key change or a security level change (that is, a method to verify that a credential change was successful).

The notification is sent as an INFORM message. If an INFORM for this event is not successfully delivered, then the element does not mark itself as being out of sync.

IMPORTANT: If INFORM user credentials do not match between a device and the UEM, then the UEM does not report any state/cause event from that device. To troubleshoot this problem, make sure that the device's active INFORM user (either MotoInformA or MotoInformB) has the same SNMPv3 configuration as the active INFORM user in the UEM.

6.4.2 Communication Loss Event Generation

The Fault Manager generates a communication loss event to modify users upon detecting the loss of communication between the Fault Manager and a particular device.

This is applicable for all managed devices. Users are immediately notified for any device that have lost communication so that the impact can be assessed immediately.

6.5 Comparative Analysis

Ensure that the security labels and passphrases are the same. These are used as SNMPv3 information gathering tools for appropriate systems.

6.5.1 SNMPv3 Test Functionality for Managers

The subsystem allows management operations and maintenance users to trigger sending a SET, GET, or GETBULK (request) to any SNMPv3 agent to verify SNMPv3 communication with the agent. Only a GET request is used (no SET or GETBULK).

This helps to verify if a particular key change has been successfully executed at both ends of a line.

6.6 Credential Override by MotoAdmin Users

To override credentials, use the configuration utility for the operating system used by the device for which credentials require override.

- For Unix (Solaris or Linux) devices, see Configuring USM User Security with the Unix Configuration Utility on page 47.
- For Windows devices, see Configuring USM User Security with the Windows Configuration Utility on page 47.

6.7 Recovering MotoAdmin Passphrases

In some instances, devices may require recovery of passphrases for the MotoAdmin user, which resets the passphrases to system default values.

Use these steps to recover passphrases for the MotoAdmin user account for one of the following devices:

- Zone Controller (ZC)
- Generic Application Server (GAS)
- Private Network Management (PNM) Servers
- Inter-System Gateway (ISGW)
- Air Traffic Router (ATR)
- Packet Data Gateway (PDG)
- Backup and Restore Server (BAR)

Prerequisites:
Obtain Active Directory account credentials. For information about setting up Active Directory users so that they can perform specific administration menu procedures, see the "Embedded Password Management" appendix in the *Authentication Services Feature Guide* and contact your Active Directory administrator.

For information on the root prompt, see the *Unix Supplemental Configuration Setup Guide*.

Procedure:

1. Log on to the Zone Controller, Generic Application Server, PNM Server, ISGW, PDG, BAR, or an ATR by using your Active Directory account that is a member of the user group with privileges to access this device.
2. At the command prompt, enter: `su -`
3. At the root prompt, enter the root password.
4. Perform one of the following actions:
    - On GAS-based platforms, enter: `/opt/MOTcagt/bin/MotoAdminRecover.sh`

- On VMS-based platforms (RHEL devices), enter: `/opt/Motorola/ca/bin/MotoAdminRecover.sh`

For security, characters in all passphrase inputs are replaced by asterisks (*) on the screen.

The recovery script displays a series of prompts on the screen.

5. Enter the authentication passphrase for the MotoAdmin user.
6. Re-enter the authentication passphrase for the MotoAdmin user.
7. Enter the privacy passphrase for the MotoAdmin user.
8. Re-enter the privacy passphrase for the MotoAdmin user.
9. To confirm, enter: `y`

   A series of success messages appears, and the command prompt returns.

6.8

Reset of SNMPv3 User Credentials to Defaults on RF Site and VPM Devices

Reset SNMPv3 user credentials only if the primary admin user credentials are lost or forgotten on devices at a remote site.

- If you are at the site and have direct access to the device, see Resetting SNMPv3 User Credentials to Defaults on Devices at a Remote Site Locally Through CSS on page 151.
- If you are not at the site (remote), and do not have direct access to the device, see Resetting the SNMPv3 User Credentials to Defaults on Devices at a Remote Site Remotely Through Telnet/SSH on page 152.

NOTE: If an upgrade was performed and you cannot log on using default passwords for the upgrade, try using passwords that were previously established.

IMPORTANT: After resetting the SNMPv3 User Credentials to factory defaults, restart the device. Plan for the device to be out of service for the reboot period.

Perform Resetting SNMPv3 User Credentials to Defaults on Devices at a Remote Site Locally Through CSS on page 151 on the following devices:

- **RF site devices:**
  - Conventional Site Controller (CSC)
  - GTR 8000 Base Radio
  - GCM 8000 Comparators
  - GRV 8000 Comparators
  - GPB 8000 Reference Distribution Module (RDM)
  - GCP 8000 Site Controller
  - GPW 8000 Receiver
- **Voice Processor Module (VPM) devices:**
  - Voice Processor Module (VPM)
  - Telephone Media Gateway (TMG)

Resetting the SNMPv3 User Credentials to Defaults on Devices at a Remote Site Remotely Through Telnet/SSH on page 152 requires that you know the FQDN or IP address of the device to connect to the remote site. For more information about using CSS, Telnet, and SSH to configure the RF site devices, see the “SSH Configuration” chapter in the *Securing Protocols with SSH Feature Guide* and the *Configuration/Service Software (CSS) Online Help*.

6.8.1 Resetting SNMPv3 User Credentials to Defaults on Devices at a Remote Site Locally Through CSS

Prerequisites: Ensure the latest version of the CSS application is installed.

Procedure:

1. Launch the CSS application and connect to the device by using a serial connection.
2. In the CSS main window, log on with the local service account username and password.
3. Type the Elevated Privileges password for administrative level access.

   Administrative access is required to perform this procedure. If Central Authentication is enabled on the device, and is required to be used per the security policy rather than using the local service account to log on, you use the defined Central Authentication credentials (username and password).

   The Elevated Password Privileges password is not managed by Central Authentication Services, but locally managed on the device and is required for performing operations requiring administration level access.

   If you fail to elevate privileges, you cannot access or execute the mechanisms utilized to reset the SNMPv3 configuration and credentials.
4. Click **OK**.
5. To confirm, click **OK**.

   The connection protocol status appears in the lower-right corner of the window and indicates that a serial connection is in use with the device.

   IMPORTANT: If you have provided the wrong user credentials, go back to step 2 and try again. Per your organization's security policies, the device may limit the number of logon attempts. If you fail to log on and exceed the maximum number of attempts, you may be locked out of the device for some time. The lockout time duration is defined by your policy (default is 15 minutes).
6. To reset the SNMPv3 user credentials to the factory default, select **Security**, **SNMPv3 Configuration**, and then **Reset SNMPv3 Configuration (Serial)**.
7. In the **Reset SNMPv3 Configuration** dialog box, click **Reset SNMPv3 Configuration**.

   The following message appears: `USM Tables will have default values after box reset!`
8. Select **Exit**.
9. Reboot the device:
   a. In the main CSS window, select **Tools**.
   b. Select **Set IP Address/Box Number**.
   c. In the**Set IP Address/Box Number** dialog box, click **Reset**.
10. In the main CSS window, select **File→Exit**, and click **OK**.

    The CSS application closes.

Postrequisites: Verify that the device reboots.

6.8.2

Resetting the SNMPv3 User Credentials to Defaults on Devices at a Remote Site Remotely Through Telnet/SSH

Prerequisites:
Ensure that the PuTTY Terminal Services are enabled.

Obtain the device’s FQDN or IP address.

Procedure:

1. To connect and log on to the device remotely over the network, use the PuTTY Terminal Services to connect to the device using SSH or Telnet.

   Depending on your system's security policy and site configuration, SSH or Telnet may be enabled or disabled. Try SSH first, as that is the preferred secure remote access service.

   The following G-series RF site devices support secure protocol operation only:

   - **Conventional:** GTR 8000 Base Radio, GPW 8000 Receiver, G-Series Subsite Link Converter (GSLC), GRV 8000 Comparator, GCM 8000 Comparator, and GCP 8000 Site Controller
   - **Trunking:** GTR 8000 Base Radio, GPW 8000 Receiver, GPB 8000 Reference Distribution Module, GCM 8000 Comparator, and GCP 8000 Site Controller
2. Type the local service user logon and password.

   If the username or password prompt appears again, you have entered the wrong credentials and must try again. If Central Authentication is enabled and is required to be used per the security policy rather than using the local service account to log on, use your defined Central Authentication username and password.

   Per your organization's security policies, the device may limit the number of logon attempts. If you fail to log on and exceed the maximum number of attempts, you may be locked out of the device for some time. The lockout time duration is defined by your policy (default is 15 minutes).
3. In the command prompt, enter: `enablepriv —E`
4. In the enablepriv command prompt, type the Elevated Privileges password and press Enter.

   If the username or password prompt appears again, you have entered the wrong credentials and must try again.

   If you fail to elevate privileges, you cannot view, access, or execute the commands utilized to reset the SNMPv3 configuration and credentials.
5. In the CSS or]-O command prompt, reset the SNMPv3 user credentials to factory defaults by entering: `redefault_usm`

   The following message appears: `USM Tables will have default values after box reset!`
6. In the CSS or]-O command prompt reset the device. Enter: `reset`
7. Close the PuTTY connection.

Postrequisites: Verify that the device reboots.

6.8.3 Resetting SNMPv3 Passphrases to Default on DSC 8000

You can use this procedure to reset the SNMPv3 configuration in the Provisioning and Configuration Agent (PCA) if the configured SNMPv3 passphrases are lost.

Prerequisites:
Obtain:

- Service laptop or the Network Management (NM) Client
- IP address or the host name of the DSC 8000. See Logon Information on page 153.
- Credentials for the **Network Security Administrator** account

Install the *MSI CA Certs* package on the service laptop to avoid certificate trust warnings from the web browser.

Procedure:

1. In the address bar of a web browser, enter one of the following:
   - IP address of your DSC 8000
   - Host name of your DSC 8000
2. Log on to the PCA as the **Network Security Administrator**.
3. From the main menu bar, select **Security Settings**.
4. From the **Security Settings** drop-down list, select **SNMP Config**.
5. In the **SNMP Config** view, set the **Erase USM and VACM** flag to active.
6. Click **Submit**.

6.8.3.1 Logon Information

Virtualized Prime Site

The IP address can be obtained from the following IP scheme:

`10.`***`<Zone_no+100>.<Site_no>.<DSC>`*** where ***`<DSC>`*** is one of the following values:

- For the Primary Prime Site with two DSC 8000s:
  DSC 1 = 228, DSC 2 = 229
- For the Geo-redundant Primary Prime Site with two DSC 8000s:
  DSC 1 = 228, DSC 2 = 229
- For the Geo-redundant Secondary Prime Site with two DSC 8000s:
  DSC 1 = 234, DSC 2 = 235
- For the Primary Prime Site with four DSC 8000s:
  DSC 1 = 228, DSC 2 = 229, DSC 3 = 230, DSC 4 = 231
- For the Geo-redundant Primary Prime Site with four DSC 8000s:
  DSC 1 = 228, DSC 2 = 229, DSC 3 = 230, DSC 4 = 231
- For the Geo-redundant Secondary Prime Site with four DSC 8000s:
  DSC 1 = 234, DSC 2 = 235, DSC 3 = 212, DSC 4 = 213

The host name scheme can be obtained from the following host name scheme:

- For the Primary Prime Site and Geo-redundant Primary Prime Site:
  `z`***`<zzz>`***`s`***`<sss>`***`rfe`***`<HH>`***`.site`***`<ss>`***`.zone`***`<z>`***

  where:

<zzz> is the Zone number, 1-7, 3 digit zero padded

<sss> is the RF Site number 1- 150, 3 digit zero padded

<HH> is the instance number used in host names and aliases, 2 digit zero padded

<ss> is the RF Site number 1- 150, 2 digit zero padded

<z> is the Zone number, 1-7

Example: `z001s001rfe01.site01.zone1`

- For the Geo-redundant Secondary Prime Site: z***<zzz>***s***<sss>***rfe***<HH>***b.site***<ss>***.zone***<z>***

  Example: z001s001rfe01b.site01.zone1

ASR Site

The IP address can be obtained from the following IP scheme:

10.***<Zone_no+100>***.***<Site_no>***.***<DSC>***

where:

<Zone_no> = Zone Number

<Site_no> = Site Number

<DSC> = DSC 1 = 228, DSC 2 = 229

The host name scheme can be obtained from the following host name scheme:

z***<zzz>***s***<sss>***rfe***<HH>***.site***<ss>***.zone***<z>***

where:

<zzz> is the Zone number, 1-7, 3 digit zero padded

<sss> is the RF Site number 1- 150, 3 digit zero padded

<HH> is the instance number used in host names and aliases, 2 digit zero padded

<ss> is the RF Site number 1- 150, 2 digit zero padded

<z> is the Zone number, 1-7

Example: `z001s001rfe01.site01.zone1`

Subsite

The IP address can be obtained from the following IP scheme:

`101110ZZ.ZZZZZPPP.PPPSSSSS.SHHHHHHH`

where:

`ZZZZZZZ` = Zone Number

`PPPPPP` = Site Number

`SSSSSS` = Subsite Number

`HHHHHHH` = DSC 1 = 1101000 (104), DSC 2 = 1101001 (105)

The host name can be obtained from the following host name scheme:

`z{ZZ}ips{PP}s{RR}rfe{H}. ipss{subsite}.site{prime}.zone{zone}`

where:

<ZZ> is the Zone number, 1-7, 2 digit zero padded

<PP> is the RF Site number 1-64, 2 digit zero padded

<RR> is the IP Subsite number 1-64, 2 digit zero padded

<H> is the instance number used in host names and aliases, 1 digit zero padded

<subsite> is the IP Subsite number 1- 64, 2 digit zero padded

<prime> is the Prime Site number 1-64, 2 digit zero padded
<zone> is the Zone number, 1-7

Example: `z01ips01s01rfe1.ipss01.site01.zone1`

NM Dispatch Conventional Site

The IP address can be obtained from the following IP scheme:

10.***<Zone_no>***.***<Site_no>***.156

where:

<Zone_no> = Zone Number
<Site_no> = NM Dispatch Conventional Site Number

The host name scheme can be obtained from the following host name scheme:

z***<zzz>***s***<sss>***rfe***<HH>***.nmd***<SS>***zone***<Z>***

where:

<zzz> is the Zone number, 1-7, 3 digit zero padded
<sss> is the NM Dispatch Conventional Site number, 1-191, 227-230, 3 digit zero padded
<HH> is the instance number used in host names and aliases, 2 digit zero padded
<ss> is the NM Dispatch Conventional Site number, 1-191, 227-230
<z> is the Zone number, 1-7

Example: `z001s001rfe01.nmd1.zone1`

AXS Dispatch Site

The IP address can be obtained from the following IP scheme:

10.***<Zone_no>***+150.***<Site_no>***.156

where:

<Zone_no> = Zone Number
<Site_no> = NM Dispatch Conventional Site Number

The host name scheme can be obtained from the following host name scheme:

z***<zzz>***s***<sss>***rfe***<HH>***.csd***<SS>***zone***<Z>***

where:

<zzz> is the Zone number, 1-7, 3 digit zero padded
<sss> is the NM Dispatch Conventional Site number, 1-191, 227-230, 3 digit zero padded
<HH> is the instance number used in host names and aliases, 2 digit zero padded
<ss> is the NM Dispatch Conventional Site number, 1-191, 227-230
<z> is the Zone number, 1-7

Example: `z001s001rfe01.csd1.zone1`

Distributed Conventional Site and K-Core

The IP address can be obtained from the following IP scheme:

10.***<conv_sub>***.***<conv_loc>***.***<DSC>***

where:

<conv_sub> = Conventional Subsystem Number + 200 if ***<conv_sub>*** is 1-47 or Conventional Subsystem Number + 200 if ***<conv_sub>*** is 48-64

<conv_loc> = Conventional Location Number
<DSC> = DSC Number

The host name scheme can be obtained from the following host name scheme:

`cs`***`<yy>`***`l`***`<xxx>`***`rfe`***`<hh>`***`convloc`***`<x>`***`.csub`***`<y>`***`.ucs`

where:

<yy> is the Conventional Subsystem number, 1-64, 2 digit zero padded
<xxx> is the Conventional Location number, 1-255, 3 digit zero padded
<hh> is the DSC number, 1-2, in ASTRO K-Core system only 2
<y> is the Conventional Subsystem Number, 1-64
<x> is the Conventional Location number, 1-255

Example: `cs01l001rfe01.convloc1.csub1.ucs`

6.9 Performing an SNMPv3 Connection Verification with CSS

Once the SNMPv3 user credentials have been created, modified, or deleted, perform a sanity check to ensure that the device is properly configured for SNMPv3.

Prerequisites: Ensure that the Configuration/Service Software (CSS) application has been installed.

Procedure:

1. Connect a service laptop or NM client with CSS to the device.
2. Launch the CSS application and connect to the device by using an Ethernet connection.
3. Type the user credentials for a CSS administrator account and click **OK**.

   If the CSS administrator security level requires these credentials, type your authentication password and encryption password.

   A confirmation dialog box appears indicating that CSS has connected with the device.
4. Click **OK**.

   If you fail to connect or log on to the device in SNMPv3 mode, then the device is not properly configured for SNMPv3. If the Ethernet connection to the site is the Site Controller service port, or the GPB 8000 RDM service port, you might need an 802.1x logon account to connect to the SC service port. An 802.1x account is a centrally managed account.

   The connection protocol status appears in the lower-right corner of the window and indicates that an SNMPv3 connection is in use.
5. In the main CSS window, select **File→Exit**, and click **OK**.

   The CSS application closes.