



Radio Authentication

APRIL 2020



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.

© 2020 Motorola Solutions, Inc. All Rights Reserved

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.

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

Disclaimer

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

Trademarks

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

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



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

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

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

Contact Us

The Solutions Support Center (SSC) 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 SSC 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
MN003347A01-A	Original release of the <i>Radio Authentication</i> manual	November 2016
MN003347A01-B	The following sections have been updated: <ul style="list-style-type: none">• Installing the AuC Client on page 48.• Installing the Primary/Backup AuC Server on page 46.	November 2017
MN003347A01-C	The following sections have been updated: <ul style="list-style-type: none">• System-Wide Settings on page 30.• Setting Radio Authentication System-Wide Status in UNC on page 53.	December 2017
MN003347A01-D	Updated section: Radio Authentication in DSR Systems on page 29	April 2020

Contents

Copyrights.....	2
Contact Us.....	3
Document History.....	4
List of Figures.....	11
List of Tables.....	12
List of Processes.....	14
List of Procedures.....	15
About Radio Authentication.....	17
What Is Covered In This Manual?.....	17
Helpful Background Information.....	17
Related Information.....	17
Chapter 1: Radio Authentication Description.....	21
1.1 Radio Authentication Terminology.....	21
1.2 Radio Authentication Security Features.....	22
1.2.1 Encryption Algorithm.....	23
1.2.2 Embedded Passwords.....	23
1.3 Radio Authentication Architecture.....	23
1.3.1 Radio Authentication – ISSI 8000/CSSI 8000.....	24
1.4 Radio Authentication Components.....	24
1.4.1 Authentication Center (AuC) Server.....	25
1.4.2 Authentication Center (AuC) Client.....	25
1.4.3 Configuration Console.....	25
1.4.4 Key Variable Loader (KVL).....	27
1.5 Radio Authentication in DSR Systems.....	29
1.6 Radio Authentication in the System.....	30
1.6.1 Configuration Management.....	30
1.6.1.1 System-Wide Settings.....	30
1.6.1.2 Individual Settings.....	31
1.6.2 Fault Management.....	32
1.6.3 Performance Monitoring.....	32
1.6.4 Fault and Performance Monitoring in the AuC.....	32
1.6.5 IP Services.....	33
1.6.5.1 Backup and Restore (BAR) Services.....	33
1.6.5.2 Active Directory (AD).....	33
1.6.6 Firewall.....	34

Chapter 2: Radio Authentication Theory of Operation.....	35
2.1 Authentication Process.....	35
2.1.1 Device Roles.....	36
2.2 Authentication Keys.....	37
2.2.1 Key Parameters.....	37
2.2.2 Key Provisioning.....	38
2.2.2.1 Authentication Key (K) Provisioning.....	38
2.2.3 Key Distribution.....	39
2.2.3.1 Ki Distribution.....	39
2.2.3.2 KEKm Distribution.....	39
2.2.3.3 SAI Distribution.....	39
2.2.4 Key Storing.....	39
Chapter 3: Radio Authentication Installation.....	40
3.1 Required Software.....	40
3.2 Installing the Radio Authentication Feature.....	40
3.3 Installing the AuC Virtual Machine.....	41
3.3.1 Configuring the vCenter for the Newly Deployed VM.....	43
3.3.2 Configuring Virtual Machine Resources.....	44
3.3.3 Applying OS-Level Identity on the Primary/Backup AuC Server.....	45
3.4 Installing the Primary/Backup AuC Server.....	46
3.5 Installing the AuC Client.....	48
Chapter 4: Radio Authentication Configuration.....	51
4.1 Configuring the Primary AuC Server.....	51
4.2 Configuring the Backup AuC Server.....	52
4.3 Enabling Radio Authentication in the System.....	52
4.3.1 Setting AuC Server as Present in UNC.....	53
4.3.2 Setting Radio Authentication System-Wide Status in UNC.....	53
4.4 Firewall Configuration.....	54
4.5 Zone Controller Configuration.....	54
4.6 Subscriber Unit Configuration.....	54
Chapter 5: Radio Authentication Optimization.....	55
Chapter 6: Radio Authentication Screen Reference.....	56
6.1 Main Window.....	56
6.1.1 Menu Bar.....	56
6.1.1.1 Backup Dialog Box.....	57
6.1.2 Tabs Area.....	57
6.1.3 Work Pane.....	57
6.1.4 Events Pane.....	58
6.1.5 Status Bar.....	58

6.2 Radios Tab.....	59
6.2.1 Radio Station Search Form.....	61
6.3 Devices Tab.....	61
6.4 Schedules Tab.....	63
6.5 KVLs Tab.....	64
6.6 K-SUID Management Tab.....	65
6.6.1 K-SUID Query.....	66
6.7 Synchronization Tab.....	67
6.8 Users Tab.....	68
6.8.1 Add User Dialog Box.....	70
6.9 Audits Tab.....	70
6.9.1 Audit Search and Purge Form.....	71
6.9.2 Audit Trail.....	72
6.10 Restoring Tab.....	72
Chapter 7: Radio Authentication Operation.....	75
7.1 Logging On to the AuC Client.....	75
7.2 Unlocking a User Account.....	76
7.3 Adding an AuC User.....	77
7.4 Changing a User Password.....	77
7.5 AuC Server Status Verification.....	78
7.6 Changing the AuC Server Operating State.....	78
7.7 Viewing the AuC Client Application Version Information.....	79
7.8 Viewing Open-Source Licenses.....	79
7.9 Exiting the AuC Client Application.....	79
7.10 Displaying Zone Status Information.....	79
7.11 AuC Server Settings Configuration.....	80
7.11.1 Enabling Debug Log Storing.....	80
7.11.2 Configuring User Name and Password Settings.....	80
7.11.2.1 User Settings.....	80
7.11.3 Configuring KVL Ports.....	81
7.12 Subscriber Unit Management and Monitoring.....	81
7.12.1 Viewing Subscriber Information Using the Radio Station Search Form.....	81
7.12.2 Exporting Subscriber Units Using the Radio Station Search Form.....	82
7.12.3 Enabling or Disabling Radio Key Updates.....	82
7.13 Event Management.....	83
7.13.1 Viewing Event Details.....	83
7.13.2 Removing Events.....	83
7.14 Audit Management.....	84
7.14.1 Viewing Audits.....	84

7.14.2 Audit Purge and Removal.....	84
7.14.2.1 Purging Audits Data from the AuC Server Database to an Archive File..	84
7.14.2.2 Removing Audits Data from the AuC Server Database.....	85
7.15 KVL Management and Monitoring.....	85
7.15.1 Viewing KVL Status and UKEK Information.....	85
7.15.2 Adding KVLs.....	86
7.15.3 Removing KVLs.....	86
7.15.4 Enabling and Disabling KVLs.....	86
7.16 User Account Management.....	87
7.16.1 Creating a User Account.....	87
7.16.2 Modifying a User Account.....	87
7.16.3 Deleting a User Account.....	88
7.17 Synchronizing the AuC with ADS Manually.....	88
7.18 Key Management.....	88
7.18.1 Setting the Master Key on the Active AuC.....	88
7.18.2 Setting the Master Key on the Standby AuC.....	89
7.18.3 Replacing the Master Key on the Primary AuC Server.....	89
7.18.4 Replacing the Master Key on the Backup AuC Server.....	90
7.18.5 Viewing the Master Key Status.....	91
7.18.5.1 Master Key Statuses.....	91
7.18.6 Viewing KEKm and Ki Status in a Zone.....	92
7.18.7 Entering UKEK into KVL	92
7.18.8 Removing UKEK from KVL.....	92
7.18.9 Distributing Ki.....	93
7.18.10 Distributing KEKm.....	93
7.18.11 Distributing SAI.....	94
7.18.12 K-SUID Management.....	94
7.18.12.1 Performing a Search Using K-SUID Query.....	94
7.18.12.2 Entering Individual K-SUIDs Manually.....	94
7.18.12.3 Deleting K-SUIDs.....	95
7.18.12.4 Sending SUID Clearout.....	95
7.18.12.5 Deleting Unmatched K-SUIDs.....	96
7.19 Dynamic System Resilience (DSR).....	96
7.19.1 Switching Over From the Primary AuC Server to the Backup AuC Server.....	96
7.19.2 Switching Over From the Backup AuC Server to the Primary AuC Server.....	96
7.19.3 Switching Over AuCs.....	98
7.19.4 Changing the Primary AuC Server Role to Standby.....	98
7.19.5 DSR ADS Configuration for AuC.....	98
Chapter 8: Radio Authentication Maintenance.....	99

8.1 AuC Server Backup and Restore.....	99
8.1.1 AuC Server Backup.....	99
8.1.1.1 Backing Up the AuC Server Using the AuC Client Application.....	99
8.1.1.2 Backing Up the AuC Server Using the Configuration Console.....	100
8.1.2 AuC Server Restoration.....	100
8.1.2.1 Restoring the AuC Server Using the Configuration Console.....	101
8.1.2.2 Completing the AuC Server Restoration Using the Configuration Console.....	101
8.1.2.3 Re-sending Keys to ZC.....	103
8.1.2.4 AuC Server Restoration Caveats.....	103
8.2 Updating Keys.....	104
8.2.1 Scheduling Key Updates.....	104
8.2.2 Performing Immediate Key Updates.....	105
8.3 Embedded Passwords.....	105
8.4 Changing the AucUser Service Account Password (Operating System Account).....	106
8.5 Changing the pguser Service Account Password.....	107
8.6 Changing the rdmuser Service Account Password.....	108
Chapter 9: Radio Authentication Troubleshooting.....	110
9.1 AuC Server Does Not Go Operational.....	110
9.2 Logging On to the AuC Client Fails.....	110
9.2.1 Checking the Motorola Authentication Center Service Status.....	110
9.3 Logging On to the AuC Client Application Fails in DSR Systems.....	110
9.4 Starting AuC Client as the Local Windows Administrator.....	111
9.5 UEM Alarms.....	112
9.6 Radio Authentication Failures.....	114
9.6.1 Provisioned Radio Failing Authentication.....	114
9.6.2 Never Provisioned Radio Failing Authentication.....	115
9.7 Unwanted Radio Failing Authentication.....	115
9.8 Stolen Radio Passing Authentication.....	115
9.9 Stolen KVL.....	115
9.10 Authenticated Radio Service.....	116
9.11 AuC Client Cohabited on NM Client.....	116
9.12 Collecting AuC Server and Client Logs.....	116
Chapter 10: Radio Authentication FRU/FRE.....	117
Chapter 11: Radio Authentication Disaster Recovery.....	118
11.1 Recovering the Authentication Center (AuC) Server.....	118
11.2 Recovering the Authentication Center (AuC) Client Cohabited on NM Client.....	119
11.3 Recovering the Standalone Authentication Center (AuC) Client.....	119
Chapter 12: Motorola Redundancy Manager.....	120

12.1 Logging On to the Motorola Redundancy Manager Client.....	120
12.2 Motorola Redundancy Manager Client Screen Reference.....	120
Appendix A: Radio Authentication Logging Messages.....	123

List of Figures

Figure 1: KVL-AuC Connection in L Core and M1/M2 Configurations.....	28
Figure 2: KVL-AuC Connection in M3 Configuration.....	29
Figure 3: Radio Authentication – DSR System.....	30
Figure 4: Radio Authentication Process.....	36
Figure 5: AuC Main Window.....	56
Figure 6: Radios Tab.....	59
Figure 7: Devices Tab.....	62
Figure 8: Schedules Tab.....	63
Figure 9: KVLs Tab.....	65
Figure 10: K-SUID Management Tab.....	66
Figure 11: Synchronization Tab.....	67
Figure 12: Users Tab.....	68
Figure 13: Add User Dialog Box.....	70
Figure 14: Audits Tab.....	71
Figure 15: Restoring Tab.....	73
Figure 16: Redundancy Manager Client Main Window.....	121

List of Tables

Table 1: Radio Authentication Acronyms.....	21
Table 2: Radio Authentication Terms.....	21
Table 3: Configuration Console Commands.....	26
Table 4: System-Wide State Impact on Individual Settings.....	31
Table 5: Device Roles.....	36
Table 6: Authentication Keys Parameters.....	37
Table 7: Fields in the Backup Dialog Box.....	57
Table 8: Buttons in the Backup Dialog Box.....	57
Table 9: Fields in the Events Information Display.....	58
Table 10: Buttons in the Events Information Display.....	58
Table 11: AuC Server States of Operation.....	58
Table 12: AuC Server Connection Status Icons.....	59
Table 13: Fields in the Radio Stations List Display.....	60
Table 14: Buttons in the Radio Stations List Display.....	60
Table 15: Fields in the Radio Station Search Form.....	61
Table 16: Buttons in the Radio Station Search Form.....	61
Table 17: Fields in the Zone Information Display.....	62
Table 18: Buttons in the Zone Information Display.....	63
Table 19: Fields in the Key Schedule Information Display.....	63
Table 20: Fields in the Key Update Currency Area.....	64
Table 21: Buttons in the Key Schedule Information Display.....	64
Table 22: Fields in the KVL Information Display.....	65
Table 23: Key Status Icons (KVLs).....	65
Table 24: Fields in the K-SUID Query.....	66
Table 25: Fields in the Synchronization Tab.....	67
Table 26: Fields in the User Information Display.....	68
Table 27: Access Permissions for AuC Users.....	69
Table 28: Buttons in the User Information Display.....	69
Table 29: Fields in the Add User Dialog Box.....	70
Table 30: Buttons in the Add User Dialog Box.....	70
Table 31: Fields in the Audit Search and Purge Form Display.....	71
Table 32: Buttons in the Audit Search and Purge Form Display.....	71
Table 33: Fields in the Audit Trail Information Display.....	72
Table 34: Restoration Tab Fields.....	73
Table 35: Restoring Tab Buttons.....	74
Table 36: AuC Server States.....	78

Table 37: Operation - AuC Server State Dependencies.....	78
Table 38: User Name and Password Settings.....	80
Table 39: Master Key Statuses.....	91
Table 40: AuC Server Restore Caveats.....	103
Table 41: Recommended Key Update Periods.....	104
Table 42: Groups and Properties for Embedded Password Management.....	105
Table 43: UEM Alarms.....	112
Table 44: UEM Alarms for AuC State Transitions.....	112
Table 45: Zone Controller States.....	113
Table 46: Advanced Distribution Service States.....	113
Table 47: Standby AuC States.....	113
Table 48: Common Link States.....	114
Table 49: Common License States.....	114
Table 50: Hardware FRU/FRE Reference.....	117
Table 51: Redundancy Status Fields.....	121
Table 52: Flexible Authentication Logging Messages.....	123
Table 53: Flexible Mobility Update Messages.....	124
Table 54: Flexible Radio Status Traffic.....	126
Table 55: AuC Operation/Permissions.....	126

List of Processes

Installing the Radio Authentication Feature	40
Configuring the Primary AuC Server	51
Configuring the Backup AuC Server	52
Enabling Radio Authentication in the System	52
Recovering the Authentication Center (AuC) Server	118
Recovering the Authentication Center (AuC) Client Cohabited on NM Client	119
Recovering the Standalone Authentication Center (AuC) Client	119

List of Procedures

Installing the AuC Virtual Machine	41
Configuring the vCenter for the Newly Deployed VM	43
Configuring Virtual Machine Resources	44
Applying OS-Level Identity on the Primary/Backup AuC Server	45
Installing the Primary/Backup AuC Server	46
Installing the AuC Client	48
Setting AuC Server as Present in UNC	53
Setting Radio Authentication System-Wide Status in UNC	53
Logging On to the AuC Client	75
Unlocking a User Account	76
Adding an AuC User	77
Changing a User Password	77
Changing the AuC Server Operating State	78
Viewing the AuC Client Application Version Information	79
Viewing Open-Source Licenses	79
Exiting the AuC Client Application	79
Displaying Zone Status Information	79
Enabling Debug Log Storing	80
Configuring User Name and Password Settings	80
Configuring KVL Ports	81
Viewing Subscriber Information Using the Radio Station Search Form	81
Exporting Subscriber Units Using the Radio Station Search Form	82
Enabling or Disabling Radio Key Updates	82
Viewing Event Details	83
Removing Events	83
Viewing Audits	84
Purging Audits Data from the AuC Server Database to an Archive File	84
Removing Audits Data from the AuC Server Database	85
Viewing KVL Status and UKEK Information	85
Adding KVLs	86
Removing KVLs	86
Enabling and Disabling KVLs	86
Creating a User Account	87
Modifying a User Account	87
Deleting a User Account	88
Synchronizing the AuC with ADS Manually	88

Setting the Master Key on the Active AuC	88
Setting the Master Key on the Standby AuC	89
Replacing the Master Key on the Primary AuC Server	89
Replacing the Master Key on the Backup AuC Server	90
Viewing the Master Key Status	91
Viewing KEKm and Ki Status in a Zone	92
Entering UKEK into KVL	92
Removing UKEK from KVL	92
Distributing Ki	93
Distributing KEKm	93
Distributing SAI	94
Performing a Search Using K-SUID Query	94
Entering Individual K-SUIDs Manually	94
Deleting K-SUIDs	95
Sending SUID Clearout	95
Deleting Unmatched K-SUIDs	96
Switching Over From the Primary AuC Server to the Backup AuC Server	96
Switching Over From the Backup AuC Server to the Primary AuC Server	96
Switching Over AuCs	98
Changing the Primary AuC Server Role to Standby	98
Backing Up the AuC Server Using the AuC Client Application	99
Backing Up the AuC Server Using the Configuration Console	100
Restoring the AuC Server Using the Configuration Console	101
Completing the AuC Server Restoration Using the Configuration Console	101
Re-sending Keys to ZC	103
Scheduling Key Updates	104
Performing Immediate Key Updates	105
Changing the AucUser Service Account Password (Operating System Account)	106
Changing the pguser Service Account Password	107
Changing the rdmuser Service Account Password	108
Checking the Motorola Authentication Center Service Status	110
Starting AuC Client as the Local Windows Administrator	111
Collecting AuC Server and Client Logs	116
Logging On to the Motorola Redundancy Manager Client	120

About Radio Authentication

The Radio Authentication feature manual provides information to support customers who purchased this feature as part of their ASTRO® 25 system. This manual contains a theoretical description of the Radio Authentication feature, as well as installation and configuration processes, operation procedures, troubleshooting, and maintenance information pertaining to the Authentication Center applications.

What Is Covered In This Manual?

The following information is covered in this manual:

- [Radio Authentication Description on page 21](#), contains an overview of the Radio Authentication feature and the architecture it uses.
- [Radio Authentication Theory of Operation on page 35](#), describes how the Radio Authentication feature operates.
- [Radio Authentication Installation on page 40](#), contains processes and procedures on how to install the hardware and software associated with the Radio Authentication feature.
- [Radio Authentication Configuration on page 51](#), contains processes and procedures how to configure the hardware and software associated with the Radio Authentication feature.
- [Radio Authentication Optimization on page 55](#), contains optimization procedures for the Radio Authentication feature.
- [Radio Authentication Screen Reference on page 56](#), contains reference information pertaining to the Authentication Center applications.
- [Radio Authentication Operation on page 75](#), describes how to operate the Authentication Center applications, after the installation and configuration is complete.
- [Radio Authentication Maintenance on page 99](#), describes how to maintain the Authentication Center applications.
- [Radio Authentication Troubleshooting on page 110](#), describes how to troubleshoot the Radio Authentication feature.
- [Radio Authentication FRU/FRE on page 117](#), contains FRU/FRE information pertaining to the hardware and software elements of the Radio Authentication feature.
- [Radio Authentication Disaster Recovery on page 118](#), contains disaster recovery procedures for the Authentication Center applications.

Helpful Background Information

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

Related Information

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

Related Information	Purpose
<i>Standards and Guidelines for Communication Sites</i>	Provides standards and guidelines that should be followed when setting up a Motorola Solutions communications site. Also known

Related Information	Purpose
	as the R56 manual. This manual may be purchased on CD 9880384V83, by calling the North America Parts Organization at 800-422-4210 (or the international number: 302-444-9842).
<i>System Overview and Documentation</i>	Provides an overview of the ASTRO® 25 new system features, documentation set, technical illustrations, and system-level disaster recovery that support the ASTRO® 25 radio communication system.
<i>KVL 4000 Key Variable Loader Radio Authentication User Guide</i>	Provides step-by-step instructions for using the Key Variable Loader (KVL) to create and store encryption keys, and then load them into other Motorola Solutions secure equipment, such as radios, fixed encryption units, digital interface units (DIUs), and others. This manual is intended for use by experienced technicians familiar with similar types of equipment.
<i>Virtual Management Server Hardware</i>	Provides information for implementing, maintaining, and replacing common Hewlett-Packard hardware for servers in ASTRO® 25 systems.
<i>Virtual Management Server Software</i>	Provides procedures for implementing and managing VMware ES-Xi-based virtual server hosts on the common Hewlett-Packard hardware platform in ASTRO® 25 systems. Includes common procedures for virtual machines/virtual appliances on the virtual server host.
<i>Authentication Services</i>	Provides information relating to the implementation and management of the Active Directory (AD) service, Remote Authentication Dial-In User Service (RADIUS), and Domain Name Service (DNS) in ASTRO® 25 systems.
<i>Zone Controller</i>	Covers the zone controller, a key component of the ASTRO® 25 system master site. Includes information on the installation, configuration and management of this software application.
<i>Private Network Management Client</i>	Describes how to install, configure and manage the Private Network Management client, a PC workstation which system administrators and technicians use to for a variety of system-related tasks such as viewing equipment operational status, monitoring network utilization and performance, or viewing alarms generated by system equipment.
<i>Dynamic System Resilience Feature Guide</i>	Provides information necessary to understand, operate, maintain, and troubleshoot the Dynamic System Resilience (DSR) feature that adds a geographically separate backup zone core to an existing zone core to protect against catastrophic zone core failures.
<i>ATIA Log Viewer</i>	Includes information and procedures on the use of the ATIA Log Viewer software application to view log files generated by the Air Traffic Router (ATR) and ZoneWatch applications. These files contain records of all recent zone activity, such as site registrations and calls processed in ASTRO® 25 systems.
<i>ZoneWatch</i>	Covers the use of the ZoneWatch software application to monitor call processing resource assignments at sites in ASTRO® 25 systems.
<i>Historical Reports</i>	Covers the use of the Historical Reports application to generate reports that show system-wide and zone-level historical data for ASTRO® 25 systems.

Related Information	Purpose
<i>Backup and Restore Services</i>	Provides information relating to the implementation and management of centralized backup and restore services for supported devices in ASTRO® 25 systems. This manual addresses server and client functions required for these services.
<i>Windows Supplemental Configuration Setup Guide</i>	Provides additional procedures for Windows-based devices in ASTRO® 25 systems.
<i>Core Security Management Server</i>	Provides information relating to the implementation and management of Core Security Management Server (CSMS). The CSMS hosts network security software components in ASTRO® 25 systems, including client and server functions supporting RADIUS authentication for remote access. This manual also includes information about managing system-wide anti-malware, anti-virus, and anti-spyware protection along with information associated with the firewall manager user interface hosted on the CSMS.
<i>SNMPv3</i>	Provides information relating to the implementation and management of the SNMPv3 protocol in ASTRO® 25 systems. Simple Network Management Protocol (SNMP) is a set of protocols used for managing complex networks.
<i>Unified Event Manager</i>	Covers the use of Unified Event Manager (UEM), the application that provides reliable fault management services for devices in ASTRO® 25 systems.
<i>Unified Network Configurator</i>	Covers the use of Unified Network Configurator (UNC), a sophisticated network configuration tool that provides controlled and validated configuration management for system devices including routers, LAN switches, site controllers and base radios, and is used to set up sites for ASTRO® 25 systems. UNC has two components: Voyence Control and Unified Network Configurator Wizards (UNCW).
<i>MAC Port Lockdown</i>	Provides information on the implementation and management of MAC Port Lockdown for standard Ethernet ports on Hewlett-Packard (HP) switches and for the internal switch of GCP 8000 Site Controllers and GPB 8000 Reference Distribution Modules (RDMs) in ASTRO® 25 systems. Additionally, the document contains instructions for configuring supplemental Ethernet port security, including the implementation of fiber optic ports on HP switches.
<i>ISSI.1 Network Gateway Feature Guide</i>	Includes information required to understand, install, manage, and troubleshoot an ISSI.1 Network Gateway Site, an interconnectivity solution for P25 ISSI.1 compatible systems.
<i>ISSI 8000/CSSI 8000 Inter-system Gateway Feature Guide</i>	Contains information and procedures for the Inter-RF Subsystem Interface 8000 (ISSI 8000)/Console Subsystem Interface 8000 (CSSI 8000) feature that provides an interconnectivity solution for P25 compatible systems and consoles to interface with ASTRO® 25 systems.
<i>Provisioning Manager</i>	Provides a description of the Provisioning Manager application, including information on how to tailor this application for system use and how to provision ASTRO® 25 systems with various system-level, user-level, and device-level configuration parameters.
<i>Fortinet Firewall</i>	Provides information on the implementation and replacement of firewall appliances that Motorola Solutions provides, including a

Related Information	Purpose
	<p>firewall in the DMZ between the ASTRO® 25 RNI and a CEN or the Motorola Solutions Support Centre, a firewall in the ISSI.1 Network Gateway between the ASTRO® 25 system and the ISSI.1 peer system, and a Telephony Firewall in the Enhanced Telephone Interconnect subsystem. These firewalls use Fortinet FortiGate models. See the <i>Zone Core Protection Infrastructure</i> manual for firewalls used for that feature.</p>
<i>License Manager</i>	<p>Provides information about the use of licenses to gain access to features and functions in ASTRO® 25 systems, including the installation of the License Manager in the system and instructions on using the web-based License Manager user interface to load, view, and manage licenses in the system.</p>

Chapter 1

Radio Authentication Description

Radio Authentication is an optional feature to ASTRO® 25 system. The Radio Authentication feature prevents unwanted (and potentially dangerous) subscribers from accessing the network. Each radio attempting to access the network is authenticated by the system infrastructure to prove that they are genuine.

1.1

Radio Authentication Terminology

Table 1: Radio Authentication Acronyms

Acronym	Meaning
AuC	Authentication Center
K	Authentication Key
KEKm	System Key Encryption Key
Ki	Infrastructure Key
KMM	Key Management Message
KS	Session Authentication Key
KVL	Key Variable Loader
RS	Random Seed
SAI	Session Authentication Information
SU	Subscriber Unit
SUID	Subscriber Unit Identity
UKEK	Unique Key Encryption Key
WACN	Wide Area Communications Network

Table 2: Radio Authentication Terms

Term	Definition
Authentication	The process of validating the identity of a subscriber radio.
Authentication Center (AuC) Client	The Authentication Center client application can be virtualized and cohabited with the AuC Server, cohabited on the NM Client, or standalone (on its own hardware). Provides user interface for key management operations.
Authentication Center (AuC) Server database	A PostgreSQL database storing all authentication keys (K).
Authentication Key (K)	A 128-bit key used to perform authentication services during the authentication.

Term	Definition
Authentication Center (AuC) Server	The Authentication Center server application, hosted on a virtual machine installed on the domain controller hardware. The AuC generates, stores, distributes, and updates encryption keys.
Infrastructure Key (Ki)	A key created by the AuC to protect the KEKm.
Key Variable Loader (KVL)	A hand-held device used for generating and uploading keys to the AuC Server and uploading the SUID to the SU.
Master Key	A key entered into the AuC Server through keyboard, used to encrypt keys that are put into the AuC Server database.
Session Authentication Information (SAI)	Random Seed (RS) and Session Authentication Key (KS) sent from AuC to ZC and between ZC.
Subscriber Unit (SU)	A radio in an ASTRO® 25 system.
Subscriber Unit Identity (SUID)	A programmed subscription used by the SU when it is authenticated by the infrastructure. It consists of the Wide Area Communications Network (WACN) ID, System ID, and Subscriber ID.
System Key Encryption Key (KEKm)	A key created by the AuC, used by AuC and ZC to protect the Session Authentication Key (KS).
Unique Key Encryption Key (UKEK)	A key used for encrypting the information sent from the KVL to the AuC Server.

1.2

Radio Authentication Security Features

The Radio Authentication feature helps to prevent the use of ASTRO® 25 system channel resources by unauthorized subscriber radios. With the Radio Authentication feature, the zone controller is able to validate the identity of subscriber radios requesting service on the system. Neither the subscriber radio hardware nor the person using the subscriber radio is allowed to access the system until authentication is accomplished by validating the subscription programmed into the subscriber radio.

Examples of malicious attacks that the Radio Authentication feature prevents, include:

Theft of resources

Cloned radios monitor traffic, causing audio routing and loading problems for legitimate users.

Theft of service

Cloned radios deployed to circumvent subscriber fees, causing losses to system owners.

Disruption of operations

Cloned radios pretend to be a public safety officer, disrupting everyday operations.

Radio Authentication security features include:

Master Key

The Master Key is entered into the AuC Server through the keyboard. It is used to encrypt keys put into the AuC Server database.

AES-128 Algorithm

The AuC Server encrypts authentication keys using the AES-128 algorithm before putting items in the database. AES encryption is also used for KVL connection to AuC, for server-client connection and for SNMPv3 encryption (if set up to do that).

SNMPv3

The AuC Server uses the SMNPv3 protocol for secure sending of the Infrastructure Key (Ki) to the ZC.

Information Assurance

Both the AuC Server (which is a Windows-based application) and the KVL (which connects to the Internet) adhere to the Motorola Solutions Information Assurance Policy. Information Assurance helps to prevent unauthorized application access.

RAPI Audit

RAPI logging messages provide detailed information about authentication activity on the control channels. After an incident, an audit provides the capability to detect the adversary.

Historical Reports

The application keeps track of the count of SUs that pass authentication, fail authentication, and are let on to the system without authenticating.

UEM Alarms

The UEM application reports an authentication failure alarm in case of a wrong response to a challenge.

1.2.1

Encryption Algorithm

The base encryption algorithm used for ASTRO® 25 system Radio Authentication is the 128-bit Advanced Encryption Standard (AES). A subscriber must have a 128-bit authentication key (K) and the infrastructure must know it. Each radio is intended to have a unique K so that a compromise of one SU does not compromise others.

1.2.2

Embedded Passwords

Motorola Solutions provides the capability to change, back up and restore embedded passwords for non-interactive accounts on specified devices. This functionality has a local device scope – it does not manage account passwords across devices. There is a common location for all the passwords belonging to multiple applications on a given device. The embedded password management functionality is provided automatically together with each of the AuC applications. If multiple supported applications are installed on the same platform, only the first one installs the embedded password management component.

1.3

Radio Authentication Architecture

The Radio Authentication feature is centered around the Authentication Center (AuC) applications. The AuC Server application provides a key management function for authentication in the system and stores the Authentication Keys (K) for all the radios in the system in the database. The AuC Server is a virtualized application installed on the Virtual Server that hosts the system-level domain controller. The AuC Client application provides the user interface for system operators to perform key management operations.

The Radio Authentication feature is supported in the following ASTRO® 25 system configurations:

- Single-Zone Small Scale Non-Redundant Configuration (L1)
- Single-Zone Small Scale Redundant Configuration (L2)
- Single-Zone Non-Redundant Configuration (M1)
- Single-Zone Redundant Configuration (M2)
- Multi-Zone Capable Configuration (M3)



NOTICE: For system diagrams presenting the AuC Server, see the *Virtual Management Server Software* manual.

The Radio Authentication feature is limited in the following ASTRO® 25 system configurations:

- **SmartX** – Authentication is only done for 9600 sites and is not supported for 3600 sites. Since the radios manually roam between 3600 and 9600, in order to protect an SUID at a 9600 site, a different ID needs to be chosen for 9600, and that ID needs to be site locked at 3600 sites.
- **HPD** – Authentication is only done for 9600 sites and HPD is not supported. HPD subscriber unit IDs need to be site restricted, so their use on 9600 sites is impossible.
- **ISSI.1** – For systems employing only ISSI.1 with the ISSI.1 Network Gateway (not the ISSI 8000/CSSI 8000 feature with the Intersystem Gateway, ISGW), no registrations or authentications go across the ISSI and the Authentication Required system-wide parameter cannot be used. Additionally, ISSI.1 SUIDs are site access-restricted, so their use on non-ISSI sites is not possible. For more details regarding ISSI.1, see the *ISSI.1 Network Gateway Feature Guide*. For an overview of ISSI 8000/CSSI 8000 and radio authentication, see [Radio Authentication – ISSI 8000/CSSI 8000 on page 24](#) and for more details regarding the ISSI 8000/CSSI 8000 feature, see the *ISSI 8000/CSSI 8000 Intersystem Gateway Feature Guide*.

The Radio Authentication feature is **not** supported in the following ASTRO® 25 system configurations:

- Single Site Express Trunking System
- Conventional Systems (including K core configurations)

1.3.1

Radio Authentication – ISSI 8000/CSSI 8000

The ISSI 8000/CSSI 8000 feature provides an interconnectivity solution for P25-compatible systems and consoles to interface with an ASTRO® 25 system.

With the ISSI 8000/CSSI 8000 feature, the Authentication Required system-wide parameter is used to support registration and authentication of subscriber units across the P25-compliant systems supported by the feature to prevent radio authentication information from being compromised (which might result in subscriber clones gaining access to RF sites) and to minimize the risk of attack by untrusted entities.

During registrations, the Intersystem Gateway (ISGW) and the zone controller encrypt the KS. IPsec is used between the ISGW and the ISSI 8000 Firewall to also protect the KS.



NOTICE: Work with field engineering and the foreign system operator to define what, if any, security is used on the intersystem links.

With ISSI 8000, radio authentication can be applied to foreign subscribers (those subscribers “foreign” to the ASTRO® 25 system) and the AuC will support radio authentication of foreign subscribers (even if local subscribers are not authenticated). Radio authentication of home subscribers roaming in a foreign system is also supported.

1.4

Radio Authentication Components

The following are the hardware components necessary for radio authentication operation:

- **Zone Controller (ZC) Host Server** - For hardware specifications, see the *Virtual Management Server Hardware* manual.
- **Domain Controller (DC) Host Server** - For more information, see the *Authentication Services* manual.
- **Key Variable Loader (KVL) 4000** - A hand-held device used to generate and upload authentication keys to the AuC Server. For more information, see [Key Variable Loader \(KVL\) on page 27](#).
- **Subscriber Radios (SUs)** - The radios in the system.

- **Standalone Authentication Center Client (AuC Client) Host** - An optional hardware platform, hosting the AuC Client application. For more details, see [Authentication Center \(AuC\) Client on page 25](#).

The following are the software components necessary for radio authentication operation:

- **Authentication Center (AuC) applications** - The AuC applications are Windows-based, client/server applications used to manage encryption keys for the ASTRO® 25 system. The AuC Server generates, stores, distributes, and updates encryption keys used by the Radio Authentication feature. The AuC applications utilize a tier approach that distributes the software application into the following separate, but inter-dependent, entities:
 - Authentication Center Server
 - Authentication Center Client
 - Motorola Redundancy Manager
- **Zone Controller application** - For more information, see the *Zone Controller* manual.
- **Configuration Console** - A management tool used for switching between Primary and Backup AuC Servers and performing AuC backup and restore operations.
- **License Manager** - A tool used to store and manage licenses in the ASTRO® 25 system, including the Radio Authentication and Radio Authentication User license. For more information, see the *License Manager* manual.
- Other - KVL software, subscriber radios software.

1.4.1

Authentication Center (AuC) Server

The Authentication Center Server (AuC Server) is a Windows 2012 Server virtual machine, hosted on an ESXi-based Virtual Server platform. The AuC Server can only be deployed in a virtualized environment – it cannot be deployed on a standalone server. The AuC Server contains a PostgreSQL database which stores key management data and key material used by the AuC Server.

For more information on the Virtual Server, see the following manuals:

- *Virtual Management Server Hardware*
- *Virtual Management Server Software*

1.4.2

Authentication Center (AuC) Client

The Authentication Center Client (AuC Client) is a Java-based client application that provides user interface to manage radio authentication. The ASTRO® 25 system supports up to 16 AuC Clients. Out of these 16 clients, 2 client sessions are cohabited with the AuC Server and are used for service purposes. The remaining 14 AuC Client applications are hosted on Microsoft Windows 7 or Windows 10 operating system, and can either use the NM Client hardware, or can be installed on a separate, standalone Hewlett-Packard (HP) Z420 or Z440 workstation.

For hardware specifications, as well as Windows 7 and Windows 10-related procedures, see the *Private Network Management Client* manual.

1.4.3

Configuration Console

The Configuration Console is a management tool, installed together with the Authentication Center (AuC) application, the main functionality of which is switching between primary and backup AuC Servers, as well as performing AuC backup and restore operations.

To start the **Configuration Console**, an account with administrative privileges is required. The **Configuration Console** window lists available commands together with their descriptions. It also shows the list of options available for each command.

Table 3: Configuration Console Commands

Product Command	Command	Parameter	Description
coco auc	role	show	Shows the current AuC role.
		active	Changes the AuC role to active.
		standby	Changes the AuC role to standby.
	backup	<path to the backup file>	Backs up the AuC Server.
	restore	<path to the backup file>	Restores the AuC Server.
	enable		Sets the AuC service start type to automatic.
	start		Starts the AuC service.
	stop		Stops the AuC service.
	status		Shows the AuC service status.
	version		Shows the AuC Server version.
	lock	enable/disable	Enables/disables key updates in AuC.
coco aucclient	version		Shows the AuC Client version.
	mergecsv	<ol style="list-style-type: none"> <path to the auc file> where <auc file> is the AuC file created after exporting subscribers <path to the pm file> where <pm file> is the Provisioning Manager (PM) file created after exporting subscribers 	After exporting subscriber units using Exporting Subscriber Units Using the Radio Station Search Form on page 82 , merges <code>csv</code> files from the AuC and the PM into one <code>csv</code> file which can be viewed in Microsoft Excel.

Product Command	Command	Parameter	Description
		3 <i><path to the output file></i> where the <i><output file></i> is the name of the merged file	
coco pg	start		Starts the database service.
	stop		Stops the database service.
	serviceconf		Changes the database service configuration.
	status		Shows the database service status.
	version		Shows the database version.
coco coco	terminate		Tries to delete exclusive access lock file.
coco rdm	status		Shows the status of the Redundancy Manager.
	version		Shows the version of the Redundancy Manager.
	switchover		Performs complete switchover of primary and backup roles.

1.4.4

Key Variable Loader (KVL)

KVL 4000 is a hand-held device used for loading the authentication key to the SU and uploading the corresponding SUID to the Authentication Center (AuC) Server. The KVL connects to the radio using the RS-232 port on the Security Adapter and provides manual and automatic authentication key generation. The keys that are manually entered into the AuC Client application are downloaded to target devices and never uploaded to the AuC Server. However, the keys that are manually entered on the KVL must also be entered into the AuC Client application. The automatically generated keys are downloaded to the target devices and need to be uploaded to the AuC Server. To increase upload security, each KVL operator is authenticated with the Active Directory account and password.

KVL 4000 consists of the following two components:

MC55 Personal Digital Assistant

The host component of the KVL 4000, responsible for controlling all operations of the device. It uses the Windows Mobile operating system.

Security Adapter

Provides secure storage of encryption keys, cryptographic operations, and port access for the KVL 4000.

The KVLs that are used in the system can be viewed and managed through the AuC. The KVL connects to the AuC in one of the following ways using the USB-to-Ethernet adapter:

Locally

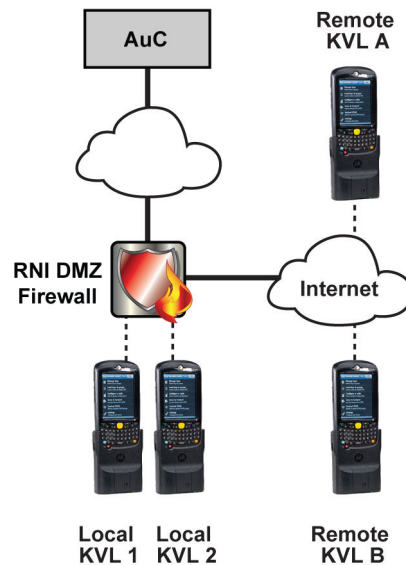
Involves connecting the KVL to allocated network switch or firewall port. In the multi-zone capable configuration (M3) configuration, the KVL connects to the DMZ LAN switch and establishes a VPN connection with the RNI-DMZ firewall. In single-zone configurations (L core, M1, M2), the KVL connects directly to the RNI-DMZ firewall.

Remotely

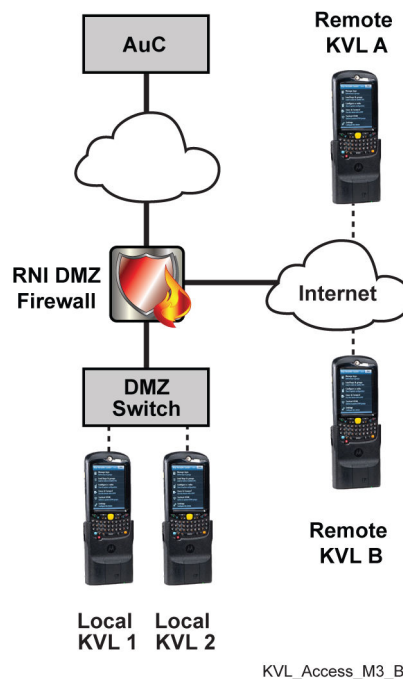
Involves connecting the KVL to the firewall through the internet, using the customer's cable or DSL connection.

The VPN provides extra confidentiality and chronological integrity between the KVL and the firewall. The firewall allows a limited number of VPN connections, so after a successful KVL transfer to the AuC, the VPN connection can be torn down by the KVL operator or will automatically drop after 180 seconds of inactivity.

Figure 1: KVL-AuC Connection in L Core and M1/M2 Configurations



KVL_Access_L1L2_M1M2_B

Figure 2: KVL-AuC Connection in M3 Configuration

For more information on using the KVL for radio authentication, see the *KVL 4000 Key Variable Loader Radio Authentication User Guide*. For information on which firewall ports are used, see the *Fortinet Firewall* manual.

1.5

Radio Authentication in DSR Systems

The Radio Authentication feature can be installed in Dynamic System Resilience (DSR) systems. In a Multizone Capable system, two virtual machines hosting the AuC Server are deployed – primary and backup – one in each core and with its own IP address. However, only one of the two AuCs is enabled at a time, and this one is called active.

Each AuC has its own database. Synchronization from the active to the standby AuC is taking place continuously. The backup database is in read-only mode – a switchover from the active to the backup AuC will automatically run AuC services on the backup AuC.

For a zone core switchover in a running and synchronized DSR system, the operator needs to perform the AuC Server switchover according to procedures contained in the section [Dynamic System Resilience \(DSR\) on page 96](#).

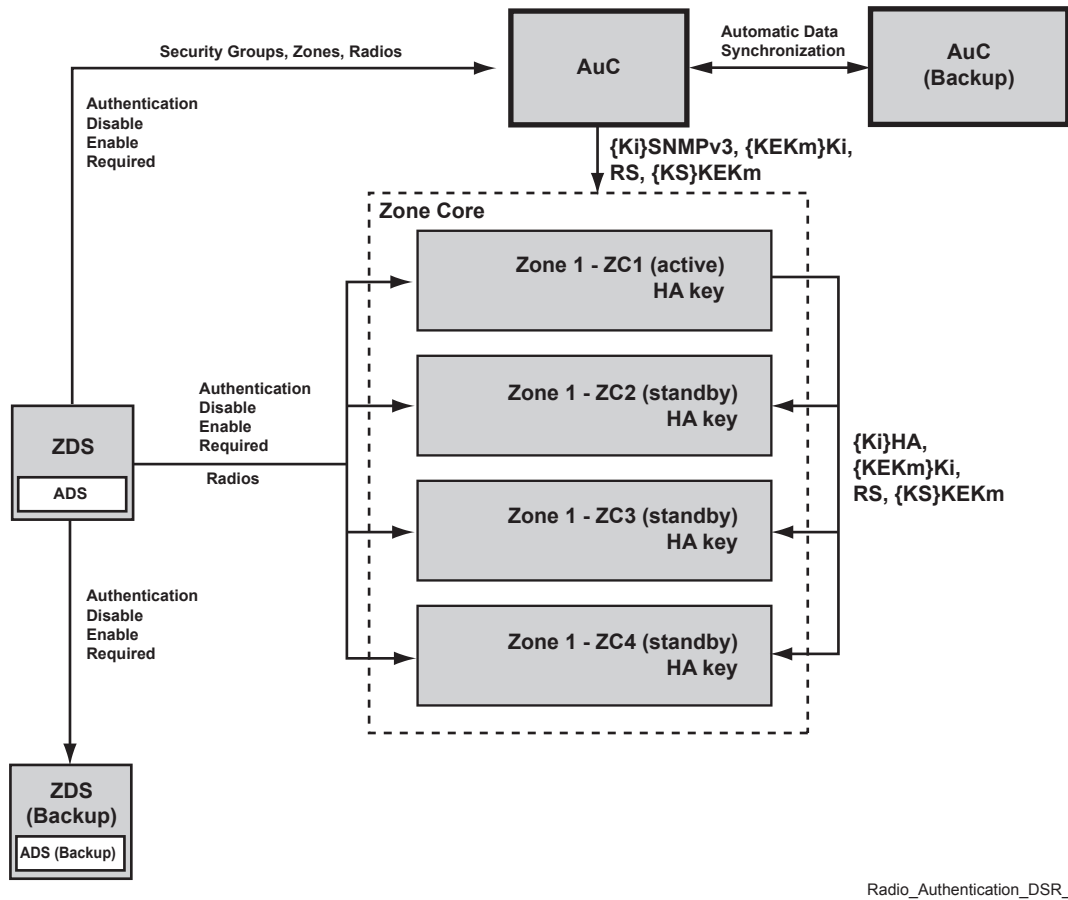
Provided there is an AuC Server in the system, the ZC will try to connect to the first enabled AuC Server it finds. If no active AuC can be found, it is considered to be an infrastructure failure to the ZC. Under this condition, the ZC will continue to authenticate those subscriber unit IDs it already has SAI for. The KVL can be used to give an actual radio a K whether or not the AuC Server is present. However, the AuC Server needs to be available to get the K-SUID pair from the KVL so that the infrastructure can authenticate the radio.

The following Dynamic System Resilience (DSR) configurations are supported:

- Multi-Zone Capable DSR configuration with ZCP
- Multi-Zone Capable DSR configuration without ZCP

The following figure shows how radio authentication is handled in a DSR system.

Figure 3: Radio Authentication – DSR System



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

1.6

Radio Authentication in the System

The Radio Authentication feature interacts with other features within an ASTRO® 25 system.

1.6.1

Configuration Management

The Radio Authentication feature can be configured at the level of the entire system using the UNC application, or at the level of an individual radio using the AuC Client.

1.6.1.1

System-Wide Settings

The Unified Network Configurator (UNC) application is used for system-level configuration of the Radio Authentication feature. The following parameters can be set in the UNC:

- A system-level **Contains Radio Authentication Center** parameter indicates if the AuC is present in the system or not. It is used by the ZC to know whether to connect with the AuC:
 - When this parameter is set to **Yes**, an AuC object is created in the Network Management subsystem and the ZC is informed there is an AuC available on the system. This provides an

indication to the ZC to initiate LAPD connection with the AuC and to report any link faults to the UEM.

- When this parameter is set to **No**, the AuC object is removed and the ZC informed of its deletion. On receiving this message, the ZC terminates the LAPD link with the AuC. However, it continues to authenticate the SUs based on the Authentication Disabled/Enabled/Required parameter.
- A system-level **Radio Authentication State** parameter manages the state of radio authentication in the system. One of three settings can be selected, and it is later sent to the ZC and the AuC. The following are the possible system-wide authentication states and their implications to the system:

Enabled

Only radios provisioned for authentication will authenticate. Radios without any Session Authentication Information (SAI) will be allowed to register, but radios whose Authentication Key is mismatched with Zone Controller SAI will be denied registration. This setting is used during migration.

Disabled

All radios can access the system and there is no radio authentication.

Required

All radios must authenticate, otherwise they cannot access the system. Upon transition to this state, all individual settings are cleared.



CAUTION: The Required setting should only be entered when all SUIDs have been provisioned for authentication. Otherwise, unprovisioned SUIDs will not be able to get on the system.



IMPORTANT:

Upon moving to the system-wide Authentication Required state, the Network Management subsystem shall retain Individual Default Access Permission (automatic Record Creation) state and automatic record creation will not be functional.

Before a transition to the system-wide Authentication Required state, the 24-bit Radio IDs should be put in the Provisioning Manager first - to avoid a potential 30 minute delay to send SAI to the ZC, when in Authentication Required. For detailed procedures, see the *Provisioning Manager* manual.

See the following procedures on how to set the system-level parameters:

- [Setting AuC Server as Present in UNC on page 53](#)
- [Setting Radio Authentication System-Wide Status in UNC on page 53](#)

1.6.1.2

Individual Settings

The AuC Client application can also be used for setting the radio authentication state on each individual radio in the AuC Server. Two possible individual settings are Enabled and Disabled. However, the system-wide state limits the possibility of individual control (see the following table).

Table 4: System-Wide State Impact on Individual Settings

System-Wide Authentication State	Individual Setting (in AuC) Impact
Enabled	If the system-wide authentication state is Authentication Enabled, individual control is allowed. Selected SUIDs can be disabled and will not be authenticated.
Disabled	If the system-wide authentication state is Authentication Disabled, individual setting is not relevant as the radios cannot be authenticated.

System-Wide Authentication State

Individual Setting (in AuC) Impact

Required

If the system-wide authentication state is Authentication Required, individual setting is not allowed as all radios must authenticate.



CAUTION: Upon moving from the system-wide Authentication Enabled to the Authentication Required state, all individually disabled SUs in the AuC must be enabled first.

See [Enabling or Disabling Radio Key Updates on page 82](#) for information on how to enable/disable individual radios.

1.6.2

Fault Management

The AuC is fault managed by the Unified Event Manager (UEM) application. If a SU sends the wrong response to a challenge, it will be trapped by the ZC and the event displayed on the UEM. This could be an adversary SU trying to access the system or a legitimate SU that was provisioned for authentication incorrectly. Decryption and link failures are also displayed on the UEM. See [UEM Alarms on page 112](#) for a detailed list of UEM alarms.

1.6.3

Performance Monitoring

The ASTRO® 25 system Radio Authentication feature introduces new logging messages to the performance applications:

- The Air Traffic Information Access (ATIA) Log Viewer application logs the site and time of authentication events in the system. For details, see the *ATIA Log Viewer* manual.
- The ZoneWatch application shows a real-life feed of which SUIDs are passing, failing, or not being authenticated. The reason for failing authentication is also displayed. For details, see the *ZoneWatch* manual.
- The Historical Reports application keeps track of the count of SUs that pass authentication, fail authentication, and are let on to the system without authenticating. For details, see the *Historical Reports* manual. The following are system-level radio authentication statistics as displayed in Historical Reports:

Passed Authentication

Number of registrations which were successful. Counted per zone, but summarized per system.

Failed Authentication

Number of registrations which failed. Counted per zone, but summarized per system.

Not Authenticated

Number of registrations which were not challenged for authentication. Counted per zone, but summarized per system.

1.6.4

Fault and Performance Monitoring in the AuC

The performance and operation of the AuC applications can be monitored in several ways on the host machine.

AuC applications are logging events using the Centralized Event Logging client. If the logged event has been triggered by the user, it will be shown in the Windows Event Viewer. The event contains a short description of what has happened along with the user's privileges. The **Privileges** value is a decimal

number matching a 7-digit binary number (xxxxxxx, where x = 0 or 1, depending on whether the user has the privilege or not). For a list of AuC user privileges, see [Users Tab on page 68](#).

In addition, AuC applications are logging information and errors directly to the Windows Event Viewer. These include successful and unsuccessful AuC Client login attempts, as well as actions performed in the Password Vault.

AuC also uses a resource monitor application to monitor available resources, such as RAM, HDD space or Java memory allocation. If the AuC host is running low on any resources, the application logs a warning to the Windows Event Viewer. The resource monitor is installed together with the AuC Server application, but it operates as an independent Windows service even if the AuC service is stopped.

1.6.5

IP Services

IP services in the system affect the AuC applications.

1.6.5.1

Backup and Restore (BAR) Services

Since the AuC is a virtualized application, the database cannot be backed up by moving it directly on to physical media such as a USB drive or a DVD. Instead, Backup and Restore (BAR) services are used to back up the AuC Server, utilizing a BAR Client application installed on the AuC Server. The AuC Server is a supported BAR client in Baseline Backup and Recovery Server, it does not require purchasing the full Backup and Recovery Server (BAR server) functionality.

The backup is stored locally on the AuC Server in a designated backup folder (D:\Motorola\BoxBackup by default). The BAR agent copies the information from that folder and pushes it to the BAR server. The customer can also manually retrieve the backed up database by creating a DVD of the archive stored on BAR server. Additionally, the AuC Server provides an option to restore the backed up database from the BAR server to a designated folder on the AuC Server.

The BAR server only backs up the data from the particular zone. In systems with the DSR feature, the backup AuC Server is not able to access the BAR server in the zone with the primary AuC Server. When starting up the backup AuC Server, a manual backup from the zone is necessary. If the other zone's BAR server is still functional, backup can be manually retrieved from there, otherwise an off-site backup is needed. Once the backup AuC Server is up and running, the BAR server in its zone backs up its database.

For more information on the Backup and Restore (BAR) services, see the *Backup and Restore Services* manual.

1.6.5.2

Active Directory (AD)

AuC Server and AuC Client will join the domain and use Active Directory (AD) authentication for operating system-level interactive account logins. However, the AuC application-level accounts are not managed by the AD authentication, permissions can be applied to them in the AuC. The KVL operator is authenticated with an Active Directory account and password when using the VPN connection to the AuC.

For more details on the Active Directory, refer to the *Authentication Services* manual.

1.6.6

Firewall

The AuC Server is in the RNI and sends information to the active ZC in each zone, which means traversing the ZCP firewall. If the NM Client hosting the AuC Client is located in a different zone than the AuC Server, then the ZCP firewall needs to be traversed as well.

A VPN is established from the KVL to the RNI-DMZ firewall for the KVL to send K-SUID to the AuC. The firewall only allows KVL traffic to go to the AuC. The design assumes that KVL source IP addresses at the firewall (source filtering) will not be used in order to facilitate upload from KVL from any Internet source.

For more information, see the *Fortinet Firewall* manual.

Chapter 2

Radio Authentication Theory of Operation

The Radio Authentication feature utilizes a challenge-response-result process to verify the validity of the subscriber. The SU identifies itself on the system by its programmed subscription. The programmed subscription is the Subscriber Unit Identity (SUID), which is comprised of the following:

- Wide Area Communication Network ID (20-bits)
- System ID (12-bits)
- Subscriber ID (24-bits)

Each SUID is assigned one secret Authentication Key (K) for authentication. A successful authentication is achieved when the SU verifies its knowledge of the K to the infrastructure by sending the correct response. Authentication happens automatically and is transparent to the user, unless it fails.

The authentication process occurs upon:

- SU power up
- ZC unit registration
- SU attempting to bypass registration
- TG conflict
- Change of authentication key
- Under rare conditions, upon SU site roaming
- Upon rare conditions, upon zone roaming

The authentication process does not occur upon:

- Local site trunking
- While the SU is in any call activity
- During call activity if the local zone is aware of the call

The AuC Server provides a key management function for authentication in the system and stores the Authentication Keys (K) for all the SU in the system. Compromise of K means having to physically contact that SU. To reduce the exposure of K in the infrastructure, the AuC passes a derivation of K to the ZC called Session Authentication Information (SAI). The SAI contains Random Seed (RS) which does not need to be protected and Session Authentication Key (KS) which needs to be protected.

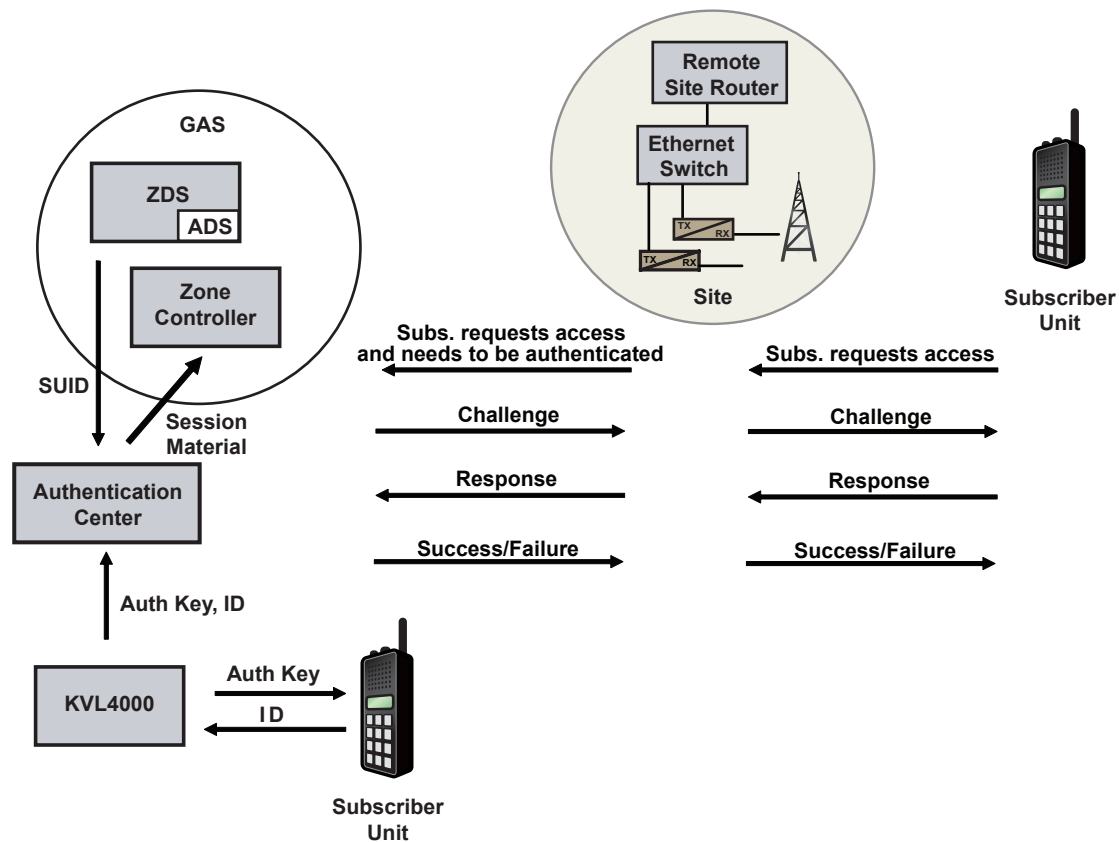
The ZC does the real-time authentication of the SU using SAI. The system is designed in such a way, that the AuC is not needed for real-time radio authentication to occur. Once SUs are provisioned for radio authentication, the AuC can be inoperable and the ZC will be able to continue to authenticate the SU. However, without an operable AuC in the system, managing keys (changing or re-sending them) would be impossible.

2.1

Authentication Process

The following diagram presents the process of authenticating a subscriber unit by the infrastructure.

Figure 4: Radio Authentication Process



Authen_ZC_SU_control_channel_B

2.1.1

Device Roles

The following table describes the role of each device (listed alphabetically) in the authentication process.

Table 5: Device Roles

Device	Role in the Process
ADS	Sends the zone information, security groups, radio records (SUID), as well as the system information (System ID, WACN ID, etc.) to the AuC.
AuC Server	Stores and manages all of the SU Authentication Keys (K) in the system. Has individual authentication disable capability.
ATR	Receives authentication logging messages from the ZC. Displays Zone-Watch.
KVL	Creates the Authentication Key (K), then loads it into the SU and sends K-SUID pair to the AuC.
Site	It is mostly transparent to authentication. It keeps track of SU in site trunking that need to be authenticated in order to inform the ZC when the site goes back to wide.

Device	Role in the Process
SU	It is authenticated by the Zone Controller. Permanently stores its own Authentication Key (K). Alerts the user if authentication fails (provided it was configured to do that).
Syslog	Responsible for logging wrong responses from SU, decryption failures, and AuC application-level logins.
UNC	Used for setting the system-wide authentication parameters.
ZC	Does the actual, real-time authentication of the SU.

2.2

Authentication Keys

Keys used for radio authentication in ASTRO® 25 system include:

Infrastructure Key (Ki)

Used to encrypt the Key Encryption Keys (KEKm) that are delivered to entities over the system infrastructure. The AuC Server is responsible for generating a unique Ki for the ZC.

Authentication Key (K)

Used for challenge-response-result authentication process.

Key Encryption Key (KEKm)

Used to encrypt key material between zones.

Session Authentication Information (SAI)

Session authentication material, contains the Session Authentication Key (KS) and Random Seed (RS).

2.2.1

Key Parameters

The following table summarizes the authentication keys used in the authentication process.

Table 6: Authentication Keys Parameters

Parameter (bits)	Name	Definition	Devices Involved
K (128)	Authentication Key	Created by KVL and given to SU and AuC.	AuC KVL SU
Ki (128)	Infrastructure Key	Created by AuC used to protect KECm.	AuC ZC
KEKm (128)	System Key Encryption Key	Created by AuC, used by AuC and ZC to protect KS.	AuC ZC
KS (128)	Session Authentication Key	AuC and SU generate KS from RS and K. AuC sends it to ZC.	AuC SU ZC
RS (80)	Random Seed	Created by AuC used for generation of KS using K. Sent to ZC and ZC sends to SU.	AuC SU ZC
SAI	Session Authentication Information	RS and KS sent from AuC to ZC and between ZC.	AuC ZC

2.2.2

Key Provisioning

Provisioning is creating new key entities in the system. In the Radio Authentication feature, the KVL and the AuC Server together manage key provisioning, while only the AuC Server handles key distribution. When key updates are enabled and a new entity is provisioned in the system, the AuC Server initiates delivery of keys to the ZCs. The AuC Server also performs key distribution for subscribers. Some of the keys must be intentionally provisioned by the user to infrastructure devices and SUs through the KVL (K), others are automatically distributed by the system if only key update is enabled.

2.2.2.1

Authentication Key (K) Provisioning

In order for radio authentication to work, a subscriber must have a 128-bit authentication key (K) and the infrastructure must know what that K is. Once the KVL creates the K, the KVL needs to connect to the SU using the RS-232 serial interface on the Security Adapter. Then, the KVL loads the K on to the SU in exchange for the SUID. The K can be created in one of two ways:

- **Automatically** - The KVL generates the K, which remains unknown to the operator throughout the provisioning process, sends it to the subscriber unit and then transfers the K-SUID pair to the AuC Server. Upon a successful transfer to the AuC Server, the K-SUID pairs are erased from the KVL automatically. The KVL can store up to 475 K-SUIDs. If a K already exists for the SUID in the SU, the KVL user will be prompted with a warning that an existing K will be overwritten and the KVL user has the option to either continue or stop the load of K.
- **Manually** - The KVL and AuC operators manually enter the K into the KVL and AuC. This is an exception scenario in case the AuC Server cannot be reached through a LAN switch or internet connection, or there is a need to quickly get a radio on to the system and have it authenticate. Manually entered Ks are never stored in the KVL and are not recallable for the KVL operator to see. Manually created keys are not transferred to the AuC.

The AES-128 algorithm is needed in the SU host to be able to respond to a challenge from the infrastructure. On every power up, the SU will manage the SUID data from the codeplug against the internally stored SUID-K pairs. If the user changed their codeplug and no longer had a system for a particular SUID, then SU would remove that SUID-K data from the internal database. Also, if the user added a new system with a new SUID, SU would create a new blank entry for that.

Afterwards, the KVL sends the K-SUID pair to the AuC Server. Each KVL will have one UKEK for radio authentication to connect to the AuC Server. In systems that have two AuC Servers (one enabled and one disabled), primary and backup AuC Server IP addresses need to be configured in the KVL. The KVL can connect to the AuC Server in two ways:

- **Locally** - The KVL connects through an allocated firewall/switch port. In the Multi-Zone Capable (M3) configuration, this is done through the DMZ LAN switch by establishing a VPN connection with the RNI-DMZ firewall. In single-zone configurations (L core, M1/M2), the KVL is connected directly through the RNI-DMZ firewall. The KVL then uploads the information, encrypted through UKEK, to the AuC Server.
- **Remotely** - The KVL connects using an internet connection. The customer needs to provide an internet connection to the firewall, and the KVL establishes a VPN connection to the RNI-DMZ firewall. The KVL then uploads the information, encrypted through UKEK, to the AuC Server.

In both cases, the KVL operator is authenticated with an Active Directory account and password.

2.2.3

Key Distribution

Key distribution for the Radio Authentication feature is managed by the AuC Server. The delivery of keys to system infrastructure devices is initiated by the AuC Server, when a new entity is provisioned and key updates are enabled.

The key distribution and update that is executed through the infrastructure network concerns the following keys:

- Infrastructure Key (Ki)
- Key Encryption Key (KEKm)
- Authentication material (SAI)

2.2.3.1

Ki Distribution

The Infrastructure Key (Ki) must be distributed to the ZCs using the AuC Server. The Ki is randomly generated by the AuC Server and not known to the AuC operator. Each zone has a different Ki and all ZCs (active and standby) in a zone use the same Ki. Since the AuC Server is not aware of standby ZCs, the active ZC is responsible for sending the Ki to them. Each time a Ki is distributed, a new one needs to be generated, as the same Ki cannot be used twice.

The Ki is securely sent to the ZCs using the SNMPv3 protocol. In order for the Ki to be provisioned, the AuC Server presence needs to be configured in the Network Management subsystem.



IMPORTANT: The Ki is intended to be installed once and replicated between the ZCs within a zone. While distributing the Ki, the HA key should not be changed. Changing the HA key while the Ki is still being replicated, will corrupt the Ki.

For a detailed procedure on how to distribute Ki, see [Distributing Ki on page 93](#).

2.2.3.2

KEKm Distribution

The AuC Server is responsible for generating the Key Encryption Key (KEKm) for each zone and distributing it to ZCs. The same KECm is used for all ZCs in all zones. KECm can be distributed once the infrastructure key (Ki) is already loaded into the ZCs. The Ki is used to decrypt/encrypt new KECm sent by the AuC Server to the ZCs.

For a detailed procedure on how to distribute KECm, see [Distributing KECm on page 93](#).

2.2.3.3

SAI Distribution

Unique authentication material (SAI) is delivered to the ZC for each SU. The authentication material keys (KS) are distributed as encrypted keys (using the KECm key) over the system infrastructure network. Once decrypted by the KECm key, the authentication material is used by the ZC to authenticate SUs.

For a detailed procedure on how to distribute SAI, see [Distributing SAI on page 94](#).

2.2.4

Key Storing

The authentication keys are stored in the AuC Server database encrypted by the Master Key. The Master Key is used to encrypt/decrypt all database data. Without the knowledge of the Master Key, the data cannot be read.

Chapter 3

Radio Authentication Installation

There are several installation procedures relating to the Radio Authentication feature.



IMPORTANT: The initial installation and configuration of the Radio Authentication feature components is performed by Motorola Solutions.

3.1

Required Software

Before installing the Radio Authentication feature, obtain:

- *Motorola Windows Box Profile* media (provided by Motorola Solutions; contains initial setup for individual devices and initial configuration scripts; drivers for Windows client and server)
- *Motorola Windows Server* media (provided by Motorola Solutions; contains the Windows Server 2012 R2 virtual machine files)
- *Authentication Center* DVD
- *Authentication Center Client* CD
- *Windows Supplemental* media



NOTICE: For information on the contents of the *Windows Supplemental* media, see the *Windows Supplemental Configuration Setup Guide*.

- *MOTOPATCH for Windows* DVD

To enable the Key Variable Loader (KVL), obtain:

- VPN Client
- Ethernet Adapter module software
- Windows Mobile patch media

3.2

Installing the Radio Authentication Feature

Prerequisites:

Perform the following actions:

- Verify that the Virtual Server hardware has been installed. See the *Virtual Management Server Hardware* manual.
- Verify that the ESXi Server, vSphere Client, and Direct Attached Storage (DAS) device have been installed. See the *Virtual Management Server Software* manual.
- Verify that the virtualized domain controllers have been installed and configured. See the *Authentication Services* manual.
- Ensure that the Radio Authentication and Radio Authentication User license has been uploaded to the License Manager. See “Uploading Licenses to the License Manager” in the *License Manager* manual.

Process:

- 1 Using vSphere, create the AuC virtual machine.

See [Installing the AuC Virtual Machine on page 41](#).

- 2 Install the AuC Server.

See [Installing the Primary/Backup AuC Server on page 46](#).

- 3 Install the AuC Client (either standalone or cohabited on an NM Client).

See [Installing the AuC Client on page 48](#).

- 4 Log on to the newly installed AuC Client and perform the initial configuration of the AuC Server.

See [Configuring the Primary AuC Server on page 51](#).

- 5 Install and set up the KVL device for radio authentication.

See the *KVL 4000 Key Variable Loader Radio Authentication User Guide*.

- 6 Enable each subscriber unit for radio authentication.

See user documentation for respective subscriber units.

- 7 Provision the AuC Server with AuC Client application accounts, SUIDs, KVLs, and synchronize the AuC Server with provisioned data in the NM.

See [Enabling Radio Authentication in the System on page 52](#).

- 8 For systems with the DSR feature, install the backup AuC Server in the backup core.

See [Installing the Primary/Backup AuC Server on page 46](#).

- 9 Upload provisioned K-SUID mappings from the KVL 4000 device to the AuC.

See “Uploading Provisioning Information to the AuC” in the *KVL 4000 Key Variable Loader Radio Authentication User Guide*.

Related Links

[Recovering the Authentication Center \(AuC\) Server on page 118](#)

3.3

Installing the AuC Virtual Machine

Prerequisites:

Obtain the *Motorola Windows Server* media (provided by Motorola Solutions; contains the Windows Server 2012 R2 virtual machine files).

Ensure the NM Client that is used for installing the AuC Virtual Machine has the vSphere Client application installed. If not, see “Installing the VMware vSphere Client on Windows-Based Devices” in the *Virtual Management Server Software* manual.

For the IP address, see the *System IP plan* or consult your system administrator.

For information on the use of the Direct Attached Storage (DAS) device, see the *Virtual Management Server Software* manual.



NOTICE: Before performing any step that requires inserting software media, ensure that the virtual machine is connected to the DVD drive where you insert the software media. Do not connect a virtual machine to the ESXi server DVD drive if the properties of the Backup and Recovery (BAR) virtual machine show that it is set up to use the ESXi server’s DVD drive as a SCSI Device. See “Connecting and Disconnecting a Drive or ISO For Loading Files to a Virtual Machine” in the *Virtual Management Server Software* manual for information about connecting DVD drives to virtual machines in ASTRO® 25 system.

Procedure:

- 1 Log on to the NM Client using the credentials for your account that is a member of the Active Directory group for logging on to this device.

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

- 2 Launch the vSphere client by double-clicking the **VMware vSphere Client** icon on the desktop, and connect to the ESXi server.

See “Logging On to the VMware vSphere Client” and “Viewing ESXi Server and Virtual Machines” in the *Virtual Management Server Software* manual.

- 3 Insert the *Motorola Windows Server* media into the CD/DVD drive of the NM Client.

- 4 Connect to the local CD/DVD drive where you inserted the *Motorola Windows Server* media.

See “Connecting and Disconnecting a Drive or ISO For Loading Files to a Virtual Machine” in the *Virtual Management Server Software* manual.

- 5 From the vSphere client **File** menu, select **Deploy OVF Template**.

- 6 In the **Deploy OVF Template** window, click **Browse** and select the `Win2012r2-ovf-<xx.xx.xx.xxxx>.ovf` file located on the *Motorola Windows Server* media.

where `<xx.xx.xx.xxxx>` is the version number of the `ovf` file

The file name and path for the virtual machine you selected appear.

- 7 Click **Next**.

- 8 In the **OVF Template Details** window, click **Next**.

The **Name and Location** window appears.

- 9 In the **Name** field, enter the name of the AuC virtual machine. Click **Next**.

Step example: UCS-AUCSVR01

- 10 Optional: If a DAS device is implemented on your system and the **Datastore** window appears, enter: `z<zzz>das<xx>datastore1`

where:

`<zzz>` is the zone number from the IP plan

`<xx>` is the number of the DAS from the IP plan

If the **Datastore** window does not appear before the **Disk Format** window, no local hard drives are configured on the ESXi-based server.

- 11 Select **Thick Provision Eager Zeroed** and click **Next**.

The **Network Mapping** window appears.

- 12 From the drop-down menu, select **ucs0**, and then click **Next**.

The **Ready to Complete** window appears.

- 13 To start the deployment task, click **Finish**.

The AuC virtual machine deployment process begins, which takes up to several minutes, followed by a confirmation message.

- 14 Click **Close**.

- 15 Apply supplemental configuration to the AuC server virtual machine.

See "Applying Supplemental Configuration to Virtual Machines" in the *Virtual Management Server Software* manual.

- 16 Only for systems with vCenter already installed:** Configure a newly deployed VM to run properly in an existing vCenter environment. See [Configuring the vCenter for the Newly Deployed VM on page 43](#).
- 17** Configure the AuC virtual machine:
- a** Configure the AuC Virtual Machine resources.
See [Configuring Virtual Machine Resources on page 44](#).
 - b** Apply OS-level identity on the AuC Server.
See [Applying OS-Level Identity on the Primary/Backup AuC Server on page 45](#).
- 18** Set the AuC virtual machine startup and shutdown order.
See “Setting the Virtual Machine Startup and Shutdown Order” in the *Virtual Management Server Software* manual.
- 19** Upgrade the VMware tools on the virtual machine.
See “Reconfiguring VMware Tools on a Windows-Based Virtual Machine” in the *Virtual Management Server Software* manual.
- 20** Optional: Create a snapshot of the AuC virtual machine:
- a** Power off the AuC virtual machine.
See “Turning Off an Individual Virtual Machine” in the *Virtual Management Server Software* manual.
 - b** In the vSphere Client, right-click the newly deployed AuC virtual machine.
 - c** From the drop-down menu, select **Snapshot → Take Snapshot**.
 - d** In the **Take Virtual Machine Snapshot** dialog box, fill in the **Name** and **Description** fields. Click **OK**.
 - e** Power on the AuC virtual machine.
See “Turning On an Individual Virtual Machine” in the *Virtual Management Server Software* manual.

Related Links

[Installing the Radio Authentication Feature on page 40](#)

[Recovering the Authentication Center \(AuC\) Server on page 118](#)

3.3.1

Configuring the vCenter for the Newly Deployed VM

For newly deployed virtual machines to run properly in an existing vCenter environment, you must override the default HA cluster settings and modify the restart priority for the new VMs. After a host failure, the VMs are restarted in the relative order determined by their restart priority.

When and where to use:

- This procedure applies only to systems where vCenter is installed.
- Run this procedure only if a VM OVF was deployed after the vCenter was originally configured.

Procedure:

- 1** Launch the Internet Explorer from a Windows-based device, such as the Network Management (NM) Client, or a service computer or laptop.
 - Connect to: `https://<vCenterIP>/vsphere-client`
 - Ignore or accept any warnings about the connection security or self-signed certificates.

- 2 In the dialog box, perform the following actions:
 - a Type in the user name `administrator@z00<Z>vcs<H>.zone<Z>`
where `<Z>` is the zone number and `<H>` is the vCenter instance number
 - b Type in the administrator user password.
 - c Click **Login**.

The vSphere Web Client homepage appears.
- 3 In the left pane, click **Hosts and Clusters**.
- 4 Expand the tree and right-click the **Zone<x> HA** cluster
where `<x>` is the zone number.
- 5 Select **Settings**.
- 6 In the **Settings** window, click **VM Overrides**.
- 7 Click **Add**.
- 8 Click the **+** button.
- 9 Select the check box for the VM you are configuring. Click **OK**.
- 10 Depending on the VM you are configuring, perform the following actions:
 - For the vCenter VM, change the **VM Restart Priority** to **Medium**.
 - For the VMs that are monitored under Fault Tolerance, change the **VM Restart Priority** to **High**.
 - For the VMs that are not monitored under Fault Tolerance/HA, change the **VM Restart Priority** to **Disabled**.
- 11 Click **OK**.
- 12 **Perform the following actions only if you are recovering the VM after a failure and the VM is not monitored under Fault Tolerance:**
 - a In the **Settings** window, click **VM/Host Groups**.
 - b Select the group for the Virtual Management Server (VMS) on which the VM resides and click **Edit**.
 - c Click **Add**.
 - d Select the check box next to the VM and click **OK**.
For information about the locations of virtual machines on the VMS and their configurations with regard to vCenter, see "Virtual Machine Locations for vCenter Configs" in the *ASTRO 25 vCenter Application Setup and Operations Guide*.
 - e Click **OK**.

The restart priority setting for the newly deployed virtual machine is configured.

3.3.2

Configuring Virtual Machine Resources

Common OS-based Virtual Machines (VMs) require a device-specific resource profile to be applied to improve their performance and resource utilization of the ESXi Server.

You can change VM resource configuration by running the script that is part of the **Motorola VM Automation Tools** package on the *Windows Supplemental* media. To perform this procedure, use a Windows-based device, such as the Network Management (NM) Client, or a service computer/laptop.

Prerequisites:

Obtain the *Motorola Windows Box Profile* media (provided by Motorola Solutions; contains initial setup for individual devices and initial configuration scripts; drivers for Windows client and server).

Install VMware PowerCLI on the Windows-based device. See "Installing VMware PowerCLI" in the *Virtual Management Server Software* manual.

Install **Motorola VM Automation Tools** on the Windows-based device. See the *Windows Supplemental Configuration Setup Guide*.

Ensure that the virtual machine is powered down.

Procedure:

- 1 Insert the *Motorola Windows Box Profile* media into the optical drive of the Windows-based device.
- 2 Open the PowerShell command prompt.
 - a From **Start**, click **Search**.
 - b In the search field, type: `powershell`
 - c Right-click **Windows PowerShell** and select **Run as administrator**.
 - d If the **User Account Control** window appears, click **Yes**.
If you are not logged on with an administrative account, enter the Administrator's credentials.
- 3 At the PowerShell prompt, enter:
`cd 'C:\Program Files\Motorola\Motorola VM Automation Tools\bin'`
- 4 At the PowerShell prompt, enter: `.\Execute_VM_Resource_Config.ps1`
- 5 At the `ESXi_IP` prompt, enter the IP address of the ESXi host.
- 6 At the `ESXi_acct` prompt, enter: `root`
- 7 At the `ESXi_password` prompt, enter the ESXi host password for the root account.
- 8 At the `VMName` prompt, enter the name of the virtual machine that you want to configure.
- 9 At the `VMResourceFile` prompt, enter the path to the `xml` file with resource configuration:
For the primary/backup Authentication Center (AuC) server:
`<cdrom>:\VM_Resource_Config\AuC_Resource.xml`
where `<cdrom>` is the drive letter, for example: `E:`
- 10 Verify that there are no error messages in the output of the script.
- 11 At the PowerShell prompt, enter: `exit`

3.3.3

Applying OS-Level Identity on the Primary/Backup AuC Server

Perform this procedure to apply Operating System (OS) configuration to the primary or backup AuC Server.

Prerequisites:

Obtain the *Motorola Windows Box Profile* media (provided by Motorola Solutions; contains initial setup for individual devices and initial configuration scripts; drivers for Windows client and server).

Procedure:

- 1 In the navigation pane of the **VMware vSphere Client** main window:
 - a In the left pane, select the AuC Server primary or backup virtual machine.
 - b Power it on, if needed.
 - c In the right pane, click the **Console** tab.
Wait for the desktop to appear.
The **Setup OS progress** window appears.
- 2 In the VM console window, if the **Waiting for Box Profile Disk on the DVD-Drive** prompt is displayed, click **Cancel** to close the automatic install.
The prompt closes after 2 minutes. The default profile is applied and a reboot occurs.
- 3 Mount the *Motorola Windows Box Profile* media.
The **Common OS Reconfigurator** launches automatically.
- 4 In the **Common OS Reconfigurator** attention window, at the **Do you want to configure computer and apply Box Profile** prompt, click **Yes**.
- 5 In the **Common OS Settings** window, **Computer Type** drop-down list, select **AuC Server** (in the primary or backup core, as needed).
- 6 In the **Astro Settings** area:
 - **For the primary AuC Server:** select the Zone ID value in the **Primary Collocated Zone ID** drop-down list.
 - **For the backup AuC Server:** select the Zone ID value in the **Backup Collocated Zone ID** drop-down list.
- 7 In the **Astro Settings** area, select the appropriate **Time Zone**.
- 8 Click **Execute**.
Ignore any messages about finding devices on the network.
- 9 Wait for OS reboot.
Ignore any messages about formatting the drive displayed during the reboot.

3.4

Installing the Primary/Backup AuC Server

Prerequisites:

Obtain the following media:

- *Authentication Center* DVD
- *Windows Supplemental* media
- *MOTOPATCH for Windows* DVD



IMPORTANT: As part of the AuC Server installation, the AuC Client application is also installed. Use this AuC Client for service purposes only. To install a standalone AuC Client, or an AuC Client cohabited on an NM Client, see [Installing the AuC Client on page 48](#).



NOTICE: Before performing any step that requires inserting software media, you need to make sure that the virtual machine is connected to the DVD drive where you insert the software media. Do not connect a virtual machine to the ESXi server's DVD drive if the properties of the Backup and Recovery (BAR) virtual machine show that it is set up to use the ESXi server's DVD drive as a SCSI Device. See "Connecting and Disconnecting a Drive or ISO For Loading Files to a Virtual Machine" in the *Virtual Management Server Software* manual for information about connecting DVD drives to virtual machines in ASTRO® 25 system.

Procedure:

- 1 Access the newly deployed AuC virtual machine. Power it on, if needed.
- 2 On the C:\ drive of the AuC virtual machine, create the `AuCInstall` folder.
- 3 Insert the *Authentication Center* DVD into the NM Client CD/DVD drive, and copy its contents to the C:\AuCInstall folder.
It may take up to several minutes.
- 4 Optional: Create a snapshot of the AuC virtual machine:
 - a Power off the AuC virtual machine.
See "Turning Off an Individual Virtual Machine" in the *Virtual Management Server Software* manual.
 - b In the vSphere Client, right-click the newly deployed AuC virtual machine.
 - c From the drop-down menu, select **Snapshot** → **Take Snapshot**.
 - d In the **Take Virtual Machine Snapshot** dialog box, fill in the **Name** and **Description** fields. Click **OK**.
 - e Power on the AuC virtual machine.
See "Turning On an Individual Virtual Machine" in the *Virtual Management Server Software* manual.
- 5 Launch the Command Prompt as the Administrator and perform the following actions:
 - a Enter: `C:\AuCInstall\precheck.bat`
 - b Verify if the operation finished successfully. Press any key to continue.
 - c Enter: `C:\AuCInstall\preupgrade.bat`
 - d Verify if the operation finished successfully. Press any key to continue.
 - e Enter: `C:\AuCInstall\terminate.bat`
 - f Verify if the operation finished successfully. Press any key to continue.
- 6 Install the Windows Supplemental components by using the `AUTHENTICATION_SERVER.xml` file.
See "Installing Components Located on the Windows Supplemental Media" in the *Windows Supplemental Configuration Setup Guide* manual.
- 7 If the Centralized Event Logging feature is implemented in your system, configure the Motorola Solutions Windows Logging Client.
See "Configuring Windows Event Logging Clients" in the *Centralized Event Logging* manual.
- 8 Perform the following actions:
 - a Launch the Command Prompt as the Administrator.
 - b Enter: `C:\AuCInstall\install.bat`
 - c Verify if the operation finished successfully. Press any key to continue.

9 Restart the OS and log on as the administrator.

If you log on to Windows with a local account, use the Windows administrator account (the default account name is `Administrator` for Windows Server 2012-based devices).

10 Perform the following actions:

a Launch the Command Prompt as the Administrator.

b Enter: `C:\AuCInstall\postinstall.bat`

c Verify if the operation finished successfully. Press any key to continue.

11 Optional: Perform “Managing Local Windows Accounts Using the Windows Supplemental Media” for the Authentication Center (AuC) Server, and any other procedures required by your organization from the *Windows Supplemental Configuration Setup Guide* manual.

12 Log on to Windows with a local administrator account.

If you log on to Windows with a local account, use the Windows administrator account (the default account name is `Administrator` for Windows Server 2012-based devices).

13 Join the AuC Server to the Active Directory (AD).

See “Joining and Rejoining a Windows-Based Device to an Active Directory Domain” in the *Authentication Services* manual.

14 Install the anti-malware software.

See “CSMS - Deploying McAfee Client Software to Anti-Malware Clients” in the *Core Security Management Server* manual.

15 Apply MOTOPATCH for Windows Server 2012 64-bit from Motorola Solutions.

See the `readme.txt` file on the *MOTOPATCH for Windows* DVD.

16 Configure SNMPv3 for the AuC Server.

See “Configuring USM User Security with the Windows Configuration Utility” in the *SNMPv3* manual.

17 Remove the `C:\AuCInstall` folder created in [step 2](#).

To log on to the AuC Client, see [Logging On to the AuC Client on page 75](#).

Related Links

[Installing the Radio Authentication Feature](#) on page 40

[Recovering the Authentication Center \(AuC\) Server](#) on page 118

3.5

Installing the AuC Client

Use this procedure to install an AuC Client application either on one of the following:

- A standalone machine
- A virtual machine
- An NM Client



IMPORTANT: An AuC Client application is also installed as part of the AuC Server installation. Use this AuC Client for service purposes only.

Prerequisites:

Obtain the following media:

- *Motorola Windows Box Profile* media (provided by Motorola Solutions; contains initial setup for individual devices and initial configuration scripts; drivers for Windows client and server)

- *Authentication Center Client* CD
- *Windows Supplemental* media
- *MOTOPATCH for Windows* DVD



IMPORTANT: If the AuC Client is installed on a standalone machine or on a virtual machine (not an NM Client), ensure that the following prerequisites are met:

- 1 The standalone AuC Client hardware is installed and connected to the zone core. For details, see the *Private Network Management Client* manual (as standalone AuC Clients and AuC Clients cohabited on an NM Client use the same Z420 or Z440 hardware platform).
- 2 Microsoft Windows 7 or Windows 10 (64-bit) operating system is installed on the standalone AuC Client hardware. For detailed procedures on installing Windows, see the *Private Network Management Client* manual.
- 3 The right NM Client profile is selected. See "Applying OS-Level Identity on the PNM Client" in the *Private Network Management Client* manual.

Procedure:

- 1 Log on to the OS using the administrator credentials.
If you log on to Windows with a local account, use the Windows administrator account (the account name set up by Motorola Solutions is `secmoto` for Windows 7 and Windows 10-based devices).
- 2 On the `C:\` drive, create the **AuCInstall** folder.
- 3 Insert the *Authentication Center Client* CD into the CD/DVD drive, and copy its contents to the **AuCInstall** folder.
- 4 Launch the Command Prompt as the Administrator:

If...	Then...
If your OS is Windows 7,	perform the following actions: <ol style="list-style-type: none"> a From Start, select All Programs → Accessories. b Right-click Command Prompt and select Run as administrator. c If prompted for administrator credentials or a confirmation, type the administrator credentials or click Yes.
If your OS is Windows 10,	perform the following actions: <ol style="list-style-type: none"> a Right-click Start and select Command Prompt (Admin). b If prompted for administrator credentials or a confirmation, type the administrator credentials or click Yes.

- 5 In the **Command Prompt** window, perform the following actions:
 - a Enter: `C:\AuCInstall\precheck.bat`
 - b Verify if the operation finished successfully. Press any key to continue.
 - c Enter: `C:\AuCInstall\preupgrade.bat`
 - d Verify if the operation finished successfully. Press any key to continue.
 - e Enter: `C:\AuCInstall\terminate.bat`
 - f Verify if the operation finished successfully. Press any key to continue.

- 6 Install the Windows Supplemental components by using the `AUTHENTICATION_CLIENT.xml` file. See “Installing Components Located on the Windows Supplemental Media” in the *Windows Supplemental Configuration Setup Guide*.
- 7 Install the Motorola Solutions Windows Logging Client by using the `Motorola Windows Logging Client.xml` file, if this feature is implemented in your system. See “Installing Components Located on the Windows Supplemental Media” in the *Windows Supplemental Configuration Setup Guide*.

On an AuC Client cohabited on an NM Client, this component may already be installed.

- 8 Perform the following actions:

- a Launch the Command Prompt as the Administrator.
- b Enter: `C:\AuCInstall\install.bat`
- c Verify if the operation finished successfully. Press any key to continue.

- 9 Restart the OS and log on as the administrator.

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

- 10 Perform the following actions:

- a Launch the Command Prompt as the Administrator.
- b Enter: `C:\AuCInstall\postinstall.bat`
- c Verify if the operation finished successfully. Press any key to continue.

- 11 Optional: Perform “Managing Local Windows Accounts Using the Windows Supplemental Media”, and any other procedures required by your organization from the *Windows Supplemental Configuration Setup Guide*.

- 12 Join the AuC Client to the Active Directory (AD). See “Joining and Rejoining a Windows-Based Device to an Active Directory Domain” in the *Authentication Services* manual.

- 13 **For a standalone AuC Client installation only:** Install the anti-malware software. See “CSMS - Deploying McAfee Client Software to Anti-Malware Clients” in the *Core Security Management Server* manual.

- 14 Perform one of the following actions:

- If you are installing a standalone AuC Client, apply MOTOPATCH for Windows 7 or Windows 10 from Motorola Solutions. See the `readme.txt` file on the *MOTOPATCH for Windows DVD*.
- If you are installing an AuC Client cohabited on an NM Client, go to [step 12](#).

- 15 Remove the `C:\AuCInstall` folder created in [step 2](#).

To log on to the AuC Client, see [Logging On to the AuC Client on page 75](#).

Related Links

[Installing the Radio Authentication Feature](#) on page 40

[Recovering the Authentication Center \(AuC\) Server](#) on page 118

[Recovering the Authentication Center \(AuC\) Client Cohabited on NM Client](#) on page 119

[Recovering the Standalone Authentication Center \(AuC\) Client](#) on page 119

Chapter 4

Radio Authentication Configuration

There are several configuration procedures relating to the Radio Authentication feature.

4.1

Configuring the Primary AuC Server

When and where to use: Use this procedure to configure the primary AuC Server by using the AuC Client application. The AuC Client installed with the primary AuC Server should be used for service purposes only. Otherwise, use either a standalone AuC Client, or an AuC Client cohabited on an NM Client.

Process:

- 1 Log on to the AuC Client application as the administrator using the initial AuC user name and password.
See [Logging On to the AuC Client on page 75](#).
When prompted for a password change, enter and confirm the new password.
- 2 Add a new user with required privileges.
See [Adding an AuC User on page 77](#).
The added user needs to have at least the Master Key Load and Server Management permission. It is possible to create a user with all permissions.
- 3 Exit the AuC Client.
See [Exiting the AuC Client Application on page 79](#).
- 4 Log back on to the AuC Client using the new user credentials.
See [Logging On to the AuC Client on page 75](#).
After the initial logging on using the new user credentials, you are prompted to change the password. Enter the new password and click **OK**.
- 5 Set the Master Key in the AuC Client.
See [Setting the Master Key on the Active AuC on page 88](#).
- 6 Switch the primary AuC Server into the Operational state.
See [Changing the AuC Server Operating State on page 78](#).

Postrequisites: To verify whether the primary AuC Server was installed successfully, start the AuC Client and see if it is connected to the primary AuC Server.

Related Links

[Installing the Radio Authentication Feature on page 40](#)

4.2

Configuring the Backup AuC Server

Use this procedure to configure the backup AuC Server by using the AuC Client application.

Process:

- 1 Log on to the host machine where the backup AuC Server application is located.
See [Logging On to the AuC Client on page 75](#).
- 2 Set the Master Key in the AuC Client.
See [Setting the Master Key on the Standby AuC on page 89](#).

Postrequisites: To verify whether the backup AuC Server was configured successfully:

- 1 On the desktop, right-click the **Configuration Console** icon and select **Run as administrator**. If prompted for administrator credentials or a confirmation, type the administrator credentials or click **Yes**.
- 2 In the Command Prompt, enter:
`coco auc status -details`
- 3 In the **Summary** column, ensure that **OK** displays in all rows.

4.3

Enabling Radio Authentication in the System

Process:

- 1 Indicate the AuC Server is present in the system. See [Setting AuC Server as Present in UNC on page 53](#).
- 2 Ensure that the system-wide authentication state is set to **Enabled**. See [Setting Radio Authentication System-Wide Status in UNC on page 53](#).
- 3 Log on to the AuC Client. See [Logging On to the AuC Client on page 75](#).
- 4 Add a KVL entry in the AuC Client and assign it an UKEK encryption key:
 - a Perform [Adding KVLs on page 86](#).
 - b Perform [Entering UKEK into KVL on page 92](#).
- 5 Create KVL operator user accounts in the Active Directory for VPN access from the KVL to the AuC Server. See “Adding User Accounts to a Domain” in the *Authentication Services* manual.
- 6 Create KVL-AuC VPN user accounts. See “KVL VPN Settings” in the *KVL 4000 Key Variable Loader Radio Authentication User Guide*.
- 7 Distribute Ki to all ZCs and verify KEK_m distribution:
 - a Ensure that the Zone Controllers are configured for SNMPv3. See “Configuring Zone Controllers for SNMPv3” in the *SNMPv3* manual.
 - b Perform [Distributing Ki on page 93](#).
 - c Perform [Viewing KEK_m and Ki Status in a Zone on page 92](#).
- 8 Discover the AuC Server(s) in the UEM. See “Discovering Groups of Network Elements” in the *Unified Event Manager* manual.
- 9 Configure the BAR Client on the AuC host machine to connect to the BAR server over SSH. See “Installing BAR Clients Through the Windows Install Framework Application” in the *Backup and Restore Services* manual.

- 10 Trigger the registration of the BAR client on the AuC Server host with the available data backup server. See “Registering and Enabling Windows-Based BAR Clients Manually” in the *Backup and Restore Services* manual.
- 11 For systems with the DSR feature, repeat [step 8](#) through [step 10](#) for the backup AuC Server in the backup core.

Related Links

[Installing the Radio Authentication Feature](#) on page 40

4.3.1

Setting AuC Server as Present in UNC

When and where to use: Follow these steps to set the AuC Server as present in the system by using the UNC application.

Procedure:

- 1 Log on to the Unified Network Configurator Wizard. See "Logging On and Installing the EMC Smarts Network Configuration Manager" in the *Unified Network Configurator* manual.
The UNC Wizard home page appears.
- 2 From the list of available wizards on the left side, select **System Configuration**.
The right side of the window is updated with the **System Configuration** form.
- 3 Under **Basic Configuration**, update the **Contains Radio Authentication Center** parameter to **Yes**. Click **Submit**.
VoyenceControl processes the update request and then audits all devices to assess whether their current configuration complies with the updates.
- 4 Approve the change:
 - a Log on to VoyenceControl. See "Logging On and Installing the EMC Smarts Network Configuration Manager" in the *Unified Network Configurator* manual.
The names EMC Smarts™ and VoyenceControl are used interchangeably for this product.
 - b From the **Tools** menu, select **Schedule Manager**.
 - c Select the job. In the **Schedule Manager** menu, select **Approve job**.



Related Links

[Enabling Radio Authentication in the System](#) on page 52

4.3.2

Setting Radio Authentication System-Wide Status in UNC

Procedure:

- 1  **CAUTION:** The Required setting should only be entered when all SUIDs have been provisioned for authentication. Otherwise, unprovisioned SUIDs will not be able to get on the system.
-  **IMPORTANT:** When in system-wide Authentication Required state, Radio IDs should be entered into the Provisioning Manager application before uploading K-SUID from KVL in order to avoid a potential 30 minute wait for system synchronizing the authentication key. This also applies when manually entering K-SUID into the AuC Client. For more information, see the *Provisioning Manager* manual.

Log on to the Unified Network Configurator Wizard. See “Logging On to the UNC Server Application with PuTTY” in the *Unified Network Configurator* manual.

The **UNC Wizard** home page appears.

- 2 From the list of available wizards on the left side, select **System Configuration**.

The right side of the window is updated with the **System Configuration** form.

- 3 Under **Basic Configuration**, use the **Radio Authentication State** drop-down box to set the desired Radio Authentication system-wide state. Click **Submit**.

By default, the radio authentication state is set to **Enabled**, regardless of AuC presence in the system.

VoyenceControl processes the update request and then audits all devices to assess whether their current configuration complies with the updates.

- 4 Approve the change:

- a Log on to VoyenceControl.

See “Logging On and Installing the EMC Smarts Network Configuration Manager” in the *Unified Network Configurator* manual.

The names EMC Smarts™ and VoyenceControl are used interchangeably for this product.

- b From the **Tools** menu, select **Schedule Manager**.

- c Select the job. In the **Schedule Manager** menu, select **Approve job**.

Related Links

[Enabling Radio Authentication in the System](#) on page 52

4.4

Firewall Configuration

Motorola Solutions provides the RNI-DMZ firewall configuration to allow traffic between the AuC Server and KVL 4000. For more information about firewalls, see the *Fortinet Firewall* manual.

4.5

Zone Controller Configuration

In order to configure the ZCs for radio authentication, a new SNMPv3 account called `MotoAuc` is created and needs to be configured with a passphrase for encryption and a passphrase for authentication. The `MotoAuc` account is used for providing the zone controller (ZC) with the infrastructure key (Ki) for radio authentication.

For more information on how to create and configure the account, see the *SNMPv3* manual.

4.6

Subscriber Unit Configuration

To authenticate, the subscriber units need to have proper firmware and have the Radio Authentication feature enabled. They will have to receive the authentication key (K) from the KVL, and this K needs to be known to the AuC Server.

For information about specific radios, refer to their respective user guides.

Chapter 5

Radio Authentication Optimization

No optimization of the Authentication Center (AuC) applications is necessary.

Chapter 6

Radio Authentication Screen Reference

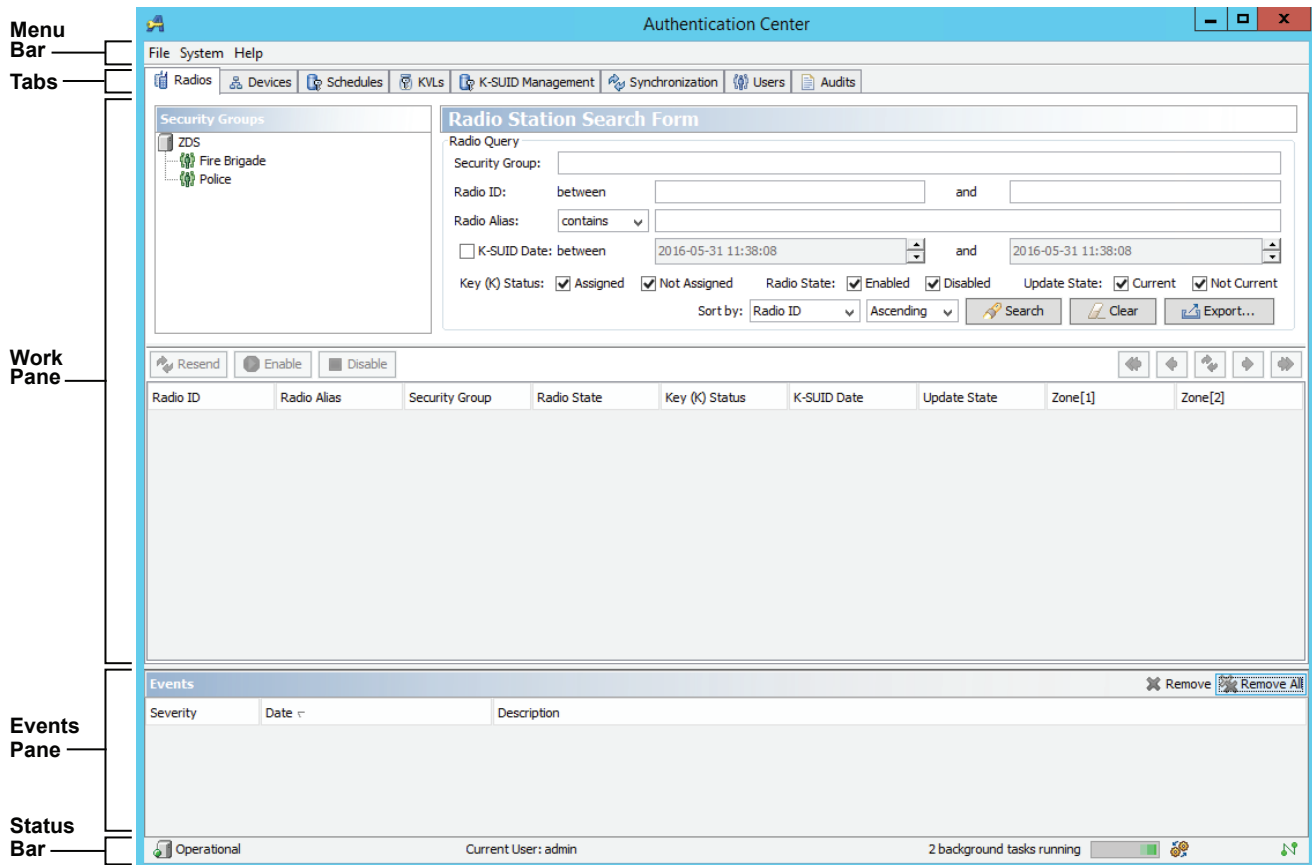
The Authentication Center (AuC) Client application consists of windows and dialog boxes through which you can perform Radio Authentication operations.

6.1

Main Window

The Authentication Center (AuC) Client application main window allows you to view status and perform tasks related to secure key management operations within the ASTRO® 25 system.

Figure 5: AuC Main Window



6.1.1

Menu Bar

The AuC Client application menu bar gives you access to the **Exit**, **System**, and **Help** drop-down sub-menus.

6.1.1.1

Backup Dialog Box

The **Backup** dialog box is accessible from the **System** menu and allows you to monitor and manage the AuC Server backup.

Table 7: Fields in the Backup Dialog Box

Field	Description
Backup in Progress	States whether an AuC Server backup is currently in progress (yes or no). During backup, you are still able to perform AuC operation. However, you are not able to start a new backup, until the current backup is complete. Once backup is initiated, it cannot be canceled.
Last Successful Backup	States when the last AuC Server backup occurred. The field displays No backups performed yet if no backup has been performed.
Path	Displays the current path for storing the AuC Server backup file. Default is D:\Motorola\Authentication Center Server\backup (on the D drive of the AuC Server virtual machine).

Table 8: Buttons in the Backup Dialog Box

Button	Action
Start Backup Now	Launches an immediate AuC Server backup.
OK	Saves the backup path.

6.1.2

Tabs Area

Clicking each tab accesses different functions of the AuC Client application. The following tabs are available:

- [Radios Tab on page 59](#)
- [Devices Tab on page 61](#)
- [Schedules Tab on page 63](#)
- [KVLs Tab on page 64](#)
- [K-SUID Management Tab on page 65](#)
- [Synchronization Tab on page 67](#)
- [Users Tab on page 68](#)
- [Audits Tab on page 70](#)
- [Restoring Tab on page 72](#)

6.1.3

Work Pane

The work pane displays content corresponding to the selected tab and the task you are performing in the Authentication Center (AuC) Client application. Acting as a container, the work pane allows you to switch among content selections using tabs.

6.1.4

Events Pane

The **Events** pane in the AuC Client application allows you to monitor actions and performance.



The AuC Client window allows you to view significant events that have occurred on the server since the user logged in. The displayed events provide a window into what is going on in the system (for example, to see if a link to a zone is down) as well as a visible confirmation of certain transactions occurring between the client and server. Some of the Event data is duplicated in the Audit Trail, and some of the data is unique to the Events area only. When the AuC window is launched, the Events Log displays the latest 300 server events. By default, new events are displayed at the top of the list, in the order they are received.

By default, events are listed as they occur (by Date). You can resort the listed events by clicking the column header. Clicking on a column header toggles the list items in forward and reverse order, respectively. A small triangle next to the column header indicates by which field the items are currently sorted.

Table 9: Fields in the Events Information Display

Field	Description
Severity	Severity of the event.
Description	Description of the event.
Date	Date of the event.

Table 10: Buttons in the Events Information Display

Button	Action
	Removes highlighted events from display.
	Removes all events from display.



6.1.5

Status Bar

The status bar provides information on the AuC Server state, name of the client current user, and various status icons.

The AuC state, AuC connection status, and name of the user logged on appears in the status bar to the left.

Table 11: AuC Server States of Operation

Icon	AuC Server Operating State	Description
	Operational	Normal operating mode.
	Out of Service	Non-operational mode. AuC Client user can only perform the following tasks: <ul style="list-style-type: none">• Loading a Master Key• All User Management tasks• Changing Authentication Center operating state







Icon	AuC Server Operating State	Description
	Encryption Failure	Missing or invalid Master Key.
	Database Restored	A sub-state of the Out of Service state.
	Database Failure	No connection between the AuC Server and the AuC Server database. Database Failure state is a sub-state of Out of Service state.

Table 12: AuC Server Connection Status Icons

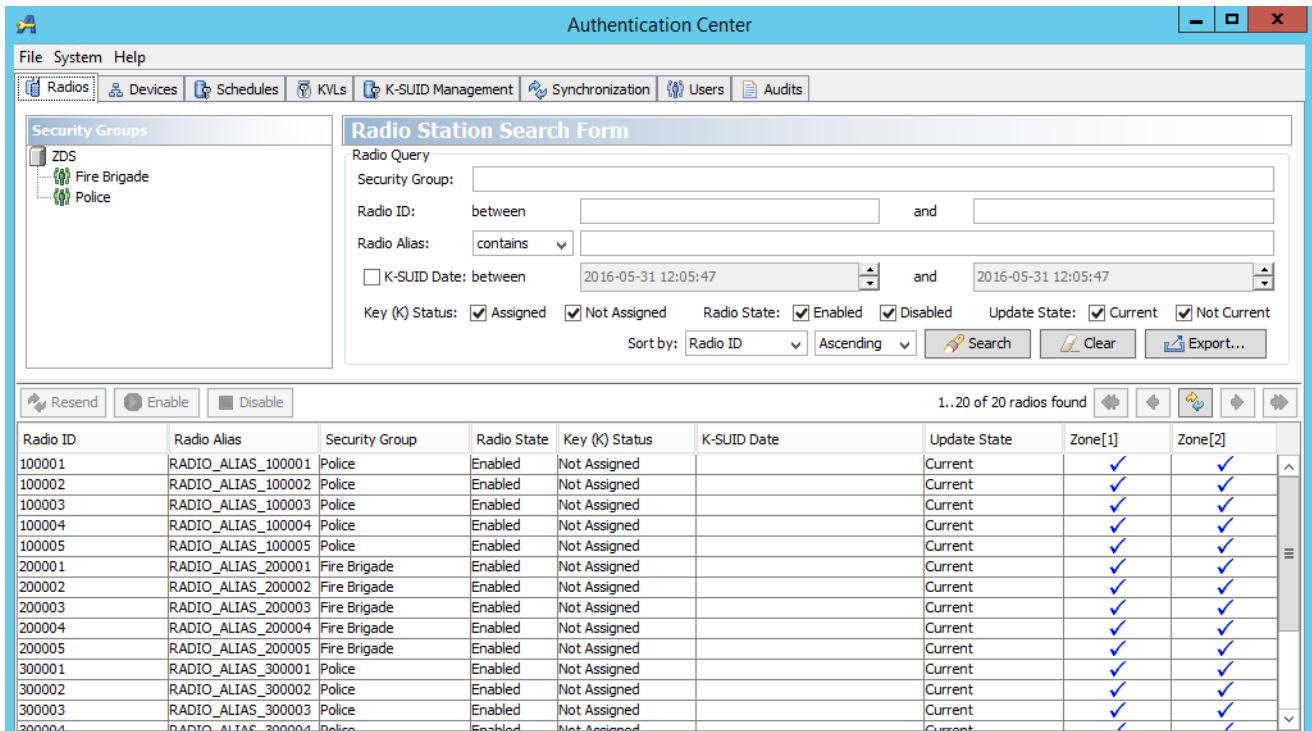
Icon	Description
	ADS is connected to the AuC Server.
	ADS is not connected to the AuC Server.
	A database backup is in progress.

6.2

Radios Tab

The **Radios** pane in the Authentication Center (AuC) allows you to monitor the authenticated subscriber units.

Figure 6: Radios Tab



Authentication Center

File System Help

Radios Devices Schedules KVLs K-SUID Management Synchronization Users Audits

Security Groups

- ZDS
 - Fire Brigade
 - Police

Radio Station Search Form

Radio Query

Security Group:

Radio ID: between and

Radio Alias: contains

☐ K-SUID Date: between and

Key (K) Status: ☒ Assigned ☒ Not Assigned Radio State: ☒ Enabled ☒ Disabled Update State: ☒ Current ☒ Not Current

Sort by: Radio ID Ascending Search Clear Export...

Resend Enable Disable

1..20 of 20 radios found

Radio ID	Radio Alias	Security Group	Radio State	Key (K) Status	K-SUID Date	Update State	Zone[1]	Zone[2]
100001	RADIO_ALIAS_100001	Police	Enabled	Not Assigned		Current	✓	✓
100002	RADIO_ALIAS_100002	Police	Enabled	Not Assigned		Current	✓	✓
100003	RADIO_ALIAS_100003	Police	Enabled	Not Assigned		Current	✓	✓
100004	RADIO_ALIAS_100004	Police	Enabled	Not Assigned		Current	✓	✓
100005	RADIO_ALIAS_100005	Police	Enabled	Not Assigned		Current	✓	✓
200001	RADIO_ALIAS_200001	Fire Brigade	Enabled	Not Assigned		Current	✓	✓
200002	RADIO_ALIAS_200002	Fire Brigade	Enabled	Not Assigned		Current	✓	✓
200003	RADIO_ALIAS_200003	Fire Brigade	Enabled	Not Assigned		Current	✓	✓
200004	RADIO_ALIAS_200004	Fire Brigade	Enabled	Not Assigned		Current	✓	✓
200005	RADIO_ALIAS_200005	Fire Brigade	Enabled	Not Assigned		Current	✓	✓
300001	RADIO_ALIAS_300001	Police	Enabled	Not Assigned		Current	✓	✓
300002	RADIO_ALIAS_300002	Police	Enabled	Not Assigned		Current	✓	✓
300003	RADIO_ALIAS_300003	Police	Enabled	Not Assigned		Current	✓	✓
300004	RADIO_ALIAS_300004	Police	Enabled	Not Assigned		Current	✓	✓

By default, query results are listed by Radio ID. You can resort the listed items by clicking the column header. Clicking on a column header toggles the list items in forward and reverse order, respectively. A small triangle next to the column header indicates by which field the items are currently sorted.

Table 13: Fields in the Radio Stations List Display


Field	Description
Radio ID	ID of the radio.
Radio Alias	Alias of the radio.
Security Group	Security group number the radio belongs to.
Radio State	State of the radio key update: Enabled Key updates enabled. New radios have the key updates enabled by default. Disabled (manually) Key updates disabled manually by a user. Disabled (K changed) Key updates disabled because the authentication key (K) for the SU has changed.
Key (K) Status	Indicates whether an authentication key (K) has been assigned to the radio station.
K-SUID Date	Creation date of a K-SUID pair assigned to the SU.
Update State	Shows whether the updates have been delivered to all zones or not (Current/Not Current).
Zone [1]	Shows the status of update delivery for each zone, whether the AuC received an update confirmation from the zone.  NOTICE: If the zone is disconnected, the field can show the update as not delivered.
Zone [2]	

Table 14: Buttons in the Radio Stations List Display

Buttons are disabled until an SU is selected from the list box.

Button	Action
Resend	Launches an immediate update of authentication material for the SUs highlighted in the list box.
Enable	Enables authentication material key updates for the SUs highlighted in the list box. Only displayed when key updates are disabled.
Disable	Disables authentication material key updates for the SUs highlighted in the list box. Only displayed when key updates are enabled.

6.2.1

Radio Station Search Form

In the **Radio Station Search Form** area, use the **Sort by** drop-down list to set how the radios are sorted.

Table 15: Fields in the Radio Station Search Form

Field	Description
Security Group	Security group to search.
Radio ID	Fields used to specify the ID range of radios (between X and Y).
Radio Alias	Fields used to search by radio alias.
K-SUID Date	Check the box to specify the time period when the radio was issued a K-SUID (between X and Y).
Key (K) Status	Check these boxes to search for radios with and/or without an assigned authentication key (K) in the AuC Server database.
Radio State	Check these boxes to search for radios with key updates enabled and/or for the radios with updates disabled.
Update State	Check these boxes to search for radios with current key updates and/or not current updates.

Table 16: Buttons in the Radio Station Search Form

Button	Action
Search	Performs search using selected criteria. Results are listed in the work pane below the search form.
Clear	Clears entries from search criteria fields.
Export	Creates and exports a <code>CSV</code> file with a list of exported subscriber units (according to the previously set search criteria).

6.3

Devices Tab

The **Devices** tab in the AuC Client application shows information about the zones, and the current key status.

Figure 7: Devices Tab

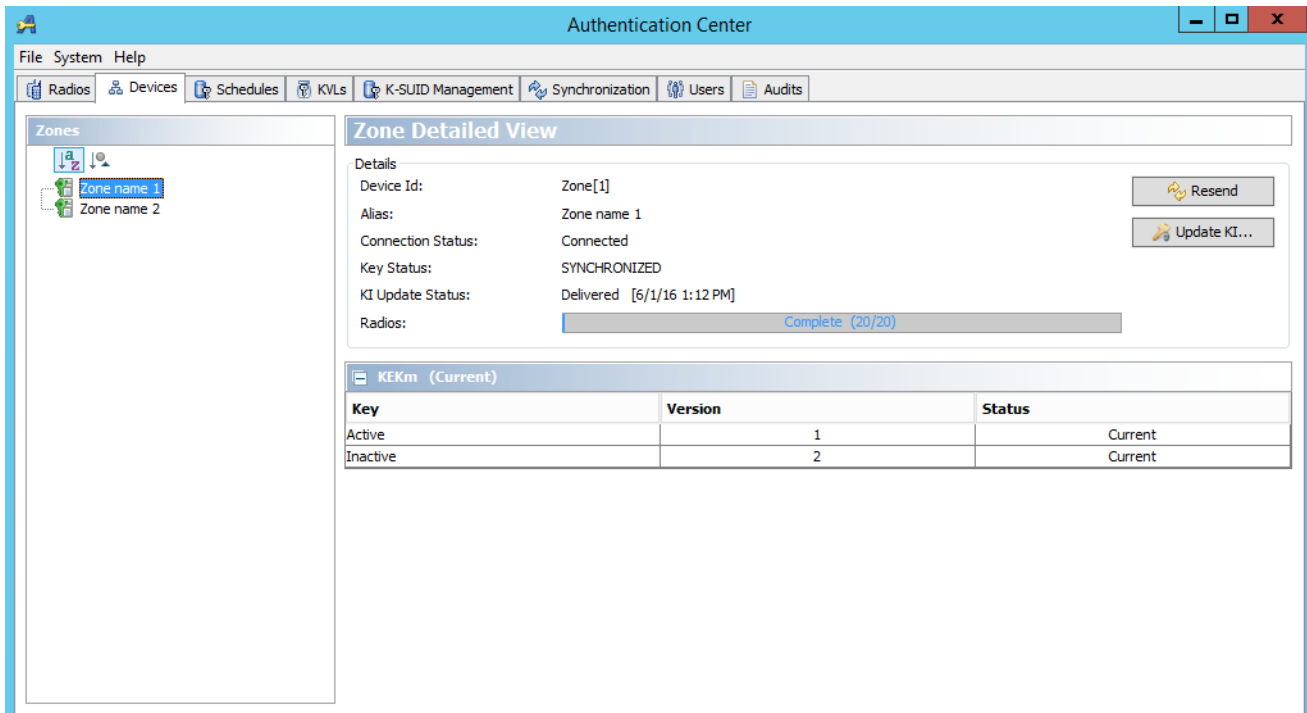


Table 17: Fields in the Zone Information Display

Field	Description
Device Id	Device identifier.
Alias	Device textual description.
Connection Status	<p>The status of connection to the Zone Controller (ZC):</p> <ul style="list-style-type: none"> Disconnected No Messaging – there is no connectivity to the ZC and no Connection Establish Request messages are received by the AuC Disconnected Wrong Ki – there is no connectivity to the ZC due to a wrong Ki Disconnected Missing Ki – there is no connectivity to the ZC due to a missing Ki in the AuC Disconnected Invalid Version – version negotiation with the ZC failed Connected
Key Status	<p>The status of keys in the zone:</p> <ul style="list-style-type: none"> Synchronized – ZC is synchronized with the current keys in the system (also indicated by the green key icon in the Zones pane) Not Synchronized – ZC is not synchronized with the current keys in the system (also indicated by the yellow key icon in the Zones pane) Blocked – key synchronization failed (also indicated by the red key icon in the Zones pane)
KI Update Status	The status of Ki, whether it has been delivered.
Radios	Progress bar showing what percentage of radios in the system had received updates.

Field	Description
KEKm	The table shows active and inactive KECm versions and their status.

Table 18: Buttons in the Zone Information Display

Button	Action
Resend	Sends all key information to the Zone Controller (ZC).
Update Ki	Assigns a new infrastructure key (Ki) to the ZCs.

6.4

Schedules Tab

The **Schedules** tab allows for scheduling key updates in the AuC Client application.

Figure 8: Schedules Tab

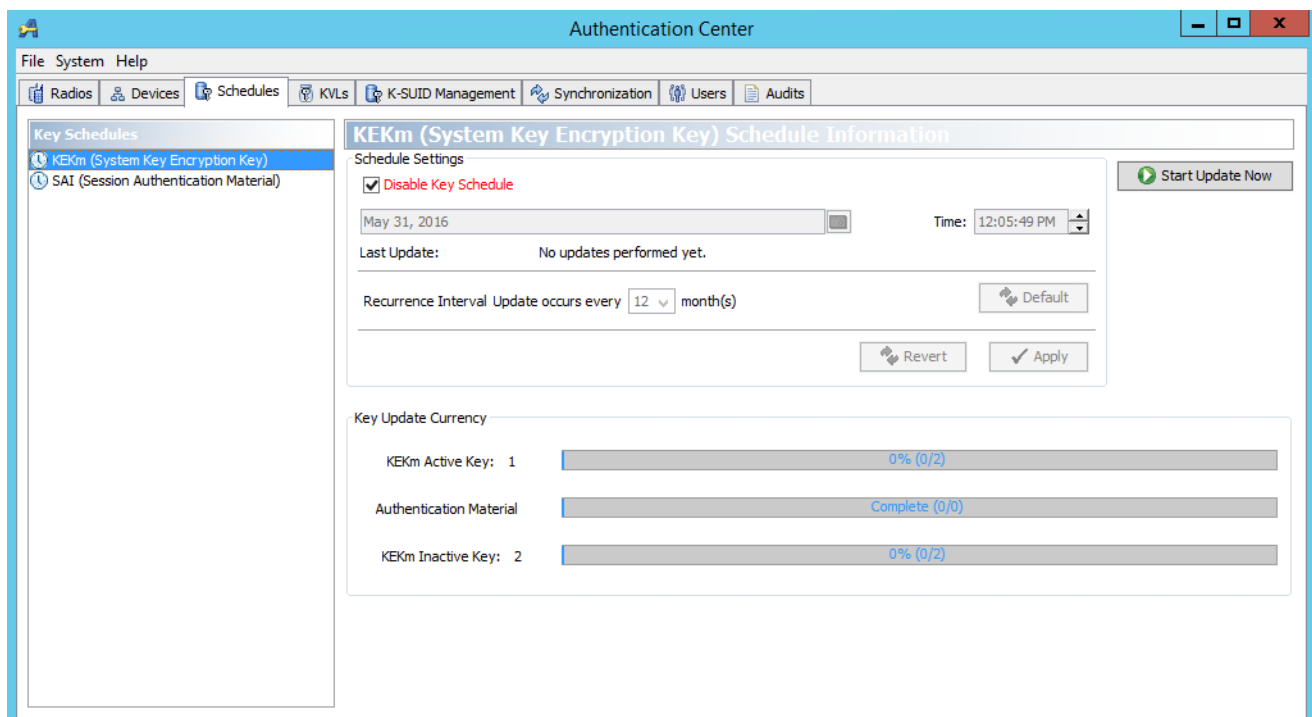


Table 19: Fields in the Key Schedule Information Display

Field	Description
Schedule Settings	Disable Key Schedule Selecting the check box disables key schedules and grays out other fields/buttons.
	Date Use the calendar icon to select the date of the next update.
	Time Use the small arrow icons to select the time of the next update.
Last Update	Shows the date and time when the last update was started.

Field	Description
Recurrence Interval Update	Shows the interval for the updates. The interval is shown in months or days, depending on the key type.

Table 20: Fields in the Key Update Currency Area

Field	Description
KEKm Active Key	Progress bar showing how many zones received the active KECm version (for example, 2/2).
Authentication Material	Progress bar showing how many enabled radios received SAI (the same progress bar is displayed when SAI is selected from the left-pane).
KEKm Inactive Key	Progress bar showing how many zones received the inactive KECm version (for example, 2/2).

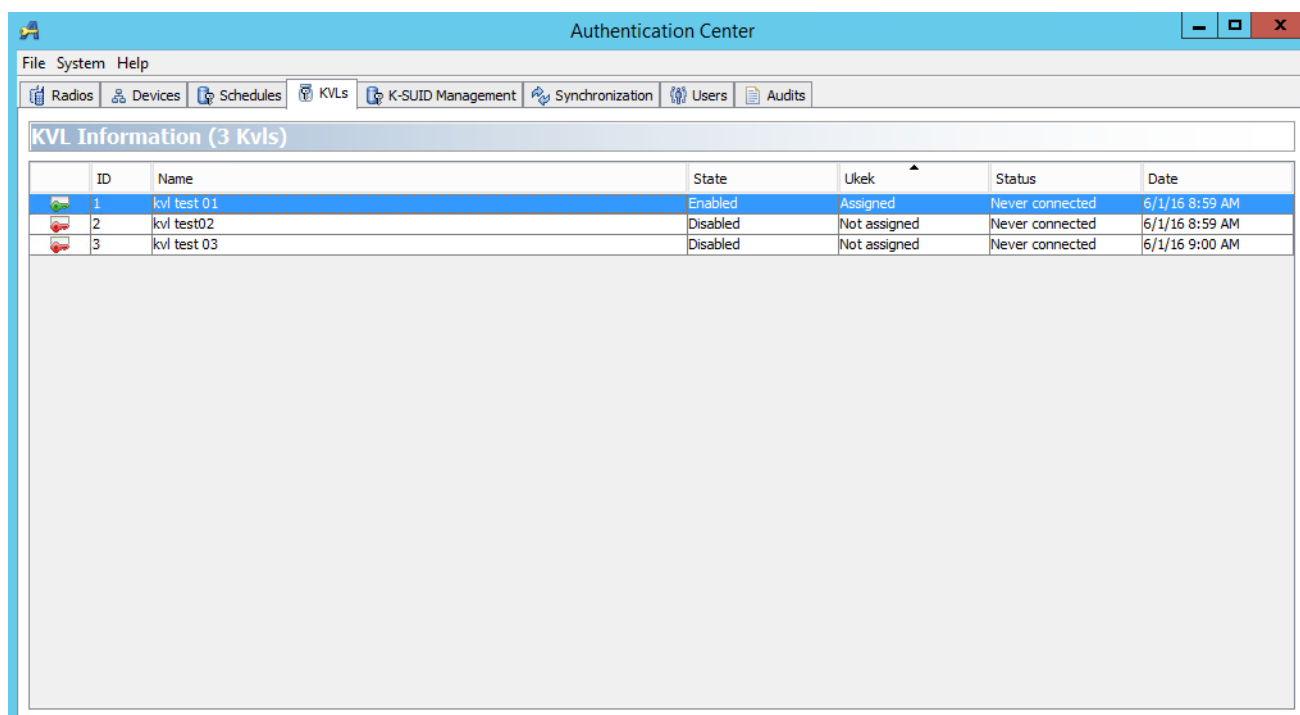
Table 21: Buttons in the Key Schedule Information Display

Button	Action
Start Update Now	Forces an update to start immediately. A manual update has no impact on the date and time of the next scheduled update.
Default	Resets to default updates interval (depends on the selected key type).
Revert	Reverts to previously set schedule.
Apply	Applies the schedule settings.

6.5

KVLs Tab

The **KVLs** tab in the AuC Client application allows you to add, remove, and edit KVLs in the system. It is also used for loading UKEK from the AuC to the KVL.

Figure 9: KVLs Tab**Table 22: Fields in the KVL Information Display**

Field	Description
ID	The ID of the KVL
Name	The name of the KVL.
State	The current setting for KVL access to AuC (enabled or disabled).
Ukek	Shows whether the UKEK has been assigned or not.
Status	Shows the KVL connection status from the last connection attempt (the KVL does not need to be connected at the moment, but if the last attempt was successful, the Status would be Successful).
Date	The date of the last KVL connection attempt.

Table 23: Key Status Icons (KVLs)

Icon	Description
Red	Locked out from AuC connectivity.
Yellow	Unprovisioned in the AuC Server database (does not have a UKEK key).
Green	Provisioned in the AuC Server database.

6.6

K-SUID Management Tab

The **K-SUID Management** tab allows for viewing and managing the K-SUID pairs in the AuC Client application.

Figure 10: K-SUID Management Tab

The screenshot shows the 'K-Suid Pairs' management window. The search criteria are set to: Type: All, WACN ID: 3, System ID: (empty), Radio ID: (empty), Provider: contains, Entry Date: between 2016-05-31 12:05 and 2016-06-30 12:00. The search results table shows 2 records found.

Type	WACN ID	System ID	Radio ID	Provider	Entry Date
unmatched	3	3	200006	admin	2016-06-01 09:04:27.733
matched	3	1	100001	admin	2016-06-01 09:09:32.671

6.6.1 K-SUID Query

Table 24: Fields in the K-SUID Query

Field	Description
Type	Use the drop-down menu to select one of the options: All All K-SUIDs will be displayed. Matched Only paired K-SUIDs will be displayed. Unmatched Only unmatched K-SUIDs will be displayed.
WACN ID	Specify the Wide Area Communications Network ID to limit the search (it is a wider identifier than System ID).
System ID	Specify the System ID to limit the search.
Radio ID	Specify the Radio ID to limit the search.
Provider	Use the drop-down menu to select one of the options: contains, equals, or begins with, and then enter the provider (either the operator or the KVL ID).
Entry Date	Check the box and enter the desired dates using the arrow buttons.

6.7

Synchronization Tab

The **Synchronization** tab allows you to synchronize the AuC Server with the ADS and check ADS current status. In the ASTRO® 25 system, the AuC Server does not synchronize with the UCS.

Figure 11: Synchronization Tab

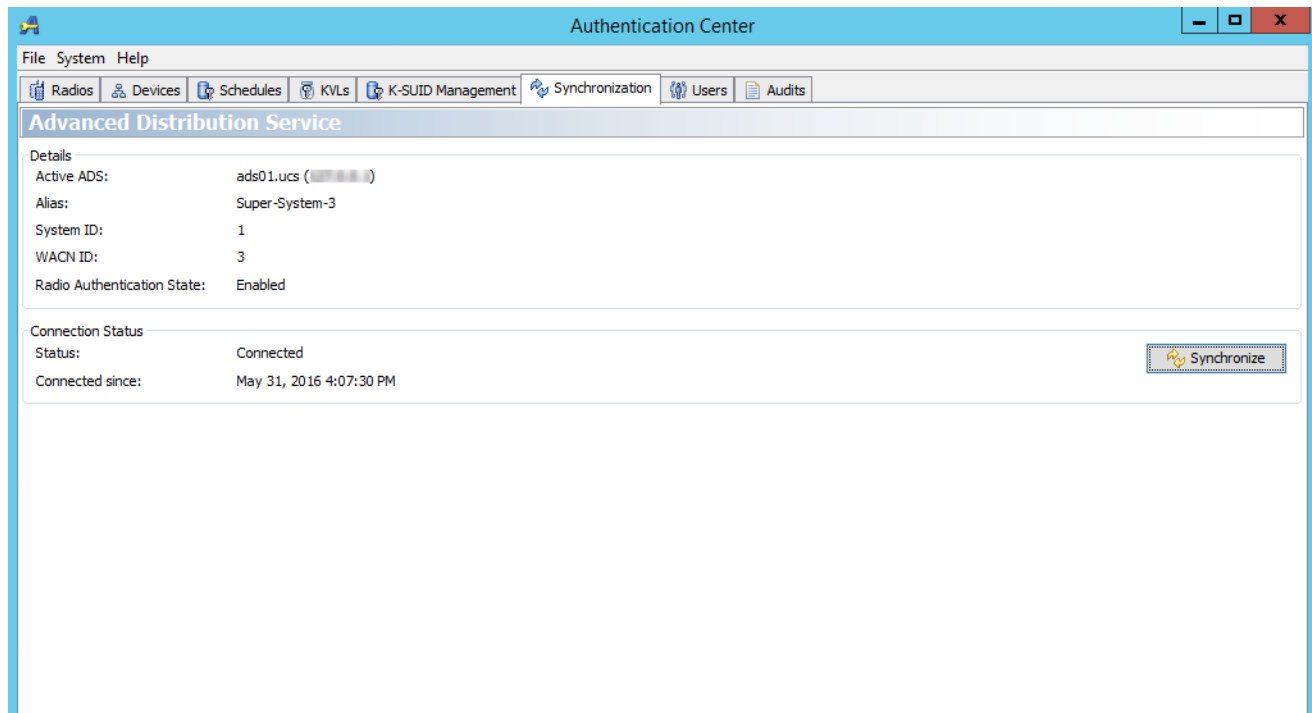


Table 25: Fields in the Synchronization Tab

Field	Description
Active ADS	The DNS address (and the IP address) of the ADS that the AuC Server is connected to.
Alias	Textual description of the system.
System ID	The ID of the system the AuC Server is in.
WACN ID	The ID of the Wide Area Communications Network the AuC Server is in.
Radio Authentication State	Shows whether radio authentication is enabled or disabled in the system.
Status	<p>Disconnected Unable to connect to the ADS from one of the following reasons:</p> <ul style="list-style-type: none"> • Application disabled • Communication failure • Authentication failure • Internal error <p>Synchronizing Synchronization with ADS is in progress.</p>

Field	Description
	Connected Connected and fully synchronized with the ADS.
Connected since	Shows since when the AuC Server is connected to the active ADS.

6.8

Users Tab


The **Users** tab in the AuC Client application allows you to create, modify, and delete AuC Client user accounts.



NOTICE: The AuC application has a pre-defined, initial user with User Management permissions only. The AuC does not allow deleting this user.

Figure 12: Users Tab

Table 26: Fields in the User Information Display

Field	Description
Login Name	Login name of the AuC user. This field allows use of spaces. Login names are case sensitive. Users are not allowed to modify their login name.
Full Name	Full name of the AuC user (optional).
Change Password	Enables New Password and Confirm New Password fields.  NOTICE: You cannot change your own password from this dialog box, when logged in as yourself, since User Management does not ask for the old password.
New Password	New password for the AuC user.

Field	Description
Confirm New Password	New password for the AuC user.
Permissions	Access permissions for the user to AuC tasks. Use the check boxes to select which task categories the user can access and perform. A user with no permissions is able to only view entity information.

Table 27: Access Permissions for AuC Users

Permission	Tasks
Infrastructure Management	Allows the user to disable zones, schedule all KEK updates and provisioning Ki.
Key Management	Allows the user to enter keys in the AuC and schedule KEKm updates.
KVL Management	Allows the user to modify KVL records, assign UKEK, disable/enable KVLs and set the KVL port.
Subscriber Management	Allows the user to manage the subscriber units and schedule all SAI updates.
Master Key Management	Allows the user to load the Master Key.
Server Management	Allows the user to change the AuC Server settings using the System menu.
User Management	Allows the user to manage user accounts and purge audit trail.
Database Management	Allows the user to back up and restore the AuC Server.

Table 28: Buttons in the User Information Display

Button	Action
Restore Settings	Restores the user account information settings before current changes are committed to the AuC Server database.
Apply Settings	Commits the user account information settings to the AuC Server database.
Delete	Deletes the user account from the AuC Server database.
Add	Launches the Add User dialog box.

6.8.1

Add User Dialog Box

The **Add User** dialog box in the AuC Client application allows you to add AuC Client user accounts.

Figure 13: Add User Dialog Box

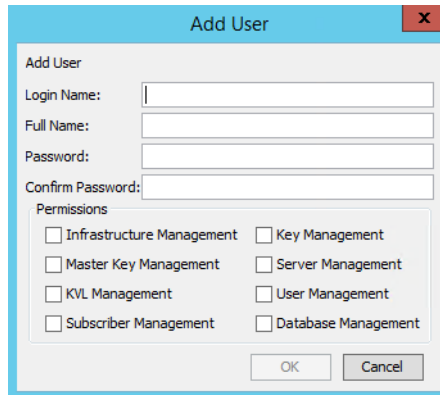


Table 29: Fields in the Add User Dialog Box

Field	Description
Login Name	Login name of the AuC user.
Full Name	Full name of the AuC user.
Password	New password of the AuC user.
Confirm Password	New password of the AuC user.
Permissions	See Table 27: Access Permissions for AuC Users on page 69 .

Table 30: Buttons in the Add User Dialog Box

Button	Action
OK	Commits user account information settings to the AuC Server database.
Cancel	Cancels user account information settings without committing them to the AuC Server database.

6.9

Audits Tab

The **Audits** tab in the AuC Client application allows you to monitor actions and performance of the AuC applications.

The AuC audit trail log stores a wide range of actions performed by the AuC. For example, the audit trail log maintains a record of all key management operations and allows you to "follow the life of a key" as it is distributed throughout the system. An audit of AuC operations can be viewed by specifying search criteria and viewing the query results in the AuC window. The data in the Audit trail sometimes overlaps with the data in the Event Log, but the Audit Trail data is in a more detailed format and is targeted for advanced users.

Figure 14: Audits Tab

The screenshot shows the 'Authentication Center' application window with the 'Audits' tab selected. The 'Audit Search & Purge Form' is displayed, featuring search criteria for Date (between 12:05:46 PM and 12:05:46 PM), User (empty), Entity Type (-All-), Key Type (-All-), Entity ID, and Key ID. Buttons for Search, Purge..., and Hide Form are on the right. Below the form is a table of audit events.

Date	Key Type	Key ID	Entity Type	Entity ID	User	Encryptin...	Encryptin...	Description
Jun 1, 2016 8:46:36 AM					admin			Removed user (user01)
Jun 1, 2016 8:46:36 AM					user01			User was removed by admin
Jun 1, 2016 8:44:00 AM					user01			Roles changed to [Database, Infrastructure, Key, KVL, M...
Jun 1, 2016 8:44:00 AM					admin			Changed roles to [Database, Infrastructure, Key, KVL, M...
Jun 1, 2016 8:43:59 AM					user01			Real name changed to Steve Johnson by admin
Jun 1, 2016 8:43:59 AM					admin			Changed real name to Steve Johnson for user (user01)
Jun 1, 2016 8:42:46 AM					admin			Created new user (user01)
Jun 1, 2016 8:42:46 AM					user01			User was created by admin
Jun 1, 2016 8:39:36 AM					user1moto			User was removed by admin
Jun 1, 2016 8:39:36 AM					admin			Removed user (user1moto)
Jun 1, 2016 8:39:25 AM					user1moto			User was created by admin
Jun 1, 2016 8:39:25 AM					admin			Created new user (user1moto)
Jun 1, 2016 8:23:38 AM					System			The AuC is unable to communicate with LM
Jun 1, 2016 8:23:38 AM					System			License audit started
Jun 1, 2016 7:23:38 AM					System			The AuC is unable to communicate with LM
Jun 1, 2016 7:23:38 AM					System			License audit started
Jun 1, 2016 6:23:38 AM					System			The AuC is unable to communicate with LM
Jun 1, 2016 6:23:38 AM					System			License audit started

6.9.1

Audit Search and Purge Form

Table 31: Fields in the Audit Search and Purge Form Display

Field	Description
Date between	Range of dates to search. Use spin boxes or manual entry to set beginning and ending time and date.
User	User login name to search.
Entity Type	Type of entity to search. Use drop-down list box to select entity type.
Entity ID	ID of entity to search.
Key Type	Type of key to search. Use drop-down list box to search key type.
Key ID	ID of key to search.

Table 32: Buttons in the Audit Search and Purge Form Display

Button	Action
Search	Performs search using selected criteria. Results are listed in the Audit Trail Information list box.
Hide Form	Removes Audit Trail Search Criteria fields from the window. Only displayed when fields are visible.
Purge	Opens the Purge Audit Trail dialog box. Removes all audits.
Show Search & Purge Form	Shows Audit Trail Search Criteria fields in the window. Only displayed when fields are invisible.

6.9.2

Audit Trail

The fields presented in the Audit Trail information display are listed below. By default, events are listed as they occurred (by Date). You can resort the listed events by clicking the column header. Clicking on a column header toggles the list items in forward and reverse order, respectively. A small triangle next to a column header indicates by which field the items are currently sorted.

Table 33: Fields in the Audit Trail Information Display

Field	Description
Date	Date of the event.
Key Type	Type of delivered key: Authentication Material, KEK _m
Key ID	ID of delivered key (assigned by AuC).
Entity Type	Type of entity: Database, SU, KVL.
Entity ID	ID of entity (assigned by AuC).
User	Login name of the user performing event task.
Encrypting Key Type	Type of the key used to encrypt delivered key for transport.
Encrypting Key ID	ID of the encryption key (assigned by AuC).
Description	Description of the event

6.10

Restoring Tab

The **Restoring** tab allows you to monitor and synchronize the active KEK_m version in zones with the inactive (or the future) version in the database. The two versions of KEK_m ensure that zone operation is not stopped when the keys are being updated.

Figure 15: Restoring Tab

NOTICE: The **Restoring** tab is only visible in the AuC Client application after the AuC Server database has been backed up and restored.

Authentication Center

File System Help

Restoring Radios Devices Schedules KVLs K-SUID Management Synchronization Users Audits

Database Restoring

KEKm Versions			
Name	Active	Inactive	Status
Backup	1	2	
Zone name 1	1	2	
Zone name 2	1	2	
New Keys (Recommended)	1	2	

Advanced Distribution Service
Current Status: Connected

☒ Wait until Advanced Distribution Service becomes connected.

Revert Enter KEM... Accept New Keys Accept Backup

Events

Severity	Date	Description
INFO	Jun 1, 2016 2:05:01 PM	Keys are current in the system.
INFO	Jun 1, 2016 2:04:58 PM	Zone[2] successfully connected.
INFO	Jun 1, 2016 2:04:58 PM	Zone[1] successfully connected.
INFO	Jun 1, 2016 2:04:57 PM	ADS connection restored.
CRITICAL	Jun 1, 2016 2:04:55 PM	Database has been restored
INFO	Jun 1, 2016 2:07:38 PM	Database backup started

Database Restored Current User: admin


Table 34: Restoration Tab Fields

Field	Description
KEKm Versions	Displays the following information about each zone: <ul style="list-style-type: none"> Zone name Active and inactive KEM versions in the zone Zone status (additionally, disconnected zones are marked with a red icon)
Advanced Distribution Service	Displays the status of the ADS.
Wait until Advanced Distribution Service becomes connected	Selecting the check box ensures that in order to accept new KEM versions in the system, the AuC needs to be connected to the ADS and the ZCs.



NOTICE: It is recommended to always have this check box selected.

Table 35: Restoring Tab Buttons

Button	Description
Revert	Restores KEK _m versions to the ones suggested by the AuC
Enter KEK_m	Opens a dialog box where the new KEK _m version can be entered.
Accept New Keys	Accepts the new KEK _m versions in the AuC and the zones (if a zone is not connected, the button is grayed out).
Accept Backup	<p>Sets the KEK_m versions from backup as the active ones. This is not recommended, as it can cause synchronization failures.</p> <p> IMPORTANT: Before accepting the backup, wait for all ZCs to be available. In some cases, such as ZC hardware failure, it is OK to accept the backup even when a zone is not available. If you do not know any of the active ZCs, wait until at least one ZC is available before accepting the backup.</p>

Chapter 7

Radio Authentication Operation

This chapter details tasks that you perform once the Radio Authentication feature is installed and operational on your system.

7.1

Logging On to the AuC Client

- Log on using your Active Directory account that is a member of the group with authority to perform the operations on the AuC Client. Contact your Active Directory administrator.
- To log on to the AuC Client machine, use an administrator account, or an account that is a member of the `auc-client-login` group.
- To start the AuC Client from the desktop, use an account that is a member of the `subsec` group.
- If you log on with local Windows administrator privileges, to start the AuC Client from the desktop, use an account that is a member of the `auc-client-app-local` group.
- To log on to the AuC Server machine, use an account that is a member of the `auc-server-login` group.
- To make SNMPv3 changes on the AuC Server, use an account that is a member of the `secadm` group.

Active Directory account login is recommended, if available. After a device joins the domain, its applications that have Roles Based Access Control in Active Directory will not be usable by the local Windows administrator for that device unless the administrator accesses the application by entering its executable path and filename at the Windows command line. The path and filename can be seen in the properties for the application desktop shortcut. Note that `motosec` is the local Windows administrator account set up by Motorola Solutions supplemental configuration for devices operating on Windows Server 2012; `secmoto` is the Windows administrator account set up by Motorola Solutions for Windows 7, and Windows 10-based devices.

Active Directory account login is necessary to start the AuC Client directly from the desktop. If Active Directory is not available, see [Starting AuC Client as the Local Windows Administrator on page 111](#).

Note that the following additional scenarios may occur while logging on to the AuC Client application:

- When logging on to the AuC Client for the first time after the installation, enter the initial account user name: `admin`, and the initial password. These credentials are only used for the initial login. A new user account with appropriate permissions needs to be created.
- When logging on to the AuC Client for the first time using a new user account, a password change is forced.
- When logging on to the AuC Client as a user who is already logged on (whose client session is already opened), an **Authentication Error** window appears with the following message:


User is already logged in from another AuC Client. Do you want to log in and terminate that session?

Selecting **Yes** results in terminating the other session of the same user from another AuC Client (informing the other session's user about it and closing the application after pressing **OK**). Selecting **No** brings back the **Authentication Center Login** dialog box.

- The maximum number of client sessions is 16. If this number is exceeded, an error window appears with the following message: Unable to login the user due to the maximum number of client sessions reached

When and where to use: Follow these steps to log on to the AuC Client application using your Active Directory account.

Procedure:

- 1 Depending on where the AuC Client is located, log on to the host machine:
 - If you are accessing an AuC Client which is either standalone or cohabited on the NM Client, log on to the AuC Client machine using your Active Directory account that is a member of the appropriate domain groups. If Active Directory is not available, see [Starting AuC Client as the Local Windows Administrator on page 111](#).
 - If you are accessing the AuC Client cohabited with the AuC Server, log on to the AuC Server machine using your Active Directory account that is a member of the appropriate domain groups. If Active Directory is not available, see [Starting AuC Client as the Local Windows Administrator on page 111](#).
- 2 On the desktop, double-click the **AuC Client**  icon.
The AuC splash screen appears. After a few seconds, the **Authentication Center Login** dialog box appears.
- 3 Enter the user name and password.
After three unsuccessful login attempts, the user account is locked out and needs to be unlocked by any user with the User Management privilege.
- 4 To enter the IP address of the AuC Server you want to connect to, click **Details**.
It is also possible to enter DNS name instead of the IP address of the AuC Server.
- 5 Click **OK**.
- 6 If prompted to change the password, perform the following actions:
 - a At the prompt, click **OK**.
 - b In the **Passwords** dialog box, enter the old password and the new password twice. Click **OK**.

Related Links

[Configuring the Primary AuC Server on page 51](#)
[Enabling Radio Authentication in the System on page 52](#)
[Recovering the Authentication Center \(AuC\) Server on page 118](#)

7.2

Unlocking a User Account

If a user enters an incorrect password three times in a row when logging on to the AuC Client, that user account is locked out and needs to be unlocked.

Procedure:

- 1 Log on to the AuC Client as a user with User Management permissions. See [Logging On to the AuC Client on page 75](#).
- 2 Select the **Users** tab.
- 3 From the left-pane, select the locked user account (the icon crossed-out in red).

- 4 Click **Unlock Account**.
- 5 To confirm, click **Yes**.

7.3

Adding an AuC User

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
To log on to the AuC Client for the first time, the default administrator user name and password are used and a new user needs to be added. Only the administrator or users with the User Management permission can add new users. See [Table 27: Access Permissions for AuC Users on page 69](#).
- 2 Select the **Users** tab.
- 3 Click **Add**.
- 4 Fill in the following fields:
 - Login Name
 - Full Name
 - Password
 - Confirm Password
- 5 Select the check boxes next to desired permissions. For details, see [Table 27: Access Permissions for AuC Users on page 69](#).
If a user is assigned no permissions, the AuC Client allows the user to access the AuC in a read-only mode. If a user is assigned multiple permissions, the AuC Client allows the user to perform all of the operations associated with each permission.
- 6 Click **OK**.
After the initial logging on with the new user account, you are prompted for a password change.

Related Links

[Configuring the Primary AuC Server on page 51](#)

7.4

Changing a User Password

When and where to use: Follow these steps to change the account password for the logged user only. To change other users passwords, see [Modifying a User Account on page 87](#).

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
- 2 From the **System** menu, select **Change Password**.
- 3 In the **Passwords** dialog box, enter the old password and the new password twice. Click **OK**.
- 4 Log on to the AuC Client application with the new password.

7.5

AuC Server Status Verification

Whenever you log on to the AuC Client, verify that the AuC Server is **Operational**. Verify that the **AuC Server Status** icon on the status bar in the bottom-left corner of the **AuC** window is green.

Table 36: AuC Server States

State Type	AuC State	Description
Enabled	Operational	The AuC is fully operational. Forced manually.
Disabled	Out of Service	Forced manually or automatically. Allows replacing the Master Key.
	Encryption Failure	Missing or invalid Master Key.
	Database Failed	Database communication problems, database corruption, or invalid database version.
	Database Restored	Database has been restored from backup.

Table 37: Operation - AuC Server State Dependencies

Operation/State	Operational	Out of Service	Encryption Failure	Database Failed	Database Restored
State Transitions	✓	✓	✗	✗	✗
Enter Master Key	✓	✓	✓	✗	✓
User Management	✓	✓	✓	✗	✓
KVL Management	✓	✗	✗	✗	✗
Subscriber Search	✓	✓	✓	✗	✓
Key Distribution	✓	✗	✗	✗	✗
Server Management	✓	✓	✓	✗	✓
Replace Master Key	✗	✓	✗	✗	✗

7.6

Changing the AuC Server Operating State

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
Only users with the Server Management permission can change the AuC operating state. See [Table 27: Access Permissions for AuC Users on page 69](#).
- 2 From the AuC Client menu bar, select **System**.
- 3 Perform one of the following actions:
 - If you want to force an operational AuC Server to go into the Out of Service state, from the **System** menu, select **Go Out of Service**.

- If you want to force a disabled AuC Server to go into the Operational state, from the **System** menu, select **Go Operational**. If the AuC Server was not successfully joined to domain, the `Go Operational` command might not work.

Related Links

[Configuring the Primary AuC Server](#) on page 51

7.7

Viewing the AuC Client Application Version Information

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
- 2 From the **Help** menu, select **About AuC**.
- 3 In the **About Authentication Center** dialog box, check the Server, Client, and Database build versions.
The Server and Client build versions should be the same.
- 4 When done, click **Close**.

7.8

Viewing Open-Source Licenses

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
- 2 From the **Help** menu, select **About AuC**.
- 3 In the **About Authentication Center** dialog box, click **Motorola Legal Notices**.
A `.txt` file with open-source licenses appears.
- 4 When done, close the `.txt` file.
- 5 In the **About Authentication Center** dialog box, click **Close**.

7.9

Exiting the AuC Client Application

Procedure:

- 1 From the **File** menu, select **Exit**.
- 2 In the **Exit** dialog box, click **Yes**.

Related Links

[Configuring the Primary AuC Server](#) on page 51

7.10

Displaying Zone Status Information

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
- 2 Select the **Devices** tab.

- 3 To view a specific zone, expand (if necessary) the tree view by clicking the plus icon next to each zone, then select the entity you want to view.

The key status for the selected zone is displayed in the work pane to the right.

7.11

AuC Server Settings Configuration

You can configure various AuC Server settings in the AuC Client application.

7.11.1

Enabling Debug Log Storing

The Debug Log can be stored and used for troubleshooting purposes.

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
Only users with the Server Management permission can enable/disable debug log. See [Table 27: Access Permissions for AuC Users on page 69](#).
- 2 From the **System** menu, select **Preferences**.
- 3 From the tree view in the left pane, select **Miscellaneous**.
- 4 To enable the storage of a debug log, select the **Debug Log Enabled** check box.
The information dialog box appears.
- 5 To close the dialog box, click **OK**.

7.11.2

Configuring User Name and Password Settings

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
Only users with the User Management permission can configure user name and password settings. See [Table 27: Access Permissions for AuC Users on page 69](#).
- 2 From the **System** menu, select **Preferences**.
- 3 In the tree view on the left, select **User Settings**.
- 4 Adjust all the restrictions you want applied to passwords. See [User Settings on page 80](#).
- 5 To save the settings, click **OK**.
If changing the user settings makes current passwords non-compliant, the impacted users will be asked to change their password next time they log on.

7.11.2.1

User Settings

Table 38: User Name and Password Settings

Field	Parameter	Description
Password Require-ments	Maximum Length	Enter the maximum password length (the default is 14).

Field	Parameter	Description
	Minimum Length	Enter the minimum password length (the default is 8).
	Passwords must contain at least one digit	Check if the password needs to contain at least one digit (enabled by default).
	Passwords must contain at least one upper case letter	Check if the password needs to contain at least one capitalized letter.
	Passwords must contain at least one non-alphanumeric character.	Check if the password needs to contain at least one character that does not contain the value of a number or a letter.
	Interval of days until passwords expire	Check to enable password expiry and enter after how many days they need to be changed (the default is 60 days).
User Name Requirements	Maximum Length	Enter the maximum user name length.
	Minimum Length	Enter the minimum user name length.
	Restore Default Settings	Click to restore the default settings.

7.11.3

Configuring KVL Ports

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
Only users with the KVL Management permission can configure KVL ports. See [Table 27: Access Permissions for AuC Users on page 69](#).
- 2 From the **System** menu, select **Preferences**.
- 3 In the tree view on the left, select the **KVL Settings** entity.
- 4 Set the **Port** and **Server ID**. Click **OK**.
The settings are stored in the AuC Server database.

7.12

Subscriber Unit Management and Monitoring

You can manage and monitor subscriber units in the AuC Client application.

7.12.1

Viewing Subscriber Information Using the Radio Station Search Form

Procedure:

- 1 Log on to the AuC Client application.
See [Logging On to the AuC Client on page 75](#).
- 2 Select the **Radios** tab.
- 3 In the **Radio Station Search Form** area in the upper part of the work pane, use the search criteria to limit the search.

See [Radio Station Search Form on page 61](#).

Any fields that are left empty are not included in the search.

- 4 Use the **Sort by** drop-down menu to set the order of displaying the radios in the work pane.

To clear the selected criteria, click **Clear**.

- 5 Click **Search**.

A list of radios is displayed in the work pane. Locate the appropriate radio in the list window for current key information. The radio's key information appears in the appropriate row in the list window.

- 6 If results take up multiple pages, use the navigation buttons in the upper-right corner of the work pane. To refresh the results, click **Refresh**.

7.12.2

Exporting Subscriber Units Using the Radio Station Search Form

Procedure:

- 1 Log on to the AuC Client application.
See [Logging On to the AuC Client on page 75](#).
- 2 Select the **Radios** tab.
- 3 Optional: In the **Radio Station Search Form** area, set the search criteria to limit the number of subscriber units to be exported.
See [Radio Station Search Form on page 61](#).
Any fields that are left empty are not included in the search.
- 4 Click **Export**.
- 5 In the **Save** window, name your file and choose the location where the file is to be saved. Click **Save**.
A successful message appears. Click **OK**.

7.12.3

Enabling or Disabling Radio Key Updates

Only enabled radios receive key updates. The system-wide **Required** and **Disabled** states override the individual disable setting in the AuC Client application. However, if the system-wide state is **Enabled**, individual disable is possible.


Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
Only users with the **Subscriber Management** permission can enable/disable individual radios. See [Table 27: Access Permissions for AuC Users on page 69](#).
- 2 Select the **Radios** tab.
- 3 Select the radios you want to enable/disable key updates for. To select multiple radios, perform one of the following actions:
 - To select a group of radios that are next to each other in the list box, click and drag the mouse over the selections (or hold down the **SHIFT** key and click each item you want to select).

- To select a group of radios that are not next to each other in the list box, hold down the **CTRL** key and click each item you want to select.

4 Perform one of the following actions:

If...	Then...
If you want to enable updates,	perform the following actions: a Click Enable . b Click Yes . A progress bar appears and updates for the selected radios are enabled.
If you want to disable updates,	perform the following actions: a Click Disable . b Click Yes . A progress bar appears and updates for the selected radios are disabled.

Postrequisites: After enabling/disabling the updates, the radios' view may be out of date. To bring it up to date, click .

7.13

Event Management

You can monitor and manage events in the AuC Client application.

7.13.1

Viewing Event Details

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
- 2 In the **Events** pane, double-click a selected event.
- 3 To close the dialog box, click **OK**.



7.13.2

Removing Events

When and where to use: Follow these steps to remove events from the AuC Client Events display.

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
- 2 From the **Events** pane in AuC Client window, select the appropriate events in the list box. To select multiple events, perform one of the following actions:
 - To select a group of events that are next to each other in the list box, click and drag the mouse over the selections (or hold down the **SHIFT** key and click each item you want to select).
 - To select a group of events that are not next to each other in the list box, hold down the **CTRL** key and click each item you want to select.
- 3 Perform one of the following actions:

- To remove an event or multiple events, click .
 - To remove all events, click .
- 4 In the confirmation dialog box, click **Yes**.

7.14

Audit Management

You can view and manage audits in the AuC Client application.

7.14.1

Viewing Audits

Procedure:

- 1 Log on to the AuC Client application.
See [Logging On to the AuC Client on page 75](#).
- 2 Select the **Audits** tab.
- 3 Define the search criteria using the fields in the **Audit Search & Purge Form**.
Any fields that are left empty are not included in the search.
- 4 Click **Search**.

The search results are displayed in the **Audit Trail Information** list box.

- 5 Double-click an audit to see its details.
- 6 Perform one of the following actions:
 - To close the **Event details** dialog box, click **OK**.
 - To remove the **Audit Search & Purge Form**, click **Hide Form**.

The **Hide/Show Form** button is a toggle button.

Step example: To remove the display when it is showing, click **Hide Form**. Once the display is hidden, the button state changes to **Show Form**.

7.14.2

Audit Purge and Removal

Since storage of audit trail data can grow rapidly, it is necessary to remove old audit trail data from the database. There are three types of possible removals:

- The audit trail can be purged from the database to an archive file stored at the same directory location as the database backup file.
- All audit trails can be deleted in one action.
- There is a task starting each day to verify if there are more than 3 million of audit trails. If so, the oldest audit trails are removed in order not to inflate the database.

7.14.2.1

Purging Audits Data from the AuC Server Database to an Archive File

Procedure:

- 1 Log on to the AuC Client application.
See [Logging On to the AuC Client on page 75](#).

Only users with the **Server Management** permission can purge/remove audits. See [Table 27: Access Permissions for AuC Users on page 69](#).

- 2 Select the **Audits** tab.
- 3 Define the appropriate search criteria using the fields in the **Audit Search & Purge Form**.
Any fields that are left empty are not included in the search.
- 4 Click **Purge**.
The **Purge Audit Trail** dialog box appears.
- 5 Select the date of data that you would like to purge using the calendar button.
The events prior to and including the specified date will be purged.
- 6 Click **Begin Purge**.
- 7 In the confirmation dialog box, click **OK**.

7.14.2.2

Removing Audits Data from the AuC Server Database

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
Only users with the **Server Management** permission can purge/remove audits. See [Table 27: Access Permissions for AuC Users on page 69](#).
- 2 Select the **Audits** tab.
- 3 Click **Clear All**.
- 4 In the confirmation dialog box, click **Yes**.

7.15

KVL Management and Monitoring

You can manage and monitor KVLs in the system in the AuC Client application.

7.15.1

Viewing KVL Status and UKEK Information

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
- 2 Select the **KVLs** tab.
- 3 On the **KVLs** list, select the KVL device.
The KVL current key status is reflected by the icon color and in the **Status** field:
 - If the key status icon is Green, the KVL is provisioned in the AuC Server database (Assigned).
 - If the key status icon is Yellow, the KVL is not provisioned in AuC Server database (Not Assigned).
 - If the key status icon is Red, the KVL is locked out from connectivity to AuC (Locked).

7.15.2

Adding KVLs

All KVLs that are used in the system need to be added manually in the AuC Client application.

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
Only AuC users with the **KVL Management** permission can add/remove KVLs. See [Table 27: Access Permissions for AuC Users on page 69](#).
- 2 Right-click anywhere in the **KVL Information** area.
- 3 From the pop-up menu, select **Add KVL**.
- 4 In the **Add KVL** dialog box, enter a unique ID and name of the KVL. Click **OK**.

Related Links

[Enabling Radio Authentication in the System on page 52](#)

7.15.3

Removing KVLs

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
Only AuC users with the **KVL Management** permission can add/remove KVLs. See [Table 27: Access Permissions for AuC Users on page 69](#).
- 2 Select the **KVLs** tab.
- 3 Select and right-click the KVL(s) you want to remove. To select multiple KVLs, perform one of the following actions:
 - To select a group of KVLs that are next to each other in the list box, click and drag the mouse over the selections (or hold down the **SHIFT** key and click each item you want to select).
 - To select a group of KVLs that are not next to each other in the list box, hold down the **CTRL** key and click each item you want to select.
- 4 From the pop-up menu, select **Remove KVL(s)**.
- 5 In the **Remove KVL** dialog box, click **Yes**.

7.15.4

Enabling and Disabling KVLs

To access the AuC Server, KVLs need to be enabled. Disabled KVLs are blocked from accessing the AuC Server.

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
Only AuC users with the **KVL Management** permission can add/remove KVLs. See [Table 27: Access Permissions for AuC Users on page 69](#).
- 2 Select the **KVLs** tab.
- 3 Select and right-click the KVL(s) you want to enable/disable. To select multiple KVLs, perform one of the following actions:
 - To select a group of KVLs that are next to each other in the list box, click and drag the mouse over the selections (or hold down the **SHIFT** key and click each item you want to select).

- To select a group of KVLs that are not next to each other in the list box, hold down the **CTRL** key and click each item you want to select.
- 4 From the pop-up menu, select **Enable** or **Disable**.
 - 5 If prompted to confirm, select **Yes**.

7.16

User Account Management

You can manage user accounts in the AuC Client application.

7.16.1

Creating a User Account

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
Only the AuC administrator or users with the **User Management** permission can add/remove users. See [Table 27: Access Permissions for AuC Users on page 69](#).
- 2 Select the **Users** tab.
- 3 Click **Add**.
- 4 In the **Add User** dialog box, enter the user profile information.
The logon name is case-sensitive. Spaces are allowed.
- 5 To set the user security permissions, select the appropriate check boxes.
For details, see [Table 27: Access Permissions for AuC Users on page 69](#).
- 6 Click **OK**.

7.16.2

Modifying a User Account

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
Only users with the **User Management** permission can add/remove users. See [Table 27: Access Permissions for AuC Users on page 69](#).
- 2 Select the **Users** tab.
- 3 From the **Users** pane, select the user account you want to modify.
The User Information for the selected user is displayed in the work pane.
- 4 Edit the user account settings:
 - To change the password for the selected user, select the **Change Password** check box and fill in the fields in the **Passwords** area. You cannot change your own password from this dialog box (when logged on as yourself). To change your own password, see [Changing a User Password on page 77](#).
 - To modify the permissions for the selected user, check the appropriate boxes in the **Permissions** area.
- 5 Click **Apply Settings**.

7.16.3

Deleting a User Account

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
Only users with the **User Management** permission can add/remove users. See [Table 27: Access Permissions for AuC Users on page 69](#).
- 2 Select the **Users** tab.
- 3 From the **Users** pane, select the user account you want to delete.
The User Information for the selected user is displayed in the work pane.
- 4 Click **Delete**.
- 5 To confirm, click **Yes**.

7.17

Synchronizing the AuC with ADS Manually

During the regular operation, synchronization with the Advanced Distribution Service (ADS) is performed automatically by the system. However, if the AuC is not fully synchronized with the ADS and the ADS status is connected, the synchronization process can be triggered manually.

Procedure:

- 1 Log on to the AuC Client application.
See [Logging On to the AuC Client on page 75](#).
Only users with the **Server Management** permission can manually synchronize AuC with ADS. See [Table 27: Access Permissions for AuC Users on page 69](#).
- 2 Select the **Synchronization** tab.
- 3 In the tree view in the left pane, select the appropriate zone icon.
The zone key status information appears.
- 4 Click **Synchronize**.
- 5 In the confirmation dialog box, click **Yes**.
The synchronization process begins. When the process is complete, the AuC is fully synchronized with the ADS.

7.18

Key Management

In the AuC Client application you can manage various key types.

7.18.1

Setting the Master Key on the Active AuC

Procedure:

- 1 Log on to the AuC Client application.
See [Logging On to the AuC Client on page 75](#).

Only users with the **Master Key Load** permission can set the Master Key. See [Table 27: Access Permissions for AuC Users on page 69](#).

- 2 From the **System** menu, select **Encryption Device**.
- 3 In the **Encryption Device** dialog box, click **Set Master Key**.
- 4 In the **Set Master Key** dialog box, type in the **<Master Key>** and click **OK**.

If the active AuC is configured correctly, it switches to the **Operational** state. Otherwise, it switches to the **Out-of-Service** state.

Related Links

[Configuring the Primary AuC Server on page 51](#)

[Recovering the Authentication Center \(AuC\) Server on page 118](#)


7.18.2

Setting the Master Key on the Standby AuC

Procedure:

- 1 In the Command Prompt, enter: `coco auc role active`
- 2 Enter: `y`

The AuC Services on the standby AuC Server are started and the startup type is set to **Automatic**.

- 3  **NOTICE:** Wait for at least a minute before continuing.

In the Command Prompt, enter: `coco auc status -details`

In the **Summary** column, ensure that **Disabled** and **Encryption Failure** messages display in the **AuC Application status** line.

- 4 Log on to the AuC Client application with the same user as in [Setting the Master Key on the Active AuC on page 88](#).

See [Logging On to the AuC Client on page 75](#).

Only users with the **Master Key Load** permission can set the Master Key. See [Table 27: Access Permissions for AuC Users on page 69](#).

- 5 From the **System** menu, select **Encryption Device**.
- 6 In the **Encryption Device** dialog box, click **Set Master Key**.
- 7 In the **Set Master Key** dialog box, type in the **<Master Key>** and click **OK**.

where **<Master Key>** is the same Master Key as in [step 4 of Setting the Master Key on the Active AuC on page 88](#).

- 8 In the Command Prompt, enter: `coco auc role standby`

7.18.3

Replacing the Master Key on the Primary AuC Server

If the Master Key was stolen or became public, it should be replaced immediately.

Procedure:

- 1 Log on to the AuC Client application.
See [Logging On to the AuC Client on page 75](#).

Only users with the **Master Key Load** and **Server Management** permissions can set the Master Key. See [Table 27: Access Permissions for AuC Users on page 69](#).


- 2 Set the AuC Server in the **Out-of-Service** state.
See [Changing the AuC Server Operating State on page 78](#).
- 3 From the **System** menu, select **Encryption Device**.
- 4 Click **Yes**.
- 5 In the **Replace Master Key** dialog box, enter the old and the new Master Key. Click **OK**.
An event is created, informing the user that the AuC Server needs to be restarted to finish the recrypting process.
- 6 Exit the AuC Client and restart the AuC Server service:
 - a From the **Start** menu, select **Control Panel**, **Administrative Tools**, and **Services**.
 - b Right-click the **Motorola Authentication Center** service, and select **Restart**.
The service is restarted.
- 7 Log back on to the AuC Client to finish the recrypting process.
The recrypting process can take up to several minutes and the progress is displayed on the AuC Client status bar. If stopped, recrypting does not resume, but starts from the beginning.
Once the recrypting process has finished, an event is created in the **Events** pane that the switchover from the old Master Key to the new one has been completed successfully.
- 8 Switch the AuC Server to the **Operational** state.
See [Changing the AuC Server Operating State on page 78](#).

Postrequisites: If you replace the Master Key on the primary AuC Server, you should also replace it on the backup AuC Server. See [Replacing the Master Key on the Backup AuC Server on page 90](#).

7.18.4

Replacing the Master Key on the Backup AuC Server

Procedure:

- 1 In the Command Prompt, enter: `coco auc role active`
- 2 Enter: `y`
The AuC Services on the standby AuC Server are started and the startup type is set to **Automatic**.
- 3  **NOTICE:** Wait for at least a minute before continuing.

In the Command Prompt, enter: `coco auc status -details`

In the **Summary** column, ensure that **Enabled** and **Reset** messages display in the AuC Application status line.
- 4 Log on to the AuC Client application with the same user as in [Setting the Master Key on the Active AuC on page 88](#).
See [Logging On to the AuC Client on page 75](#).
Only users with the **Master Key Load** permission can set the Master Key. See [Table 27: Access Permissions for AuC Users on page 69](#).
- 5 Set the AuC Server in the **Out-of-Service** state.

See [Changing the AuC Server Operating State on page 78](#).

- 6 From the **System** menu, select **Encryption Device**.
- 7 Click **Yes**.
- 8 In the **Replace Master Key** dialog box, enter the old and the new Master Key. Click **OK**.
An event is created, informing the user that the AuC Server needs to be restarted to finish the reencrypting process.
- 9 Exit the AuC Client and restart the AuC Server service:
 - a From the **Start** menu, select **Control Panel**, **Administrative Tools**, and **Services**.
 - b Right-click the **Motorola Authentication Center** service, and select **Restart**.
The service is restarted.

- 10 Log back on to the AuC Client to finish the reencrypting process.

The reencrypting process can take up to several minutes and the progress is displayed on the AuC Client status bar. If stopped, reencrypting does not resume, but starts from the beginning.

Once the reencrypting process has finished, an event is created in the **Events** pane that the switchover from the old Master Key to the new one has been completed successfully.

- 11 In the Command Prompt, enter: `coco auc role standby`

7.18.5

Viewing the Master Key Status

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
- 2 From the **System** menu, select **Encryption Device**.
- 3 In the **Encryption Device** dialog box, check the Master Key Status.
For a list of possible Master Key states, see [Master Key Statuses on page 91](#).

7.18.5.1

Master Key Statuses

Table 39: Master Key Statuses

Status	Description
Not Entered	The Master Key has not been entered in the AuC yet.
Valid	The Master Key verification passed.
Invalid	The Master Key verification failed.
Failed	One of the following scenarios occurred: <ul style="list-style-type: none"> The Master Key storage does not exist. The Master Key storage has wrong format. The AuC does not have access to the Master Key storage.



IMPORTANT: If the Master Key Status is **Failed**, contact Motorola Solutions for support.

7.18.6

Viewing KEKm and Ki Status in a Zone

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
- 2 Select the **Devices** tab.
- 3 From the **Zones** list in the left pane, select the zone you wish to view.
If KEKm and Ki keys are provisioned correctly, the Key Status is **Synchronized** and the zone icon in the left pane is green.
The **Zone Detailed View** for the selected zone is displayed in the work pane.

Related Links

[Enabling Radio Authentication in the System on page 52](#)

7.18.7

Entering UKEK into KVL

The AuC indicates on the **KVLs** tab that it is necessary to enter a Unique Key Encryption Key (UKEK) key for the KVL.

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
Only users with the **KVL Management** permission can set the UKEK key. See [Table 27: Access Permissions for AuC Users on page 69](#).
- 2 From the AuC Client main window, select the **KVLs** tab.
- 3 From the list in the KVL Information pane, right-click on the appropriate KVL.
A pop-up menu appears.
- 4 To assign a new UKEK key for the KVL, select **Assign New UKEK**.
The **KVL UKEK Assignment** dialog box appears.
- 5 In the **Key Value** fields, type the UKEK key. To see the digits, select the **Show Key Data** check box.
The UKEK entered must match the one stored in the KVL.
- 6 Click **OK**.
The key assignment is confirmed in the **Events** display.

Related Links

[Enabling Radio Authentication in the System on page 52](#)

7.18.8

Removing UKEK from KVL

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
Only users with the **KVL Management** permission can set the UKEK key. See [Table 27: Access Permissions for AuC Users on page 69](#).

- 2 From the AuC Client main window, select the **KVLs** tab.
- 3 From the list in the **KVL Information** pane, right-click on the appropriate KVL.
A pop-up menu appears.
- 4 From the menu, select **Remove UKEK(s)**.
- 5 In the confirmation dialog box, click **Yes**.

7.18.9

Distributing Ki

The Ki is generated by the AuC Client application, but you need to update the zone with it manually. Perform this procedure to update the Ki in a zone.

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
Only users with the **Infrastructure Management** permission can distribute Ki. See [Table 27: Access Permissions for AuC Users on page 69](#).
- 2 From the AuC Client main window, select the **Devices** tab.
- 3 From the Zones list in the left pane, select the zone you wish to distribute Ki for.
The Zone Detailed View for the selected zone is displayed in the work pane.
- 4 In the work pane, click **Update KI**.
The option to update Ki becomes available when the zone begins connecting to the AuC Server.
- 5 In the **Update Ki** dialog box, enter the Authentication Passphrase, the Encryption Passphrase and select the zone IP address. Click **OK**.
These SNMPv3 passphrases are the passphrases set up for the ZC in that zone. For details, see “Modifying User Passphrases for Zone Controllers” in the *SNMPv3* manual.
The Ki is provisioned to the selected zone.

Related Links

[Enabling Radio Authentication in the System](#) on page 52

7.18.10

Distributing KEKm

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
Only users with the **Key Management** permission can distribute KEKm. See [Table 27: Access Permissions for AuC Users on page 69](#).
- 2 From the AuC Client main window, select the **Schedules** tab.
- 3 From the Key Schedules list in the left pane, select **KEKm (System Key Encryption Key)**.
The KEKm Schedule Information is displayed in the work pane.
- 4 Click **Start Update Now**.
The update progress is displayed in the **Key Update Currency** area.

7.18.11

Distributing SAI

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
Only users with the **Subscriber Management** permission can distribute SAI. See [Table 27: Access Permissions for AuC Users on page 69](#).
- 2 From the AuC Client main window, select the **Schedules** tab.
- 3 From the Key Schedules list in the left pane, select **SAI (Session Authentication Material)**.
The SAI Schedule Information is displayed in the work pane.
- 4 Click **Start Update Now**.
Only one update at a time is possible.
The update progress is displayed in the **Key Update Currency** area.

7.18.12

K-SUID Management

K-SUID pairs can be entered either in the AuC Client application or using the KVL.

7.18.12.1

Performing a Search Using K-SUID Query

Procedure:

- 1 Log on to the AuC Client application.
See [Logging On to the AuC Client on page 75](#).
- 2 Select the **K-SUID Management** tab.
- 3 To limit the search criteria, use the parameters in the **K-SUID Query** area.
For information on the available criteria, see [K-SUID Query on page 66](#).
- 4 Click **Search**.
The search results are displayed in the work pane.

7.18.12.2

Entering Individual K-SUIDs Manually

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
Only users with the **Subscriber Management** permission can enter K-SUIDs. See [Table 27: Access Permissions for AuC Users on page 69](#).
- 2 From the AuC Client main window, select the **K-SUID Management** tab.
- 3 Click **Enter K-SUID**.
- 4 In the **New K-SUID Pair** dialog box, type in the K, and select the WACN, System, and Radio IDs. Click **Enter**.



7.18.12.3

Deleting K-SUIDs

You can delete matched and unmatched K-SUIDs in the AuC Client application.

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
Only users with the **Key Management** permission can delete K-SUIDs. See [Table 27: Access Permissions for AuC Users on page 69](#).
- 2 From the AuC Client main window, select the **K-SUID Management** tab.
- 3 To select search criteria, use the **K-SUID Query** field. Click **Search**. To search by date, select the **Entry Date** check box and select the time period.
The list of K-SUID pairs appears.
- 4 Perform one of the following actions:

If...	Then...
If you want to remove unmatched K-SUIDs,  NOTICE: Unmatched K-SUIDs can be removed as a group.	perform the following actions: a Click Remove Unmatched . b Click Yes .
If you want to remove matched K-SUID pairs,  NOTICE: Matched K-SUID pairs can be removed one at a time only.	perform the following actions: a Right-click the K-SUID pair you want to remove. b Select Remove K-SUID(s) . c Click Yes .

Postrequisites: If a K was erased while the ZC replication was in progress and the replication did not complete, this erase could be missed by the ZCs. This can lead to a valid SUID existing in the system without a K assigned (as it was erased). To alleviate this problem, resend the SUID clearout to all ZCs. See [Sending SUID Clearout on page 95](#)

7.18.12.4

Sending SUID Clearout

If a K was erased while the ZC replication was in progress, perform this procedure to resend SUID clearout to all ZCs for a selected radio.

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
Only users with the **Key Management** permission can delete K-SUIDs. See [Table 27: Access Permissions for AuC Users on page 69](#).
- 2 From the AuC Client main window, select the **Radios** tab.
- 3 From the list of radios, select the radio you want to send SUID clearout for.
You need to know which radios had their K erased.
- 4 Click **Resend**.
- 5 In the confirmation message, click **Yes**.
- 6 At the prompt to refresh the view, click **Yes**.

7.18.12.5

Deleting Unmatched K-SUIDs

If the K-SUID pairs are not matched to radios, you can delete them manually in the AuC Client application.

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
Only users with the **Key Management** permission can delete K-SUIDs. See [Table 27: Access Permissions for AuC Users on page 69](#).
- 2 Select the **K-SUID Management** tab.
- 3 Click **Remove unmatched**.
- 4 Click **Yes**.

All unmatched K-SUID pairs are removed from the system.

7.19

Dynamic System Resilience (DSR)

In systems with the DSR feature, you can perform the AuC Server switchover.



NOTICE:

If everything is working properly, perform [Switching Over AuCs on page 98](#).

In case of the active AuC outage or failure, perform [Switching Over From the Primary AuC Server to the Backup AuC Server on page 96](#).

7.19.1

Switching Over From the Primary AuC Server to the Backup AuC Server

Perform this procedure in case of the active AuC outage or failure.

Procedure:

- 1 Log on to the virtual machine hosting the backup AuC Server as the administrator.
- 2 On the desktop, right-click the **Configuration Console** icon and select **Run as administrator**.
If prompted for administrator credentials or a confirmation, type the administrator credentials or click **Yes**.
- 3 In the Command Prompt, enter: `coco auc role active`
The AuC Services on the backup AuC Server are started and the startup type is set to **Automatic**.

Postrequisites: When the backup AuC is used, the KVLs need to select the backup AuC instead of the primary one. See the *KVL 4000 Key Variable Loader Radio Authentication User Guide*.

7.19.2

Switching Over From the Backup AuC Server to the Primary AuC Server

Prerequisites:


Obtain the IP addresses from the IP plan or your system administrator.

Ensure the primary AuC Server has been fixed and it is switched off or its role is set to Standby.

Procedure:

- 1 Log on to the virtual machine hosting the backup AuC Server as the administrator.
- 2 Log on to the AuC Client by entering the IP address of the backup AuC Server in the **Server** field of the **AuC Login** dialog box.
- 3 Set the backup AuC Server to the **Out of Service** state. See [Changing the AuC Server Operating State on page 78](#).
- 4 Exit the AuC Client. See [Exiting the AuC Client Application on page 79](#).
- 5 On the desktop, right-click the **Configuration Console** icon and select **Run as administrator**. If prompted for administrator credentials or a confirmation, type the administrator credentials or click **Yes**.
- 6 In the Command Prompt, enter: `coco auc role standby`
The AuC Services on the backup AuC Server are stopped and the startup type is set to **Manual**.
- 7 Log on to the virtual machine hosting the primary AuC Server.
- 8 On the desktop, right-click the **Configuration Console** icon and select **Run as administrator**. If prompted for administrator credentials or a confirmation, type the administrator credentials or click **Yes**.
- 9 In the Command Prompt, enter: `coco auc role active`
The AuC Services on the primary AuC Server are started and the startup type is set to **Automatic**.
- 10 Log on to the AuC Client by entering the IP address of the primary AuC Server in the **Server** field of the **AuC Login** dialog box. See [Logging On to the AuC Client on page 75](#).
- 11 Perform one of the following actions:

If...	Then...
If there is no user with the Master Key Management privileges,	perform the following actions: <ul style="list-style-type: none">• Add a user with Master Key Management privileges. See Adding an AuC User on page 77.• Exit the AuC and log back on as the user you created.
If the user with the Master Key Management privileges already exists,	exit the AuC and log back on as the user with Master Key Management privileges.

- 12  **NOTICE:**
The following steps should be performed only when the Master Key was **not** set on both AuCs during configuration.

If the Master Key is not set, set the Master Key.

See [Setting the Master Key on the Active AuC on page 88](#).

Ensure that you set the same Master Key as the one that was used to encrypt the AuC Server database during the last backup.
- 13 Synchronize keys after restoring the AuC Server.
See [Synchronizing the AuC with ADS Manually on page 88](#).

Related Links

[Recovering the Authentication Center \(AuC\) Server](#) on page 118

7.19.3

Switching Over AuCs

Procedure:

- 1 Log on to the virtual machine hosting the primary AuC Server as the administrator.
- 2 Log on to the AuC Client by entering the IP address of the primary AuC Server in the **Server** field of the **AuC Login** dialog box.
- 3 Set the active AuC Server to the **Out of Service** state.
See [Changing the AuC Server Operating State](#) on page 78.
- 4 Exit the AuC Client.
See [Exiting the AuC Client Application](#) on page 79.
- 5 On the desktop, right-click the **Configuration Console** icon and select **Run as administrator**. If prompted for administrator credentials or a confirmation, type the administrator credentials or click **Yes**.
- 6 In the Command Prompt, enter: `coco rdm switchover`
The AuC Services on the primary AuC Server are stopped and the startup type is set to **Manual**.
- 7 Wait for up to five minutes for the synchronization to finish.
- 8 To verify, in the Command Prompt, enter: `coco rdm status`
The `SYNCHRONIZED` statuses appear.

7.19.4

Changing the Primary AuC Server Role to Standby

Procedure:

- 1 Log on to the virtual machine hosting the primary AuC Server as the administrator.
- 2 On the desktop, right-click the **Configuration Console** icon and select **Run as administrator**. If prompted for administrator credentials or a confirmation, type the administrator credentials or click **Yes**.
- 3 In the Command Prompt, enter: `coco auc role standby`

7.19.5

DSR ADS Configuration for AuC

The primary and backup Advanced Distribution Service (ADS) names on which the IP address is obtained from the DNS are configured automatically for each AuC during the installation. The default DNS values are:

AuC primary
ads01.ucs

AuC backup
ads02.ucs

In DSR configuration, the AuC allows for configuration of two time servers, one at the primary zone core and one at the backup zone core.

Chapter 8

Radio Authentication Maintenance

Radio Authentication maintenance involves AuC backup and restore, key updates, and embedded password management.

8.1

AuC Server Backup and Restore

The AuC Server maintains a storage of key material used for the authentication functions. The key material is stored in a database, encrypted using a Master Key supplied by the AuC. The correct Master Key must be used to read encryption keys from the AuC Server database. The AuC Server database not only stores copies of key material currently loaded in system entities, but also maintains a repository of new key material for future use.

8.1.1

AuC Server Backup

The AuC Server can be backed up in two ways:

- **Automatically** - through scheduled backups triggered by the BAR Server. By default, the BAR Client (which is installed by default with the AuC Server application) is doing the weekly update of the AuC Server. Additionally, archive all the data backed up to BAR offline on a weekly or a monthly basis. Only this form of archiving fully protects from a hardware failure. For more information, see the *Backup and Restore Services* manual.
- **Manually** - using the **Backup** option in the AuC Client application or using the Configuration Console. By default, the backup files are stored in the **D:\Motorola\Authentication Center Server\backup** folder. A manual backup does not protect from a hardware failure. It only protects against the AuC virtual machine failure.

When planning backups, consider the following factors:

- When provisioning an increased number of K-SUIDs, the AuC Server should be backed up daily and archived offline using the BAR Server.
- After provisioning an increased number of K-SUIDs, it is strongly advised to back up the AuC Server, and transfer the files onto DVDs to move them to a safe, off-site location.
- If the provisioning information was lost with no backup available, all of the subscribers would have to be re-provisioned.



IMPORTANT: The AuC operator needs to pay attention to AuC Server states when performing a backup. The restored authentication settings will be the same as they were when the last backup was performed, regardless of any changes happening afterwards. For example, any radios disabled after the last backup was performed, will show up as enabled when the AuC Server is restored.

8.1.1.1

Backing Up the AuC Server Using the AuC Client Application

Prerequisites: Only users with the **Database Management** permission can perform a backup. See [Table 27: Access Permissions for AuC Users on page 69](#).

Procedure:

- 1 Log on to the AuC Client application.
See [Logging On to the AuC Client on page 75](#).
- 2 From the **System** menu, select **Backup**.
- 3 Click **Start Backup Now**.
- 4 In the confirmation dialog box, click **Yes**.

The AuC Server backup starts. The backup file is created in D:\Motorola\Authentication Center Server\backup.

8.1.1.2

Backing Up the AuC Server Using the Configuration Console

Procedure:

- 1 Log on to the virtual machine hosting the AuC Server as the administrator.
- 2 On the desktop, right-click the **Configuration Console** icon and select **Run as administrator**.
If prompted for administrator credentials or a confirmation, type the administrator credentials or click **Yes**.
- 3 In the Command Prompt, enter:
`coco auc backup "D:\Motorola\Authentication Center Server\backup\<file_name>.zip"`
where: <file_name>.zip is the backup file created

8.1.2

AuC Server Restoration

The following methods of restoring the AuC Server are available:

- **Automatically** - by triggering the AuC restore on the BAR Server, provided the backup was performed earlier by the BAR Server. For a detailed procedure, see “Executing a BAR Client Data Restore” in the *Backup and Restore Services* manual. The backup files are automatically copied from the BAR Server to the C:\Restore folder on the AuC machine. The AuC service is stopped during the restore and restarted when it is finished. After the automatic restore is finished, perform [Completing the AuC Server Restoration Using the Configuration Console on page 101](#).
- **Manually** - using the Configuration Console. See [Restoring the AuC Server Using the Configuration Console on page 101](#).



IMPORTANT:

The AuC operator needs to pay attention to AuC states when performing a restore. The restored authentication settings will be the same as they were when the last backup was done, regardless of any changes happening afterwards. For example, any radios disabled after the last backup was done, will show up as enabled when the AuC Server is restored.

The AuC Server should be restored with the system-wide authentication state set to Enabled. If you want to restore the AuC Server while in Required system-wide authentication state, only attempt to do so if the backup was done also in the Required state, and otherwise set the Enabled state. See [Setting Radio Authentication System-Wide Status in UNC on page 53](#).

8.1.2.1

Restoring the AuC Server Using the Configuration Console



IMPORTANT: To complete this procedure, the AuC service will be stopped automatically until the restoration process is complete.

Procedure:

- 1 Log on to the AuC Server virtual machine as the administrator.
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 On the desktop, right-click the **Configuration Console** icon and select **Run as administrator**. If prompted for administrator credentials or a confirmation, type the administrator credentials or click **Yes**.
- 3 In the Command Prompt, enter: `coco auc restore "D:\<backup_path>"`
where: `<backup_path>` is the location of the latest backup file

Postrequisites: Complete the AuC Server restoration. See [Completing the AuC Server Restoration Using the Configuration Console on page 101](#).

Related Links

[Recovering the Authentication Center \(AuC\) Server on page 118](#)

8.1.2.2

Completing the AuC Server Restoration Using the Configuration Console








NOTICE: Only users with the **Database Management** permission can complete the restoration. See [Table 27: Access Permissions for AuC Users on page 69](#).

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
- 2 In the bottom-left corner of the AuC window, verify the AuC Server status. Perform one of the following actions:
 - If the AuC Server status is `Database Restored`, skip to [step 3](#).
 - If the AuC Server status is `Encryption Failure`, set the Master Key. See [Setting the Master Key on the Active AuC on page 88](#).
- 3 Select the **Restoring** tab.
- 4 Ensure that the **Wait until Zone Database Server becomes connected** check box is selected.
This setting is recommended by Motorola Solutions, so that all data can be monitored.
- 5 Perform one of the following actions:

If...	Then...
If the AuC Server has a connection to an active Zone Controller (ZC) and the KEKm versions are synchronized between the zone(s) and the AuC Server,	accept the KEKm versions from the backup as the active ones: <ol style="list-style-type: none"> a Select Accept Backup. b In the warning message, click Yes.

If...	Then...
 NOTICE: Motorola Solutions recommends waiting for at least one ZC to be available, before accepting KEKm versions.	<p>The backup KEKm versions are accepted.</p>
<p>If the AuC Server has a connection to an active ZC, the KEKm versions are not synchronized between the zone(s) and the AuC Server, and at least one zone has the <code>Zone is advanced status</code>,</p>  NOTICE: Motorola Solutions recommends waiting for at least one ZC to be available, before accepting KEKm versions. <p>The <code>Zone is advanced status</code> appears if the KEKm versions in a ZC are higher (but no more than by 10) than the KEKm versions in the AuC Server database.</p>	<p>synchronize the KEKm versions between the zone(s) and the AuC Server. Perform one of the following actions:</p> <ul style="list-style-type: none"> • If you want to use the KEKm versions calculated by the AuC, select Accept New Keys. • If you want to enter the KEKm version manually, perform the following actions: <ol style="list-style-type: none"> a Select Enter KEKm. b In the Enter KEKm dialog box, enter the new KEKm version number. Click OK. c Select Accept New Keys. <p>The AuC switches to the Operational state.</p>
<p>If the AuC Server has a connection to an active ZC, the KEKm versions are not synchronized between the zone(s) and the AuC Server, and no zones have the <code>Zone is advanced status</code>,</p>  NOTICE: Motorola Solutions recommends waiting for at least one ZC to be available, before accepting KEKm versions. <p>The <code>Zone is advanced status</code> appears if the KEKm versions in a ZC are higher (but no more than by 10) than the KEKm versions in the AuC Server database.</p>	<p>accept the KEKm versions from the backup as the active ones:</p> <ol style="list-style-type: none"> a Select Accept Backup. b In the warning message, click Yes. <p>The backup KEKm versions are accepted.</p>
<p>If no ZCs are available due to a known and prolonged issue (due to a link failure),</p>  IMPORTANT: This solution can potentially cause KEKm synchronization problems between the AuC and the ZCs once they become available. See Re-sending Keys to ZC on page 103 .  NOTICE: If there are no ZCs in the system (due to a major hardware failure), there are no other KEKm versions, so de-synchronization is not an issue.	<p>accept the KEKm versions from the backup as the active ones:</p> <ol style="list-style-type: none"> a Select Accept Backup. b In the warning message, click Yes. <p>The backup KEKm versions are accepted.</p>

Related Links

[Recovering the Authentication Center \(AuC\) Server](#) on page 118

8.1.2.3

Re-sending Keys to ZC

If the key versions between the AuC Server and the ZC got de-synchronized after database restoration, it is possible to manually synchronize them. This can happen in rare cases, such as a prolonged ZC failure, or a link failure. Perform this procedure to re-send keys to the zone in case the key versions got de-synchronized after database restoration.

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
Only users with the **Infrastructure Management** permission can distribute keys. See [Table 27: Access Permissions for AuC Users on page 69](#).
- 2 Select the **Devices** tab.
- 3 Select the zone you wish to re-send keys to in the left pane. Click **Resend**. Once the keys have been successfully resent, the status goes back to `SYNCHRONIZED`.

The Key status in the **Details** area changes to `UNSYNCHRONIZED` and the following event is created in the **Events** pane.

```
Starting forced synchronization for Zone[X] by user [Y].
```

Related Links

[Recovering the Authentication Center \(AuC\) Server](#) on page 118

8.1.2.4

AuC Server Restoration Caveats

When the AuC Server is restored, some of the operations that occurred after the backup may have been lost. The impact is based on the current system-wide authentication state. The AuC logs the system-wide authentication state changes it receives to the Centralized Logging Client. This table describes the impact of a lost operation and the way to resolve it.

Table 40: AuC Server Restore Caveats

Scenario	Impact	Resolution
Individual Enable is lost	An adversary SUID will be allowed on the system in system-wide Enabled state. Assumes K was good.	Check Syslog to find the impacted SUID. Individually enable the impacted SUID.
Individual Disable is lost	In the system-wide Enabled and Required states, SUID will fail authentication. Assumes K was bad.	Check Syslog to find the impacted SUID. Individually disable the impacted SUID.
Erase of K is lost	In the system-wide Enabled and Required states, SUID will fail authentication. Assumes SUID is still intended to use by the system and had a bad K.	Check Syslog to find the impacted SUIDs. Erase K again for these SUIDs. Provision K again for these SUIDs.

Scenario	Impact	Resolution
Provision of K is lost	In the system-wide Required state, SUID will not be allowed on the system. You have to provision the SUID again.	AuC operator checks to see which SU have not been provisioned. Use the system-wide Enabled state until all SUs are provisioned.
Change of K is lost	In the system-wide Enabled and Required states, SUID will fail authentication.	Check Syslog to find the impacted SUID. Individually disable the SUID to give more time to provision K again.

8.2

Updating Keys

This table describes the approximate ranges for the lifetime authentication keys and infrastructure keys supported by the system.

Table 41: Recommended Key Update Periods

Key Type	Minimum Period	Typical Period	Maximum Period
Authentication Key (K)	if compromised	lifetime of SU	lifetime of SU
Infrastructure Key (Ki)	if compromised	lifetime of ZC	lifetime of ZC
Authentication Material (SAI)	if compromised	6 months	12 months
System Key Encryption Key (KEKm)	if compromised	12 months	18 months

The procedures in this section apply to the following key-types:

- KECm
- SAI



IMPORTANT: After updating KECm, it is required to update SAI as well.

8.2.1

Scheduling Key Updates

Procedure:

- 1 Log on to the AuC Client application.
See [Logging On to the AuC Client on page 75](#).
Only users with the **Key Management** permission can perform key updates. See [Table 27: Access Permissions for AuC Users on page 69](#).
- 2 From the AuC main client window, select the **Schedules** tab.
- 3 In the **Key Schedules** list in the left pane, locate and click on the appropriate key.
The schedule information for the selected key appears in the work pane.

- 4 If not already cleared, clear the **Disable Key Schedules** check box.
The fields and buttons in the **Schedule Settings** area become available.
- 5 Set the key schedule:
 - a Select the schedule date using the calendar button.
 - b Set the schedule time by typing it in or using the arrow buttons next to the **Time** field.
 - c From the **Recurrence Interval Update** drop-down menu, select the recurrence interval.
Selected date and time must be greater than actual time plus 5 minutes.
- 6 Click **Apply**.
To go back to previous settings, click **Revert**.

8.2.2

Performing Immediate Key Updates

Procedure:

- 1 Log on to the AuC Client application. See [Logging On to the AuC Client on page 75](#).
Only users with the **Key Management** permission can perform key updates. See [Table 27: Access Permissions for AuC Users on page 69](#).
- 2 From the AuC main client window, select the **Schedules** tab.
- 3 From the **Key Schedules** list in the left pane, select the key type.
- 4 Click **Start Update Now**.
Starting a manual update has no impact on the date and time for the next scheduled update.
- 5 To confirm, click **Yes**.
The key update process starts.

8.3

Embedded Passwords

For more information on embedded passwords, see “Embedded Password Management” in the *Authentication Services* manual.

Table 42: Groups and Properties for Embedded Password Management

Group	Property	Value
ssl_server_group	ssl_server_account	Password used by the AuC Server to read SSL keystore/truststore for server (changed on the AuC Server).
ssl_client_group	ssl_client_account	Password used by all AuC clients (for example, AuC Client application, BAR Client) to read SSL keystore/truststore (changed on the AuC Client and AuC Server).

Group	Property	Value
server_db_group	server_db_account	Password for the AuC Server database user (changed on the AuC Server).
admin_db_group	admin_db_account	Password for the database used in Restore database (changed on the AuC Server).
ads_group	ads_account	Password for the Advanced Distribution Service (ADS)
rdm_auth_client_group	rdm_auth_client_account	Password for the Redundancy Manager Client (changed on the AuC Server).
rdm_auth_group	rdm_auth_account	Password used to authenticate the connection between the primary AuC and the backup AuC (changed on the AuC Server). Password must be: <ul style="list-style-type: none">• The same on both servers.• For DSR systems, set first on the primary AuC, and then on the backup AuC.
rdm_db_group	replicator_db_account	Password used to synchronize data in databases between the primary AuC and the backup AuC (changed on the AuC Server). Password must be: <ul style="list-style-type: none">• The same on both servers.• For DSR systems, set first on the primary AuC, and then on the backup AuC.
rdm_ssl_group	rdm_ssl_account	Password used by the Redundancy Manager to read SSL keystore/truststore (changed on the AuC Server).

8.4

Changing the AucUser Service Account Password (Operating System Account)

Change the **AucUser** service account password as required by your organization's policies. If you change the **AucUser** service account password, you must set the same password on the following services:

- **Motorola Authentication Center**
- **Motorola Authentication Center Resource Manager**

- **Motorola Authentication Center SNMP Agent**

Procedure:

- 1 On the desktop, select **Start** → **Control Panel**.
- 2 In the **All Control Panel Items** window, select **Administrative Tools**.
- 3 In the **Administrative Tools** window, select **Computer Management**.
- 4 In the **Computer Management (Local)** tree, select **System Tools** → **Local Users and Groups** → **Users**.
- 5 On the list, right-click **AucUser** and select **Set Password**.
- 6 On the warning message, select **Proceed**.
- 7 In the **Set Password for AucUser** dialog box, perform the following actions:
 - a In the **New password** field, enter the password.
 - b In the **Confirm password** field, re-enter the password.
 - c Click **OK**.
- 8 On the confirmation message, select **OK**.
- 9 In the **Computer Management (Local)** tree, select **Services and Applications** → **Services**.
- 10 On the **Services** list, right-click **<service name>** and select **Properties**.
where **<service name>** is one of the following services:
 - **Motorola Authentication Center**
 - **Motorola Authentication Center Resource Manager**
 - **Motorola Authentication Center SNMP Agent**
- 11 In the **<service name> Properties** dialog box, select the **Log On** tab, and perform the following actions:
 - a Ensure that the **This account** option is selected.
 - b In the **Password** field, enter the password.
 - c In the **Confirm password** field, re-enter the password.
 - d Select **Apply**.
- 12 In the **Services** dialog box, click **OK**.
- 13 In the **<service name> Properties** dialog box, click **OK**.
- 14 On the **Services** list, right-click **<service name>** and select **Restart**.
- 15 Repeat [step 10](#) through [step 14](#) for the remaining two services.

8.5

Changing the pguser Service Account Password

Change the **pguser** service account password as required by your organization's policies. If you change the **pguser** service account password, you need to set the same password on the **Motorola Redundancy Manager** service.

Procedure:

- 1 On the desktop, select **Start** → **Control Panel**.
- 2 In the **All Control Panel Items** window, select **Administrative Tools**.
- 3 In the **Administrative Tools** window, select **Computer Management**.

- 4 In the **Computer Management (Local)** tree, select **System Tools** → **Local Users and Groups** → **Users**.
- 5 On the list, right-click **pguser** and select **Set Password**.
- 6 On the warning message, select **Proceed**.
- 7 In the **Set Password for pguser** dialog box, perform the following actions:
 - a In the **New password** field, enter the password.
 - b In the **Confirm password** field, re-enter the password.
 - c Click **OK**.
- 8 On the confirmation message, select **OK**.
- 9 In the **Computer Management (Local)** tree, select **Services and Applications** → **Services**.
- 10 On the **Services** list, right-click **Motorola Redundancy Manager** and select **Properties**.
- 11 In the **Motorola Redundancy Manager Properties** dialog box, select the **Log On** tab, and perform the following actions:
 - a Ensure that the **This account** option is selected.
 - b In the **Password** field, enter the password.
 - c In the **Confirm password** field, re-enter the password.
 - d Select **Apply**.
- 12 In the **Services** dialog box, click **OK**.
- 13 In the **Motorola Redundancy Manager Properties** dialog box, click **OK**.
- 14 On the **Services** list, right-click **Motorola Redundancy Manager** and select **Restart**.
- 15 In the **Restart Other Services** dialog box, click **Yes**.

8.6

Changing the rdmuser Service Account Password

Change the **rdmuser** service account password as required by your organization's policies. If you change the **rdmuser** service account password, you need to set the same password on the **Motorola Redundancy Manager** service.

Procedure:

- 1 On the desktop, select **Start** → **Control Panel**.
- 2 In the **All Control Panel Items** window, select **Administrative Tools**.
- 3 In the **Administrative Tools** window, select **Computer Management**.
- 4 In the **Computer Management (Local)** tree, select **System Tools** → **Local Users and Groups** → **Users**.
- 5 On the list, right-click **rdmuser** and select **Set Password**.
- 6 On the warning message, select **Proceed**.
- 7 In the **Set Password for rdmuser** dialog box, perform the following actions:
 - a In the **New password** field, enter the password.
 - b In the **Confirm password** field, re-enter the password.
 - c Click **OK**.
- 8 On the confirmation message, select **OK**.
- 9 In the **Computer Management (Local)** tree, select **Services and Applications** → **Services**.

- 10** On the **Services** list, right-click **Motorola Redundancy Manager** and select **Properties**.
- 11** In the **Motorola Redundancy Manager Properties** dialog box, select the **Log On** tab, and perform the following actions:
 - a** Ensure that the **This account** option is selected.
 - b** In the **Password** field, enter the password.
 - c** In the **Confirm password** field, re-enter the password.
 - d** Select **Apply**.
- 12** In the **Services** dialog box, click **OK**.
- 13** In the **Motorola Redundancy Manager Properties** dialog box, click **OK**.
- 14** On the **Services** list, right-click **Motorola Redundancy Manager** and select **Restart**.
- 15** In the **Restart Other Services** dialog box, click **Yes**.

Chapter 9

Radio Authentication Troubleshooting

Troubleshooting information related to the Radio Authentication feature helps you react quickly in case you observe any issues.

9.1

AuC Server Does Not Go Operational

If the AuC Server cannot be switched to the Operational state after the installation, try changing the default KVL port, as it can sometimes cause a conflict. See [Configuring KVL Ports on page 81](#).

9.2

Logging On to the AuC Client Fails

If you try to log on to the AuC Client application and a message that the server is not available appears, check the Motorola Authentication Center service status. See [Checking the Motorola Authentication Center Service Status on page 110](#). If the service status is `Stopped`, contact your system administrator.

9.2.1

Checking the Motorola Authentication Center Service Status

Procedure:

- 1 Log on to the AuC Server virtual machine as the administrator.
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 On the desktop, right-click the **Configuration Console** icon and select **Run as administrator**.
If prompted for administrator credentials or a confirmation, type the administrator credentials or click **Yes**.
- 3 In the Command Prompt, enter: `coco auc status`
The service status appears.

9.3

Logging On to the AuC Client Application Fails in DSR Systems

For Dynamic System Resilience (DSR) systems, if you try to log on to the AuC Client application and a message that the server is not available appears, ensure that you are trying to connect to the currently active AuC Server and not to the standby AuC Server.

For more information about the DSR feature, see [Radio Authentication in DSR Systems on page 29](#).

9.4

Starting AuC Client as the Local Windows Administrator

After a device joins the domain, its applications that have Roles Based Access Control in Active Directory will not be usable by the local Windows administrator for that device unless the administrator accesses the application by entering its executable path and filename at the Windows command line. The path and filename can be seen in the properties for the application desktop shortcut.

If the Active Directory is unavailable, the administrator can launch the AuC Client locally using this procedure.

Procedure:

- 1 Depending on where the AuC Client is located, log on the host machine:
 - If you are accessing an AuC Client which is either standalone or cohabited on the NM Client, log on to Windows with a local account.
Use the Windows administrator account (the account name set up by Motorola Solutions is `secmoto` for Windows 7 and Windows 10-based devices).
 - If you are accessing the AuC Client cohabited with the AuC Server, 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 Depending on your OS, launch the Command Prompt as the Administrator:

If...	Then...
If your OS version is Windows 7,	perform the following actions: <ol style="list-style-type: none"> a From Start, select All Programs → Accessories. b Right-click Command Prompt, and select Run as administrator. c If prompted for administrator credentials or a confirmation, type the administrator credentials or click Yes.
If your OS version is Windows 10,	perform the following actions: <ol style="list-style-type: none"> a Right-click Start and select Command Prompt (Admin). b If prompted for administrator credentials or a confirmation, type the administrator credentials or click Yes.

- 3 In the Command Prompt, perform the following actions:
 - a Enter:
`C:\Program Files (x86)\Motorola\Authentication Center Client\client`
 - b Enter: `aucclient.exe`
 The AuC Client applications starts.

9.5

UEM Alarms

Table 43: UEM Alarms

This table lists common faults and how they are announced in the Unified Event Manager (UEM).

Fault	Description	UEM Alarm
Decryption failure	Upon a decryption failure of KS or KEKm, the Zone Controller subsystem sends an event to the Network Management subsystem indicating the decryption failure.	No alarm on UEM for SAI (KS), since there could be hundreds of them and that would disrupt the UEM. Alarm on UEM for KEKm.
Link to AuC failure	Upon a failure of the link between the Key Management subsystem and the ZC subsystem, the ZC subsystem sends an event to the NM subsystem indicating the link failure.	Alarm on UEM. Most of the time the ZC has SAI, so the link going down does not impact authentication.
Establishing a link to AuC	Upon link establishment between the Key Management subsystem and the ZC subsystem, the ZC subsystem sends an event to the NM subsystem indicating the link established.	Alarm on UEM. Most of the time the ZC has SAI so the link going down does not impact authentication.
Wrong response to challenge trap	Upon receiving the wrong response to a challenge, the ZC subsystem sends an event to the NM subsystem indicating authentication failed. This can mean a potential adversary attack, but it could also be a legitimate radio that has been incorrectly provisioned.	Alarm on UEM.
UEM critical data replication	Upon completion of all critical data replication, the Zone Controller subsystem sends an event to the NM subsystem indicating all data replication complete. Critical data replication triggers replication of non-critical data.	Alarm on UEM.
UEM non-critical data replication	Upon completion of all data replication, the ZC subsystem sends an event to the NM subsystem indicating all data replication complete. Non-critical data includes Ki, KEKm and SAI.	Alarm on UEM.

Table 44: UEM Alarms for AuC State Transitions

This table lists how AuC state transitions are shown in the UEM.

AuC State	UEM Managed Object State
Operational	enabled
Out of Service	disabled/(operatorCommand or reset)
Encryption Failure	disabled/encryptionFailure
Database Failure	disabled/databaseFailure
Database Restored	disabled/databaseRestore

Table 45: Zone Controller States

Connection Status	Key Status	UEM Managed Object State
Connected	SYNCHRONIZED	enabled/normal
	UNSYNCHRONIZED	enabled/synchronizing
	BLOCKED	critical malfunction/synchronization failure
Disconnected No Messaging		disabled/communication failure
Disconnected Wrong Ki		major malfunction/wrong Ki
Disconnected Missing Ki		major malfunction/missing Ki
Disconnected Invalid Version		major malfunction/invalid protocol version

Table 46: Advanced Distribution Service States

Status	Condition	UEM Managed Object State
Connected	Synchronization with ADS completed successfully	up/normal
Synchronizing		up/synchronizing
Disconnected	AuC Server is disabled or is in out of service state	down/application_disabled
	ADS is disconnected due to communication failure	down/communication_failure
	Synchronization with ADS failed due to invalid password	down/authentication_failure
	Synchronization with ADS is incomplete due to invalid entries	down/internal_failure

Table 47: Standby AuC States

Status	Condition	UEM Managed Object State
Connected	Standby AuC data is synchronized with Active AuC	synchronized/normal
Unsynchronized	The synchronization mechanism is starting up	unsynchronized/initializing
	Wrong synchronization configuration	unsynchronized/invalid configuration
	No connectivity between Standby AuC and Active AuC	unsynchronized/link down
	Version incompatibility between Standby AuC and Active AuC	unsynchronized/version mismatch

Status	Condition	UEM Managed Object State
	Some data cannot be synchronized properly (db, pwv, Master Key)	unsynchronized/synchronization error
	Both AuCs are in Standby role	unsynchronized/duplicated standby role
	Both AuCs are in Active role	unsynchronized/duplicated active role
	Synchronization mechanism is disabled	unsynchronized/application disabled

Table 48: Common Link States

This table describes link states obtained during the recent query to the License Server.

Condition	UEM Managed Object State
Successfully connected to LM	up/noErrorsDetected
Server is down	down/unreachable
Authentication failure	down/authenticationFailure
Could not query LM during audit	down/ErrorToSend
Unable to get response from LM	down/ErrorToReceive

Table 49: Common License States

Condition	UEM Managed Object State
AuC server is down or first audit not run	unknown/audit not run
Error during query of License Server	unknown/audit failure
Number of licenses is compliant	license compliant/usage in limit
Number of defined licenses is less than number of licenses used in the system	license violation/contract exceeded

9.6

Radio Authentication Failures

When a radio fails authentication and the system is not in Authentication Required system-wide state, the AuC operator can individually disable authentication to allow the radio in the system. If the system is in Authentication Required system-wide state, there is no quick way to allow the radio to access the system besides going out of Authentication Required state. There are two following scenarios when a radio fails authentication.

9.6.1

Provisioned Radio Failing Authentication

The radio has been given K by the KVL and now the infrastructure challenges the radio, but the radio fails authentication. When the radio was provisioned, it could be that two KVLs provisioned the same radio and reversed the order when uploading to the AuC. When the radio fails authentication, an alarm on the UEM will occur and ZoneWatch will show the authentication failure. AuC logs keep track of which KVL has loaded what SUID to track down provisioning issues. Another way to cause this failure

is to change the authentication key in the radio and cycle power on the radio before KVL uploading to the AuC. Correctly provisioning the radio resolves these issues.

9.6.2

Never Provisioned Radio Failing Authentication

The radio has never been given K by the KVL and now the infrastructure challenges the radio. The infrastructure believes that the radio was provisioned for authentication, but it was not. A radio with authentication software will indicate that authentication failed, but will not respond to the challenge (no alarm on the UEM). A radio without authentication software will ignore the challenge but will not indicate authentication failure. There will be no alarm on the UEM, but ZoneWatch will show an authentication timeout. Disabling authentication for that radio at the AuC will allow the radio to access the system. The reason of the problem could be that there are two radios with the same SUID or the AuC operator entered K for a radio that was not given K.

9.7

Unwanted Radio Failing Authentication

An unwanted radio is a radio that should not be allowed on the system. It may or may not be using the same SUID as a radio already on the system. An alarm on the UEM indicates that authentication failed. This radio cannot be inhibited, as it cannot register and an attempted inhibit could accidentally inhibit the customer radio if it is already on the system. It may not be clear if this is an unwanted radio that is failing authentication. If the radio has been passing authentication it probably is an unwanted radio. Your organization's policies dictate what steps should be taken next. The reason for pursuing this radio is that its user may be involved with criminal activity.

9.8

Stolen Radio Passing Authentication

If no actions are taken, a stolen radio will pass authentication and be allowed onto the system. If another radio with the same SUID does not replace it immediately, change the authentication key at the AuC. If the stolen radio is on the system, then it will be asked to register again and it will fail authentication and will not have access to the system any more. If the stolen radio is not on the system, then the next time it tries to register on the system it will fail authentication and not have access to the system. If another radio with same SUID will replace it, use the KVL to give the replacement radio another authentication key (K) and then upload K to the AuC.

Depending on your organization's procedures, in some cases the the stolen radio may be allowed onto the system. Usually to either inhibit it, track and recover it, or zero end-to-end encryption keys. If this is the case, do not immediately change the authentication key as the stolen radio will not have access to the system.

9.9

Stolen KVL

A stolen KVL is not able to upload keys into the AuC since the KVL operator Active Directory account and password should not be known to the adversary. However, the AuC operator should lock out the stolen KVL to prevent keys from being uploaded into the AuC in case the KVL operator account and password have been compromised. For security purposes, the replacement KVL needs to use a different KVL Unique Key Encryption Key (UKEK) than the UKEK used by the stolen KVL.

9.10

Authenticated Radio Service

The radio is designed so that an authentication key cannot be extracted from it. Your organization's policies dictate if an authentication key mismatch between the AuC and the radio should be created, preventing the radio from being used on the system while it is out for service. When the radio returns to the system, it needs to be provisioned with K again in order to resolve the mismatch. If the board in the radio containing K is replaced by the service shop, then the radio needs to be provisioned with K again.

9.11

AuC Client Cohabited on NM Client

If the AuC Client is to be cohabited on an NM Client that was already joined to domain prior to AuC Client installation, reboot the computer after installing the AuC Client application. Otherwise, processing errors may occur.

9.12

Collecting AuC Server and Client Logs

Before contacting Motorola Solutions for support, collect AuC Server and/or Client logs.

Procedure:

- 1 Perform one of the following actions:
 - If you want to collect logs from the AuC Server and co-habited AuC Client, log on to the AuC Server with local Windows administrator privileges.
 - If you want to collect logs from a standalone AuC Client, log on to the AuC Client with local Windows administrator privileges.
- 2 On the desktop, right-click the **Configuration Console** icon and select **Run as administrator**. If prompted for administrator credentials or a confirmation, type the administrator credentials or click **Yes**.
- 3 In the Command Prompt, enter: `coco coco report -l`
A .zip file containing logs is created in D:\Motorola. The file name is `report_<timestamp>.zip`.

Chapter 10

Radio Authentication FRU/FRE

There is no FRU/FREs unique to the Radio Authentication feature. For FRU/FREs of the ASTRO® 25 system hardware components that take part in the authentication process, see their respective manuals.

Table 50: Hardware FRU/FRE Reference

Hardware Component	Source Reference
Authentication Center Host Server	<i>Virtual Management Server Hardware</i>
KVL 4000	<i>KVL 4000 Key Variable Loader Radio Authentication User Guide</i>
Standalone AuC Client/NM Client	<i>Private Network Management Client</i>
Zone Controller Host Server	<i>Virtual Management Server Hardware</i>

Chapter 11

Radio Authentication Disaster Recovery

Disaster Recovery information enables you to recover the Radio Authentication feature in the event of a failure.

11.1

Recovering the Authentication Center (AuC) Server

Process:

- 1 Verify if the AuC installation prerequisites have been met. See Prerequisites in [Installing the Radio Authentication Feature on page 40](#).
- 2 Install the AuC virtual container using vSphere. See [Installing the AuC Virtual Machine on page 41](#).
- 3 Install the AuC Server. See [Installing the Primary/Backup AuC Server on page 46](#).
- 4 If needed, install the AuC Client (either standalone or cohabited on the NM Client). See [Installing the AuC Client on page 48](#).

For configuration purposes, you can also use the AuC Client cohabited with the AuC Server.

- 5 If needed, copy the latest available backup from the BAR server.
See [Backup and Restore \(BAR\) Services on page 33](#).
- 6 Restore the AuC Server by using the Configuration Console. See [Restoring the AuC Server Using the Configuration Console on page 101](#).
- 7 Log on to the AuC Client as the existing user with the permissions to set the Master Key. See [Logging On to the AuC Client on page 75](#).
- 8 Set the Master Key:
 - For the primary AuC server, see [Setting the Master Key on the Active AuC on page 88](#).
 - For the backup AuC server, see [Setting the Master Key on the Standby AuC on page 89](#).



IMPORTANT: Ensure that you set the same Master Key as the one that was used to encrypt the AuC Server database during the last backup.

- 9 Complete the AuC Server restoration. See [Completing the AuC Server Restoration Using the Configuration Console on page 101](#).
- 10 If necessary, re-synchronize the keys between the AuC Server and the ZC. See [Re-sending Keys to ZC on page 103](#).
- 11 For DSR systems only: If the backup AuC was active, and the primary AuC has been recovered, switch over to the primary AuC. See [Switching Over From the Backup AuC Server to the Primary AuC Server on page 96](#).
- 12 Apply supplemental configuration to the AuC server virtual machine.
See "Applying Supplemental Configuration to Virtual Machines" in the *Virtual Management Server Software* manual.

11.2

Recovering the Authentication Center (AuC) Client Cohabited on NM Client

Process:

- 1 Recover the HP Z420 or Z440 hardware and connect it to the zone core.
- 2 Recover the NM Client. See “Recovering the PNM Client” in the *Private Network Management Client* manual.
- 3 Install the AuC Client. See [Installing the AuC Client on page 48](#).

11.3

Recovering the Standalone Authentication Center (AuC) Client

Process:

- 1 Recover the HP Z420 or Z440 hardware and connect it to the zone core.
- 2 If MAC Port Lockdown is enabled, unlock the HP Switch Port corresponding to the failed client. See “Unlocking/Locking HP Switch Ports When Replacing Connected Devices” in the *MAC Port Lockdown* manual. Complete the steps related to disabling the MAC Port Lockdown.
- 3 Re-install Windows OS.
Obtain the following media provided by Motorola Solutions, depending on your implementation scenario:
 - *Motorola Windows Client* media (contains the Windows 10 virtual machine files) **or** *Motorola Windows Client* media (contains the Windows 10 standalone image files)
 - *Motorola Windows Box Profile* media (contains initial setup for individual devices and initial configuration scripts; drivers for Windows client and server)
- 4 Install the AuC Client.
See [Installing the AuC Client on page 48](#).
- 5 If MAC Port Lockdown was enabled at the beginning of the device recovery, verify that the new MAC address has been learned by the HP Switch and re-enable MAC Port Lockdown.

Chapter 12

Motorola Redundancy Manager

Motorola Redundancy Manager is a software tool designed and provided by Motorola Solutions.

12.1

Logging On to the Motorola Redundancy Manager Client

Procedure:

- Log on to the AuC Server machine using the administrative account.
- To start the Redundancy Manager Client application from the desktop, your operating system's account must be a member of the **subssec** group.
You need to add your account to this group on the Domain Controller.
- On the desktop, double-click the **Motorola Redundancy Manager Client** icon.



- In the **Motorola Redundancy Manager** window, type in the user name and password. Click **Login**.
- Change your password, if necessary.
See [Embedded Passwords on page 105](#) and "Modifying the Embedded Password on a Device" in the *Authentication Services* manual.

12.2

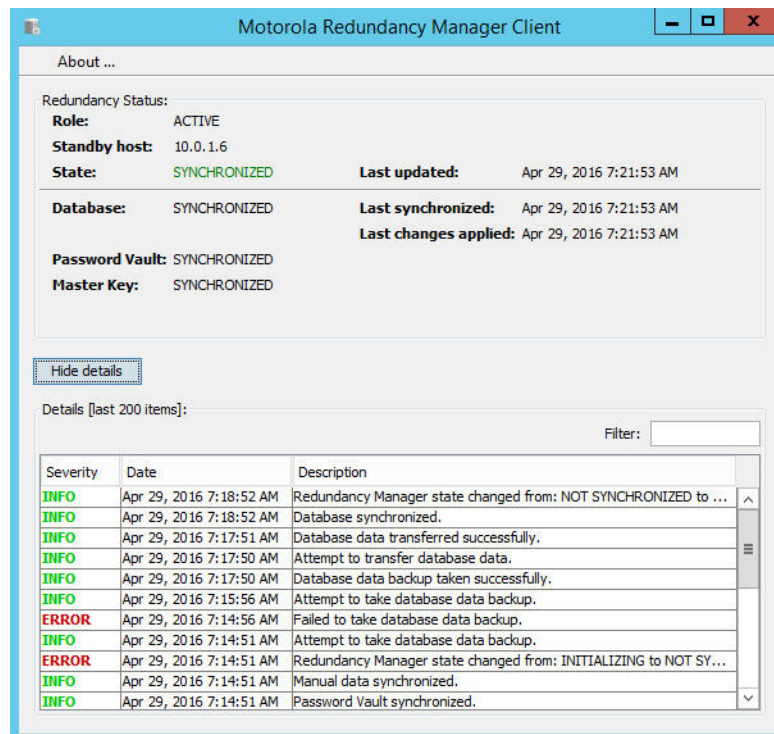
Motorola Redundancy Manager Client Screen Reference

The Redundancy Manager Client application provided by Motorola Solutions consists of the main window with dialog boxes through which you can perform the following Redundancy Manager operations:

- Check the Redundancy Status

- Display a list of events

Figure 16: Redundancy Manager Client Main Window



Motorola Redundancy Manager Client Redundancy Status

Table 51: Redundancy Status Fields

Field	Description
Role	Shows the current role: ACTIVE Default AuC primary server role. STANDBY Default AuC backup server role.
Active/Standby host	For active AuC, shows the IP of the host in the standby role. For standby AuC, shows the IP of the host in the active role.
State	Shows one of the following current states: SYNCHRONIZED This is the desired state. DISCONNECTED For systems without the Dynamic System Resilience (DSR) feature, this is the desired state. It indicates that there is no connection between Active and Standby AuC.

Field	Description
	NOT SYNCHRONIZED Indicates an error. Error details are displayed in the Details area.
	SYNCHRONIZING Shows that synchronization is in progress.
	INITIALIZING Shows that Redundancy Manager is being initially configured and starts up.
	VERSION MISMATCH Shows that Password Vault, Redundancy Manager, AuC Server, or PostgreSQL versions do not agree.
	DUPLICATED STANDBY ROLE Both AuC servers are in the standby state.
	DUPLICATED ACTIVE ROLE Both AuC servers are in the active state.
	INVALID CONFIGURATION Redundancy Manager has not been configured correctly.
	AUTHENTICATION FAILURE AuC primary and AuC backup rdm_auth_group passwords are incompatible.
Last updated	Shows the last time the current state was updated.
Database	Shows the database synchronization substate.
Password Vault	Shows the Password Vault data synchronization substate.
Master Key	Shows the manual Master Key synchronization substate.
Last synchronized	Shows the last time data synchronization was performed.
Last changes applied	Shows the last time data was sent.



NOTICE:

The current **State** can be SYNCHRONIZED only when **Database**, **Password Vault**, and **Master Key** substates are all SYNCHRONIZED.

If the current state is DISCONNECTED, the **Database**, **Password Vault**, and **Master Key** substates display as N/A.

Motorola Redundancy Manager Client Hide/Show Details

The **Hide/Show details** button displays the details of the last 200 Redundancy Manager events.

Use the **Filter** field to narrow down your search.

Appendix A

Radio Authentication Logging Messages

Table 52: Flexible Authentication Logging Messages

Event / Analysis	Block Op-code	Authentication Result Reason	Authentication Type
<p>Event: SU authentication is successful. SU responds to AUTH_DMD with correct AUTH_RESP.</p> <p>Analysis: Indicates that this is a valid SU.</p>	Authentication Success	Successful	Explicit
<p>Event: SU authentication fails. SU responds to AUTH_DMD with incorrect AUTH_RESP.</p> <p>Analysis: Indicates that an adversary SU has gone to the extent of putting an authentication key into the SU to access the system.</p>	Authentication Failure	Wrong Response from radio	Explicit
<p>Event: SU authentication timeout. SU never responds to AUTH_DMD with correct AUTH_RESP within authentication timer. This includes bad responses or no response.</p> <p>Analysis: When there is no wrong response from a radio authentication failure, it indicates an adversary SU that cannot perform authentication attempted access to the system or a valid SU was unable to respond due to RF coverage issues.</p>	Authentication Timeout	No response from radio	Explicit
<p>Events: Cancel of authentication. Authentication session in progress and U_REG_REQ or LOC_REG_REQ or U_DE_REG_REQ received from same SUID in same zone. Also, sent if in authentication session with SU and site transitions from wide to site trunking.</p> <p>Analysis: Cancels due to registration messages indicate that there are adversaries trying to register on the system or a valid SU had to re-try their registration or deregister due to RF coverage issues. If during site transition from wide to site trunking then it just reflects the site transition happened during an authentication.</p>	Authentication Failure	Canceled by ZC	Explicit
<p>Event: Authentication rejected by Zone Controller. U_REG_REQ while in system wide authentication Required with no SAI and authentication will not be delayed.</p>	Authentication Failure	Rejected by ZC	Unprovisioned

Event / Analysis	Block Op-code	Authenticata- tion Result Reason	Authentica- tion Type
Analysis: Indicates system wide required was entered before all valid SU were provisioned with authentication keys and the authentication keys received by the AuC. Alternatively, the SU not in Network Management attempts to Unit Register.			
Event: Authentication rejected by Zone Controller. U_REG_REQ while in system wide authentication Required with Clearout and authentication will not be delayed.	Authentica- tion Failure	Rejected by ZC	Clearout
Analysis: RS/KS clearout is accomplished by erasing K in the AuC or individual disable of authentication for a SU in the AuC. In this case the clearout was unresolved (no K in AuC), system wide authentication is in Required and the SU Unit Registers. Or AuC has K and AuC Operator did not individually enable the SU before system wide Required occurred and the SU Unit Registers.			
Event: ZC receives a response to a challenge when there is no authentication session in progress for that SU.	Authentica- tion Failure	Unexpected Authentication Response	Explicit
Analysis: Indicates an authentication race condition between valid and adversary SU or the valid SU responding to the repeat of the Authentication Demand right after authentication has passed or that the valid SU missed the registration response and resent the authentication response.			

Table 53: Flexible Mobility Update Messages

Event / Analysis	Block Op-code	Mobility Request Result	Authentica- tion Type	MU Gener- ic Reason
Event: SU authentication is successful. SU responds to AUTH_DMD with correct AUTH_RESP. Analysis: Indicates that this is a valid SU.	Unit Regis- tration, Lo- cation Reg- istration	Accepted	Explicit	Not appli- cable
Event: SU authentication fails. SU responds to AUTH_DMD with incorrect AUTH_RESP. Analysis: Indicates that an adversary SU has gone to the extent of putting	Unit Regis- tration	Refused	Explicit	Not appli- cable

Event / Analysis	Block Op-code	Mobility Request Result	Authentication Type	MU Gener-ic Reason
an authentication key into the SU to access the system.				
<p>Event: Legacy SU attempts registration at same site as a Valid SU.</p> <p>Analysis: Indicates that adversary SU without authentication capability attempted to register at the same site where valid SU is.</p>	Unit Registration	Refused	None	Not applicable
<p>Event: Authentication is Delayed due to infrastructure failure.</p> <p>Analysis: Infrastructure failure prevented authentication and an adversary could have been allowed on to the system along with valid SU, authentication is delayed to a later time.</p>	Unit Registration, Location Registration	Accepted	Delayed	Not applicable
<p>Event: The ZC receives site trunking registration / affiliation maintenance information in SITE MOBILITY DATABASE UPLOAD ICP indicating authentication is needed and authentication is enabled and Clearout, will delay authentication.</p> <p>Analysis: An SU is having authentication issues since the infrastructure has the SU on individual disable for authentication and this SU registered during site trunking.</p>	Site Trunking Registration / Affiliation Maintenance	Accepted	Delayed	Registered / Affiliate by Site Upload
<p>Events: No Authentication, U_REG_REQ, and System Wide Authentication is Disabled or LOC_REG_REQ without authentication.</p> <p>Analysis: Authentication has been disabled system wide, no SU will be authenticated, and adversary SU may be allowed on. If location registration it is usual processing without authentication</p>	Unit Registration, Location Registration	Accepted	None	Registered / Affiliate by Site Upload
<p>Event: Unprovisioned SU allowed on. In System Wide authentication Enabled and no SAI.</p> <p>Analysis: SU that have not been provisioned for authentication in the system will be allowed on. Used dur-</p>	Unit Registration, Location Registration	Accepted	Unprovisioned	Registered / Affiliate by Site Upload

Event / Analysis	Block Op-code	Mobility Request Result	Authentication Type	MU Generic Reason
ing migration of the system to full authentication capability.				
Event: Authentication Clearout allows SU to register without authentication. Analysis: AuC has disabled authentication for this SU.	Unit Registration, Location Registration	Accepted	Clearout	Registered / Affiliate by Site Upload
Event: SU was commanded to register and failed authentication or SU failed authentication on location registration. Analysis: ZC no longer has this SU registered.	Deregistration	Not applicable	Not applicable	De-registered due to Authentication Failure

Table 54: Flexible Radio Status Traffic

Event	Block Op-code	Subscriber Reject Reason	Generic Reason
Event: SU authentication fails during location registration. SU responds to AUTH_DMD with incorrect AUTH_RESP. Analysis: Indicates that an adversary SU has gone to the extent of putting an authentication key into the SU and had gained access to the system due to delayed authentication.	Radio Subscriber Reject	Authentication Deny	Not applicable.

Table 55: AuC Operation/Permissions

Operation/Permission	Master Key Mgmt	User Mgmt	KVL Mgmt	Subscriber Mgmt	Key Mgmt	Infrastructure Mgmt	Server Mgmt
Ki Delivery						✓	
Configure and Start SAI Distribution				✓			
Configure and Start KEKm Distribution					✓		
Delete Unmatched K-SUIDs					✓		
Add/Modify/Delete KVL/Assign UKEK			✓				
Enter Master Key	✓						

Operation/Permission	Master Key Mgmt	User Mgmt	KVL Mgmt	Subscriber Mgmt	Key Mgmt	Infrastructure Mgmt	Server Mgmt
Individual Enable/Disable Subscribers				✓			
Configure Server/System Settings							✓
Configure KVL Port Settings			✓				
View/Add/Modify/Delete Users, Permissions		✓					
Purge/Delete Audit Trail							✓
Replace Master Key (re-crypt)	✓						
Resend Keys					✓		
K-SUID Entry				✓			