



Authentication Services

APRIL 2021



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.

© 2021 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
MN003236A01-A	Original release of the <i>Authentication Services</i> manual	November 2016
MN003236A01-B	This update includes the following updated topics: <ul style="list-style-type: none">• RADIUS Client Configuration Parameters on page 49.• Applying Post-Install AD Configuration on page 74.	May 2017
MN003236A01-C	The new section added: Manually Reimporting Specific Domain Group Policy Object Settings on page 160	September 2019
MN003236A01-D	The following section has been updated: Configuring Virtual Machine Resources on page 61	November 2019
MN003236A01-E	Updated section: Recovering a Domain Controller Using Backup on page 189 (additional substeps in step 10)	June 2020
MN003236A01-F	Updated section: <ul style="list-style-type: none">• Managing FSMO Roles on page 177 New section: <ul style="list-style-type: none">• Updating Zone Core LMP DNS Entries Manually on page 139	September 2020
MN003236A01-G	Updated Recovering a Domain Controller Using Backup on page 189	April 2021

Contents

Copyrights.....	2
Contact Us.....	3
Document History.....	4
List of Figures.....	12
List of Tables.....	13
List of Processes.....	15
List of Procedures.....	16
About Authentication Services.....	19
What Is Covered In This Manual?.....	19
Helpful Background Information.....	19
Related Information.....	20
Chapter 1: Authentication Services Description.....	23
1.1 Active Directory Functional Description.....	23
1.2 Introduction to Centralized Authentication for Unix Devices.....	24
1.3 Identification, Authentication, and Authorization.....	24
1.3.1 Identification.....	24
1.3.2 Authentication.....	24
1.3.2.1 Central Database Functions.....	25
1.3.2.2 Central User Accounts.....	25
1.3.2.3 Local Administrator and Domain Administrator Accounts.....	25
1.3.2.4 Local Caching of Central User Accounts.....	26
1.3.2.5 Windows Logon.....	26
1.3.2.6 Device Authentication.....	26
1.3.3 Authorization.....	27
1.3.3.1 User Rights.....	27
1.3.3.2 Single Sign-On.....	27
1.4 Authentication Servers in ASTRO 25 Systems.....	28
1.5 Domain Controllers and ASTRO 25 Zone Core Configurations.....	29
1.6 Domain Controller and Trunking Subsystem Prime Site.....	30
1.7 Authentication Servers in ASTRO 25 Systems with Dynamic System Resilience.....	30
Chapter 2: Active Directory Theory of Operations.....	31
2.1 Active Directory Technical Overview.....	31
2.1.1 Delegation in Active Directory.....	31
2.1.2 Objects.....	31
2.1.3 System Account.....	32

2.1.4 Network Time Protocol (NTP) as the ASTRO 25 Time Source.....	32
2.2 Active Directory Group Usage for ASTRO 25 Systems.....	33
2.2.1 Domain Groups.....	33
2.2.2 Roles in ASTRO 25 Active Directory.....	33
2.2.2.1 Zone Groups.....	35
2.2.3 Domain Users.....	36
2.2.3.1 Active Directory Client Devices and Applications.....	36
2.2.4 User Account Management.....	38
2.2.5 Group Account Management.....	39
2.2.6 User/Group Name Restrictions.....	39
2.3 Flexible Single Master Operation.....	39
2.4 Active Directory Data – Backup and Restore	40
2.4.1 Domain Controller Storage Structure.....	41
2.5 Replication.....	41
2.6 Security Policies for Organizational Units.....	41
2.7 Agency Partitioning.....	41
Chapter 3: RADIUS Theory of Operations.....	43
3.1 RADIUS Technical Overview.....	43
3.2 RADIUS in ASTRO 25 Systems.....	43
3.2.1 RADIUS vs. Local Authentication for Sessions Between a Device and UNC.....	45
3.2.2 Password Restrictions for Local and RADIUS Accounts.....	46
3.2.3 Authentication for Devices Accessed with CSS.....	47
3.3 RADIUS Authentication.....	47
3.3.1 RADIUS Authentication – Device-Level vs. 802.1x Ethernet Port.....	49
3.4 RADIUS Remote Access Policies.....	49
3.5 RADIUS Client Configuration Parameters.....	49
Chapter 4: DNS Theory of Operations.....	51
4.1 DNS Introduction.....	51
4.1.1 Domains and Zones.....	52
4.1.2 Resource Records.....	53
4.2 Service Detail.....	54
4.2.1 Network IP Services.....	54
4.2.2 Domain Names.....	54
4.2.3 Accessibility and Availability.....	55
4.2.4 Server Location.....	55
4.2.4.1 Domain Setup.....	56
4.2.4.2 Domain Controller Functions in a Dynamic System Resilience System....	56
4.2.4.3 Configuration of DNS IP Addresses on Clients.....	57
4.2.5 DNS Backup and Restore.....	57

Chapter 5: AD/DNS Installation and Configuration.....	58
5.1 Installing and Configuring Domain Controller Software for AD/DNS.....	58
5.1.1 Importing the Domain Controller Virtual Machine.....	59
5.1.2 Configuring Virtual Machine Resources.....	61
5.1.3 Applying Supplemental Configuration to Virtual Machines.....	62
5.1.4 Configuring the vCenter for the Newly Deployed VM.....	63
5.1.5 Connecting and Powering on a New Virtual Machine.....	64
5.1.6 Applying OS-Level Identity on the Domain Controller.....	65
5.1.7 Activating a Domain Controller Virtual Machine.....	66
5.1.8 Reconfiguring VMware Tools on a Windows-Based Virtual Machine.....	66
5.1.9 Adding the Domain Controller to an Existing System.....	68
5.1.10 Domain Controller Installation.....	69
5.1.10.1 Installing the First System-Level DC.....	69
5.1.10.2 Installing the Backup System-Level DC.....	70
5.1.10.3 Installing First and Backup Zone-Level DCs.....	71
5.1.10.4 Installing the Domain Controller at a Console Site (Non-Tsub).....	72
5.1.10.5 Installing the Domain Controller at a Tsub Prime Site.....	73
5.1.11 Clearing the Post-Install Configuration Warning on the Domain Controller.....	74
5.1.12 Applying Post-Install AD Configuration.....	74
5.2 User Input Requirements for Server Installation/Configuration.....	75
5.3 Adding CEN Records into DNS.....	77
Chapter 6: RADIUS Server Installation/Configuration.....	79
6.1 Creating and Transferring a List of RADIUS Clients for Importing to a RADIUS Server.....	79
6.2 Batch Importing RADIUS Clients to the Primary RADIUS Server for a Zone.....	80
6.3 Verifying Import of RADIUS Client Data.....	82
Chapter 7: RADIUS Client Configuration.....	83
7.1 RADIUS Configuration on an HP Switch with VoyenceControl.....	83
7.1.1 Configuring HP Switch Authentication Sources for Telnet or SSH Access.....	84
7.1.2 Configuring HP Switch Authentication Sources for 802.1x.....	86
7.1.3 Hostnames of RADIUS Authentication Sources for DSR and Non-DSR Switches.....	89
7.2 Entering the RADIUS Shared Secret on MNR Routers and GGM 8000 Gateways.....	90
7.3 RADIUS Configuration on Fortinet Firewall Manager.....	90
7.3.1 Logging on to the Fortinet Firewall Manager.....	90
7.3.2 Configuring RADIUS Shared Secret on the Fortinet Firewall Manager.....	90
7.4 RADIUS Configuration on Fortinet Firewalls.....	91
7.4.1 Configuring RADIUS Shared Secret on Fortinet Firewalls.....	91
7.5 Configuring RADIUS on RF Site and VPM Devices.....	92
7.6 Centralized Authentication Configuration on RF Site and VPM Devices with VoyenceControl.....	93

7.6.1 DNS Configuration on RF Site and VPM Devices with VoyenceControl.....	93
7.6.1.1 DNS Nameservers for Devices in DSR and Non-DSR Sites.....	94
7.6.1.2 Configlet Editor Information for Configuring DNS on RF Site and VPM Devices.....	95
7.6.2 Configuring RADIUS on RF Site and VPM Devices with VoyenceControl.....	96
7.6.3 Setting the Local Cache Size for Central Authentication on RF Site and VPM Devices with VoyenceControl.....	97
7.7 Centralized Authentication Configuration on RF Site and VPM Devices with CSS.....	97
7.7.1 Enabling/Disabling Authentication Services with CSS.....	98
7.7.2 Configuring DNS with CSS.....	100
7.7.3 Configuring RADIUS Sources and Parameters with CSS.....	102
7.7.3.1 RADIUS Service Configuration with CSS.....	103
7.7.3.2 FQDN of RADIUS Authentication Sources.....	105
7.7.4 Setting the Local Cache Size for Central Authentication with CSS.....	106
7.7.5 Enabling/Disabling Centralized Authentication with CSS.....	107
7.8 Configuring RADIUS on SDM3000 RTU and SNT.....	108
7.8.1 Disabling RADIUS on SDM3000 RTU and SNT.....	110
7.9 Configuring DNS for MCC 7500 Aux I/O with UNC.....	110
7.10 Configuring NTP for MCC 7500 Aux I/O with UNC.....	113
7.11 Configuring RADIUS for MCC 7500 Aux I/O with UNC.....	114
7.11.1 Disabling RADIUS for MCC 7500 Aux I/O with UNC.....	116
7.12 Configuring RADIUS for MCC 7500 Aux I/O on MCC 7500 Aux I/O Server.....	117
7.12.1 Disabling RADIUS on MCC 7500 Aux I/O Server.....	119
7.13 RADIUS Configuration on PTP 600 and PTP 800 Devices.....	119
7.14 Configuring RADIUS Shared Secret on Console Telephony Media Gateway.....	120
7.15 Configuring RADIUS Shared Secret on Terminal Servers.....	121
7.16 RADIUS Configuration on UNC.....	121
Chapter 8: Active Directory Server Operation.....	122
8.1 Creating Active Directory User Accounts.....	122
8.2 Adding User Accounts to a Domain.....	122
8.3 Adding Groups to a Domain.....	124
8.4 Assigning Group Membership to a User Account.....	124
8.5 Enabling User Accounts in Active Directory.....	125
8.6 Resetting User Passwords in Active Directory.....	126
8.7 Disabling User Accounts in Active Directory.....	127
8.8 Modifying User Account Attributes for Accessing Unix-Based Devices.....	127
8.9 Adding a Unix-Enabled Group to the Active Directory Domain.....	129
8.10 MOSCAD NFM Operations Local to a Server.....	130
8.10.1 Logging on to the Server with a Local Account.....	130
8.10.2 Adding Users to a Local Server.....	130

8.10.3 Adding Groups to a Local Server.....	131
8.10.4 Adding Groups to a User Account for a Local Server.....	131
8.11 Deleting a Computer Object from an Active Directory Domain.....	132
8.12 Adding/Removing a Standalone Backup Core Domain.....	133
8.13 Modifying Active Directory Tombstone Lifetime.....	134
Chapter 9: Active Directory Client Operation.....	135
9.1 Adding Windows-Based Devices to an Active Directory Domain.....	135
9.2 Adding Hostname into DNS on Windows-Based Devices.....	136
9.3 Configuring and Validating DNS on Windows-Based Devices.....	136
9.3.1 Verifying the DNS Domain Name Configuration on Windows-Based Devices.....	137
9.3.2 Configuring DNS Suffix and DNS Server Addresses List on Windows-Based Devices.....	137
9.3.2.1 DNS Suffixes.....	138
9.3.3 Updating Zone Core LMP DNS Entries Manually.....	139
9.4 Joining and Rejoining a Windows-Based Device to an Active Directory Domain.....	140
9.5 Starting the Windows Command Line as Administrator.....	142
9.6 Adding Unix-Based Devices to an Active Directory Domain.....	142
9.7 Implementation of Centralized Authentication on Devices.....	143
9.8 Joining Multiple Solaris-Based Servers to an Active Directory Domain.....	143
9.9 Joining a Linux-Based Device to the Domain.....	144
9.10 Obtaining the IP Address Inventory from the Domain Controller.....	145
Chapter 10: RADIUS Service Operation.....	146
10.1 Adding RADIUS Clients Manually to a RADIUS Server.....	146
10.2 Deleting a RADIUS Client from a RADIUS Server.....	147
10.3 Setting Up User Accounts for RADIUS Authentication/802.1x.....	148
10.3.1 Enabling Reverse Password Encryption.....	148
10.4 Adding a Remote Access Policy Manually.....	149
10.5 Enabling 802.1x on the Technician Laptop.....	149
10.6 Authenticating a User at an 802.1x Port on a Device.....	150
Chapter 11: AD/DNS/RADIUS Maintenance.....	151
11.1 Performing AD/DNS/RADIUS Maintenance.....	151
Chapter 12: AD/DNS Troubleshooting.....	152
12.1 General Troubleshooting for AD/DNS.....	152
12.2 Batch Importing ASTRO 25 System Users and Groups into Active Directory.....	156
12.3 Creating ASTRO 25 System Organizational Units.....	156
12.4 Fixing Dcpromo Failure.....	157
12.5 Troubleshooting Group Policy Objects (GPOs).....	157
12.5.1 General Considerations for Modifying Group Policy in an ASTRO 25 System....	158
12.5.1.1 Modifying Your Organization's Computer/Machine Configurations.....	158

12.5.1.2 Modifying Your Organization's User Configurations.....	158
12.5.1.3 Adding a Site to the Dynamic Trusted Sites Group Policy.....	159
12.5.2 Forcing GPO Setting Changes.....	159
12.5.3 Reimporting ASTRO 25 System Group Policy Objects (GPOs).....	159
12.5.4 Manually Reimporting Specific Domain Group Policy Object Settings.....	160
12.5.5 Manually Linking a GPO to an OU.....	161
12.6 Cohabitation Procedures.....	162
12.6.1 System/Device Specific Requirements Identification.....	162
12.6.2 Creating New Organizational Units.....	163
12.6.3 Linking Base Group Policy Objects to New Organizational Units.....	163
12.6.4 Creating a New Cohabitation GPO.....	163
12.6.5 Adding a Cohabitation GPO to a New OU.....	163
12.6.6 Merge Situations Configuration.....	164
12.6.6.1 Identifying a Merge GPO.....	164
12.6.6.2 Creating a Merge GPO.....	164
12.6.6.3 Moving Computer Objects (CO) to a New OU.....	165
12.7 Failure to Join an Active Directory Domain.....	165
12.7.1 Failure to Enable Services.....	165
12.7.2 Failure Due to TCP/IP Settings Misconfiguration.....	165
12.7.2.1 Configuring the IP Address.....	166
12.7.3 Failure Due to Improper Time Synchronization Configuration.....	166
12.7.4 Failure Due to Hostname and DNS Domain Name Misconfiguration.....	167
12.8 Services Required for Active Directory Operation.....	167
12.9 The Repadmin Tool Usage.....	167
12.9.1 Checking Replication Status with Repadmin.....	168
12.10 Setting the Time Source.....	168
12.11 Authentication Failure Troubleshooting.....	169
12.11.1 Failure Between the User and Authenticating Server.....	169
12.11.2 Failure Between a Device and Domain Controller.....	169
12.12 Authorization Failure Troubleshooting.....	170
12.13 Troubleshooting Single-Sign On (SSO) on CAM.....	170
12.14 Failure of Application Access by Administrator on Windows-Based Device.....	171
12.15 Failure Between the Domain Controller and a Device.....	172
12.16 Rejoining a Linux-Based Server to an Active Directory Domain.....	172
12.17 Rejoining a Solaris-Based Server to an Active Directory Domain.....	172
12.18 Domain Controller Health Report in UEM.....	173
12.19 DNS Misconfiguration.....	174
12.19.1 Interpreting Device DNS Misconfiguration.....	175
12.19.2 Device DNS Misconfiguration State Verification.....	176

12.19.3 Fixing the DNS Misconfiguration in the DNS Server or UNC.....	176
12.20 Managing FSMO Roles.....	177
12.20.1 Determining the FSMO Role Owner.....	177
12.20.2 Seizing FSMO Roles.....	177
12.20.3 Transferring FSMO Roles.....	178
12.20.4 Seizing Active Directory Lightweight Directory Services (AD LDS) FSMO Roles.....	179
12.21 Deleting a Domain Controller Server Object in a Domain.....	179
12.22 Deleting an AD LDS Server Object in an AD LDS Configuration Set.....	181
12.23 Deleting an Active Directory Domain	182
12.24 Transferring AD LDS FSMO Roles.....	183
Chapter 13: RADIUS Troubleshooting.....	184
13.1 RADIUS Authentication Failures.....	184
13.2 Viewing Centralized Authentication Event Logs.....	184
13.2.1 Viewing Remote Access Logging Information.....	185
13.2.2 Centralized Authentication Log Information for RF Site and VPM Devices.....	185
13.3 Updating Syslog and RADIUS IP Addresses for RF Site and VPM Devices.....	185
13.4 Disabling RADIUS on an HP Switch.....	186
Chapter 14: Domain Controller Disaster Recovery.....	189
14.1 Recovering a Domain Controller.....	189
14.1.1 Recovering a Domain Controller Using Backup.....	189
14.1.2 Recovering a Domain Controller Using Reinstall.....	192
14.2 Validating Successful Disaster Recovery.....	198
14.3 Recovering RADIUS Configuration.....	199
Appendix A: EMC Smarts Quick Reference.....	201
A.1 Config and Configlet Editors.....	201
A.2 Updating the EMC Smarts Network Configuration Manager Credentials for a Device.....	202
A.3 Scheduling Jobs.....	202
Appendix B: Embedded Password Management.....	206
B.1 Embedded Password Management Overview.....	206
B.2 Modifying the Embedded Password on a Device.....	206
B.3 Rotating the Encryption Keys.....	208
B.4 Embedded Password Management Variables and Procedures.....	209
B.4.1 Embedded Password Management Variables and Procedures (Interdependent Devices).....	217
B.4.2 STM Application Group Considerations.....	224
B.5 Embedded Password Backup and Restore.....	225
B.6 Embedded Password Troubleshooting.....	225
B.7 Embedded Password Maintenance Failure.....	226

List of Figures

Figure 1: RADIUS Authentication at an 802.1x-Enabled Ethernet Port	48
Figure 2: RADIUS Authentication at a Device Where Centralized Authentication is Implemented	48
Figure 3: Forward Zone Tree Hierarchy	51
Figure 4: Reverse Zone Tree Hierarchy	52
Figure 5: DNS Domains Versus DNS Zones	53
Figure 6: Undelegated DNS Domains	53
Figure 7: CSS Login Banner	99
Figure 8: Security Services Configuration Window	99
Figure 9: CSS Network Services Configuration – DNS Tab	100
Figure 10: DNS Service Wizard	101
Figure 11: CSS – RADIUS Service Configuration Tab	103
Figure 12: Schedule Job Window	203
Figure 13: Tasks Tab Fields	204
Figure 14: Pwvadmin changeproperty Example	207

List of Tables

Table 1: Domain Controller NTP Elements and Configuration	32
Table 2: Roles in ASTRO 25 Active Directory	33
Table 3: Creating User Accounts – Attribute Considerations	38
Table 4: Password Restrictions for Local and RADIUS Accounts on ASTRO 25 System Devices	46
Table 5: RADIUS Authentication – Device-Level vs. 802.1x Ethernet Port	49
Table 6: RADIUS Client Configuration Parameters	50
Table 7: Additional Active Directory Servers Required	56
Table 8: User Input Requirements – Domain Controller Configuration	75
Table 9: Hostnames of RADIUS Authentication Sources for DSR and Non-DSR Switches	89
Table 10: Configuring RADIUS on RF Site and VPM Devices	92
Table 11: DNS Nameservers for Devices in DSR and Non-DSR Sites	94
Table 12: Configlet Editor Information for Configuring DNS on RF Site and VPM Devices	95
Table 13: FQDN of RADIUS Authentication Sources for Devices in DSR and Non-DSR Sites	105
Table 14: DNS Suffixes	139
Table 15: Procedures for Implementing Centralized Authentication on Devices	143
Table 16: Troubleshooting Scenarios for Active Directory and DNS	152
Table 17: Domain Controller Health Report in UEM	173
Table 18: Locations of Log Files	174
Table 19: Embedded Password Management Variables and Procedures	209
Table 20: Embedded Password Management Variables and Procedures (Interdependent Devices)	217
Table 21: Embedded Password Management Variables and Procedures (Interdependent Devices)	218
Table 22: Embedded Password Management Variables and Procedures (Interdependent Devices)	218
Table 23: Embedded Password Management Variables and Procedures (Interdependent Devices)	218
Table 24: Embedded Password Management Variables and Procedures (Interdependent Devices)	218
Table 25: Embedded Password Management Variables and Procedures (Interdependent Devices)	219
Table 26: Embedded Password Management Variables and Procedures (Interdependent Devices)	219
Table 27: Embedded Password Management Variables and Procedures (Interdependent Devices)	219
Table 28: Embedded Password Management Variables and Procedures (Interdependent Devices)	220
Table 29: Embedded Password Management Variables and Procedures (Interdependent Devices)	220
Table 30: Embedded Password Management Variables and Procedures (Interdependent Devices)	220
Table 31: Embedded Password Management Variables and Procedures (Interdependent Devices)	221
Table 32: Embedded Password Management Variables and Procedures (Interdependent Devices)	221
Table 33: Embedded Password Management Variables and Procedures (Interdependent Devices)	221
Table 34: Embedded Password Management Variables and Procedures (Interdependent Devices)	222
Table 35: Embedded Password Management Variables and Procedures (Interdependent Devices)	222
Table 36: Embedded Password Management Variables and Procedures (Interdependent Devices)	222

Table 37: Embedded Password Management Variables and Procedures (Interdependent Devices) .	222
Table 38: Embedded Password Management Variables and Procedures (Interdependent Devices) .	223
Table 39: Embedded Password Management Variables and Procedures (Interdependent Devices) .	223
Table 40: Embedded Password Management Variables and Procedures (Interdependent Devices) .	223
Table 41: Embedded Password Management Variables and Procedures (Interdependent Devices) .	224
Table 42: Embedded Password Management Variables and Procedures (Interdependent Devices) .	224
Table 43: Embedded Password Troubleshooting	225
Table 44: Embedded Password Maintenance Failure	226

List of Processes

Installing and Configuring Domain Controller Software for AD/DNS	58
Creating Active Directory User Accounts	122
Adding Windows-Based Devices to an Active Directory Domain	135
Adding Unix-Based Devices to an Active Directory Domain	142
Setting Up User Accounts for RADIUS Authentication/802.1x	148
Performing AD/DNS/RADIUS Maintenance	151
Recovering a Domain Controller	189
Recovering a Domain Controller Using Backup	189
Recovering a Domain Controller Using Reinstall	192

List of Procedures

Importing the Domain Controller Virtual Machine	59
Configuring Virtual Machine Resources	61
Applying Supplemental Configuration to Virtual Machines	62
Configuring the vCenter for the Newly Deployed VM	63
Connecting and Powering on a New Virtual Machine	64
Applying OS-Level Identity on the Domain Controller	65
Activating a Domain Controller Virtual Machine	66
Reconfiguring VMware Tools on a Windows-Based Virtual Machine	66
Adding the Domain Controller to an Existing System	68
Installing the First System-Level DC	69
Installing the Backup System-Level DC	70
Installing First and Backup Zone-Level DCs	71
Installing the Domain Controller at a Console Site (Non-Tsub)	72
Installing the Domain Controller at a Tsub Prime Site	73
Clearing the Post-Install Configuration Warning on the Domain Controller	74
Applying Post-Install AD Configuration	74
Adding CEN Records into DNS	77
Creating and Transferring a List of RADIUS Clients for Importing to a RADIUS Server	79
Batch Importing RADIUS Clients to the Primary RADIUS Server for a Zone	80
Verifying Import of RADIUS Client Data	82
Configuring HP Switch Authentication Sources for Telnet or SSH Access	84
Configuring HP Switch Authentication Sources for 802.1x	86
Logging on to the Fortinet Firewall Manager	90
Configuring RADIUS Shared Secret on the Fortinet Firewall Manager	90
Configuring RADIUS Shared Secret on Fortinet Firewalls	91
Configuring RADIUS on RF Site and VPM Devices with VoyenceControl	96
Setting the Local Cache Size for Central Authentication on RF Site and VPM Devices with VoyenceControl	97
Enabling/Disabling Authentication Services with CSS	98
Configuring DNS with CSS	100
Configuring RADIUS Sources and Parameters with CSS	102
Setting the Local Cache Size for Central Authentication with CSS	106
Enabling/Disabling Centralized Authentication with CSS	107
Configuring RADIUS on SDM3000 RTU and SNT	108
Disabling RADIUS on SDM3000 RTU and SNT	110
Configuring DNS for MCC 7500 Aux I/O with UNC	110

Configuring NTP for MCC 7500 Aux I/O with UNC	113
Configuring RADIUS for MCC 7500 Aux I/O with UNC	114
Disabling RADIUS for MCC 7500 Aux I/O with UNC	116
Configuring RADIUS for MCC 7500 Aux I/O on MCC 7500 Aux I/O Server	117
Disabling RADIUS on MCC 7500 Aux I/O Server	119
Configuring RADIUS Shared Secret on Console Telephony Media Gateway	120
Configuring RADIUS Shared Secret on Terminal Servers	121
Adding User Accounts to a Domain	122
Adding Groups to a Domain	124
Assigning Group Membership to a User Account	124
Enabling User Accounts in Active Directory	125
Resetting User Passwords in Active Directory	126
Disabling User Accounts in Active Directory	127
Modifying User Account Attributes for Accessing Unix-Based Devices	127
Adding a Unix-Enabled Group to the Active Directory Domain	129
Logging on to the Server with a Local Account	130
Adding Users to a Local Server	130
Adding Groups to a Local Server	131
Adding Groups to a User Account for a Local Server	131
Deleting a Computer Object from an Active Directory Domain	132
Adding/Removing a Standalone Backup Core Domain	133
Modifying Active Directory Tombstone Lifetime	134
Adding Hostname into DNS on Windows-Based Devices	136
Verifying the DNS Domain Name Configuration on Windows-Based Devices	137
Configuring DNS Suffix and DNS Server Addresses List on Windows-Based Devices	137
Updating Zone Core LMP DNS Entries Manually	139
Joining and Rejoining a Windows-Based Device to an Active Directory Domain	140
Starting the Windows Command Line as Administrator	142
Joining Multiple Solaris-Based Servers to an Active Directory Domain	143
Joining a Linux-Based Device to the Domain	144
Obtaining the IP Address Inventory from the Domain Controller	145
Adding RADIUS Clients Manually to a RADIUS Server	146
Deleting a RADIUS Client from a RADIUS Server	147
Enabling Reverse Password Encryption	148
Adding a Remote Access Policy Manually	149
Batch Importing ASTRO 25 System Users and Groups into Active Directory	156
Creating ASTRO 25 System Organizational Units	156
Fixing Dcpromo Failure	157
Adding a Site to the Dynamic Trusted Sites Group Policy	159

Forcing GPO Setting Changes	159
Reimporting ASTRO 25 System Group Policy Objects (GPOs)	159
Manually Reimporting Specific Domain Group Policy Object Settings	160
Manually Linking a GPO to an OU	161
Creating New Organizational Units	163
Linking Base Group Policy Objects to New Organizational Units	163
Creating a New Cohabitation GPO	163
Adding a Cohabitation GPO to a New OU	163
Identifying a Merge GPO	164
Creating a Merge GPO	164
Moving Computer Objects (CO) to a New OU	165
Configuring the IP Address	166
Checking Replication Status with Repadmin	168
Setting the Time Source	168
Troubleshooting Single-Sign On (SSO) on CAM	170
Rejoining a Solaris-Based Server to an Active Directory Domain	172
Fixing the DNS Misconfiguration in the DNS Server or UNC	176
Determining the FSMO Role Owner	177
Seizing FSMO Roles	177
Transferring FSMO Roles	178
Seizing Active Directory Lightweight Directory Services (AD LDS) FSMO Roles	179
Deleting a Domain Controller Server Object in a Domain	179
Deleting an AD LDS Server Object in an AD LDS Configuration Set	181
Deleting an Active Directory Domain	182
Transferring AD LDS FSMO Roles	183
Updating Syslog and RADIUS IP Addresses for RF Site and VPM Devices	185
Disabling RADIUS on an HP Switch	186
Validating Successful Disaster Recovery	198
Recovering RADIUS Configuration	199
Updating the EMC Smarts Network Configuration Manager Credentials for a Device	202
Scheduling Jobs	202
Modifying the Embedded Password on a Device	206
Rotating the Encryption Keys	208

About Authentication Services

Authentication refers to the system activities that take place when users or devices attempt to access or join the ASTRO® 25 system. Authentication services include the services, components (hardware and software), and methods available to support user and device authentication when users or devices attempt to access or join the ASTRO® 25 system. This manual provides a high-level description of the following authentication services:

- Active Directory (AD)
- Remote Authentication Dial-In User Service (RADIUS)
- Domain Name Services (DNS)

What Is Covered In This Manual?

The chapters in this manual provide explanations, procedures, and guidance related to:

The server functionality

For Active Directory, RADIUS, and DNS services in ASTRO® 25 systems. In this manual, the Windows-based servers that provide these functions are referred to as Domain Controllers.

The client functionality

For Active Directory, RADIUS, and DNS services in ASTRO® 25 systems. This manual provides information for the devices that are supported as clients of these services as part of the standard features of your ASTRO® 25 system, as well as the option of connecting Solaris-based and Linux-based devices to Active Directory.

See [Authentication Services Description on page 23](#) for a description of the authentication methods that are covered in this manual.

This manual is not designed to provide standard information about these services if that information is available through sources other than ASTRO® 25 system documentation.

Also, features for message authentication/encryption are not in the scope of this manual. For information about these features, see the following ASTRO® 25 system manuals:

- *Encrypted Integrated Data Feature Guide*
- *Key Management Facility User Guide*
- *Link Encryption and Authentication*
- *MCC 7500 Dispatch Console with Voice Processor Module*
- *MCC 7100 IP Dispatch Console Setup and User Guide*

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	Description
<i>Standards and Guidelines for Communication Sites (6881089E50)</i>	Provides standards and guidelines that should be followed when setting up a Motorola Solutions communications site. Also known as R56 manual. This 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>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 ESXi-based virtual server hosts on the common Hewlett-Packard hardware platform in ASTRO® 25 systems.
<i>802.1x Service Ports on Switches</i>	Provides information relating to the implementation and management of 802.1x standards to authenticate service users at designated Ethernet ports on HP switches and on the internal switch of GCP 8000 Site Controllers and GPB 8000 Reference Distribution Modules (RDMs), in ASTRO® 25 systems.
<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>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.
GGM 8000, MNR S6000 and MNR S2500 hardware user guides	Available on the Motorola Online website: https://businessonline.motorolasolutions.com To access the manuals:

Related Information	Description
	<ol style="list-style-type: none"> 1 Follow the instructions on the website to create an account if you do not already have one. 2 Once you are logged in, put your cursor over the Resource Center icon in the top bar, then select Resource Center from the pull-down menu. 3 On the left hand side of the window, scroll down if needed, then click Product Information→Manuals→Network Infrastructure→Routers and Gateways. <p>The following manuals are available:</p> <ul style="list-style-type: none"> • <i>Motorola GGM 8000 Hardware User Guide</i> • <i>Motorola Network Router (MNR) S6000 Hardware User Guide</i> • <i>Motorola Network Router (MNR) S2500 Hardware User Guide</i>
<i>MOSCAD Network Fault Management Feature Guide</i>	Provides information required to install, configure, manage, and use the MOSCAD® Network Fault Management (NFM), an optional ASTRO® 25 systems solution that provides tools to configure, monitor, and control auxiliary system devices, such as tower lights or power and environmental equipment, in communication sites.
<i>SDM3000 (Site Device Manager) Owner's Manual</i>	Provides information for the Motorola Solutions SDM3000 hardware-based devices and SDM3000 I/O Expansion Unit models. This documentation is installed with the SDM3000 Builder application on the MOSCAD NFM Graphical Master Computer (GMC) and on some service laptops.
<i>SDM3000 Builder User Guide</i>	Provides information required to install, configure, manage and use the SDM3000 Builder software that is used to set up and configure SDM3000 hardware-based devices (SDM3000 RTU and SNT). This documentation is installed with the SDM3000 Builder application on the MOSCAD NFM Graphical Master Computer (GMC) and on some service laptops.
<i>GMC/GWS for MOSCAD NFM Operator Manual</i>	Provides operational information about the MOSCAD NFM Graphical Master Computer (GMC), which is a PC-based Graphical User Interface (GUI) that provides the display and logging of information received from the SDM3000 RTUs. The MOSCAD NFM Graphical Workstation (GWS) is the remote client of the GMC. The GMC Application (installed on GMC and on GWS) is used to view the Digital Inputs and to

Related Information	Description
	use the Digital Outputs to control the connected devices. This documentation is installed on the GMC and on GWS as part of the GMC Application from the <i>GMC/GWS GUI and SDM3000 Config S/W and Doc for MOSCAD NFM DVD</i> .

Chapter 1

Authentication Services Description

This chapter provides a high-level description of Active Directory (AD), Remote Authentication Dial-In User Service (RADIUS), and Domain Name Services (DNS). It also describes the multiple servers that contribute to authentication functions in ASTRO® 25 systems.

1.1

Active Directory Functional Description

A directory service, such as Active Directory, is the combination of a specialized database and protocol for accessing the database. Active Directory is used to centrally manage and control access to various information, such as user accounts and physical assets. Servers, workstations, and applications are configured to look up user information in the directory instead of creating their own databases.

Active Directory provides the following services:

A central location for network administration and delegation of administrative authority

Allows access to objects representing all network users, devices, and resources. This central location also enables you to group objects for ease of management and application of security and group policy. See [Troubleshooting Group Policy Objects \(GPOs\) on page 157](#).

Information security and single sign-on for user access to network resources

Tight integration with security eliminates costly tracking of accounts for authentication and authorization between systems. A single user name and password combination identifies each network user. This identity follows the user throughout the network.

Scalability

Active Directory includes one or more domains, each with one or more domain controller virtual machines, enabling you to scale the directory to meet any network requirements.

Flexible and global searching

Users and administrators use desktop tools to search in Active Directory. By default, searches are directed to the global catalog, which provides forest-wide search capabilities.

Systematic synchronization of directory updates

Updates are distributed throughout the network through secure and cost-efficient replication between domain controllers.

Remote administration

You can connect to any domain controller remotely from any Windows-based computer that has administrative tools installed.

Integration of object names

Object names are integrated with Domain Name System (DNS), the Internet-standard computer location system. Active Directory uses DNS to implement an IP-based naming system so that Active Directory services and domain controllers can be located over standard IP both on intranets and the Internet. (The implementation of Domain Name System in ASTRO® 25 systems is Microsoft's Domain Name Service. In the rest of this manual, the acronym DNS refers to Domain Name Service.)

Integrated Windows, Solaris, and Linux administration

Enhancement of Unix administration menus by providing a framework for assigning authorization groups to individual user accounts in Active Directory.

1.2

Introduction to Centralized Authentication for Unix Devices

Centralized authentication for Unix devices is a part of the system that extends administrative and security benefits for the ASTRO® 25 network by providing one control point for identification, authentication, and authorization services. Centralized authentication for Unix devices extends central management of user accounts in Active Directory to Solaris-based servers and Linux-based servers in the ASTRO® 25 network.

For a list of devices that support centralized authentication in an ASTRO® 25 system, see [Active Directory Client Devices and Applications on page 36](#).

1.3

Identification, Authentication, and Authorization

The following sections provide an introduction to three security concepts relating to services provided by an ASTRO® 25 system.



NOTICE: For the purpose of this manual, the three basic security concepts described in the following sections are named as Identification, Authentication, and Authorization. However, the same concepts also function under different names such as, for example: Authentication, Authorization, and Accounting (AAA).

1.3.1

Identification

Access control policies are based on identity. Access control policies are used within the system, with appropriate access enforcement methods, to restrict access between users and objects in the system (for example, devices, files, records, programs, or domains). An authenticated user has an associated security identifier or user/group identifier, which is used by appropriate enforcement methods.

For example:

- In a Windows-based system, access control lists enforce access based on the unique security identifier.
- In Unix-based systems, user/group identifiers are implemented for access control.
- When RADIUS is the authentication method, access control is implemented through user identifiers.

Identity management is provided using the Active Directory's Lightweight Directory Access Protocol (LDAP) functionality. LDAP defines the data that is stored in the directory.

1.3.2

Authentication

Within the security boundary of the network and subject to any applicable access control restrictions, the system provides the ability to uniquely identify and authenticate dispatch, operations, maintenance, and other users irrespective of the logon location. A single user name and password combination identifies each individual user, and this identity follows the user throughout the network. The end-user experience when logging on to system devices, is the same regardless of whether centralized authentication or local authentication is used.

There are three primary methods of authentication, which share a common user credentials database:

- Kerberos authentication using native Microsoft Windows access to Active Directory-based domain credentials
- RADIUS-based authentication services using a RADIUS server to access credentials stored in Active Directory

- Kerberos authentication for Solaris and Linux devices using the Pluggable Authentication Modules (PAM) proxy to interface to Active Directory

An ASTRO® 25 system Radio Network Infrastructure (RNI) applies these methods of authentication as follows:

- As part of standard ASTRO® 25 system features, Windows-based and Unix-based devices in the RNI are authenticated using Active Directory services. When they join the Active Directory domain, they become Active Directory clients.
- As part of standard ASTRO® 25 system features, the following devices are authenticated using Remote Authentication Dial-In User Service (RADIUS) client/server functionality provided by Microsoft Windows Network Policy Server (NPS):
 - Transport devices (switches, routers, gateways, firewalls, and terminal servers)
 - PTP 600 and 800 devices
 - RF site devices (GCP 8000 Site Controllers, GTR 8000 Radios, GCM 8000 Comparators, GPB 8000 Reference Distribution Module and GPW 8000 Receivers)
 - Devices based on the Voice Processor Module (VPM), including the SmartX Site Converter, a VPM component of the MCC 7500 dispatch console, and Telephone Media Gateway (TMG)

When these devices are configured with a RADIUS key that matches a shared secret for that device in NPS, they become RADIUS clients. They do not join the Active Directory domain.

1.3.2.1

Central Database Functions

The centralized database facilitates global administration for procedures such as:

- Enabling user accounts
- Enabling authentication and authorization across systems
- Disabling authentication and authorization across systems

1.3.2.2

Central User Accounts

Users have personal accounts created on the Active Directory to access resources. The access privileges of these personal accounts are determined by the users assigned system roles. The system roles equate to domain groups. Access to system resources is based on the privileges of the domain groups. For the default groups in an ASTRO® 25 system, see [Domain Groups on page 33](#).

All personal accounts are managed in the central database. Users use their personal accounts for logon sessions.

1.3.2.3

Local Administrator and Domain Administrator Accounts

When a user is logging on to Windows using a local administrator or a domain administrator account, launching an application requires additional steps due to Access Control Lists and Microsoft security paradigm. Access Control Lists (ACL) are applied to the executables of applications and utilities on Windows machines. A user in both the domain and local administrators group, who is categorized as an admin account, needs to start the program by starting cmd.exe as administrator, then go to the

folder with the application executable and run it. For details see [Starting the Windows Command Line as Administrator on page 142](#).



NOTICE: The administrator can run some applications, for example MOSCAD NFM applications, by using the **Run as administrator** option, available when right-clicking the **Start** menu option or the desktop icon, without the need to open the command prompt window. For detailed information, see the logon section in the appropriate device manual.

1.3.2.4

Local Caching of Central User Accounts

The credentials of users that have been successfully authenticated with the central authority are saved locally. Caching of user credentials provides a means for the users to log on when the central authentication service is not available.



NOTICE: User credentials are not cached on the Solaris and Linux servers.

1.3.2.5

Windows Logon

When a person logs on to a Windows-based device for the first time, a new local profile is created. If the user is set up with a roaming profile, the information stored in the user's roaming profile on the server is copied from the domain controller to the local Windows-based device. This provides the same environment that the user has set up and used on other Windows-based devices. If this user is not set up with a roaming profile, or if this is the first time the user has logged on to any Windows-based device, then a new profile is created from the profile information on the local device. This is the user's environment while logged on to this device. The user can customize the environment however they desire.

If the user has a roaming profile and this is the first time this user has logged on to this Windows-based device, then the profile stored for this user on the domain controller is copied down to the local device. This is the same environment as the user had when they were previously logged on elsewhere. Once the profile is copied down, the user's desktop environment is set up.

If the user has a roaming profile and this is not the first time this user has logged on to this Windows-based device, then the profile stored on the domain controller is compared to what is stored locally. The normal comparison is timestamps. If the local profile has more recent information, then some data is not copied down. Only information stored in the profile for this user on the domain controller that is newer than what is stored locally, is copied to the local machine. This prevents duplicate information from being copied, which saves time.

When a user logs off a Windows-based device, if the user has a roaming profile, any changes made to the local profile are compared to what is stored on the domain controller. If the local machine has newer information, it is copied up to the domain controller. This allows the user to get back the same environment when they log back on, whether to the same Windows-based device or a different one. Only information that is newer on the local machine compared to what is on the domain controller, is copied up to the domain controller. The same or older information, is not copied from the local machine. Once the profile has been backed up to the domain controller, then the user logout finishes.

1.3.2.6

Device Authentication

Device authentication identifies and authenticates specific devices before establishing a connection. Device authentication is a part of network access control, which includes mechanisms to authenticate nodes, control network connections, and maintain the security of the network services.

Device authentication for local connections prevents unauthorized access on Ethernet ports; ensuring that access to system resources is not compromised by the connection of an unauthorized computer.

For remote communication paths, device authentication supports the ability to protect valid peer-device entities, which is the basis of secure communication paths and device trust relationships.

Microsoft remote access policy authentication method Protected Extensible Authentication Protocol (PEAP) together with the Microsoft Extensible Authentication Protocol – Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MS-CHAPv2) is used to authenticate the peer device.

For more information, see the *802.1x Service Ports on Switches* manual.

1.3.3

Authorization

The process of controlling access to resources or objects on the network is called Authorization. In addition to confirming the identity of the user attempting to access the network, centralized authentication prevents unauthorized access of system resources through verification that the connection attempt is allowed.

Once a user account has received authentication and can potentially access an object, the type of authorized access is determined by either the user rights that are assigned to the groups a user is a member of or the access control permissions that are attached to the object.

1.3.3.1

User Rights

Users are given a specific set of privileges based on their user accounts group membership. Depending on which group or groups a user is assigned to, they can perform only the operations enabled for this particular group.

For more information on Active Directory user rights, see [Active Directory Group Usage for ASTRO 25 Systems on page 33](#).

1.3.3.2

Single Sign-On

Single sign-on (SSO) is a system where a user is authenticated for multiple services with a single username and password. One of the ways to implement single sign-on is using Windows authentication. Windows-authenticated logins pass an access token instead of a name and password to the application. The access token is assigned by Windows (Active Directory Domain or local operating system) when the user logs on. It contains a unique security ID (SID) for that user and the SIDs of any local or domain Windows groups to which the user belongs. These SIDs are compared to all the SIDs that are authorized to access the application. Based on the results of this comparison, the login is either granted or denied access to the application and access level is determined. A login dialog does not appear when the user runs the application, or if it does the same username and password is used as for logging on to the OS. The applications use the credentials that were provided on log on to the workstation.

Single-sign on is available for the following applications:

- Affiliation Display
- ATIA Log Viewer
- Dynamic Reports
- IP Packet Capture User Interface
- MCC 7100 IP Dispatch Console
- MCC 7500 Dispatch Console with VPM
- MKM 7000 Console Alias Manager (CAM) Web Interface/Client

- MOSCAD NFM GMC
- NFM Report Generator
- Provisioning Manager
- RCM
- Syslog Viewer
- System Historical Reports
- Zone Historical Reports
- ZoneWatch

Many applications authenticate users with Active Directory through the single sign-on technology, where the user only enters credentials at the initial operating system authentication. For this reason, it is recommended to use domain level accounts when logging into operating system of client machines, instead of using local administrator accounts.

To log into an application using different credentials from those provided to log on to the device, select the **Run as different user** option available when right-clicking the **Start** menu option or the desktop icon.



NOTICE: The NM, MCC 7100 and MCC 7500-type Console accounts are integrated with the Provisioning Manager. The NM and Console user account information is initially created in AD, then it is supplied from within the Provisioning Manager to be stored in the Provisioning Manager database.

For MCC 7100, single sign-on only works inside the RNI.

1.4

Authentication Servers in ASTRO 25 Systems

Multiple servers contribute to authentication functions in ASTRO® 25 systems:

Domain Controllers

Servers referred to as Domain Controllers provide the Active Directory functionality. All Domain Controllers are peers of each other. Active Directory provides mechanisms that keep Domain Controllers synchronized.

Domain Controllers are configured in an ASTRO® 25 system as follows:

- There is a single Active Directory domain in the system. All domain controllers in the system belong to the same Active Directory domain. Users in the Active directory domain can be created on any one of the domain controllers.
- There is only one Active Directory forest and one Active Directory domain in the forest.
- The client host that joined the Active Directory domain can use the domain users credentials to log on if the user has been placed in proper groups and given the privilege.
- Users can name the Active Directory domain themselves, depending on their needs, provided that they follow the format specified in [User Input Requirements for Server Installation/ Configuration on page 75](#).

For more information on Domain Controller configurations, see [Domain Controllers and ASTRO 25 Zone Core Configurations on page 29](#).

All domain controllers in an ASTRO® 25 system run on the Windows Server 2012 R2 operating system.

For details on the virtual HP DL380 hardware used for domain controllers in an ASTRO® 25 system, see the *Virtual Management Server Hardware* manual.

RADIUS servers

Specific Domain Controller servers function as synchronized RADIUS servers (RADIUS “authentication sources”). See [RADIUS Theory of Operations on page 43](#).

DNS servers

Specific Domain Controller servers function as DNS servers. See [DNS Theory of Operations on page 51](#).

Fortinet FortiGate firewall and Terminal Server(s)

The Fortinet FortiGate firewall and Terminal Server(s) provide single-factor authentication for remote users. Additionally, the FortiGate firewall can provide 2-factor authentication (with optional FortiToken feature) which requires the remote user to log in with Active Directory credentials and a token.

Users that are configured for 2-factor authentication must have their accounts managed in both the Active Directory and the FortiGate firewall. Active Directory users are added to the `vpnusers` group. RNI-DMZ firewall users are added with the same username as it appears in the Active Directory. See the *Service Access Architecture* manual.

1.5

Domain Controllers and ASTRO 25 Zone Core Configurations

The following section describes types of ASTRO® 25 Master Site (Zone Core) or Core and its respective Domain Controller (DC) configurations.

K core

The K core does not employ a Domain Controller. Mapping a device name to an IP address for each device in the K core system is done by using a host file template and host file naming conventions.

L core

For the **L1 (non-redundant)** core, the system-level Domain Controller virtual machine and zone-level Domain Controller virtual machine are placed on a single DL380 host server.

For the **L2 (redundant)** core, the system-level Domain Controller virtual machine is placed on a DL380 host server and zone-level Domain Controller virtual machine is placed on a second DL380 host server.

M1/M2 Single Zone system

For the **M1 (non-redundant)** primary zone core, the system-level Domain Controller virtual machine and zone-level Domain Controller virtual machine are placed on a single DL380 host server. For the M1 (non-redundant) backup zone core with Dynamic System Resilience (DSR), the system-level Domain Controller virtual machine and zone-level Domain Controller virtual machine are placed on a single DL380 host server.

For the **M2 (redundant)** zone core, the system-level Domain Controller virtual machine is placed on a DL380 host server and the zone-level Domain Controller virtual machine is placed on a second DL380 host server.

M3 Multi Zone Capable Redundant system

For the **M3 Primary zone core**, the system-level Domain Controller virtual machine is placed on a DL380 host server and zone-level Domain Controller virtual machine is placed on a second DL380 host server.

For each **M3 Add-On zone core** (multi zone capable), a zone-level Domain Controller virtual machine is placed on a single DL380 host server in each add-on zone to support the add-on zone core.

For the **M3 Primary Backup zone core** with Dynamic System Resilience (DSR), the system-level Domain Controller virtual machine is placed on one DL380 host server and zone-level Domain Controller virtual machine is placed on a second DL380 host server.

For each **M3 Add-On Backup zone core** with DSR, a zone-level Domain Controller virtual machine is placed on a single DL380 host server in each add-on zone to support the add-on backup zone core.



NOTICE: Additional Domain Controller virtual machines can be placed at a large site for support.

For more detailed information regarding the VMS host servers (Virtual Management Server) and the Virtual Machines (VMs for each host server) see the *Virtual Management Server Hardware* manual and the *Virtual Management Server Software* manual.

To see where all the VMs reside on the various VMS hosts in the system, see the “Virtual Machine Combinations” appendix in the *Virtual Management Server Software* manual.

For details on differences between configurations in an ASTRO® 25 system, see the *Master Site Infrastructure Reference Guide*.

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

1.6

Domain Controller and Trunking Subsystem Prime Site

The zone core is a typical location for the Domain Controller. Additionally, a Trunking Subsystem (Tsub) is an optional expansion of a zone, where the Domain Controller is also located.

In the ASTRO® 25 system with the Edge Availability with Wireline Console feature implemented, the Trunking Subsystem (Tsub) prime site is equipped with the following devices residing on the same Gen9 Tsub server:

- Tsub Zone Controller (ZC)
- Tsub IP Packet Capture
- Tsub Domain Controller
- Tsub Transcoder (optional)

The Domain Controller provides Active Directory, RADIUS, and DNS support during Tsub local area operation.

For more information, see the *Edge Availability with Wireline Console Feature Guide for Trunking Subsystems* manual.

1.7

Authentication Servers in ASTRO 25 Systems with Dynamic System Resilience

In systems with the Dynamic System Resilience (DSR) feature implemented, each authentication server in the primary core has a corresponding server in the backup core for the same zone.

For details about DSR, see the *Dynamic System Resilience Feature Guide*.

Chapter 2

Active Directory Theory of Operations

This chapter explains Active Directory in the context of your ASTRO® 25 system, including information specific to extending authentication services to Solaris-based servers and Linux-based servers in an ASTRO® 25 system.

2.1

Active Directory Technical Overview

Each Active Directory server is called a Domain Controller (DC). A DC contains all information for a specific Windows Active Directory domain. There is a single Active Directory domain for the entire ASTRO® 25 system.

Active Directory follows a tree hierarchy, which is like the Domain Name Service (DNS) domain hierarchy.

In the ASTRO® 25 system, AD domain namespace does not correspond one to one with the DNS namespace. This is called a “disjoint” AD domain namespace and is used to span a single AD domain across multiple DNS zones.

In ASTRO® 25 system, all DNS functionality resides on Domain Controllers.

2.1.1

Delegation in Active Directory

Active Directory domain is split off from the top, in a manner like DNS delegation. The child Active Directory domain inherits some items from its parents. The child Active Directory domain also contains information specific to its particular portion of the Windows Active Directory environment.



NOTICE: In the ASTRO® 25 system, a single Active Directory domain is provided by default. Delegated Active Directory domains are not provided.

The information within an Active Directory domain is logically grouped into Organizational Units (OUs). OUs provide greater flexibility in managing and maintaining the objects associated with a given Active Directory domain.

2.1.2

Objects

The information contained within an Active Directory is referred to as records. A record is made up of objects. Objects are made up of attributes and the values associated with those attributes. Each record is identified by its Distinguished Name (DN). Each DN is unique throughout the entire Active Directory forest.

Objects typically found within an Active Directory domain include the following:

Computers

Identify the servers and workstations that are part of the Active Directory domain.

Users

Identify the users that have access to the resources belonging to the Active Directory domain.

Groups

Define a collection of users or other groups. Groups are used to help administer what resources in the Active Directory domain are available to whom.

Security Policies

Define who can do what with the Active Directory resources

Organizational Units (OUs)

Define logical groupings of the other objects; help in administering and maintaining the Active Directory domain. Some settings can be changed in one place on a Domain Controller and the change propagates to all of the computers located in a given OU.

Attributes typically found within an Active Directory domain include the following:

Distinguished Name (DN)

Identifier for a particular record within the Active Directory domain. It must be unique throughout the entire Active Directory forest.

Common Name (CN)

Used to help provide a common identifier to the record.

Name

The complete name of the resource.

objectClass

Defines what attributes must exist for a given record and which attributes are optional for a given record. Each record has at least one objectClass, but it can have more.

2.1.3

System Account

In ASTRO® 25 systems, system account is a permanent user account for which the password never expires, so the user is not required to change the account password.

2.1.4

Network Time Protocol (NTP) as the ASTRO 25 Time Source

The Domain Controllers are time sources for Windows-based devices that are joined to the Active Directory domain.

Whenever a device that is part of a Windows Active Directory domain interacts with a Domain Controller, the time from the device is included in the messages. If the time the device supplies in the message differs by a certain amount of time compared to the time on the DC, that message is considered invalid.

The Domain Controllers get their time from the ASTRO® 25 system Network Time Protocol (NTP) servers. The hostnames of the NTP servers for the Domain Controllers depend on whether Dynamic System Resilience (DSR) is implemented:

Table 1: Domain Controller NTP Elements and Configuration

Location of the Domain Controller:	Non-DSR 1st NTP Source	Non-DSR 2nd NTP Source	DSR 1st NTP Source	DSR 2nd NTP Source
Primary Core	N/A	N/A	ntp02.zone<Z>*	ntp03.zone<Z>
Backup Core	N/A	N/A	ntp05.zone<Z>	ntp06.zone<Z>
Zone Core	ntp02.zone<Z>	ntp03.zone<Z>	N/A	N/A
Tsub Prime Site**	ntp02.zone<Z>	ntp03.zone<Z>	ntp02.zone<Z>	ntp05.zone<Z>

* where <Z> is the zone to which the DC belongs

** For the Trunking Subsystem (Tsub) Domain Controllers, while there is no backup Tsub when a system is DSR-enabled, the time source configuration is dependent on the DSR configuration of the host zone core. The non-DSR configuration applies to Tsub DC when the host zone core is non-DSR. The DSR configuration applies to Tsub DC when the host zone core is DSR.

The Domain Controller configuration script specifies the NTP servers that Domain Controllers use (you do not need to enter this information when installing and configuring Domain Controllers.)

For more information about NTP configuration in an ASTRO® 25 system, see the following manuals:

- *Network Time Protocol Server*
- *Virtual Management Server Software*

If the time source needs to be configured before configuring RADIUS, see the *Network Time Protocol Server* manual and the appropriate manual for the configured device.

2.2

Active Directory Group Usage for ASTRO 25 Systems

The following sections describe the use of groups in Active Directory in an ASTRO® 25 system.

2.2.1

Domain Groups

There are two kinds of domain groups in the ASTRO® 25 systems: Device Login groups and Role groups. Both are associated with Authorization.

If a user requires login privileges into a device, this user must be a member of appropriate Device Login groups to get access. For example, if a user “user1” wants to log on to a zone controller, “user1” must be a member of the `zc-login` group to get access.



NOTICE: For logging on to Unix devices, a number of other attributes must be set. See [Modifying User Account Attributes for Accessing Unix-Based Devices on page 127](#).

If a user needs to perform an operation on a device, this user must be a member of certain Role groups. This role is available on all devices that the user has access to. For example, if the user “user1” wants to view the log files, “user1” must be a member of the `secadm` group. The `secadm` group is associated with operations that a Security Administrator would perform in a system (for example, viewing log files).

For a list of all operations that can be performed by particular roles, see [Table 2: Roles in ASTRO 25 Active Directory on page 33](#) or contact your system administrator.


2.2.2

Roles in ASTRO 25 Active Directory

Table 2: Roles in ASTRO 25 Active Directory

This table includes higher-level application groups. Application-specific groups are already allocated into these system roles.

AD Group	Role Name	Role Definition
auditors	System Audit Administrator	Handles users operation trail information, as well as centralized and local logs auditing.
bkupadm	Backup Administrator	Handles databases, software installations, and configurations. This role has the ability

AD Group	Role Name	Role Definition
		to back up platform/OS and application-specific data.
confgaud	System Infrastructure Operator	Read-only access to system configuration data.
dbadm	Database Administrator	Administration of database
domain admins	Domain Administrator	Handles creation and maintenance of centralized user accounts, as well as centralized and local authentication and authorization administration.
domuser	Domain User	Default primary group for all Unix users.
infradm	Subscriber Infrastructure Administrator	Has ability to add, configure, and remove data, channels, voice channels, and console sites. Handles active standby control. Essentially, servers as ZCM and CSS Administrator. Handles device local call processing configuration. Also, has ability to load license keys required by applications to add additional resources or enable additional functionality in existing application. Handles database management.
instadm	Installation Administrator	Handles installations and patches. Also, has ability to restore backed up platform/OS and application-specific data.
infrsup	System Infrastructure Supervisor	Has ability read the system configuration and access fault management applications.
netwadm	Network Administrator	Handles configuration and administration of transport equipment.  NOTICE: RADIUS users should be members of the netwadm group to have administrative capabilities on the devices.
platadm	Platform Administrator	Handles reboot and shutdown. Has ability to control local peripherals, Unix administration such as NTP, local IP address, and local log files related to device performance monitor-

AD Group	Role Name	Role Definition
		ing and faults. Also, enables/disables services such as communication protocols.
secadm	Network Security Administrator	Handles keys and phrases. When key/phrase material is created, edited, or visible, it falls under this role. OS and network level keys such as SSH, SSL, and SNMPv3 are managed through this role.
subsadm	Subscriber Administrator	Has ability to add, configure, and remove radio users. Essentially, serves as Provisioning Manager and Radio Programming Software Administrator. Handles database management of subscriber data.
subssec	Subscriber Security Administrator	Handles keys for radio operations, such as payload encryption and subscriber authentication.
subsusr	Subscriber	Fixed/Mobile terminal operator such as dispatch console operator, data terminal user.
suppadm	Super Role Group	This is a super set of the role groups.
trafadm	System Traffic Administrator	Has access to system statistics, payload logging and recording applications.



NOTICE: Active Directory contains pre-created application access control groups in addition to the role groups covered in the table. It is recommended to use role groups for streamlined access control. Role groups provide more abstract access control management, and already have application groups nested in them. However, application groups can be used in situations when finer application-based access control is required.

2.2.2.1

Zone Groups

In addition to role groups that control access to application type, the following Network Management applications require configuration of zone-level access schema (NM user accounts are defined in Active Directory):

- Affiliation Display
- ATIA Log Viewer
- Dynamic Reports
- RCM
- System Historical Reports
- Zone Historical Reports

- ZoneWatch

In order for the user to be permitted to launch an application in a specific zone, the user must be added to a pre-configured domain group corresponding to that zone number.

For example, a user that should be permitted to only launch ZoneWatch application in Zone 1, should be a member of the “zone_1” domain group. For accounts that should have access to applications in all zones, the “all_zone” domain group is available to simplify the configuration. Only the Network Management Historical Reports application has zone- and system-level components. The user that should be allowed to use the system component of this application, also needs to be a member of the “sys_zone” domain group.

Zone-level access schema is also required for the Enhanced CADI protocol.

2.2.3

Domain Users

Few users are created by Motorola Solutions. Your organization needs to create users and make them members of appropriate groups in order to log on to devices and perform operations.



NOTICE: A user belonging to the local built-in `Administrators` group has administrative privileges only to that device. Only users belonging to the AD Domain Administrators group have administrative privileges (including login) to any Windows network element that is part of that AD domain.

2.2.3.1

Active Directory Client Devices and Applications

The following Windows and Unix (Linux and Solaris) devices support centralized authentication in an ASTRO® 25 system:

Windows-Based Active Directory Clients:

- MKM 7000 Console Alias Manager (CAM) Server
- MCN Server 8000™ Remote Comparator Display Software
- MCC 7500 Dispatch Console
- MCC 7100 IP Dispatch Console



NOTICE: If deployed in the CEN, the MCC 7100 Console will not join the RNI domain. Single sign-on for MCC 7100 Console only works inside the RNI.

- PRX 7000 Console Proxy
- Archiving Interface Server (AIS)
- NICE devices



NOTICE: Verint is an alternate solution to NICE in an ASTRO® 25 system.

- Network Management Client
- Core Security Management Server (CSMS)
- Data Collection Device (DCD)
- InfoVista Server

- MOSCAD NFM Graphical Master Computer (GMC)



NOTICE: With the ASTRO® 25 7.16 system release, device reporting supported by MOSCAD NFM GMC can be supported using the Unified Event Manager (UEM) for a Centralized UEM Mode. In the Centralized UEM Mode with an appropriate UEM license, the SDM3000 Network Translator, the MOSCAD NFM GMC, and other related MOSCAD NFM components can be decommissioned to implement a more centralized fault management solution. For more information, see the *UEM/GMC Transition Setup Guide*.

- MOSCAD NFM Graphical WorkStation (GWS)
- Authentication Center (AuC) Server
- Authentication Center (AuC) Client
- NEC SphericaII Manager IP PBX Media Gateway
- Dynamic Transcoder
- Group Data Gateway (GDG)

Linux-Based Active Directory Clients:

- Air Traffic Router (ATR)
- Unified Event Manager (UEM) Server
- System Statistics Server (SSS)
- Zone Database Server (ZDS)
- Zone Statistics Server (ZSS)
- Unified Network Configurator (UNC) Server
- Unified Network Configurator Device Servers (UNCDS)
- Zone Controller (ZC)
- Centralized Event Logging Server
- Fortinet Firewall Manager
- Backup and Restore Server
- HPD PDG (PDR component for HPD)
- Intersystem Gateway (ISGW)
- Trunked IV&D PDG (PDR component for IV&D)
- Conventional IV&D PDG (PDR component for Conventional IV&D)
- User Configuration Server (UCS)
- License Manager
- IP Packet Capture

Solaris-Based Active Directory Clients:

- ISSI.1 Network Gateway: ISSI.1 Gateway Module and Site Link Relay Module (Solaris-based/GAS)
- Public Safety LTE Push To Talk (PS PTT) Gateway: PS-LTE PTT Gateway module and Site Link Relay Module



NOTICE: The PS LTE PTT Gateway joins the ISSI Gateway Organizational Unit.

For the list of **RADIUS Active Directory Clients**, see [RADIUS in ASTRO 25 Systems on page 43](#).

The following applications use Active Directory to authenticate users (Role Based Access Control applications):

- Affiliation Display
- AIS Administrator
- ATIA Log Viewer
- Dynamic Reports
- MCC 7100 IP Dispatch Console
- PRX 7000 Console Proxy
- MCC 7500 Dispatch Console with VPM
- MKM 7000 Console Alias Manager (CAM) Web Interface/Client
- MOSCAD NFM Suite
- NICE Inform Lite or Audiolog™ Insight Center
- Provisioning Manager
- RCM
- Enhanced CADI
- SNMPv3 User Credential Tool
- System Historical Reports
- Zone Historical Reports
- ZoneWatch

2.2.4

User Account Management

When performing user account management, consider the following information:

Table 3: Creating User Accounts – Attribute Considerations

Attributes	Required when...	Comments
Login name	Creating any user account	Must be unique. Users with the same login name are not allowed within the same address space (a domain or a local Windows/Unix system).
Full name	Creating any user account	
User ID (UID)	Creating an account that needs to log on to Unix-based resources	<p>Must be unique. Duplicate UIDs for users or duplicate GIDs for groups:</p> <ul style="list-style-type: none">• Can lead to breach of access control• Are not a recommended security practice• Violate auditing standards <p>Accepting the default UID ensures the uniqueness of the UID.</p> <p>UID range varies from 10000 to 60000 (where 60000 is the maximum permitted UID in the Unix system). It is to be used for non-system user accounts (local or domain) created by the customer or Motorola Solutions support personnel after system installation and initial configuration. These are typically interactive accounts.</p>

Attributes	Required when...	Comments
Primary group ID (GID)	Creating an account that needs to log on to Unix-based resources	Primary group for the Unix servers is <code>domuser</code> .



NOTICE: User names are case insensitive.

2.2.5

Group Account Management

In ASTRO® 25 system, group accounts are predefined. Most of the role-based groups created have a domain-local scope.



NOTICE: Universal Groups are available in all domains within an AD forest. Domain local groups are available only in that AD domain.

2.2.6

User/Group Name Restrictions

The following common restrictions on user and group names should be followed to prevent errors due to excessively long user names and/or disallowed characters.

All user/group name restrictions are intended for use on Windows, RF site and VPM-based devices, Linux, and Solaris platforms.

User/group name:

- Cannot exceed a maximum of 8 characters for Windows and Solaris platforms or 32 characters for users exclusive to Linux platforms
- Characters other than alphabets and special characters such as: " / \ [] : ; | = , + * ? < > @ are not allowed
- Cannot differ only by a diacritic mark
- Cannot solely consist of periods (.) and/or spaces
- First character should be lower case or underscore



NOTICE: Login names that are used exclusively on Windows can exceed the eight character limit.

Group names that are used exclusively on Windows and groups used purely for device access control on Unix like the device-login groups can exceed the eight character limit.

2.3

Flexible Single Master Operation

This section describes Flexible Single Master Operation (FSMO) roles (also known as operations master roles) as used in Active Directory.

In a forest, at least five FSMO roles are assigned to one or more Domain Controllers:

Schema Master

The schema master Domain Controller controls all updates and modifications to the schema. To update the schema of a forest, you must have access to the schema master. There can be only one schema master in the whole forest.

Domain naming master

The domain naming master Domain Controller controls the addition or removal of domains in the forest. There can be only one domain naming master in the whole forest.

Infrastructure Master

The infrastructure is responsible for updating references from objects in its domain to objects in other domains. At any one time, there can be only one Domain Controller acting as the infrastructure master in each domain.

Relative ID (RID) Master

The RID master is responsible for processing RID pool requests from all Domain Controllers in a particular domain. At any one time, there can be only one Domain Controller acting as the RID master in the domain.

PDC Emulator

The PDC emulator is a Domain Controller that advertises itself as the Primary Domain Controller (PDC) to workstations, member servers, and Domain Controllers that are running earlier versions of Windows. It is also the Domain Master Browser, and it handles password discrepancies. At any one time, there can be only one Domain Controller acting as the PDC emulator master in each domain in the forest.

You can transfer FSMO roles by using the `Ntdsutil.exe` command-line utility or by using a Microsoft Management Console (MMC) snap-in tool. Depending on the FSMO role that you want to transfer, you can use one of three MMC snap-in tools:

- Active Directory Schema snap-in
- Active Directory Domains and Trusts snap-in
- Active Directory Users and Computers snap-in

If a computer no longer exists, the role must be seized. To seize a role, use the `Ntdsutil.exe` utility.

2.4

Active Directory Data – Backup and Restore

Active Directory data is backed up and restored as follows:

- Domain Controllers are automatically backed up locally every day and to the BAR server once a week by the ASTRO® 25 system centralized backup/restore solution. See the *Backup and Restore Services* manual.



NOTICE: Trunking Subsystem (Tsub) DCs are not backed up to the BAR server. For Tsub DCs, an optional Tsub prime site NAS can be added for backups.

- Domain Controllers can be restored using image recovery. If one domain controller fails, the recovery can also be performed by reinstalling the domain controller; see [Domain Controller Disaster Recovery on page 189](#). Since all the domain controllers belong to the same domain, Active Directory data is automatically replicated from the DC that is operational. For the caveats, see [Domain Controller Disaster Recovery on page 189](#).
- Active Directory data can only be restored using the Active Directory Restore Mode. It is important that a Domain Controller is restored with its correct backup and not the backup of any other DC. For example, Zone DC can be restored using only Zone1 DC backup and not Zone2 DC backup. It is important that all of the DCs are backed up since each of them has different data in terms of RADIUS and DNS.



NOTICE: In a Single Zone Non-Redundant configuration both DCs are virtual machines on the same virtual server. Therefore, for reliability reasons, they are always backed up to the baseline BAR.

2.4.1

Domain Controller Storage Structure

Each Active Directory Domain Controller stores one domain directory partition consisting of information about the domain in which it is located. There are at least two Domain Controllers per Active Directory domain which contain the same Active Directory information.

Active Directory information for the entire system is stored as follows:

- Each Domain Controller stores the schema and configuration directory partitions for the entire system.
- Domain Controllers that are designated as global catalog servers store the objects from all domains in the system. For each object that is not in the domain for which the global catalog server is authoritative as a domain controller, a limited set of attributes is stored in a partial replica of a corresponding domain. The partial replicas on a global catalog server are not writable, which means you cannot update an object in a partial replica on a global catalog server, but only on a domain controller that stores a full replica.

2.5

Replication

Active Directory replication is the process by which the changes that are made on one domain controller are automatically synchronized with other domain controllers.

Data integrity is maintained by tracking changes on each domain controller and updating other domain controllers in a systematic way.

By default, Active Directory replication uses a connection topology that is created automatically. This replication topology makes optimal use of physical network connections and frees administrators from having to determine which domain controllers replicate with one another. The replication topology can also be created manually. Active Directory replication is designed to maximize directory consistency and minimize the impact to network traffic.

2.6

Security Policies for Organizational Units

Each computer belongs to a specific Organizational Unit (OU). These OUs are logical groupings of computers to help in administration. Security policies applied to each OU control which services are run on these machines, who can and cannot log on to these machines, and other security-related settings.

2.7

Agency Partitioning

To allow for agency partitioning, each RNI zone Active Directory domain contains Organizational Units (OUs) for each organization. These OUs are given authority over particular sites “owned” by that agency. If a site is delegated to its own Active Directory domain from the parent RNI zone Active Directory domain, the OUs for that agency or agencies are created in the site’s Active Directory domain as well.



NOTICE: To support Agency Partitioning, contact the Motorola Solutions Support Center (SSC) to provide the configuration of OUs.

For greater security, a site could be delegated off the zone-level Active Directory domain for a particular agency. The delegation hides the information stored in the parent. Agency partitioning through OUs does not provide this. However, delegation to the zone-level Active Directory domain is done on a per-site basis. Thus, if a single agency has multiple dispatch console sites, administration is easier using OUs.

Initially, there are no delegated Active Directory domains. Delegated domains are not installed automatically.



NOTICE: Your organization is responsible for installing the delegated domains.

The console site-level Active Directory domain (non-Tsub) requires its own Domain Controllers.

Chapter 3

RADIUS Theory of Operations

This chapter explains RADIUS in the context of your ASTRO® 25 system.

This chapter pertains to the RADIUS functionality provided by Microsoft Network Policy Server (NPS) in an ASTRO® 25 system.

3.1

RADIUS Technical Overview

Remote Authentication Dial-In User Service (RADIUS) is a client-server protocol that enables devices in a network which are set up as RADIUS clients to submit authentication requests to a RADIUS server.

RADIUS provides the following functions:

- Provides a centralized authentication and authorization service for all access requests that are sent by RADIUS clients.
- Validates user credentials against the user accounts stored in an Active Directory domain.
- Supports the Protected Extensible Authentication Protocol (PEAP) for 802.1x and the Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) for centralized authentication.
- Provides a log of all access requests sent by the RADIUS clients.

Communication between the server where RADIUS resides and the RADIUS client is encrypted by using a text string known as a shared key or shared secret. In this way, the password entered by the user is encrypted before sending it to the server where RADIUS resides.



IMPORTANT: The shared key must be configured to be identical on the RADIUS server and on the RADIUS client. The shared key should meet the length and complexity requirements for a strong password.

3.2

RADIUS in ASTRO 25 Systems

In an ASTRO® 25 system, Microsoft Windows Network Policy Server (NPS) is installed on each Domain Controller in a zone, as well as in the Trunking Subsystem (Tsub), to provide RADIUS services.

The ASTRO® 25 implementation of RADIUS using NPS adds the following authentication capabilities to the system:

- Authentication of network access through the following types of devices:
 - Routers
 - GGM 8000 Gateways
 - HP Switches
 - Fortinet Firewall
 - Fortinet Firewall Manager
 - GTR 8000 Base Radios
 - GCP 8000 Site Controllers

- GCM 8000 Comparators
- GPB 8000 Reference Distribution Module (RDM)
- Voice Processor Module (VPM) devices:
 - + SmartX Site Converter
 - + MCC 7500 Voice Processor Module (VPM)
 - + Telephone Media Gateway (TMG)
- Console Telephony Media Gateway
- MOSCAD Network Fault Management (NFM) devices:
 - + SDM3000 Remote Terminal Unit (SDM3000 RTU)
 - + SDM3000 Network Translator (SNT)
 - + MCC 7500 Aux I/O Server
- Point-to-Point (PTP) radio devices (PTP 600 Series and PTP 800 Series)
- Extreme E4G series switches
- KVL 4000
- Unified Network Configurator
- Console Telephony Media Gateway
- Authentication of users connecting to the network through service ports on the following devices is implemented using the IEEE 802.1x standard:
 - HP Switches
 - GCP 8000 Site Controller (integrated and/or managed Ethernet switches)
 - GPB 8000 Reference Distribution Module (RDM) (integrated and/or managed Ethernet switches)



NOTICE: For more information concerning the 802.1x standard, see the *802.1x Service Ports on Switches* manual.

For the authentication to take place, the following conditions must be fulfilled:

- User accounts and groups in Active Directory must be defined.
- Devices must be added to the Active Directory domain.
- RADIUS authentication sources and parameters on the device must be configured.
- Matching shared secrets on the RADIUS servers and RADIUS clients must exist.
- For RF site and VPM-based devices, DNS must be operating in the system and DNS must be configured on the device.

In ASTRO® 25 systems, for central authentication services, RF site and VPM devices are configured to access the RADIUS service through a Fully Qualified Domain Name (FQDN), so that the IP addresses for the RADIUS service can be changed without changing the configuration on every device.



IMPORTANT: The RF Site and VPM devices support a maximum length of 31 readable characters for RADIUS usernames and 127 characters for passwords. Any names or passwords longer than this will be truncated to this length before transmission to the central RADIUS servers, possibly leading to authentication failures. Any account that must be able to log on to an RF Site or VPM device must be restricted to this length.



NOTICE: The HP switches must use the IP address of the RADIUS server because they do not support FQDN. For RF site and VPM devices, the use of an FQDN is recommended.

3.2.1

RADIUS vs. Local Authentication for Sessions Between a Device and UNC

In ASTRO® 25 systems, RADIUS enables authentication for Telnet, FTP, Secure Shell (SSH), and serial console sessions with a RADIUS client, including the following sessions using the VoyenceControl component of the Unified Network Configurator (UNC) application:

- Interactive Cut-Through sessions
- Non-interactive configuration pushes and pulls



NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

Global Account credentials in VoyenceControl minimize management and entry of usernames and passwords required for authenticating a VoyenceControl session. After setting up a VoyenceControl Account credential's username and password, you can specify that VoyenceControl use that Account credential whenever VoyenceControl performs a management function (such as a configuration push) on a device. When a VoyenceControl Account credential is selected for a device, VoyenceControl can automatically respond to the logon prompt from that device with the username and password set up for that Account credential.



NOTICE:

For interactive Cut-Through sessions, you may want to configure the device not to use VoyenceControl Account credentials, in which case the device prompts you to enter the username and password manually.

For management functions which are executed as scheduled jobs in VoyenceControl, such as a configuration push, selecting a VoyenceControl account credential for the device eliminates the need for you to be available to enter the username and password when the scheduled job executes.

In an ASTRO® 25 system, if a device has RADIUS authentication enabled, the VoyenceControl Account credential selected for that device must have a username and password that match the username and password for a corresponding account on the RADIUS server. This requires that you:

- **Use the VoyenceControl Credentials Manager to create a global Account credential with a username and password that match a username and password on the RADIUS server.** (Do not change the username or password of the VoyenceControl Account credentials that are pre-defined for use by VoyenceControl during initial discovery of devices. This includes accounts for various categories of switches, routers, gateways, and terminal servers as listed in the ASTRO® 25 system *Unified Network Configurator* manual. Keep the default usernames and passwords for these Accounts so that they can be used in a recovery situation.)
- **Use the Update Credentials window for a device to select the VoyenceControl Account credential with the same username and password as the account for that device on the RADIUS server.**

In addition to setting up global Account credentials in VoyenceControl that have the same username and password as accounts on the RADIUS server, you can set up global Account credentials in VoyenceControl that match the username and password set up locally on a device. The following are examples of when you would use VoyenceControl Account credentials that match local usernames and passwords on a device (if allowed by your organization's policies):

- When you set up a scheduled job in VoyenceControl for a device where RADIUS authentication is not enabled yet.

- When you set up a scheduled job in VoyenceControl for a RADIUS-enabled device where RADIUS authentication has failed and you have confirmed that the shared secret on the switch is the same as the shared secret for this device on the RADIUS server.



NOTICE:

If a global Account credential in VoyenceControl is supposed to match the username and password maintained locally on the device, and a local technician changes the local username or password on the device, then the global Account credential in VoyenceControl no longer works for communicating with that device. The local technician should communicate local username and password changes to a VoyenceControl administrator so that the change can be made in any corresponding VoyenceControl credentials.

Changes to local usernames and passwords on a device do not require any changes on the RADIUS server.

Changes to local usernames and passwords on a device do not require any changes to VoyenceControl Account credentials that are set up to match a username and password on the RADIUS server.

For additional information about the UNC, refer to the *Unified Network Configurator* manual. For information about managing local credentials on a device, see the ASTRO® 25 system manual specific to that device.

3.2.2

Password Restrictions for Local and RADIUS Accounts

Table 4: Password Restrictions for Local and RADIUS Accounts on ASTRO 25 System Devices

Device	Local Password (max number of characters)	RADIUS Password (max number of characters)	Active Directory password (min num- ber of characters)
ProCurve J9085A Switch 2620–24	15	15	12
ProCurve Switch 2626	15	15	12
HP ProCurve Switch 5308xl	16	16	12
ProCurve Switch 3500yl	64	64	12
HP Switch E3800-48	64	32	12
Routers (ASTRO® 25 7.11 system release and after)	15	31	12
Routers (prior to the ASTRO® 25 7.11 sys- tem release)	15	15	12
Fortinet Firewall	128	128	12
Fortinet Firewall Man- ager	80	127	14
Terminal Server	32	32	12
Site and VPM devices	255	127	12

Device	Local Password (max number of characters)	RADIUS Password (max number of characters)	Active Directory password (min num- ber of characters)
PTP 600 and 800	31	31	12
Unified Network Con- figurator	100	100	12



NOTICE: RADIUS account passwords cannot be changed on the device, so there is no interaction between device minimum password length for local accounts, and RADIUS server minimum/maximum password length.

3.2.3

Authentication for Devices Accessed with CSS

Users of Configuration/Service Software (CSS) are required to authenticate using local or centralized credentials to access the following devices, depending on what authentication methods are enabled on these devices:

- GTR 8000 Base Radios
- GCP 8000 Site Controllers
- GCM 8000 Comparators
- Voice Processor Module (VPM) devices:
 - SmartX Site Converter
 - MCC 7500 Voice Processor Module (VPM)
 - Telephone Media Gateway (TMG)
- GPB 8000 Reference Distribution Module (RDM)

This includes access through the local Serial Service Port, local Ethernet Service Port, or remotely over the network.

The CSS user can still access the device using its local account, in addition to the centralized accounts.



NOTICE: If, in addition to centralized authentication, the 802.1x security feature has been implemented on the GCP 8000 Ethernet service port or GPB 8000 Reference Distribution Module (RDM), then a CSS user encounters two separate login prompts when connected to the service port:

- 802.1x login to permit access to the network
- CSS login to permit access when connecting to the GCP 8000 or GPB 8000, or when connecting through the GCP 8000 or GPB 8000 switch to other devices at the site

3.3

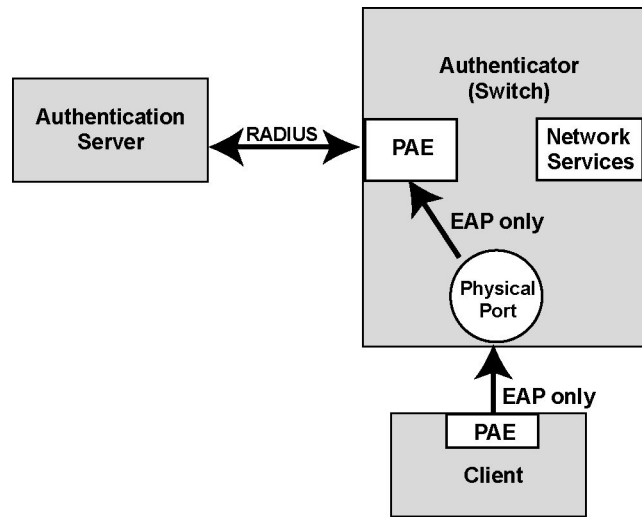
RADIUS Authentication

RADIUS messages provide authentication and authorization for devices on a network in the following way:

- 1 The RADIUS server receives an authentication request containing the user's credentials.
- 2 The RADIUS server communicates with Active Directory to validate the user credentials.
- 3 Active Directory verifies the user and permits the RADIUS server to authenticate the user.
- 4 The RADIUS server authorizes the user based on the Remote Access policies and the user's dial-in policy.

The following figure shows an example of how RADIUS is used to authenticate a service user at an 802.1x-enabled Ethernet port. It shows the conditions **before the service user authenticates through RADIUS, when the user has no access to Network Services**. The Port Access Entity (PAE) component of 802.1x on the 802.1x client (service laptop) and the PAE component at the 802.1x-enabled Ethernet service port of the device exchange messages through EAP only.

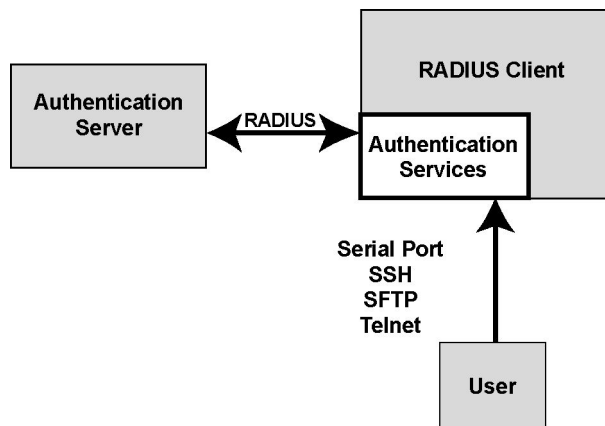
Figure 1: RADIUS Authentication at an 802.1x-Enabled Ethernet Port



Ethernet_Port_Security_RADIUS_Access

The following figure shows an example of how RADIUS is used to authenticate a user at a device where centralized authentication is implemented.

Figure 2: RADIUS Authentication at a Device Where Centralized Authentication is Implemented



Centralized_Auth_RADIUS_Access

In an ASTRO® 25 system, 802.1x authentication is supported only by the following devices:

- HP switches
- Internal switches on GCP 8000 Site Controllers
- Internal switches on GPB 8000 Reference Distribution Modules (RDMs)

3.3.1

RADIUS Authentication – Device-Level vs. 802.1x Ethernet Port

The following table lists the differences between RADIUS authentication at an 802.1x-enabled Ethernet service port compared to RADIUS authentication at a device where centralized authentication is implemented.

Table 5: RADIUS Authentication – Device-Level vs. 802.1x Ethernet Port

RADIUS Authentication at a Device	RADIUS Authentication at an 802.1x Ethernet Port
RADIUS authentication provides the user with access to the RADIUS client.	The 802.1x port provides the user with access to the network.
The user can access the device locally or remotely.	The user accesses the network through the 802.1x port.
Local access is through a local serial service port or Ethernet port.	
Remote access can be through Secure Shell (SSH), Secure File Transfer Protocol (SFTP), TELNET, or FTP.	

3.4

RADIUS Remote Access Policies

When RADIUS is used to authenticate a user in the ASTRO® 25 system, the following must be configured:

- The **Control access through Remote Access Policy** option must be selected on the **Dial-In** tab of the **Properties** for that user or user's group in Active Directory.
- A Remote Access Policy must be created in the Network Policy Server (NPS) which specifies that user or group and the characteristics of network resources which are allowed to be accessed by that user or group.



NOTICE: RADIUS authentication can be configured to allow user access only to devices in a selected network segment. Consult RADIUS configuration documentation provided by Microsoft Network Policy Server (NPS), or the Motorola Solutions Support Center (SSC) for details.

3.5

RADIUS Client Configuration Parameters

This section specifies configuration parameters required from the RADIUS client with the appropriate interface to the RADIUS server.

The following conditions are important for the RADIUS client configuration:

- Each RADIUS client is configured with a minimum of two RADIUS servers and a maximum of three RADIUS servers.
- Each client is configured at minimum with the RADIUS server in its RNI zone as the primary and the RADIUS server in the UCS subnet as the secondary.

For Trunking Subsystems (Tsubs), the Tsub prime site RADIUS server is the secondary.

- RADIUS service hostnames or IP addresses (where applicable), as defined in the system IP plan, are used instead of the primary IP address of the domain controllers.

Table 6: RADIUS Client Configuration Parameters

System	Primary DC	Secondary DC	Tsub Prime Site DC
Non-DSR	z<zzz>rad01 where <zzz> is the zone number	ucs-rad01	z<zzz>s<ppp>rad0 1 where: <zzz> is the zone number <ppp> is the prime site number
DSR	z<zzz>rad03 where <zzz> is the zone number	ucs-rad03	z<zzz>s<ppp>rad0 1 where: <zzz> is the zone number <ppp> is the prime site number



NOTICE: RADIUS replication is unidirectional. Only RADIUS clients are replicated. The changes in the zone-level domain controller are replicated to ucs-dc but not the other way. As network policies are not replicated, changes to the network policies need to be performed manually.

Chapter 4

DNS Theory of Operations

This chapter explains Domain Name Services (DNS) in the context of your ASTRO® 25 system.

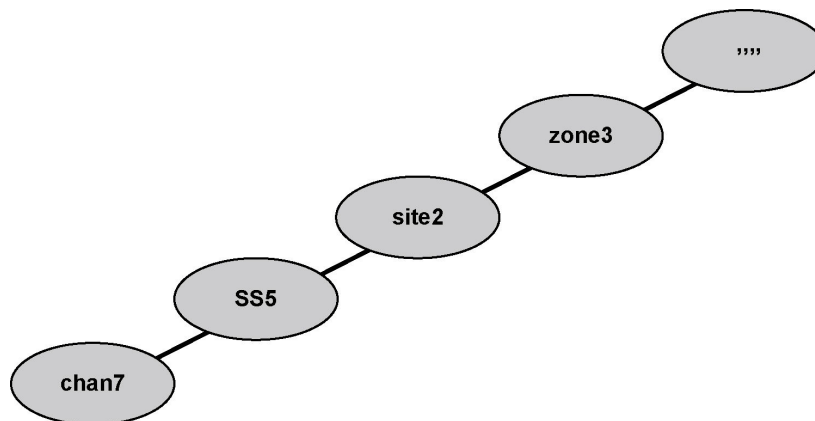
4.1

DNS Introduction

The main goal of DNS is to provide hostname IP address mapping. It can take a hostname and return the IP address associated with that hostname. It can also do the opposite. It can take an IP address and return the hostname associated with that IP address. It provides functionality to look up other data, but hostname/IP address resolution is the primary goal of DNS.

DNS is set up as a tree structure. Each portion of the tree is a DNS domain. Each domain can be administered separately from the other domains. Each DNS domain can reside on a different DNS server. For hostname to IP address resolution (also called forward lookup), the tree follows the dotted names. Each node in the tree is part of the domain name. The leaf of the tree is the short hostname of the device. The top of the tree is the root. The root is a null value. For example, the tree structure for chan7.ss5.site2.zone3 looks as shown in the following figure.

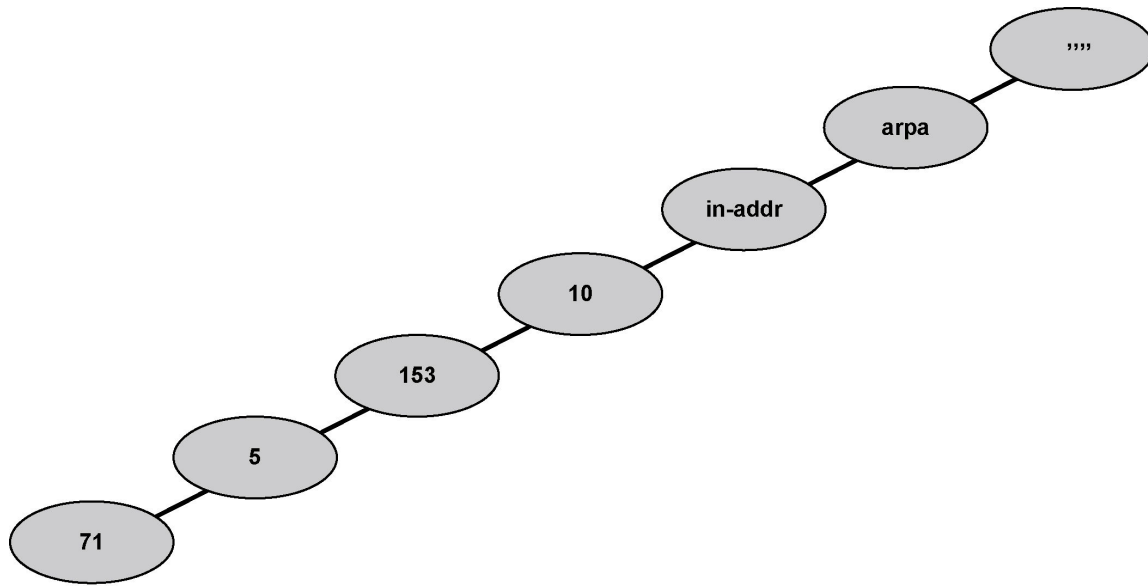
Figure 3: Forward Zone Tree Hierarchy



ActiveDirectory_forward_hierarchy

A slightly different tree structure is followed for IP address-to-hostname resolution (or reverse lookup). The reverse tree structure starts with a null as the root. This is followed by "in-addr.arpa." The first three octets of an IPv4 address are nodes. The fourth octet is the leaf. For example, the tree structure for the IP address 10.153.5.71 looks as shown in the following figure.

Figure 4: Reverse Zone Tree Hierarchy



ActiveDirectory_reverse_hierarchy

Each DNS server is called a nameserver. A nameserver owns (that is, is authoritative for) a portion of the DNS domain space. This portion is called a DNS zone. A nameserver can be authoritative for one or more DNS zones.

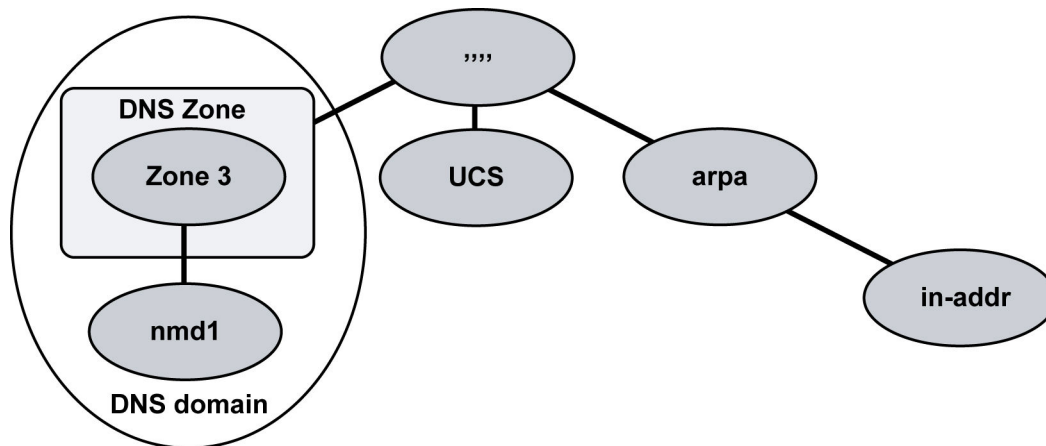
4.1.1

Domains and Zones

The main difference between a DNS domain and a DNS zone has to do with delegation. A DNS domain is all data associated with a particular node in the tree and everything underneath it. A DNS zone is the collection of information for a particular portion of a DNS domain for which a DNS server is authoritative.

In the example shown in the following figure, ucs, zone3 and nmd1.zone3 are DNS domains (zone3 is also a DNS zone). The DNS server authoritative for zone3 delegated the nmd1.zone3 domain to a different DNS server. That other DNS server is now authoritative for the nmd1.zone3 DNS domain. That DNS server's zone of authority includes nmd1.zone3. It does not include zone3, and the DNS server for zone3 is not authoritative for the nmd1.zone3 DNS domain. The DNS server for zone3 just knows how to redirect queries for the nmd1.zone3 DNS domain because of the delegation.

Figure 5: DNS Domains Versus DNS Zones

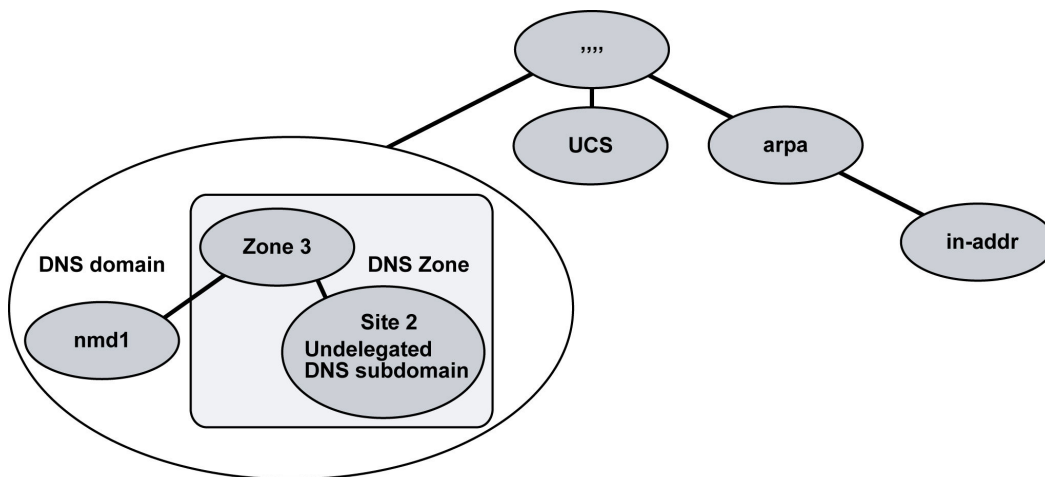


ActiveDirectory_DNS_domains_zones_A

Delegation is what allows for distribution of administrative responsibilities. Each portion of the DNS domain namespace is delegated to a different DNS zone. If a DNS domain contains information about its children in the same DNS zone, the child DNS domains are termed undelegated subdomains.

Extending the example given in the following figure, if the host sc1.site2.zone3 exists, but that information exists in the zone3 DNS zone, the site2.zone3 DNS domain is an undelegated subdomain of zone3.

Figure 6: Undelegated DNS Domains



ActiveDirectory_undelegated_DNS_domains_A

4.1.2

Resource Records

DNS data is stored as a collection of records known as Resource Records (RRs). Each RR follows a certain syntax. Each DNS zone data file contains RRs specific for that zone. Depending on the type of zone, different types of RRs exist.

The following are some of the more common types of RRs:

Start of Authority (SOA)

Signifies the start of the DNS zone, and identifies various parameters associated with this particular DNS zone.

Name Server (NS)

Identifies the set of DNS servers that are authoritative for a particular DNS domain. Provides the “glue” that helps tie the DNS system together.

Address (A)

Provides the hostname to IP address mapping.

Alias (CNAME)

CNAMEs are DNS aliases. Allows the host to be known by more than one name.

Pointer (PTR)

Provides IP-address-to-hostname mapping.

Service Resource Records (SRV)

Primarily used by Windows clients to find the Domain Controllers, but some applications may use them to find other services.

4.2

Service Detail

Active Directory depends on dynamic DNS. Consequently, the existing DNS environment must be modified to support dynamic updates made by the Active Directory elements (DCs and/or clients).

4.2.1

Network IP Services

Each radio network infrastructure (RNI) zone acts as an independent entity from a network IP perspective. Each RNI zone houses its own set of IP services.

The Network IP services in each RNI zone are tied together by the Operations Support Systems (OSS) portion of the radio network, which is the “UCS subnet” (the subnet where the User Configuration Server resides).

The UCS subnet includes the following devices:

- User Configuration Server (UCS)
- Network Management (NM) Client
- Core Security Management Server (CSMS)
- Fortinet Firewall Manager
- Domain Controller
- InfoVista Server – if present in the system
- System Statistics Server (SSS) – if present in the system
- AuC Server
- Baseline Backup and Recovery Server or Backup and Recovery Server (BAR) – if present in the system
- Unified Network Configurator (UNC) server
- Unified Network Configurator Device Servers (UNCDS)

4.2.2

Domain Names

The UCS subnet contains the root of the DNS namespace. All DNS domains for the radio network infrastructure (RNI) zones are tied into the UCS DNS domain.

For Active Directory, this means the system-level domain controller (UCS-dc01) acts as the central authority for the Active Directory domain structure since it is built first and has special roles associated

with it. All Active Directory domain controllers for the RNI zones are tied into the same Active Directory domain. Active Directory follows the DNS namespace. The following are naming conventions for the DNS domain setup:

- The system-level DNS domain is called `ucs`.
- Each RNI zone is its own DNS domain. Each RNI zone-level DNS domain is called `zone<z>`, where `<z>` is the zone ID.
- Each RNI zone contains DNS subdomains for the various manned and unmanned sites:
 - Domain names for site-level devices are based on the site ID and zone ID, such as `site<x>.zone<z>` or `nmd<x>.zone<z>`
where:
 - `<x>` is the site number
 - `<z>` is the zone number
 - If applicable, a subsite (remote site) ID is also included, such as `ss<x>.site<y>.zone<z>` (for a circuit simulcast subsite) or `ipss<x>.site<y>.zone<z>` (for an IP simulcast subsite)
where:
 - `<x>` is the subsite number
 - `<y>` is the site number
 - `<z>` is the zone number

4.2.3

Accessibility and Availability

Redundancy is tied into both the Active Directory and DNS services. To achieve that redundancy:

- The information housed on the Active Directory domain servers (also called the Domain Controllers or DCs) must reside on more than one server.
- The information housed on the DNS servers must reside on more than one server.

Therefore, each Active Directory domain or DNS domain must have at least two DCs or two DNS servers. These servers need not be mutually exclusive. DNS redundancy is achieved by having the zone-level DC as the primary DNS server for that Zone DNS data and UCS DC as the secondary DNS server for all Zone DNS data. In ASTRO® 25 systems, the Active Directory DCs are also DNS servers.

To install and initialize Active Directory in an RNI zone, a network connection must exist between the RNI zone's Active Directory Domain Controller and the master DNS server for the RNI zone.

In an ASTRO® 25 system, network connectivity is also required when the DNS servers are installed. The installation process tests for connectivity, because connectivity is required to configure the DNS servers. Connectivity between the DNS masters is also required so that they can update each other.

Kerberos authentication against Active Directory depends on DNS availability. Hence, a client must have at least one DNS server accessible to be able to use any one of the Domain Controllers in the system for authentication purposes.

4.2.4

Server Location

For Active Directory, at least one Domain Controller resides in both the UCS subnet, and another Domain Controller resides in the zone core. Other DCs should be added to a non-Tsub console site based on the number of devices located at that site. They would reside on their own ESXi-based virtual

servers. The following table specifies the number of those Windows-based devices (MCC 7500s and MCC 7100s).

Table 7: Additional Active Directory Servers Required

Active Directory Domain Controllers	Number of Windows-Based MCC 7500 Devices and/or MCC 7100 Devices
0	<15
1	15 to 30
1 or 2	>30

The DNS service in an ASTRO® 25 system is provided by the Domain Controllers.

Domain Controllers in the system are interconnected over the network and replicate the DNS and Active Directory data for increased availability and reliability. Because the Domain Controller contains the same information and interface with each other using Active Directory Two Way Trusts, the relationships between domains establish a trusted communication path through which a network device in one domain can communicate with network devices in the other domain.

Additional Domain Controllers can be added to each subnet, if additional processing is needed.

The Domain Controllers are Windows-based servers. They are implemented as Virtual Machines on a Virtual Server.

4.2.4.1

Domain Setup

The domain controller in the UCS subnet is the top of the Active Directory domain setup. All other Active Directory domains are tied to it through the trusts. This domain contains user accounts used throughout the radio network.

As there is a single Active Directory domain for the entire system, all DCs are peers to each other. Any device joined into the AD domain communicates with any domain controller. The join operation creates a computer account in the AD domain, and authentication material that establishes client-server mutual trust. This domain contains the user and groups used throughout the radio network, as well as security policies for all RNI zones.

The UCS domain controller is at the top of the DNS hierarchy (that is, it is the root DNS server). It delegates portions of the DNS namespace to the DNS servers (that is, the zone-level Domain Controllers) in each RNI zone.

4.2.4.2

Domain Controller Functions in a Dynamic System Resilience System

When the Dynamic System Resilience (DSR) feature is added to an ASTRO® 25 system:

- A system-level Domain Controller (`ucs-dc03.ucs`) is added in the backup core for the zone which includes the system-level domain controllers.
- A zone-level Domain Controller (`z<zzz>dc03.zone<z>`) is added in the backup core for the zone.
- You can view and change Active Directory data using any of the domain controllers. Synchronization of Active Directory data occurs automatically between domain controllers.
- RADIUS clients can be added, updated, or deleted in the primary or backup zone DC. Changes made to the RADIUS client list in the primary core are replicated to the backup core when you trigger RADIUS replication. Only RADIUS client changes are replicated. Changes to network policy are not replicated and need to be performed manually.
- The DNS data is replicated to all domain controllers, just like the Active Directory data.

- For redundancy, clients must be configured with a minimum of two DNS nameservers for the DSR system (primary and secondary).

4.2.4.3

Configuration of DNS IP Addresses on Clients

Any computer that is part of an Active Directory domain must be configured with DNS Service IP addresses before it can be joined to the Active Directory domain.

The hostnames of the DNS nameservers are listed in [DNS Nameservers for Devices in DSR and Non-DSR Sites on page 94](#), however, it is the IP address that must be entered when configuring DNS. The DNS client cannot perform a DNS query to resolve the nameserver hostname into an IP address. The IP addresses for these hosts are available in the *System IP Plan*. For redundancy, clients must be configured with a minimum of two DNS nameservers.

4.2.4.3.1

Dynamic DNS

Clients can update DNS with their hostname and IP address dynamically. In order for this to work, the DNS zones must be set up to allow for dynamic DNS updates.

Windows clients are able to use the dynamic aspect of DNS to automatically enter themselves into DNS. If the Windows client is joined to the domain, then the dynamic updated message can be secured/encrypted. Other clients, such as Unix clients, must either be statically entered (at nameserver install time) or must supply the functionality to dynamically enter themselves into DNS.

For a list of Windows and Unix clients, see [Active Directory Client Devices and Applications on page 36](#).

4.2.5

DNS Backup and Restore

The backup and restore of DNS is handled as part of the backup and restore of the Domain Controllers.

For backup and restore of the Active Directory data, see [Active Directory Data – Backup and Restore on page 40](#).

Chapter 5

AD/DNS Installation and Configuration

This chapter provides information on installing and configuring Active Directory (AD) and Domain Name Services (DNS) in an ASTRO® 25 system.

5.1

Installing and Configuring Domain Controller Software for AD/DNS

Perform this process to set up a domain controller as a virtual machine on a virtual server. To determine on which virtual server to install a domain controller virtual machine, see [Authentication Servers in ASTRO 25 Systems on page 28](#).

This process applies to the following Domain Controllers (DCs) in the ASTRO® 25 system:

- System-level
- Zone-level
- At a site (non-Tsub console site and Tsub prime site)

Prerequisites:

Obtain the information from your system administrator, as indicated in [User Input Requirements for Server Installation/Configuration on page 75](#).

Ensure that all hardware setup has been completed. See the *Virtual Management Server Hardware* manual.

Process:

- 1 For all DCs:** Import the Domain Controller Virtual Machine.
See [Importing the Domain Controller Virtual Machine on page 59](#).
- 2 For all DCs:** Configure the Domain Controller Virtual Machine resources.
See [Configuring Virtual Machine Resources on page 61](#).
- 3 For all DCs:** Apply supplemental configuration to the ESXi server-based Virtual Machine.
See [Applying Supplemental Configuration to Virtual Machines on page 62](#).
- 4 Only for systems with vCenter already installed:** Configure vCenter.
See [Configuring the vCenter for the Newly Deployed VM on page 63](#).
- 5** Set the Virtual Machine startup and shutdown order.
See “Setting the Virtual Machine Startup and Shutdown Order” in the *Virtual Management Server Software* manual.
- 6 For all DCs:** Power up the virtual machine.
See [Connecting and Powering on a New Virtual Machine on page 64](#).
- 7 For all DCs:** Apply OS-level identity.
See [Applying OS-Level Identity on the Domain Controller on page 65](#).
- 8 For all DCs:** Configure the Domain Controller Virtual Machine.

See [Activating a Domain Controller Virtual Machine on page 66](#).

- 9 For all DCs:** Upgrade the VMware tools on the virtual machine.

See [Reconfiguring VMware Tools on a Windows-Based Virtual Machine on page 66](#).

- 10 Optional:** If you are adding domain controllers to an existing system, see [Adding the Domain Controller to an Existing System on page 68](#).

- 11** Install the system-level DCs in the following order:

- a** Install the **first system-level DC**.

See [Installing the First System-Level DC on page 69](#).

- b** Install the **backup system-level DC**.

See [Installing the Backup System-Level DC on page 70](#).

- 12** Install the **zone-level DC**.

See [Installing First and Backup Zone-Level DCs on page 71](#).

- 13** Install the **DC at a non-Tsub console site**.

See [Installing the Domain Controller at a Console Site \(Non-Tsub\) on page 72](#).

- 14 For Trunking Subsystem (Tsub):** Install the DC at a Tsub prime site.

See [Installing the Domain Controller at a Tsub Prime Site on page 73](#).

- 15 For all DCs:** Clear the post-install configuration warning on the DC.

See [Clearing the Post-Install Configuration Warning on the Domain Controller on page 74](#).

- 16 For all DCs:** Only after all domain controllers are installed, apply post-install AD configuration.

See [Applying Post-Install AD Configuration on page 74](#).

- 17** Import RADIUS clients into the RADIUS Server.

See [Batch Importing RADIUS Clients to the Primary RADIUS Server for a Zone on page 80](#).

Postrequisites: All Unix devices in the UCS subnet should be joined into the domain only after the colocated zone domain controller is installed. If the Unix devices in the UCS subnet are joined to the domain before the colocated zone domain controller is set up, they do not have domain controller redundancy. For a list of Unix devices, see [Active Directory Client Devices and Applications on page 36](#).

5.1.1

Importing the Domain Controller Virtual Machine

Prerequisites:

Obtain the following from your system administrator:

- *Motorola Windows Server* media (provided by Motorola Solutions; contains the Windows Server 2012 R2 virtual machine files)
- Virtual Server host (ESXi-based server) **<IP address>**
- ESXi-based server administrator account name **<password>**

Location, Hostname, and destination network for the Domain Controller you are setting up. See [User Input Requirements for Server Installation/Configuration on page 75](#).

Procedure:

- 1** Double-click the **VMware vSphere Client** icon on the Windows server where it is installed.
- 2** At the login screen, type in:

- a The ESXi-based server **<IP address>**
 - b The account name `root`.
 - c The root account **<password>**.
- 3 Click **Login**.
The **vSphere Client** main window appears.
- 4 In the DVD drive of the Windows server where the client resides, insert the *Motorola Windows Server* media.
- 5 Optional: For optimal speed during the import process, copy all the files from the DVD to a temporary location on the hard drive of the Windows-based device that you are using for this import.
- 6 In the **vSphere Client** main window menu, select **File→Deploy OVF Template**.
- 7 In the **Deploy OVF Template** window, **Source** screen, click **Browse**.
- 8 In the **Open** dialog box, ensure that OVF (*.ovf) is the selected file type.
- 9 Navigate to the *.ovf file on the DVD.
If you copied this file to the hard drive, navigate to the directory where you pasted it.
- 10 Select the file. Click **Open**.
The **Open** dialog box closes and the file name appears in the **Deploy OVF Template** window, **Deploy from a file or URL** field.
- 11 In the **Deploy OVF Template** window, **Source** screen, click **Next**.
- 12 In the **OVF Template Details** screen, click **Next**.
- 13 In the **Name and Location** screen, perform the following actions:
 - a In the **Name** field, enter the appropriate **<DC hostname>**.
See [User Input Requirements for Server Installation/Configuration on page 75](#).
 - b Click **Next**.
- 14 In the **Deploy OVF Template** window, perform one of the following actions:
 - If the **Datastore** screen appears , select **z<xxx>das<yy>_datastore1**. Click **Next**.
Where:
<xxx> is the Zone ID of the VMS that the application is being installed upon
<yy> is the instance of the DAS associated with the VMS
 - If the **Datastore** screen does not appear before the **Disk Format** screen appears in the **Deploy OVF Template** window, local hard drives are not implemented on the ESXi-based server.
- 15 In the **Disk Format** screen, perform one of the following actions:
 - Select the **Thick Provision Eager Zeroed** option, if it is available.
 - If the option is not available, select the **Thick Provision** option. Click **Next**.
- 16 In the **Deploy OVF Template** window, **Network Mapping** screen, select the appropriate zone network for the domain controller virtual machine from **Destination Networks** drop-down list. Click **Next**.
Step example:ZNM0 destination network for the zone-level DC
- 17 In the **Ready to Complete** screen, verify the information that is displayed. Click **Finish**.
The import begins. A progress window displays the status of the installation.

18 In the **Deployment Completed Successful** window, click **Close**.

19 Remove the media from the drive.

Related Links

[Installing and Configuring Domain Controller Software for AD/DNS](#) on page 58

5.1.2

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 CommonOS 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 CommonOS 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:
 - **System-level DCs and zone-level DCs in an M1 or L1 system:**
`<cdrom drive>:\VM_Resource_Config\Domain_Controller_Low_Resource.xml`
 - **System-level DCs and zone-level DCs in all other systems:**

```
<cdrom drive>:\VM_Resource_Config
\Domain_Controller_High_Resource.xml
```

- **Trunking Subsystem (Tsub) DCs:**

```
<cdrom drive>:\VM_Resource_Config
\Domain_Controller_High_Resource.xml
```

- **Console Site DCs:**

```
<cdrom drive>:\VM_Resource_Config\Domain_Controller_Low_Resource.xml
```

where **<cdrom drive>** 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`

5.1.3

Applying Supplemental Configuration to Virtual Machines

Virtual machines hosted on the ESXi-based Virtual Management Server (VMS) require supplemental configuration to improve their security settings. You apply the supplemental configuration by running a script stored on the *VMware vSphere Configuration Media* disc.

Prerequisites:

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

When and where to use: To perform this procedure, use a Windows-based device, such as the Network Management (NM) Client, Dispatch Console, or service computer/laptop.

Procedure:

- 1 Insert the *VMware vSphere Configuration Media* disc into the optical drive of the Windows-based device.
- 2 Open the PowerShell command prompt as administrator, using the actions that apply to the Windows operating system version present on the device.

If...	Then...
For Windows 7 or Windows Server 2008,	perform the following actions: <ol style="list-style-type: none"> a From Start, in the Search programs and files field, enter: <code>Command Prompt</code> b Right-click Command Prompt and select Run as administrator. c If the User Account Control window appears, click Continue or Yes, depending on the prompt you see. d If you are not logged on with an administrative account, enter the domain admin credentials. e At the command prompt, enter: <code>powershell</code>
For Windows 10 or Windows Server 2012,	perform the following actions: <ol style="list-style-type: none"> a From Start, click Search. b In the search field, type in <code>powershell</code> c Right-click Windows PowerShell, and select Run as administrator.

If...	Then...
	<ul style="list-style-type: none"> • If the User Account Control window appears, click Yes. • If you are not logged on with an administrative account, enter the domain admin credentials.

- 3 At the PowerShell prompt, enter the drive letter of the optical drive that contains the *VMware vSphere Configuration Media* disc followed by a colon.

Step example:E :

The directory is changed to the root directory of the *VMware vSphere Configuration Media* disc.

- 4 At the PowerShell prompt, enter: `cd common\bin`

The directory is changed to the `common\bin` directory of the *VMware vSphere Configuration Media* disc.

- 5 At the PowerShell prompt, enter: `.\Configure-VMHardening.ps1`

- 6 At the ESXi host IP prompt, enter the IP address of the ESXi host.

- 7 At the user name prompt, enter the ESXi host user name for an administrative account.

- 8 At the password prompt, enter the ESXi host password for an administrative account.

- 9 At the PowerShell, prompt, enter the name of the virtual machine for which you want to update the configuration.



NOTICE: Ensure that the name matches the name of the virtual machine as it appears in the left pane of the vSphere Client inventory view when connected to the ESXi host.

The virtual machines supplemental configuration is applied.

- 10 Verify that there are no messages stating `[FAILED]` in the output of the script.

- 11 At the PowerShell prompt, enter: `exit`

- 12 At the Windows command prompt, enter: `exit`

5.1.4

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.

5.1.5

Connecting and Powering on a New Virtual Machine

Prerequisites: Obtain the name of the appropriate zone network for the server you are setting up as a virtual machine from your system administrator.

Procedure:


1 Edit the configuration settings for the virtual machine you imported:

a In the navigation pane, right-click the virtual machine that you imported.

b In the pop-up menu, select **Edit Settings**.

c In the dialog box, select each one of the network adapters.

d If not already selected, select the **Connect at power on** check box.

- e Ensure that the correct zone network connection displays for **Network Label**.
 - f Click **OK**.
- 2 Turn on power to the virtual machine:
- a In the navigation pane, right-click the virtual machine that you imported.
 - b From the context menu, select **Power**→**Power On**.
-  **NOTICE:** Selecting an incorrect zone network may cause problems with the installation of the domain controller.
- c Select the virtual machine from the pane on the left and click the **Console** tab for this virtual machine.
- Ignore any failure messages displayed during power on of the virtual machine.

Related Links

[Installing and Configuring Domain Controller Software for AD/DNS](#) on page 58

5.1.6

Applying OS-Level Identity on the Domain Controller

Perform this procedure to apply Operating System (OS) configuration to the Domain Controller virtual machine.

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 Domain Controller 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:
 - a Select **Domain Controller**.
 - b Ensure the selected time zone is correct.
 - c Click **Execute**.

Ignore any messages about finding devices on the network.
- 6 Wait for OS reboot.

Ignore any messages about formatting the drive displayed during the reboot.

5.1.7

Activating a Domain Controller Virtual Machine

Perform this procedure to activate a domain controller virtual machine on the Windows Server 2012.

Procedure:

- 1 After powering on the domain controller virtual machine for the first time, click the domain controller virtual machine in the navigation pane on the left side of the screen, and then click the **Console** tab on the right side of the screen.
- 2 From **Start**, select **Control Panel**→**System and Security**→**System**.
- 3 In the **Windows activation** area, click **Activate Windows**.
- 4 Enter the new *<Windows Server 2012 Product Key>*,
where *<Windows Server 2012 Product Key>* is the Virtual Product/License key associated with the Microsoft Windows Server 2012 media. It may be located on a sticker that came with the media or it may be attached to the hardware.

Windows attempts to activate online with the new product key, or displays the **Windows Activation Wizard** which you can follow to complete the activation process.

Related Links

[Installing and Configuring Domain Controller Software for AD/DNS](#) on page 58

5.1.8

Reconfiguring VMware Tools on a Windows-Based Virtual Machine

Reconfiguring VMware tools is performed after an ESXi-based virtual server is installed and operational in your system.

When and where to use:

In the desktop taskbar of a Windows-based virtual machine, in the notification area on the far right, if a VMware Tools icon is displayed, do not use it to initiate a VMware Tools upgrade.

Instead, for upgrading VMware Tools on a Windows-based virtual machine, follow the steps in the *Readme* file on the *MOTOPATCH for VMware* media. If the upgrade fails, see any known issue workarounds in the *Readme* file, then contact Motorola Solutions Support Center if needed.

Procedure:

- 1 Launch the **VMware vSphere Client** from the Windows-based device where it resides.
A desktop shortcut was created during installation.
- 2 Connect to the ESXi server as `root`.
- 3 In the navigation pane of the **VMware vSphere Client** main window, right-click a Windows-based virtual machine.
- 4 Ensure the virtual machine does not have any CD/DVD drives configured, by performing the following:
 - a In the navigation pane of the VMware Infrastructure Client main window, right-click the virtual machine that is connected to the DVD drive.
 - b On the pop-up menu for the selected virtual machine, click the **Edit Settings** option.

- c In the **Settings** dialog box, click the **Hardware** tab and select **CD/DVD Drive**.

The properties for the CD/DVD Drive appear on the right.

- d Ensure both of the following check boxes are cleared.

- **Connected power on**
- **Connected**



NOTICE: The Connected option is available for editing only if the virtual machine is powered on.

- e Click **OK**.

- 5 In the navigation pane, right-click the virtual machine name.

- 6 In the pop-up menu, select **Guest→Install/Upgrade VMware Tools**.

- 7 Perform one of the following actions:

- If the Install/Upgrade Tools dialog box appears, select the **Interactive Tools Upgrade** option. Click **OK**.
- If no dialog box appears, click **OK**.

A virtual CD-ROM containing the VMware tools software is now connected to this virtual machine.

- 8 Click the **Console** tab for this virtual machine.

- 9 Log on to the virtual machine as a user with administrative privileges.

- 10 In the virtual machine console, perform one of the following actions:

If...	Then...
If autorun is enabled,	click OK to confirm that you want to install VMware Tools and start the installation wizard.
If autorun is not enabled,	navigate to the optical drive in the VM and execute the appropriate file for the Windows OS on that VM: <ul style="list-style-type: none"> • For 32-bit, run <code>setup.exe</code> • For 64-bit, run <code>setup64.exe</code> or ,

- 11 If the User Access Control prompt appears, click **Yes**.

- 12 Follow the on-window instructions. Leave the default selections.

The VMware Tools are upgraded.

- 13 After the VMware Tools are upgraded, a prompt to reboot may appear. Click **Yes** or **OK**.

The virtual machine reboots.

Related Links

[Installing and Configuring Domain Controller Software for AD/DNS](#) on page 58

5.1.9

Adding the Domain Controller to an Existing System


Perform this optional procedure to add the domain controller to a forest that already has security policies applied.

Procedure:

- 1 Log on to the domain controller using the local administrator account ("Administrator").
The administrator's desktop appears.
- 2 Insert the *Domain Controller Plugin* media and navigate to the drive.
- 3 Double-click **ADC_RXX.XX.XX.msi** to install the DC scripts to the following location:
`C:\Program Files\Motorola\AstroDC`.

Domain controller MSI installation takes a couple of seconds. It does not require any user interaction.

If no window appears, the installation is successfully finished.
- 4 Insert the *Windows Supplemental* media into the drive.
- 5 Open PowerShell:
 - a From **Start**, click **Search**.
 - b In the search field, type in `powershell`
 - c Click **Windows PowerShell**.
- 6 At the PowerShell prompt, go to `C:\Program Files\Motorola\AstroDC\common\scripts` and enter one of the following commands:
 - If the Centralized Event Logging Server is not available in the system, enter:
`.\InstallDC.ps1 -interactive -noSyslogCli -hostname <DC hostname>`
 - If the Centralized Event Logging Server is available in the system, enter:
`.\InstallDC.ps1 -interactive -hostname <DC hostname>`where `<DC hostname>` is the hostname of the DC being added to the existing system.
Step example:The `<DC hostname>` of the DC in the first DSR zone is `z001dc03`
- 7 In the **Date and Time** window, set the date, time, and time zone. Click **OK**.
- 8 If prompted, enter the local `<AD domain admin password>` twice.

AD domain administrator password was set while installing the first system-level domain controller. See [User Input Requirements for Server Installation/Configuration on page 75](#).
- 9  **NOTICE:** During the installation, several reboots occur. After the first reboot, the "Administrator" account is renamed to "motosec".

If prompted, at the Windows logon screen, provide domain user credentials.
- 10 If any of the WIF error messages appear, wait for a couple of minutes and click **Retry**.

Do **not** click **Continue** or **Cancel** on the WIF installation error dialog box. Contact Motorola Solutions Support Center (SSC) if the problem persists.
- 11 At the installation finished prompt, click **OK**.

Domain controller installation logs can be checked at: `C:\Windows\Debug\DCInstall.log`. Search for `FinishDCInstall.ps1` and ensure it exited with 0 to verify that the installation was successful.

Related Links

[Installing and Configuring Domain Controller Software for AD/DNS on page 58](#)

5.1.10

Domain Controller Installation

This section provides information on how to install a domain controller, depending on its location in the system.



NOTICE: Follow [Installing and Configuring Domain Controller Software for AD/DNS on page 58](#) to install the domain controllers in the appropriate order.

5.1.10.1

Installing the First System-Level DC

Prerequisites:

Ensure that you know the values that replace the following variables in the procedure:

`<DC hostname>`

`<AD Domain Name>`

colocated zone `<#>`

See [User Input Requirements for Server Installation/Configuration on page 75](#) and contact your system administrator.

Obtain the following media:

- *Domain Controller Plugin*
- *Windows Supplemental*

Procedure:

- 1 In the navigation pane of the **VMware vSphere Client** main window, select a Windows-based virtual machine.
- 2 Insert the *Domain Controller Plugin* media and navigate to the drive.
- 3 Double-click **ADC_RXX.XX.XX.msi** to install the DC scripts to the following location:
`C:\Program Files\Motorola\AstroDC.`
 Domain controller MSI installation takes a couple of seconds. It does not require any user interaction.
 If no window appears, the installation is successfully finished.
- 4 Insert the *Windows Supplemental* media into the drive.
- 5 Open PowerShell:
 - a From **Start**, click **Search**.
 - b In the search field, type in `powershell`
 - c Click **Windows PowerShell**.
- 6 At the PowerShell prompt, change directory to `C:\Program Files\Motorola\AstroDC\common\scripts` and enter one of the following commands:
 - If the Centralized Event Logging Server is not available in the system, enter:
`.\InstallDC.ps1 -interactive -noSyslogCli -hostname <DC hostname>`
 - If the Centralized Event Logging Server is available in the system, enter:
`.\InstallDC.ps1 -interactive -hostname <DC hostname>`

The **<DC hostname>** of the system-level DC in the primary core is `ucs-dc01`.

- 7 In the **Date and Time** window, set the date, time, and time zone. Click **OK**.

- 8 At the prompt, enter: **<AD Domain Name>**.

The AD domain name should have two levels: **<system name>.<customer name>**.

- 9 At the prompt, enter the ucs colocated zone **<#>**.

- 10 If any of the WIF error messages appear, wait for a couple of minutes and click **Retry**.

Do **not** click **Continue** or **Cancel** on the WIF installation error dialog box. Contact the Motorola Solutions Support Center (SSC), if the problem persists.

- 11 At the installation finished prompt, click **OK**.

DC installation logs can be checked at: `C:\Windows\Debug\DCInstall.log`.

Related Links

[Installing and Configuring Domain Controller Software for AD/DNS](#) on page 58

5.1.10.2

Installing the Backup System-Level DC

Prerequisites: Ensure that you know the values that replace the following variables in the procedure:

<DC hostname>

colocated zone **<#>**

<AD domain admin password>

See [Table 8: User Input Requirements – Domain Controller Configuration on page 75](#) and contact your system administrator.

For troubleshooting information, see [Table 16: Troubleshooting Scenarios for Active Directory and DNS on page 152](#).

Procedure:

- 1 Log on to the domain controller using the local administrator account (“Administrator”).

The administrator's desktop appears.

- 2 Insert the *Domain Controller Plugin* media and navigate to the drive.

- 3 Double-click **ADC_RXX.XX.XX.msi** to install the DC scripts to the following location:

`C:\Program Files\Motorola\AstroDC`.

Domain controller MSI installation takes a couple of seconds. It does not require any user interaction.

If no window appears, the installation is successfully finished.

- 4 Insert the *Windows Supplemental* media into the drive.

- 5 Open PowerShell:

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

b In the search field, type `in powershell`

c Click **Windows PowerShell**.

- 6 Go to `C:\Program Files\Motorola\AstroDC\common\scripts` and enter one of the following commands:

- If the Centralized Event Logging Server is not available in the system, enter:

`.\InstallDC.ps1 -interactive -noSyslogCli -hostname <DC hostname>`

- If the Centralized Event Logging Server is available in the system, enter:
`.\InstallDC.ps1 -interactive -hostname <DC hostname>`

The <DC hostname> of the system-level DC in the backup core is ucs-dc03.

- 7 At the prompt, enter the ucs colocated zone <#> for the backup core.
- 8 At the prompt, enter the <AD domain admin password> twice.
 AD domain administrator password was set while installing the first system-level domain controller. It is the password set for the local administrator in the system-level DC.
- 9 If any of the WIF error messages appear, wait for a couple of minutes and click **Retry**.
 Do **not** click **Continue** or **Cancel** on the WIF installation error dialog box. Contact the Motorola Solutions Support Center (SSC), if the problem persists.
- 10 At the installation finished prompt, click **OK**.
 DC installation logs can be checked at: C:\Windows\Debug\DCInstall.log

Related Links

[Installing and Configuring Domain Controller Software for AD/DNS](#) on page 58

5.1.10.3

Installing First and Backup Zone-Level DCs

Prerequisites: Ensure that you know the values that replace the following variables in the procedure:

<DC hostname>

<AD domain admin password>

See [Table 8: User Input Requirements – Domain Controller Configuration on page 75](#) and contact your system administrator.

Procedure:

- 1 Log on to the domain controller using the local administrator account ("Administrator").
 The administrator's desktop appears.
- 2 Insert the *Domain Controller Plugin* media and navigate to the drive.
- 3 Double-click **ADC_RXX.XX.XX.msi** to install the DC scripts to the following location:
 C:\Program Files\Motorola\AstroDC.
 Domain controller MSI installation takes a couple of seconds. It does not require any user interaction.
 If no window appears, the installation is successfully finished.
- 4 Insert the *Windows Supplemental* media into the drive.
- 5 Open PowerShell:
 - a From **Start**, click **Search**.
 - b In the search field, type in powershell
 - c Click **Windows PowerShell**.
- 6 Go to C:\Program Files\Motorola\AstroDC\common\scripts and enter one of the following commands:
 - If the Centralized Event Logging Server is not available in the system, enter:
`.\InstallDC.ps1 -interactive -noSyslogCli -hostname <DC hostname>`
 - If the Centralized Event Logging Server is available in the system, enter:

```
.\InstallDC.ps1 -interactive -hostname <DC hostname>
```

The <DC hostname> of the zone-level DC is z00<Z>dc01 in the primary core and z00<Z>dc03 in the backup core.
where <Z> is the zone number

- 7 In the **Date and Time** window, set the date, time, and time zone. Click **OK**.
- 8 Enter the <AD domain admin password> twice.
AD domain administrator password was set while installing the first system-level domain controller. It is the password set for the local administrator in the system-level DC.
- 9 If any of the WIF error messages appear, wait for a couple of minutes and click **Retry**.
Do **not** click **Continue** or **Cancel** on the WIF installation error dialog box. Contact Motorola Solutions Support Center (SSC), if the problem persists.
- 10 At the installation finished prompt, click **OK**.
DC installation logs can be checked at: C:\Windows\Debug\DCInstall.log

Related Links

[Installing and Configuring Domain Controller Software for AD/DNS](#) on page 58

5.1.10.4

Installing the Domain Controller at a Console Site (Non-Tsub)

Prerequisites:

For details of required user input information, such as passwords or hostnames, see [Table 8: User Input Requirements – Domain Controller Configuration](#) on page 75.

Obtain the following media:

- *Domain Controller Plugin*
- *Windows Supplemental*

When and where to use:

Procedure:

- 1 Log on to the domain controller using the Local Administrator account ("Administrator").
- 2 Insert the *Domain Controller Plugin* media and navigate to the drive.
- 3 To install the DC scripts to the C:\Program Files\Motorola\AstroDC location, double-click **ADC_RXX.XX.XX.msi**.
- 4 Insert the *Windows Supplemental* media into the drive.
- 5 Open PowerShell:
 - a From **Start**, click **Search**.
 - b In the search field, type in powershell
 - c Click **Windows PowerShell**.
- 6 At the PowerShell prompt, go to C:\Program Files\Motorola\AstroDC\common\scripts and run one of the following commands:
 - If the Centralized Event Logging Server is not available in the system, enter:
.\InstallDC.ps1 -interactive -noSyslogCli -hostname <DC hostname>
 - If the Centralized Event Logging Server is available in the system, enter:
.\InstallDC.ps1 -interactive -hostname <DC hostname>

The **<DC hostname>** of the zone-level DC at a site is **z<ZZZ>nmd<SSS>dc<NN>** where:

- <ZZZ>** is the zone number
- <SSS>** is the site number
- <NN>** is the domain controller number

On the WIF execution log window, a message states that the installation finished. You are prompted to enter the administrator restore password.

7 Install the domain controller at a site.

See [step 8](#) through [step 10](#) from [Installing First and Backup Zone-Level DCs on page 71](#).

Related Links

[Installing and Configuring Domain Controller Software for AD/DNS on page 58](#)

5.1.10.5

Installing the Domain Controller at a Tsub Prime Site

Prerequisites:

For details of required user input information, such as passwords or hostnames, see [Table 8: User Input Requirements – Domain Controller Configuration on page 75](#).

Obtain the following media:

- *Domain Controller Plugin*
- *Windows Supplemental*

Procedure:

- 1** Log on to the domain controller using the Local Administrator account ("Administrator").
- 2** Insert the *Domain Controller Plugin* media and navigate to the drive.
- 3** To install the DC scripts to the `C:\Program Files\Motorola\AstroDC` location, double-click **ADC_RXX.XX.XX.msi**.
- 4** Insert the *Windows Supplemental* media into the drive.
- 5** Open PowerShell:
 - a** From **Start**, click **Search**.
 - b** In the search field, type in `powershell`
 - c** Click **Windows PowerShell**.
- 6** At the PowerShell prompt, go to `C:\Program Files\Motorola\AstroDC\common\scripts` and run one of the following commands:
 - If the Centralized Event Logging Server is not available in the system, enter:
`.\InstallDC.ps1 -interactive -noSyslogCli -hostname <DC hostname>`
 - If the Centralized Event Logging Server is available in the system, enter:
`.\InstallDC.ps1 -interactive -hostname <DC hostname>`

The **<DC hostname>** of the prime site-level DC at a site is **z<ZZZ>s<PPP>dc01** where:

- <ZZZ>** is the zone number
- <PPP>** is the prime site number

7 In the **Date and Time** window, set the date, time, and time zone. Click **OK**.

- 8 Install the domain controller at a site.

See [step 8](#) through [step 10](#) from [Installing First and Backup Zone-Level DCs on page 71](#).

On the WIF execution log window, an installation finished message appears.

Related Links

[Installing and Configuring Domain Controller Software for AD/DNS on page 58](#)

5.1.11

Clearing the Post-Install Configuration Warning on the Domain Controller

Perform this procedure on **all Domain Controllers (DCs)** to clear a warning that Server Manager is requesting Post-Install Configuration to promote the server to a domain controller.

Prerequisites:

Ensure that the Domain Controller is powered on.

Procedure:

- 1 Log on to the Domain Controller using a motosec account.
- 2 Click the **Start** menu and open **Server Manager**.
- 3 Click **Configure this local server**.
Server Manager refreshes the status of the Local Server.
- 4 In the upper task menu next to **Manage**, click the flag with a yellow triangle with exclamation.
- 5 Click **Promote this server to a domain controller**.
Wait until the **Active Directory Domain Services Configuration Wizard** shows an error determining whether the target server is already a domain controller.
- 6 In the **Active Directory Domain Services Configuration Wizard**, click **Cancel** and click **Yes** to confirm canceling.
The message requesting Post-Install Configuration to promote the server to a domain controller is cleared.
- 7 Exit **Server Manager**.
Post-Install Configuration is complete.

Related Links

[Installing and Configuring Domain Controller Software for AD/DNS on page 58](#)

5.1.12

Applying Post-Install AD Configuration

Perform this procedure **on all Domain Controllers (DCs)** to set each DC as a backup DNS server and to apply the Motorola Solutions-provided Group Policy Objects (GPOs) on the DC.

Procedure:

- 1 Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group (the account name set up by Motorola Solutions is "motosec").
The domain administrator's desktop appears.

- 2 Open PowerShell:
 - a From **Start**, click **Search**.
 - b In the search field, type in `powershell`
 - c Click **Windows PowerShell**.**NOTICE:** If PowerShell privilege elevation is required, right-click **Windows PowerShell** and select **Run as administrator**.

Postrequisites:

DCs are fault managed by Unified Event Manager (UEM). See “Alarms and Events” in the *UEM Online Help* for the alarms, events, and error messages that may appear.

Tsub systems only: Perform additional configuration as part of Tsub expansion and conversion to ensure that the static DNS list is properly configured on all Domain Controllers. See “DNS Entries for Sites Added to or Removed from a Tsub” section in the *Edge Availability with Wireline Console Feature Guide* for detailed instructions.

Related Links

[Installing and Configuring Domain Controller Software for AD/DNS](#) on page 58

5.2

User Input Requirements for Server Installation/Configuration

Before beginning the installation process for domain controllers, obtain the information from the following table in order to prevent interruption of the process.

The required user input information is indicated by *<text in brackets>* in the following table and in the procedures that require this input.




NOTICE: Contact your system administrator or refer to the system IP plan for specific IP addresses or hostnames (where applicable).

For more information about the backup core domain controllers, see the *Dynamic System Resilience Feature Guide*. These domain controllers only need to be installed in systems that are implementing the DSR feature.

Table 8: User Input Requirements – Domain Controller Configuration

User Input Required	Description
<i><DC hostname></i>	<ul style="list-style-type: none">For system-level DC in the primary core: <code>ucs-dc01</code>For system-level DC in the backup core (DSR systems only): <code>ucs-dc03</code>

User Input Required	Description
	<ul style="list-style-type: none"> For zone-level DC in the primary core: z<ZZZ>dc01 For zone-level DC in the backup core (DSR systems only): z<ZZZ>dc03 For zone-level DC at a site: z<ZZZ>nmd<SSS>dc<NN> For Tsub prime site DC: z00<X>s<PPP>dc01 <p>where:</p> <p><ZZZ> is the number of the zone in which the VMS hosting the DC is located. The possible values are: 1–7.</p> <p><SSS> is the site number</p> <p><NN> is the domain controller number</p> <p><PPP> is the 3-digit zero-padded number of the prime site in which the Zone Controller is located. The possible values are: 001-064.</p>
colocated zone <#>	<p>The zone in which the system-level DC01 is located in the primary core.</p> <p>If installing system-level DC03, the zone in which the system level DC03 is located in the backup core.</p> <p><#> is a number from 1 to 7</p>
<Windows Server 2012 Product Key>	<p>Virtual Product/License key associated with the Microsoft Windows Server 2012 media. It may be located on a sticker that came with the media or it may be attached to the hardware.</p> <p> NOTICE: You can use the same Product/License Key for up to four virtual machines that reside on the same physical Virtual Server. See Activating a Domain Controller Virtual Machine on page 66.</p>
<administrator password>	The default password for the built-in administrator account entered during the initial setup.
<AD Domain Name>	<p>An AD domain name specified by the user. The AD domain name should have two levels: <system name>.<customer name>.</p> <p>For example: astro.abc.</p>
<Domain Administrator account>	<p>The Domain Administrator account for the Active Directory domain.</p> <p>The domain administrator name is “motosec”.</p>
<AD domain admin password>	Password associated with the Domain Administrator account for the AD domain.

User Input Required	Description
	<p>The password must be at least 14 characters long and must have three out of the following four characteristics:</p> <ul style="list-style-type: none"> • At least one upper case letter (A-Z) • At least one lower case letter (a-z) • At least one number (0-9) • At least one of the following symbols: hyphen (-), underscore (_), dollar (\$), pound/ hash (#)
<Admin Restore password>	<p>Password associated with <Admin Restore username></p> <p>This is the Directory Service Restore password, set during installation/reinstallation, typically the same password as the “motosec” account password.</p> <p>The password must be at least 14 characters long and must have three out of the following four characteristics:</p> <ul style="list-style-type: none"> • At least one upper case letter (A-Z) • At least one lower case letter (a-z) • At least one number (0-9) • At least one of the following symbols: hyphen (-), underscore (_), dollar (\$), pound/ hash (#)

5.3

Adding CEN Records into DNS

Perform this procedure to add Customer Enterprise Network (CEN) records into the Domain Name Services (DNS) in an ASTRO® 25 system.

The procedure is applicable to the zone-level DC in the primary core of the zone where CEN devices reside. For example: if there is a KMF server in zone 2 and zone 3, then this procedure needs to be performed on the primary DC for zone 2 and zone 3 (z002dc01 and z003dc01).

Prerequisites: Obtain the `CenNatReport.csv` file generated in the Transport Network Configuration Tool (TNCT) from `C:\Program Files (x86)\Motorola\TNCT\<release>\local_configurations\<system name>\reports`.

When and where to use:

Additionally, perform this procedure in each of the following scenarios:

- On all zone-level DCs, if more servers are added, or if a new primary DCs is added.
- As part of the zone-level DC disaster recovery. See [Recovering a Domain Controller on page 189](#).

- In a non-DSR scenario, if the system-level domain controller and the first zone-level domain controller (primary DC for the zone where CEN devices reside) are down.

Procedure:

- 1 Double click the **VMware vSphere Client** desktop icon on the Windows-based client where the application resides.
- 2 In the **VMware vSphere Client** dialog box, type in:
 - a The **<IP address>** of the ESXi-based virtual CSA server.
 - b The `root` username.
 - c The **<root password>** of the ESXi-based virtual CSA server.
- 3 Click **Login**.
- 4 In the left pane of the **vSphere Client Inventory** window, select the primary zone DC.
- 5 In the right pane of the **vSphere Client Inventory** window, click the **Console** tab.
- 6 Log on to the zone-level DC using your Active Directory account that is a member of the Domain Admins group.
The account name set up by Motorola Solutions is "motosec".
- 7 Copy the `CenNatReport.csv` file to `C:\Program Files\Motorola\AstroDC\DNS\data`.
- 8 Open the PowerShell command prompt as administrator:
 - a From **Start**, click **Search**.
 - b In the search field, type in `powershell`
 - c Right-click **Windows PowerShell**, and select **Run as administrator**.
If the **User Account Control** window appears, click **Yes**. If you are not logged on with an administrative account, enter the domain admin credentials.
- 9 At the **Windows PowerShell** prompt, enter: `cd 'C:\Program Files\Motorola\AstroDC\DNS\scripts'`
The directory changes to `C:\Program Files\Motorola\AstroDC\DNS\scripts`.
- 10 Enter: `.\AddCenRecords.ps1`
The script is executed and CEN entries are added. The script exits with `AddCenRecords.ps:Exit with 0.`

Chapter 6

RADIUS Server Installation/ Configuration

This chapter provides information for installing and configuring the RADIUS service on domain controllers in an ASTRO® 25 system.

6.1

Creating and Transferring a List of RADIUS Clients for Importing to a RADIUS Server

Perform this procedure to create a list of RADIUS clients in your ASTRO® 25 system and transfer it to the zone-level domain controller that is the primary RADIUS server for its zone in your ASTRO® 25 system.



NOTICE: The list created and transferred in this procedure is used in [Batch Importing RADIUS Clients to the Primary RADIUS Server for a Zone on page 80](#).

When and where to use:

It is recommended that you perform this procedure from a Network Management client, because the process requires that you have access to a text editor and the VoyenceControl component of the Unified Network Configurator, and that you can access the system drive of the primary zone-level Domain Controller.

For instructions regarding VoyenceControl:

- See the *Unified Network Configurator* manual.
- In VoyenceControl, click **Help**→**Help Contents** from the menu bar.



NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

Procedure:

- 1 Ensure all your ASTRO® 25 system devices are discovered in VoyenceControl.
- 2 Locate or create a **Devices** view in VoyenceControl that shows only Device Name and IP Address columns for the RADIUS devices for that zone (primary and backup).
For the devices that support RADIUS in an ASTRO® 25 system, see [RADIUS in ASTRO 25 Systems on page 43](#).
Ensure that you do not include any devices that are not RADIUS clients in your ASTRO® 25 system. Contact your system administrator for a list of devices in your system.
- 3 Make sure that each device name in the **Devices** view is unique.
- 4 From the **Devices** view in the previous step:
 - Select **File**→**Export**.
 - Select `.csv` as the file format.
 - Save the file to a location where you will be able to edit it.
- 5 Edit the `.csv` file in a text editor such as Notepad, as follows:

- a Replace the comma (,) between each device name and its IP address with a question mark (?).
- b Delete data in the file that is not a device name or its IP address. Alternatively, you can insert a hash symbol (#) before each line of this data so that the import script will ignore it.

Step example: The following is an example of data in the file that is not a device name or its IP address:

```
VoyenceControl
```

```
"Astro 25 Radio Network - <Name of Device View, Day, Date, Time>"
```

```
<Column headings - Device Name, IP Address>
```

- 6 Save the file using a path and file name that you want to use when executing the procedure under [Batch Importing RADIUS Clients to the Primary RADIUS Server for a Zone on page 80](#).
- 7 Perform the following actions:
 - a Press **Windows icon key+R** to open the **Run** dialog box.
 - b Type the following, and click **OK**: `\\<IP address of the primary RADIUS server for the zone>\c$`
 where the primary RADIUS server for the zone is the first zone-level domain controller in that zone
 - c If prompted, type credentials in the following format:
 user name: `<domain name>\<ip address>`
 password: `<password>`

An **Explorer** window displays the contents of the `C : \` drive on the primary RADIUS server.

- 8 Copy the file from [step 6](#) to the `C : \` folder of the primary RADIUS server.

Postrequisites: Continue to [Batch Importing RADIUS Clients to the Primary RADIUS Server for a Zone on page 80](#).

6.2

Batch Importing RADIUS Clients to the Primary RADIUS Server for a Zone

Follow these steps to add RADIUS clients to the primary RADIUS server, located on the first zone-level domain controller in each zone of the ASTRO® 25 system.



IMPORTANT:

- Always add, update, or delete RADIUS clients only in the zone RADIUS Servers.
- Both the primary and backup zone RADIUS clients can be imported either into the first zone-level domain controller or the backup zone-level domain controller.
- Do **not** change the RADIUS configuration in the first system-level domain controller, backup domain controller, or a Tsub domain controller. Any changes made directly to the system-level domain controllers (ucs-dc01, ucs-dc03) or Tsub domain controllers will be lost.

Prerequisites: See [Creating and Transferring a List of RADIUS Clients for Importing to a RADIUS Server on page 79](#).

Procedure:

- 1 Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.

The account name set up by Motorola Solutions is “motosec”.

The domain administrator’s desktop appears.

- 2 Ensure that this domain controller has the file that lists RADIUS clients for that zone in your ASTRO® 25 system.
- 3 Open PowerShell:
 - a From **Start**, click **Search**.
 - b In the search field, type in `powershell`
 - c Click **Windows PowerShell**.
- 4 At the **PowerShell** prompt, change directory to: `C:\Program Files\Motorola\AstroDC\RADIUS\scripts`
- 5 At the prompt, enter:
`.\AddRADIUSClients.ps1 -RADIUSFilePath <Path to the RADIUS file>-secret <common shared secret>`

where:

<Path to the RADIUS file> is the file with the list of the RADIUS clients that you copied to this domain controller

<common shared secret> is the secret to be set for all the RADIUS clients



NOTICE: If a unique secret for each client is required to be set, it can be set through the RADIUS client file. The template for the file exists at: `C:\Program Files\Motorola\AstroDC\RADIUS\data\RADIUSclientFile.txt`.

If a shared secret is not provided at the command prompt or in the RADIUS client file, then a random secret will be provisioned for all the RADIUS clients, and you will need to enter a secret in the properties of each RADIUS client in the Network Policy Server. The secret must be available to be entered in the local configuration of the RADIUS client devices themselves, which is not the case if the secret is randomly generated.

A message states that the clients were added successfully. Replicating the data can take up to half an hour.



NOTICE: Contact the Motorola Solutions Support Center (SSC) if any error messages appear on any RADIUS client list generated by Motorola Solutions.

- 6 After adding/updating/deleting clients from the RADIUS server on the zone-level domain controller, trigger the replication to the system-level DCs:
 - a Go to `C:\Program Files\Motorola\AstroDC\RADIUS\scripts`
 - b Enter: `.\TriggerRADIUSReplication.ps1`
- Once replication is triggered, it takes up to 30 minutes for the data to get replicated to the backup RADIUS servers.

Postrequisites: To verify a RADIUS client import, see [Verifying Import of RADIUS Client Data on page 82](#).

Related Links

[Installing and Configuring Domain Controller Software for AD/DNS on page 58](#)

6.3

Verifying Import of RADIUS Client Data

Prerequisites: Ensure that you have imported RADIUS clients to the RADIUS server. See [Batch Importing RADIUS Clients to the Primary RADIUS Server for a Zone on page 80](#).

When and where to use: If there are devices in your ASTRO® 25 system that support RADIUS which do not appear as RADIUS clients in the following procedure, you can manually add them as RADIUS clients. See [Adding RADIUS Clients Manually to a RADIUS Server on page 146](#). For devices that support RADIUS in an ASTRO® 25 system, see [RADIUS in ASTRO 25 Systems on page 43](#).

Procedure:

- 1 Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.
The account name set up by Motorola Solutions is “motosec”.
- 2 Open **Network Policy Server**:
 - a From **Start**, click **Search**.
 - b In the search field, type in `administrative`
 - c Click **Administrative Tools**.
 - d In the **Administrative Tools** window, double-click **Network Policy Server**.
- 3 In the **Network Policy Server** window, expand **RADIUS Clients and Servers**, then double-click **RADIUS Clients** to verify that the RADIUS clients were added to this RADIUS server.
The list of RADIUS clients appears in a window on the right side of the screen.

Related Links

[Installing and Configuring Domain Controller Software for AD/DNS on page 58](#)

Chapter 7

RADIUS Client Configuration

This chapter provides information for configuring the RADIUS service on RADIUS client devices in an ASTRO® 25 system.



IMPORTANT: Devices are configured properly by Motorola Solutions when a system is implemented. Changes to configuration provided in this chapter should be performed only by personnel with ASTRO® 25 system expertise.

For details about using RADIUS specifically for 802.1x ports on HP switches and the internal switches of GCP 8000 Site Controllers and GPB 8000 Reference Distribution Modules, see the *802.1x Service Ports on Switches* manual.

Whenever the RADIUS hostname or IP address (where applicable) is configured, the service hostname or service IP address of the RADIUS Server needs to be entered. For the exact values to use, refer to the *System IP Plan*.

If the time source needs to be configured before configuring RADIUS see the *Network Time Protocol Server* manual and the appropriate manual for the configured device.

7.1

RADIUS Configuration on an HP Switch with VoyenceControl

Perform the following procedures for configuring Remote Authentication Dial-In User Service (RADIUS) sources for HP switches that are connected and have their configuration maintained in the VoyenceControl component of the Unified Network Configurator:



NOTICE:

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

For additional information, see the *Unified Network Configurator* manual.

- **RADIUS authentication sources for accessing devices through telnet or SecureShell (SSH).**
See [Configuring HP Switch Authentication Sources for Telnet or SSH Access on page 84](#)
- **RADIUS authentication sources for accessing an HP switch through its 802.1x service port.**
See:
 - [Configuring HP Switch Authentication Sources for 802.1x on page 86](#)
 - Procedure for enabling/disabling 802.1x on a switch port. See the *802.1x Service Ports on Switches* manual.



IMPORTANT:

In these procedures, VoyenceControl templates generate a “radius-host server” command with the IP address of a RADIUS authentication source. Each time this command is pushed to the same HP switch, it is saved in the configuration of the switch as an additional RADIUS authentication source. However, the HP switch configuration should include only one “radius-host server” command for the primary RADIUS IP address, and only one “radius-host server” command for the secondary RADIUS IP address.

To make sure that the switch configuration includes the proper RADIUS authentication source commands in the correct order, do not push the “radius-host server” command to the switch more than once with the same IP address. Follow the instructions in to delete the “radius-host server” command from the Configlet Editor if you have already pushed that “radius-host server” IP address to the switch.

7.1.1

Configuring HP Switch Authentication Sources for Telnet or SSH Access

Follow these steps to set up the primary and secondary authentication Remote Authentication Dial-In User Service (RADIUS) sources for accessing an HP switch by telnet or Secure Shell (SSH).

Using the procedure, you will configure **one** primary RADIUS source and **one** secondary RADIUS source on the HP switch.

Prerequisites:

Contact your system administrator for the information concerning **RADIUS source IP addresses**. See [Table 9: Hostnames of RADIUS Authentication Sources for DSR and Non-DSR Switches on page 89](#). The IP addresses you need depend on where the switch is located and whether your system includes the Dynamic System Resilience (DSR) feature. For information about DSR, see the *Dynamic System Resilience Feature Guide*.

Establish whether RADIUS authentication sources have already been configured on the switch. For example, they may have been configured already by the 802.1x authentication sources template, if that feature is being implemented in your system. If you are not sure what is currently configured on the switch, you can use VoyenceControl to:

- 1 Pull the current configuration from the switch: From the right-click menu for the switch, select **Pull→Pull Config**.
- 2 View current configuration and the history of configuration changes for the switch. From the right-click menu for the switch, select **Properties** and then click the **Configuration** tab and the **History** tab.

For additional information, see the *Unified Network Configurator* manual.


Procedure:

- 1 Log into VoyenceControl.
- 2 In the **VoyenceControl** main window, in the navigation pane on the left side of the window, double-click the name of the network that contains the switch you want to access.
The selected network tree expands to display the Devices node.
- 3 In the navigation pane on the left side of the window, double-click **Devices**.
The list of devices and associated properties are displayed in the pane on the right side of the screen.
- 4 Right-click the desired switch on the right side of the screen.
- 5 From the context menu, select **Properties**, then the **Communications** tab.
- 6 Optional: If needed, click **Update Credentials** to:
 - Ensure that a Management Mechanism (protocol) appropriate for your organization's policies has been selected for this device.
 - Ensure that the Management Account field is appropriately configured. For example, if RADIUS authentication is not currently enabled on the device, make sure that the VoyenceControl Management Account credential for this device matches the local username and password for this device.

For information on adding and modifying credentials, see “EMC Smarts Network Configuration Manager Credential Modification” in the *Unified Network Configurator* manual.

- 7 Return to the **Devices** view and right-click the switch again.
- 8 From the context menu, select **Editor→Configlet**.

- 9 In the **Configlet Editor** window, click inside the **Common Configlet** text box.
The **Insert Template** icon becomes active in the tool bar of the **Configlet Editor** window.
- 10 Click **Insert Template**.
- 11 In the **Select Item** dialog box, click the folder icon at the top of the dialog box, to the right of the **Look in** field. Continue to click this icon until the **System** folder displays in the list of folders.
- 12 In the list of folders on the **Select Item** dialog box, double-click **System**→**Motorola**→**HP**.
- 13 In a list of templates on the **Select Item** dialog box, perform the following actions, depending on whether you are configuring the primary or secondary RADIUS authentication source:

If...	Then...
You are setting up the primary authentication source,	<p>perform the following actions:</p> <ol style="list-style-type: none"> a Select the Authentication Source for RADIUS Server template.  NOTICE: For the HP 2610 switch, select the Authentication Source for RADIUS Server – 2610 Model template. b In the Template Variable Substitution window, type the IP address that corresponds to the hostname for the primary RADIUS source for this switch. See Table 9: Hostnames of RADIUS Authentication Sources for DSR and Non-DSR Switches on page 89.
You are setting up the secondary authentication source,	<p>perform the following actions:</p> <ol style="list-style-type: none"> a Select the Additional Authentication Source for RADIUS server. b Type the IP address that corresponds to the hostname for the secondary RADIUS source for this switch. See Table 9: Hostnames of RADIUS Authentication Sources for DSR and Non-DSR Switches on page 89.

- 14 In the **Key Value** field, type the shared secret entered for the RADIUS client (the switch) on the RADIUS server. Click **OK**.

The Common Configlet field displays authentication commands, starting with the “radius-server host” command.

- 15 Optional: If you still need to configure the other authentication source:

- a Copy and paste the “radius-server host” command to the second line in the **Common Configlet** field.

Step example:radius-server host ###.111.111.0 key #####radius-server host ###.111.111.0 key #####
- b In the second “radius-server host” command, replace the IP address with the IP address of the secondary RADIUS service.

Step example:radius-server host ###.111.111.0 key #####radius-server host ###.222.222.0 key #####

- 16  **IMPORTANT:** Before proceeding:

- Ensure that the two IP addresses in the Common Configlet field are not the same.
- Ensure that there is no “radius-server host” IP address in the Common Configlet field that is the same as a “radius-server host” IP address in the current configuration for the device.

If needed, delete the “radius-server host” line from the Common Configlet field so that the same IP address will not appear in the device configuration twice.

The other commands generated by the **Authentication Source for RADIUS Server** template must be pushed to the switch to complete the configuration, even if you delete the “radius-server host” command.

17 Perform the following steps to push changes to the device:

- a** In the **Configlet Editor** window, click **Schedule**.
- b** In the **Schedule Job** window, on the **Schedule Job** tab, enter the job name in the relevant field.
- c** On the **Tasks** tab, make sure that the selected **Mechanism** is appropriate for your organization's policies.

Keep the defaults of “running-configuration” and “Copy to Start” and “Pull Configs” in the other fields for this job.
- d** Click **Approve & Submit** or **Submit**, depending on your permissions.



NOTICE: If you select the **Run upon approval** option and then click **Approve & Submit** on the **Schedule Job** window, the job begins immediately. The operation may take a few minutes, before successful completion is reported on the **Schedule Manager** window.

18 After the job completes successfully in VoyenceControl, verify the success of the operation by logging on to the switch with the RADIUS username and password for the switch.

If you want to use VoyenceControl for this logon verification, first ensure that the Account credentials are configured appropriately for this device. Since RADIUS authentication is now enabled on the device, make sure that the VoyenceControl Account credentials for this device match the username and password for this device on the RADIUS server, or make sure that no credential is selected, so that the device will prompt you to enter the username and password. For example, if you want to verify logon using the Quick Command called Test Credentials, then make sure that the Management Account credential is appropriate. If you want to verify logon using Cut-Through, make sure that the Cut-Through Account credential is appropriate.

You can view and update credentials on the **Communications** tab in the **Properties** for the device. For information on adding and modifying credentials, see “EMC Smarts Network Configuration Manager Credential Modification” in the *Unified Network Configurator* manual.

7.1.2

Configuring HP Switch Authentication Sources for 802.1x

Prerequisites:

Contact your system administrator for RADIUS source IP addresses. See [Table 9: Hostnames of RADIUS Authentication Sources for DSR and Non-DSR Switches on page 89](#). The IP addresses you need depends on where the switch is located and whether your system includes the Dynamic System Resilience (DSR) feature. For information about DSR, see the ASTRO® 25 system *Dynamic System Resilience Feature Guide*.

Before performing the procedure you need to know whether RADIUS authentication sources have already been configured on the switch. If you are not sure what is currently configured on the switch, you can use VoyenceControl to:

- 1** Pull the current configuration from the switch: From the right-click menu for the switch, select **Pull→Pull Config**.
- 2** View the current configuration and the history of configuration changes for the switch, as follows: From the right-click menu for the switch, select **Properties** and then click the **Configuration** tab and the **History** tab.

For additional information, see the *Unified Network Configurator* manual.

When and where to use:

Follow these steps to set up the primary and secondary authentication Remote Authentication Dial-In User Service (RADIUS) sources for 802.1x access through the Ethernet service port on an HP switch.

Using the procedure, you will configure **one primary** RADIUS source and **one secondary** RADIUS source on the HP switch.

Procedure:

- 1 Log into VoyenceControl.
The VoyenceControl main window appears.
- 2 In the navigation pane on the left side of the window, double-click the name of the network that contains the switch you want to access.
The selected network tree expands to display the Devices node.
- 3 In the navigation pane on the left side of the window, double-click **Devices**.
The list of devices and associated properties are displayed in the pane on the right side of the screen.
- 4 Right-click the desired switch on the right side of the screen.
- 5 In the context menu, select **Properties**, then select the **Communications** tab.
If needed, use the **Update Credentials** button to:
 - Make sure that a Management Mechanism (protocol) appropriate for your organization's policies has been selected for this device.
 - Make sure that the Management Account field is appropriately configured. For example, if RADIUS authentication is not currently enabled on the device, make sure that the VoyenceControl Management Account credential for this device matches the *local* username and password for this device.

For information on adding and modifying credentials, see “EMC Smarts Network Configuration Manager Credential Modification” in the *Unified Network Configurator* manual.
- 6 Return to the Devices view, and right-click the switch again.
- 7 From the context menu, select **Editor→Configlet**.
- 8 At the top of the **Configlet Editor** window, click inside the **Common Configlet** text box.
- 9 Click the **Insert Template** icon.
- 10 In the **Select Item** dialog box, click the folder icon at the top of the dialog box, to the right of the **Look in** field. Continue to click this icon until the **System** folder displays in the list of folders.
- 11 In the list of folders on the **Select Item** dialog box, double-click **System→Motorola→HP**.
A list of templates displays on the **Select Item** dialog box.
- 12 Perform the following actions, depending on whether you are configuring the primary or secondary RADIUS authentication source:

If...	Then...
You are setting up the primary authentication source,	perform the following actions: <ol style="list-style-type: none"> a Select the template named Authentication source for 802.1x connection. b In the Template Variable Substitution window, type the IP address that corresponds to the hostname for the primary RADIUS

If...	Then...
	source for this switch, as indicated in Table 9: Hostnames of RADIUS Authentication Sources for DSR and Non-DSR Switches on page 89 .
You are setting up the secondary authentication source,	<p>perform the following actions:</p> <ul style="list-style-type: none"> a Select the template named Additional Authentication Source for RADIUS server. b Type the IP address that corresponds to the hostname for the secondary RADIUS source for this switch, as indicated in Table 9: Hostnames of RADIUS Authentication Sources for DSR and Non-DSR Switches on page 89.

- 13** In the **Key Value** field, type the shared secret entered for the RADIUS client (the switch) on the RADIUS server. Click **OK**.

The Common Configlet field displays authentication commands, starting with the “radius-server host” command.

- 14** If you still need to configure the other authentication source:

- a** Copy and paste the “radius-server host” command to the second line in the Common Configlet field.

Step example:radius-server host ###.111.111.0 key #####radius-server host ###.111.111.0 key #####

- b** In the second “radius-server host” command, replace the IP address with the IP address of the secondary RADIUS service.

Step example:radius-server host ###.111.111.0 key #####radius-server host ###.222.222.0 key #####



IMPORTANT: Before proceeding, ensure that the two IP addresses in the Common Configlet field are not the same.

- 15** Before proceeding, ensure that there is no “radius-server host” IP address in the Common Configlet field that is the same as a “radius-server host” IP address in the current configuration for the device.



IMPORTANT: If needed, delete the “radius-server host” line from the Common Configlet field so that the same IP address will not appear in the device configuration twice. The other commands generated by the **Authentication source for 802.1x connection** template must be pushed to the switch to complete the configuration, even if you delete the “radius-server host” command.

- 16** Perform the following steps to push changes to the device:

- a** On the **Configlet Editor** window, click **Schedule**.
- b** On the **Schedule Job** tab, enter the job name in the relevant field.
- c** On the **Tasks** tab, make sure that the selected Mechanism is appropriate for your organization's policies. Keep the defaults of “running-configuration” and “Copy to Start” and “Pull Configs” in the other fields for this job.

d Click **Approve & Submit** or **Submit**, depending on your permissions.



NOTICE: If you select the **Run upon approval** option and then click the **Approve & Submit** button on the **Schedule Job** window, the job begins immediately. The operation may take a few minutes, before successful completion is reported on the **Schedule Manager** window.

The **Schedule Job** window appears.

17 After the job completes successfully in VoyenceControl, you can verify the success of the operation by:

- Viewing the results of the job in Schedule Manager, accessible from the **Tools** menu in VoyenceControl.
- Enabling 802.1x on the service port of the switch, then verifying that you can log on through that port with the RADIUS username and password. For instructions, see the *802.1x Service Ports on Switches* manual.

7.1.3

Hostnames of RADIUS Authentication Sources for DSR and Non-DSR Switches

Table 9: Hostnames of RADIUS Authentication Sources for DSR and Non-DSR Switches

To configure the following on a switch:	Non-DSR system	DSR system		
	When switch is located in: zone core or RF/ Prime/ GeoPrime/ Subsite/NMD sites	When switch is located in: a primary zone core	When switch is located in: a standalone DSR backup core*	When switch is located in: RF/ Prime/ GeoPrime/ Subsite/NMD sites
Primary RADIUS source	Use RADIUS Service IP address for: z<zzz>rad01	Use RADIUS Service IP address for: z<zzz>rad01	Use RADIUS Service IP address for: z<zzz>rad03	Use RADIUS Service IP address for: z<zzz>rad01
Secondary RADIUS source	Use RADIUS Service IP address for: ucs-rad01	Use RADIUS Service IP address for: ucs-rad01	Use RADIUS Service IP address for: ucs-rad03	Use RADIUS Service IP address for: z<zzz>rad03

Where:

<zzz> is the number of the zone to which the switch belongs

* *standalone DSR backup core* refers to a DSR backup core at a master site where there is no primary core sharing the switch with the backup core. For more information, see the *Dynamic System Resilience Feature Guide*.

7.2

Entering the RADIUS Shared Secret on MNR Routers and GGM 8000 Gateways

This section applies to the following ASTRO® 25 system devices:

- MNR S2500 routers
- MNR S6000 routers
- GGM 8000 gateways

For more information, see the *S6000 and S2500 Routers* manual and the *GGM 8000 System Gateway* manual.

The RADIUS authentication sources are already set up by Motorola Solutions in configuration files which are downloaded to the routers and gateways. The only RADIUS configuration you need to perform on MNR routers and GGM 8000 gateways is to enter the secret key that matches the shared secret from the properties for this RADIUS client on the RADIUS server.

You can enter the secret key at the MNR router or GGM 8000 gateway command prompt, as follows:

```
SETDefault -AC Secret = "<secret_key>"
```

where **<secret_key>** is the shared secret entered for this RADIUS client on the RADIUS server.

7.3

RADIUS Configuration on Fortinet Firewall Manager

Fortinet FortiManager must be present in the system in order to perform procedures in this section. See the *Fortinet Firewall Manager* manual.

7.3.1

Logging on to the Fortinet Firewall Manager

Prerequisites: Obtain the username and password for the FortiManager administrative account from your system administrator.

Procedure:

- 1 Log on to the Network Management (NM) client using the Windows administrator account.
The account name set up by Motorola Solutions for Windows 7 and Windows 10-based devices is "secmoto".
- 2 From the NM client, open the **Internet Explorer**.
- 3 In the **Internet Explorer** address bar, enter: `https://ffwm01`
- 4 At the prompt, type the username and password for the FortiManager administrative or local account. Click **Login**.
The default account name is `suppuser`.
- 5 At the disclaimer prompt, click **Accept**.

Postrequisites: The **FortiManager** main window appears.

7.3.2

Configuring RADIUS Shared Secret on the Fortinet Firewall Manager

Prerequisites:

Obtain the following from your system administrator:

- Username and password for the FortiManager administrative account
- Primary and secondary shared secret.

Procedure:

- 1 Log on to the Fortinet FortiManager.
See [Logging on to the Fortinet Firewall Manager on page 90](#).
- 2 Click the **System Settings** tab.
- 3 From the tree view in the left pane, select **Admin**→**Remote Auth Server**.
- 4 Click inside the **Name** field for the desired server to open the **Edit RADIUS Server** window.
- 5 In the **Server Name/IP** field, enter: `ucs-rad01.ucs`
- 6 In the **Server Secret** field, enter the shared secret of the primary RADIUS server.
- 7 In the **Secondary Server Name/IP** field, perform one of the following actions:
 - If this is a DSR system, enter: `ucs-rad03.ucs`
 - If this is a non-DSR system, enter: `z<zzz>rad01.zone<z>`
where `<zzz>` and `<z>` indicate the zone to which the device belongs
- 8 In the **Secondary Server Secret** field, enter the shared secret of the secondary RADIUS server.
- 9 Click **OK**.

7.4

RADIUS Configuration on Fortinet Firewalls

In the ASTRO® 25 system, RADIUS authentication sources are already set up in firewall configurations by Motorola Solutions. The only RADIUS configuration you need to perform on Fortinet FortiGate 100D and 1000C firewalls is to ensure that the shared secret in the firewall configuration matches the shared secret entered for the firewall RADIUS client on the RADIUS server.

7.4.1

Configuring RADIUS Shared Secret on Fortinet Firewalls

Procedure:

- 1 Perform the following actions to open a WebUI connection and log on to the firewall:
 - a Log on to the Network Management (NM) client using the Windows administrator account.
 - b Launch a web browser from the NM client.
 - c In the web browser URL field, enter: `https://<IP address of the firewall>`
 - d In the **Login Disclaimer** window, click **Accept**.
 - e In the logon window, type the username and password for the firewall's administrator account.
 - f Click **Login**.
- 2 In the firewall's WebUI home page, from the left pane of the WebUI, select:
 - For all Fortinet firewalls except ZCP: **User & Devices**→**Authentication**→**RADIUS Servers**
 - For ZCP Fortinet firewalls only: **Virtual Domains**→**root**→**User & Devices**→**Authentication**→**RADIUS Servers**
- 3 In the middle pane of the WebUI, click **RADIUS_User**, then **Edit**.

- 4 In the **Edit RADIUS Server** window, **Primary Server Secret** field, type the shared secret entered for the firewall RADIUS client on the Primary RADIUS server.
- 5 In the **Secondary Server Secret** field, type the shared secret entered for the firewall RADIUS client on the Secondary RADIUS server.
- 6 Click **OK**.

7.5

Configuring RADIUS on RF Site and VPM Devices

RADIUS authentication can be set up for the following devices by entering the RADIUS authentication sources, RADIUS Specific Key (shared secret), and RADIUS service parameters in the device configuration:

- **RF site devices:**
 - GTR 8000 Base Radio
 - GCM 8000 Comparator
 - GCP 8000 Site Controller
 - GPB 8000 Reference Distribution Module (RDM)
 - GPW 8000 Receiver
- **Voice Processor Module (VPM) devices:**
 - SmartX Site Converter
 - MCC 7500 Voice Processor Module (VPM)
 - Telephone Media Gateway (TMG)

The following table shows procedures for configuring RADIUS on RF site and VPM devices using:

- The VoyenceControl component of the Unified Network Configurator (UNC) application



NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.
For additional information, see the *Unified Network Configurator* manual.

- Configuration/Service Software (CSS)

See the following for specific instructions on the UNC application and CSS:

- ASTRO® 25 system *Unified Network Configurator* manual
- VoyenceControl online help (Online User's Guide)
- ASTRO® 25 system *Core CSS Online Help*



NOTICE: Procedures performed using VoyenceControl are the preferred approach for configuring RADIUS on RF Site and VPM Devices. Using CSS for performing those procedures is optional.

Table 10: Configuring RADIUS on RF Site and VPM Devices

	Using VoyenceControl (preferred)	Using CSS (optional)
1	DNS Configuration on RF Site and VPM Devices with VoyenceControl on page 93	Configuring DNS with CSS on page 100
2	Configuring RADIUS on RF Site and VPM Devices with VoyenceControl on page 96	Configuring RADIUS Sources and Parameters with CSS on page 102

	Using VoyenceControl (preferred)	Using CSS (optional)
3	Setting the Local Cache Size for Central Authentication on RF Site and VPM Devices with VoyenceControl on page 97	Setting the Local Cache Size for Central Authentication with CSS on page 106
4	N/A	Enabling/Disabling Centralized Authentication with CSS on page 107

7.6

Centralized Authentication Configuration on RF Site and VPM Devices with VoyenceControl

This section provides the procedures for configuring centralized authentication on devices using the VoyenceControl component of the Unified Network Configurator (UNC) application.



NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.
For additional information, see the *Unified Network Configurator* manual.

7.6.1

DNS Configuration on RF Site and VPM Devices with VoyenceControl

VoyenceControl can be used to configure Domain Name Service (DNS) on the following devices:

- **RF site devices:**
 - GTR 8000 Base Radio
 - GCM 8000 Comparator
 - GCP 8000 Site Controller
 - GPB 8000 Reference Distribution Module (RDM)
 - GPW 8000 Receiver
- **Voice Processor Module (VPM) devices:**
 - SmartX Site Converter
 - MCC 7500 Voice Processor Module (VPM)
 - Telephone Media Gateway (TMG)



NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

To configure DNS, use the information provided in [DNS Nameservers for Devices in DSR and Non-DSR Sites on page 94](#) and [Table 12: Configlet Editor Information for Configuring DNS on RF Site and VPM Devices on page 95](#).

7.6.1.1

DNS Nameservers for Devices in DSR and Non-DSR Sites

The following table shows Domain Name Services (DNS) configuration for devices in ASTRO® 25 systems with and without the Dynamic System Resilience (DSR) feature implemented. The order column represents primary, secondary, and further (up to four, if needed) numbers of DNS servers.

Table 11: DNS Nameservers for Devices in DSR and Non-DSR Sites

Location	Order	Non-DSR	DSR
Remote Site	1	z<ZZZ>dns01.zone<Z>	z<ZZZ>dns01.zone<Z>
	2	ucs-dns01.ucs	z<ZZZ>dns04.zone<Z>
	3	N/A	ucs-dns01.ucs
	4	N/A	ucs-dns04.ucs
Tsub Prime and Subsites	1	z<ZZZ>dns01.zone<Z>	z<ZZZ>dns01.zone<Z>
	2	z<ZZZ>s<PPP>dns01.site<PPP>.zone<Z>	z<ZZZ>s<PPP>dns01.site<PPP>.zone<Z>
	3	ucs-dns01.ucs	z<ZZZ>dns04.zone<Z>
	4	N/A	ucs-dns01.ucs
Primary Zone Core	1	z<ZZZ>dns01.zone<Z>	z<ZZZ>dns01.zone<Z>
	2	ucs-dns01.ucs	ucs-dns01.ucs
System (Primary)	1	ucs-dns01.ucs	ucs-dns01.ucs
	2	z<ZZZ>dns01.zone<Z> (collocated zone)	z<ZZZ>dns01.zone<Z> (collocated zone)
Standalone DSR Backup Core	1	N/A	z<ZZZ>dns04.zone<Z>
	2	N/A	ucs-dns04.ucs
System (Backup)	1	N/A	ucs-dns04.ucs
	2	N/A	z<ZZZ>dns04.zone<Z> (collocated zone)
Conventional Sub-system	1	z<ZZZ>dns01.zone<Z> (collocated zone)	z<ZZZ>dns01.zone<Z> (collocated zone)
	2	ucs-dns01.ucs	z<ZZZ>dns04.zone<Z> (collocated zone)
	3	N/A	ucs-dns01.ucs
	4	N/A	ucs-dns04.ucs
PTP Devices	1	z<ZZZ>dns01.zone<Z> (collocated zone)	z<ZZZ>dns01.zone<Z> (collocated zone)
	2	ucs-dns01.ucs	ucs-dns01.ucs

where:




<ZZZ> and <Z> indicate the zone to which the device belongs

<PPP> is the 3-digit zero-padded number of the prime site in which the IP Packet Capture virtual machine is located. The possible values are: 001-064.

7.6.1.2

Configlet Editor Information for Configuring DNS on RF Site and VPM Devices

Table 12: Configlet Editor Information for Configuring DNS on RF Site and VPM Devices

Task You Are Performing	Information to Enter in the Configlet Editor
<p>Configuring primary DNS</p> <p> NOTICE: Domain names for remote site devices are based on the site ID and zone ID (such as siteX.zoneZ or nmdX.zoneZ, where X is the site number and Z is the zone number).</p> <p>If applicable, a subsite (remote site) ID is also included, such as ssX.siteY.zoneZ (for a circuit simulcast subsite) or ipssX.siteY.zoneZ (for an IP simulcast subsite), where X is the subsite number, Y is the site number and Z is the zone number.</p>	<p>DNS Domain Name = <DNS Domain Name></p> <p>DNS Service: 1</p> <p>DNS Server IP Address = <DNS IP Address 1>END</p>
<p>Configuring secondary DNS (if present in the system)</p> <p> NOTICE: Secondary Requested DNS Server IP Address and Row Status should be configured only if the primary Requested DNS Server IP Address and Row Status is configured.</p>	<p>DNS Service: 2</p> <p>DNS Server IP Address = <DNS IP Address 2>END</p>
<p>Configuring tertiary DNS (if present in the system)</p> <p> NOTICE: Tertiary Requested DNS Server IP Address and Row Status should be configured only if both a primary Requested DNS Server IP Address and Row Status and a secondary Requested DNS Server IP Address and Row Status are configured.</p>	<p>DNS Service: 3</p> <p>DNS Server IP Address = <DNS IP Address 3>END</p>
<p>Configuring DNS Host Name</p> <p>For the following devices:</p> <ul style="list-style-type: none"> • GTR 8000 Conventional Base Radio • GCM 8000 Conventional Comparator • MCC 7500 Voice Processor Module (VPM) <p>For the following devices, if deployed in a Trunking Subsystem (Tsub):</p> <ul style="list-style-type: none"> • Repeater Site Controller • Repeater Base Radio 	<p>DNS Host Name = <DNS Host Name></p>

Task You Are Performing	Information to Enter in the Configlet Editor
<ul style="list-style-type: none">• HPD Site Controller• HPD Base Radio	

7.6.2

Configuring RADIUS on RF Site and VPM Devices with VoyenceControl

When and where to use: This is the preferred approach for configuring RADIUS on RF Site and VPM Devices.

Procedure:

- 1 Log into VoyenceControl.
- 2 In the navigation pane on the left side of the **VoyenceControl** main window, double-click **Astro 25 Radio Network**.
The selected network tree expands to display the Devices node.
- 3 In the navigation pane on the left side of the window, double-click **Devices**.
The **Devices View** appears. The list of devices and associated properties are displayed in the pane on the right side of the screen.
- 4 Press and hold **SHIFT** and use the arrow keys to select a group of the following devices within a single zone:
 - **GTR 8000**
 - **GCP 8000**
 - **GCM 8000**
 - **GPB 8000**
 - **GPW 8000**
 - **MCC7500 VPM**
 - **SmartX Site Converter** and/or **Telephone Media Gateway**
- 5 Right-click the selected devices group.
- 6 From the context menu, select **Saved Commands**.
- 7 In the **Select Item** window, click the folder icon at the top of the dialog box, to the right of the **Look In** field. Continue to click this icon until the **System** folder displays on the list of folders, on the **Select Item** dialog box.
- 8 Navigate to the folder where the saved command files are stored: `System\Motorola\RADIUS`.
A list of saved commands displays in the **Select Item** dialog box.

- 9 Double-click the **Enable RADIUS Authentication** Saved Command on RF site devices to enable RADIUS authentication on these devices.



NOTICE: For more information on the Saved Commands, see the *Unified Network Configurator* manual.

You are prompted for the system's RADIUS Global Key as part of the Saved Command, as well as username and password for domain user account enabled for RADIUS authentication.



NOTICE: This account will be used by the Saved Command for centralized authentication with devices, and it will automatically verify the RADIUS client configuration.

7.6.3

Setting the Local Cache Size for Central Authentication on RF Site and VPM Devices with VoyenceControl

Perform this procedure on the following devices:

- **RF site devices:**
 - GTR 8000 Base Radio
 - GCP 8000 Site Controller
 - GCM 8000 Comparator
 - GPB 8000 Reference Distribution Module (RDM)
 - GPW 8000 Receiver
- **Voice Processor Module (VPM) devices:**
 - MCC 7500 Voice Processor Module (VPM)
 - SmartX Site Converter
 - Telephone Media Gateway (TMG)

Procedure:

Set the local cache size for central authentication.

See [EMC Smarts Quick Reference on page 201](#).

- If you are setting the number of cached credentials allowed, in the Configlet Editor, enter:
`Central Authentication Cache Size= <x>`
where <x> is a number in the range of 1 to 6 to specify the number of cached credentials allowed
- If you are disabling cached credentials, in the Configlet Editor, enter: `Central Authentication Cache Size= 0`

7.7

Centralized Authentication Configuration on RF Site and VPM Devices with CSS

This section provides the optional Configuration/Service Software (CSS) procedures for configuring centralized authentication on the following devices:

- **RF site devices:**
 - GTR 8000 Base Radio
 - GCM 8000 Comparator

- GCP 8000 Site Controller
- GPB 8000 Reference Distribution Module (RDM)
- GPW 8000 Receiver
- **Voice Processor Module (VPM) devices:**
 - SmartX Site Converter
 - MCC 7500 Voice Processor Module (VPM)
 - Telephone Media Gateway (TMG)

7.7.1

Enabling/Disabling Authentication Services with CSS

Follow these steps to configure the Authentication Services parameter in Configuration/Service Software (CSS).



IMPORTANT: This procedure is optional. Perform this procedure only in the following cases:

- Configuration of a site device before the Master Site is installed, or before the Site Link is up.
- Configuration of a replacement site device offline, before adding it to an existing site.

If neither of those cases applies, perform [Configuring DNS with CSS on page 100](#).

Prerequisites:

Contact your system administrator for the following information:

- DNS Domain Name
- DNS Server IP addresses (primary, secondary, tertiary)
- DNS Hostname (for GTR 8000 Conventional Base Radio, GCM 8000 Conventional Comparator, and MCC 7500 Voice Processor Module (VPM) only).

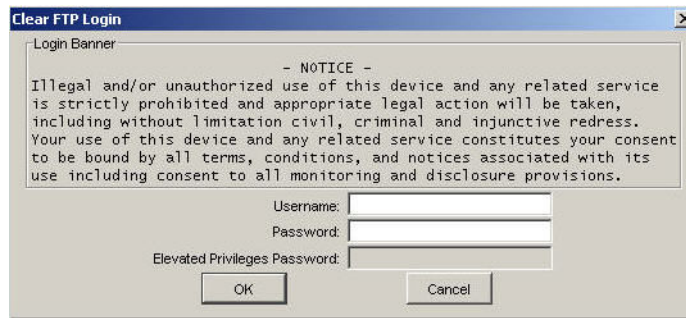
When and where to use: Before enabling this parameter, any login and password may be used on the File Transfer Access Services login window to access a device. After Authentication Services are enabled, the login and password provided will be checked against the following authentication sources:

- **Stored password** – RF site devices support a configurable password for the Local Service and Elevated Privileges accounts. The password is verified against the stored password for these accounts.
- **Built-in logins and passwords** – RF site devices support built-in login/password combinations for login by services such as Software Download Manager (SWDL). Only certain SWDL login names are authenticated in this way.
- **Centralized Authentication** – For authentication through centralized accounts instead of Local Service, Elevated Privileges, and built-in user accounts, you need to configure the centralized authentication parameter in CSS for the **CHAP** protocol as described in this procedure. Note that this procedure requires an Ethernet connection to the device being configured.

[Figure 7: CSS Login Banner on page 99](#) shows the **File Transfer Access Services** login window for CSS. This login is used when communicating to a device through CSS using either an Ethernet connection or serial port connection. If Authentication Services are enabled on a device, enter your username and password. An elevated privileges password is also required if the security level for an operation requires this credential. If Authentication Services are not enabled on a device, type any alphanumeric characters to populate the Username, Password, and Elevated Privileges Password fields, as they cannot be left blank.

The text of the **Login Banner** shown in [Figure 7: CSS Login Banner on page 99](#) can also be configured in CSS. From the menu, select **Security→Device Security Configuration→Remote Access/Login Banner (Ethernet)**. On the **Login Banner** tab, edit the text of the banner and click **Apply**.

Figure 7: CSS Login Banner



For more information regarding the **File Transfer Access Services** login window for CSS, see the *Core CSS Online Help*.

Procedure:

- 1 Launch the **CSS** application.
- 2 From the **Tools**→**Connection Configuration**.
- 3 On the **Connection Screen**, select **Serial** for Connection Type, and click **Connect**.

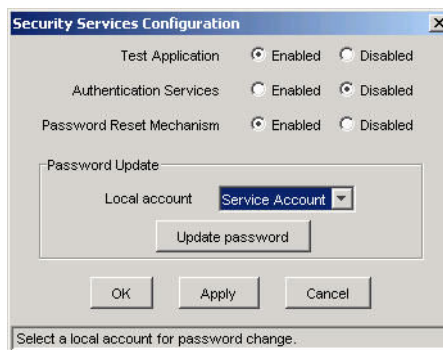


NOTICE: If an authentication window appears, enter your credentials. A message states that CSS successfully connected to this device.

- 4 From the menu, select **Security**→**Device Security Configuration**→**Security Services (Serial)**.

The following window appears.

Figure 8: Security Services Configuration Window



NOTICE: See the *Core CSS Online Help* for information about the other fields on the Security Services Configuration window. Passwords for the Local Service and Elevated Privileges accounts are set using the Password Update area on this Security Services Configuration window. The passwords for the centralized authentication accounts are set using Network Policy Server (NPS) on the Authentication Servers (see [Setting Up User Accounts for RADIUS Authentication/802.1x on page 148](#)).

- 5 Select the **Enable** option for **Authentication Services**.
- 6 Click **Apply** and then click **OK**.

Authentication Services are enabled for the device.

7.7.2

Configuring DNS with CSS

Configuring DNS is required before entering the Fully Qualified Domain Name (FQDN) for server(s) on the Network Security Configuration window in Configuration/Service Software (CSS).

For information on DNS-related failures that may occur during or after DNS configuration, see the [AD/DNS Troubleshooting on page 152](#) chapter.

Using this procedure and [DNS Nameservers for Devices in DSR and Non-DSR Sites on page 94](#), enter the **<IP addresses>** for the primary, secondary, and tertiary DNS servers for this device.

Procedure:

- 1 Launch the **CSS** application.
- 2 From the **File** menu, select **Read Configuration From Device**.
A message states that an Ethernet connection must be established.
- 3 Click **OK**.
- 4 In the **Connection Screen**, enter the **<IP address>** of the device you want to access. Click **Connect**.
If an authentication window appears, enter your credentials.
A message states that CSS successfully connected to this device, and that CSS successfully read the configuration data.
- 5 When prompted, click **OK**.
The device configuration displays in CSS.
- 6 Expand the selections in the navigation pane on the left as needed, then select **Network Services Configuration**.
- 7 In the **Network Services Configuration** window, select the **DNS Service Configuration** tab.

Figure 9: CSS Network Services Configuration – DNS Tab

DNS Server ID	Actual DNS Se...	Requested DN...	Row Status
Primary	0.0.0.0	0.0.0.0	Disabled
Secondary	0.0.0.0	0.0.0.0	Disabled
Tertiary	0.0.0.0	0.0.0.0	Disabled

Domain Name

Actual DNS Domain Name:

Requested DNS Domain Name:

Actual DNS Host Name:

Requested DNS Host Name:

System Name:

DNS Service Wizard

- 8 In the **Requested DNS Server IP** field, enter the IP addresses for the Primary, Secondary, and Tertiary DNS servers.
- 9 Double-click the **Row Status** field to display a drop-down menu, then select one of the following options:
 - **Enabled:** to enable use of the DNS source on this row

- **Disabled:** to disable use of the DNS source on this row

10 Set the Primary DNS Server ID Row Status to **Enabled** to configure the Secondary DNS Server IP.

11 Set the Secondary DNS Server ID Row Status to **Enabled** to configure the Tertiary DNS Server IP.



NOTICE:

The **Actual DNS Server IP** field shows the currently configured values on the device.

It is updated after the configuration is read from the device. To see if the written values are used by the device, the configuration must be read back after write.

12 Click **DNS Service Wizard**.

The wizard always calculates and displays information only for the device that is currently being configured. Using the wizard is the recommended approach.

13 In the **DNS Service Wizard**, perform the following:

Figure 10: DNS Service Wizard

a From the **Subnet** drop-down list, choose the subnet of the device.

b Depending on the device, fill in the information in the active fields.

14 Click **OK** to automatically populate the following:

- **Requested DNS Domain Name**
- **Requested DNS Host Name**
 - For GTR 8000 Conventional Base Radio, GCM 8000 Conventional Comparator, and MCC 7500 VPM
 - For Repeater Site Controller, Repeater Base Radio, HPD Site Controller, HPD Base Radio, if deployed in a Trunking Subsystem (Tsub)
- **System Name**
 - For GTR 8000 Conventional Base Radio, GCM 8000 Conventional Comparator, MCC 7500 VPM, and Conventional Site Controller located in the Conventional subsystem
 - For any device located in the Tsub



NOTICE:

The content of **System Name** is only used by the NM site to enable device discovery.

Using the **System Name** of the managed device the UNC can apply the discovered devices in the appropriate folders.

For more information on how to use the **DNS Service Wizard**, see the *Core CSS Online Help*.

15 From the **File** menu, select one of the following options:

- **Save** to save the configuration changes.
- **Write Configuration to Device** to update the configuration changes on the device.

For details on saving the configuration changes and then updating these changes on the device, see the *Core CSS Online Help*.

The DNS servers are configured for the device.

7.7.3

Configuring RADIUS Sources and Parameters with CSS

Prerequisites: See [RADIUS Service Configuration with CSS on page 103](#).



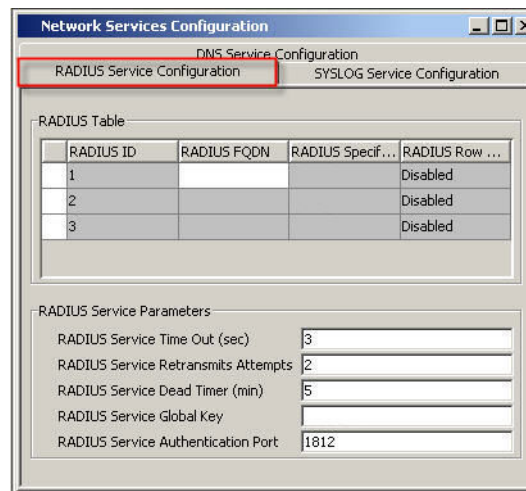
CAUTION: Devices are configured properly by Motorola Solutions when a system is implemented. Changes to configuration should be performed only by personnel with ASTRO® 25 system expertise.

When and where to use:

Follow these steps to configure **one primary** RADIUS source and **one secondary** RADIUS source on the device.

Procedure:

- 1 Launch the **CSS** application.
- 2 From the menu, select **File**→**Read Configuration From Device**.
A message states that an Ethernet connection must be established.
- 3 Click **OK**.
- 4 In the **Connection Screen**, enter the IP address of the device you want to access and click **Connect**.
If an authentication window appears, enter your credentials.
A message states that CSS successfully connected to this device, and that CSS successfully read the configuration data.
- 5 When prompted, click **OK**.
The device configuration displays in CSS.
- 6 Expand the selections in the navigation pane on the left as needed, then select **Network Services Configuration**.
- 7 In the **Network Services Configuration** window, select the **RADIUS Service Configuration** tab.

Figure 11: CSS – RADIUS Service Configuration Tab


Network Services Configuration

DNS Service Configuration
RADIUS Service Configuration
 SYSLOG Service Configuration

RADIUS Table

RADIUS ID	RADIUS FQDN	RADIUS Specif...	RADIUS Row ...
1			Disabled
2			Disabled
3			Disabled

RADIUS Service Parameters

RADIUS Service Time Out (sec) 3

RADIUS Service Retransmits Attempts 2

RADIUS Service Dead Timer (min) 5

RADIUS Service Global Key

RADIUS Service Authentication Port 1812

8 For each RADIUS authentication source, enter:

a RADIUS FQDN

FQDN of a zone-level DC for the zone to which this device belongs. See [Table 13: FQDN of RADIUS Authentication Sources for Devices in DSR and Non-DSR Sites on page 105](#).

b Optional: RADIUS Specific Key

If entered, must match the shared secret for this device on the server entered in the RADIUS FQDN field. If not used, must be set to blank.

9 Double-click the **RADIUS Row Status** field to display a drop-down menu, then select one of the following:

- **Enabled** to enable use of the RADIUS source on this row
- **Disabled** to disable use of the RADIUS source on this row

10 Make changes required to the RADIUS service parameters below the authentication source table.



NOTICE: The RADIUS Service Global Key (preferred) cannot be blank. The global key must match the shared secret on the RADIUS server for this device.

11 From the menu, select **File**→**Save** to save the configuration changes.

12 From the menu, select **File**→**Write Configuration to Device** to update the configuration changes on the device.

For details on saving the configuration changes and then updating these changes on the device, refer to the *Core CSS Online Help*.

7.7.3.1

RADIUS Service Configuration with CSS

The **RADIUS Service Configuration** tab of the **Network Security Service** window in the Configuration/Service Software (CSS) provides two types of fields:

- RADIUS server-specific fields, located in the table on the RADIUS Service Configuration tab

- General RADIUS parameter fields on the lower half of the RADIUS Service Configuration tab

RADIUS Server-Specific Fields

The following RADIUS server-specific fields are located on the upper half of the **RADIUS Service Configuration** tab:

RADIUS ID

A read-only field that displays the ID.

RADIUS FQDN

When configuring the Fully Qualified Domain Name (FQDN) for the RADIUS server, the RADIUS FQDN parameter can be configured only after configuring DNS in CSS.

RADIUS Specific Key

Optional field. The value can be 1-63 alphanumeric characters.

If used, the RADIUS Specific Key entered in CSS must be the same as the shared secret entered for this RADIUS client on the RADIUS server.

RADIUS Global Key



NOTICE: Recommended field instead of **RADIUS Specific Key**.

If the RADIUS Service Global key is used, then for all configured RADIUS servers, the RADIUS Specific Key must be set to blank.

RADIUS Row Status

The RADIUS Row Status parameter allows the CSS user to enable or disable the use of a RADIUS source that is configured on that row.

The Row Status field should not be used to disable individual features that use RADIUS, such as 802.1x, because the **Row Status** field disables RADIUS for all features that might be using it, not just 802.1x. For disabling just the 802.1x feature on a port-by-port basis, through CSS, use the **Port Security** field on the Switch window refer to the procedures for enabling/disabling 802.1x on a GCP 8000 and GPB 8000 Ethernet service port in the *802.1x Service Ports on Switches* manual.

Contact your system administrator for the shared secret entered for the RADIUS client on the RADIUS server.

For more information, see [Configuring DNS with CSS on page 100](#).

For the RADIUS server FQDN to enter in the first row and second row on the RADIUS Service Configuration tab, see [Table 13: FQDN of RADIUS Authentication Sources for Devices in DSR and Non-DSR Sites on page 105](#)

General RADIUS Parameter Fields

The following general RADIUS parameter fields are located on the lower half of the **RADIUS Service Configuration** tab:

RADIUS Service Time Out

Value can be 1-15 seconds.

RADIUS Service Retransmit Attempts

Value can be 1-5.

RADIUS Service Dead Timer

In minutes. Value 0 = disabled, enabled values can be 1-1440.

RADIUS Service Global Key

Recommended field. Value can be 1-63 alphanumeric characters.

The **RADIUS Service Global Key** field:

- Cannot be blank. It provides a fallback mechanism in case no RADIUS Specific Key (optional) is included in the configuration for this device. The global key must match the shared secret on the RADIUS server for this device.
- If the **RADIUS Service Global** key is used, then for all configured RADIUS servers, the **RADIUS Specific Key** must be set to blank.



IMPORTANT: Do **not** change the value for the **RADIUS Service Authentication Port**. This is a standard value for the RADIUS port. Communications with the RADIUS server will fail if this port number is changed.

RADIUS parameters configured for a device, such as the number of Retransmit Attempts, are applicable to all RADIUS sources configured for that device.

7.7.3.2

FQDN of RADIUS Authentication Sources

In ASTRO® 25 systems, for central authentication services, RF site and VPM devices are configured to access the RADIUS service through a Fully Qualified Domain Name (FQDN), so that the IP addresses for the RADIUS service can be changed without changing the configuration on every device.

Table 13: FQDN of RADIUS Authentication Sources for Devices in DSR and Non-DSR Sites

An FQDN consists of two parts: `<hostname>.<domain name>`

The order column represents the order of the RADIUS source.

Location of a device	Order	FQDN Non-DSR	FQDN DSR
Site	1.	z<zzz>rad01.zone<z>	z<zzz>rad01.zone<z>
	2.	ucs-rad01.ucs	z<zzz>rad03.zone<z>
	3.	N/A	ucs-rad01.ucs
	4.	N/A	ucs-rad03.ucs
Tsub Site	1.	z<zzz>rad01.zone<z>	z<zzz>rad01.zone<z>
	2.	z<zzz>s<ppp>rad01.zone<z>	z<zzz>s<ppp>rad01.zone<z>
	3.	ucs-rad01.ucs	z<zzz>rad03.zone<z>
	4.	N/A	ucs-rad01.ucs
UCS Primary Subnet	1.	z<zzz>rad01.zone<z> where <zzz> is colocated with the UCS subnet	z<zzz>rad01.zone<z> where <zzz> is colocated with the UCS subnet
	2.	ucs-rad01.ucs	ucs-rad01.ucs
	3.	N/A	z<zzz>rad03.zone<z> where <zzz> is colocated with the UCS subnet
	4.	N/A	ucs-rad03.ucs
UCS Secondary Subnet	1.	N/A	z<zzz>rad03.zone<z> where <zzz> is colocated with the UCS subnet
	2.	N/A	ucs-rad03.ucs

Location of a device	Order	FQDN Non-DSR	FQDN DSR
	3.	N/A	z<zzz>rad01 z<zzz>rad03.zone<z> where <zzz> is colocat- ed with the UCS subnet
	4.	N/A	ucs-rad01.ucs
	1.	z<zzz>rad01.zone<z>	z<zzz>rad01.zone<z>
	2.	ucs-rad01.ucs	ucs-rad01.ucs
Primary Zone Core	3.	N/A	z<zzz>rad03.zone<z>
	4.	N/A	ucs-rad03.ucs
	1.	N/A	z<zzz>rad03.zone<z>
	2.	N/A	ucs-rad03.ucs
Backup Zone Core	3.	N/A	z<zzz>rad01.zone<z>
	4.	N/A	ucs-rad01.ucs
	1.	N/A	z<zzz>rad03.zone<z> where <zzz> is the zone paired with the stand- alone backup core
	2.	N/A	ucs-rad03.ucs
Standalone Backup Core	3.	N/A	z<zzz>rad01.zone<z>
	4.	N/A	ucs-rad01.ucs
	1.	N/A	z<zzz>rad03.zone<z> where <zzz> is the zone paired with the stand- alone backup core
	2.	N/A	ucs-rad03.ucs
	3.	N/A	z<zzz>rad01.zone<z>
	4.	N/A	ucs-rad01.ucs

where:

<zzz> and <z> indicate the zone to which the device belongs
<ppp> is the prime site number

7.7.4

Setting the Local Cache Size for Central Authentication with CSS

When and where to use:

Follow these steps to use Configuration/Service Software (CSS) to set the number of local cached credentials allowed for a device.

Procedure:

- 1 Launch the **CSS** application.
- 2 From the menu, select **File→Read Configuration From Device**.
A message states that an Ethernet connection must be established.
- 3 Click **OK**.
- 4 In the **Connection Screen** window, enter the IP address of the device you want to access and click **Connect**.
If an authentication window appears, enter your credentials.
A message states that CSS successfully connected to this device, and that CSS successfully read the configuration data.

- 5 When prompted, click **OK**.
The device configuration displays in CSS.
- 6 From the menu, select **Security**→**Device Security Configuration**→**Remote Access/Login Banner (Ethernet)**.
- 7 On the **Remote Access Configuration** tab of the **Remote Access/Login Banner** screen, perform one of the following actions:
 - In the **Local Cache Size** field, enter a number in the range 1 to 6 to specify the number of cached credentials allowed.
 - In the **Local Cache Size** field, enter 0 if you do not want to allow cached credentials.
- 8 Click **Apply** for the changes to take effect.
- 9 Click **OK** to close the **Remote Access/Login Banner** window.

7.7.5

Enabling/Disabling Centralized Authentication with CSS

Prerequisites: Establish an Ethernet connection to the device.

When and where to use: This procedure should be performed when there is no UNC available. If the UNC is available, use a UNC saved command to enable RADIUS and local authentication automatically. For more information, see the *Unified Network Configurator* manual.

Procedure:

- 1 Launch the **CSS** application.
- 2 From the menu, select **File**→**Read Configuration From Device**.
A message states that an Ethernet connection must be established.
- 3 Click **OK**.
- 4 In the **Connection Screen** window, enter the IP address of the device you want to access and click **Connect**.
If an authentication window appears, enter your credentials.
A message states that CSS successfully connected to this device, and that CSS successfully read the configuration data.
- 5 When prompted, click **OK**.
The device configuration displays in CSS.
- 6 From the menu, select **Security**→**Device Security Configuration**→**Remote Access/Login Banner (Ethernet)**.
- 7 On the **Remote Access Configuration** tab of the **Remote Access/Login Banner** screen, perform one of the following actions, depending on whether you have configured Authentication Services before:

If...	Then...
You are setting the Authentication Service for the first time,	proceed to step 8 .
You have already set Authentication Service in the past and Authentication Service is already set to RADI-	perform the following steps to enable Local Authentication Services :

If...	Then...
US-CHAP , but Local Authentication Services are not enabled,	<p>a From the Authentication Service drop-down list, under Centralized Authentication, select None.</p> <p>b Click Apply.</p> <p>c Set Authentication Service back to RADIUS-CHAP.</p> <p>d Click Apply.</p> <p>e Proceed to step 10</p>

8 From the **Authentication Service** drop-down list under **Centralized Authentication**, select one of the following:

- **RADIUS-CHAP** to enable centralized authentication on the device
- **None** to disable centralized authentication on the device

9 Click **Apply**.



NOTICE: Changing the Authentication Service from **None** to **RADIUS-CHAP** will also enable **Local Authentication Services** on the device.
When **Local Authentication Services** are enabled, the device local service account and local privileged account passwords are set to their default values.

10 Click **OK** to close the **Remote Access/Login Banner** screen.

7.8

Configuring RADIUS on SDM3000 RTU and SNT

This procedure needs to be performed only when DNS and NTP services are enabled and configured properly.

For details, refer to the *SDM3000 (Site Device Manager) Owner's Manual*.

Prerequisites: Obtain the `<password>` for the SDM3000 Builder user.

When and where to use:

This section provides the procedures for configuring RADIUS authentication on the following MOSCAD Network Fault Management (NFM) devices:

- SDM3000 Remote Terminal Unit (RTU)
- SDM3000 Network Translator (SNT)

For more information, see the *MOSCAD Network Fault Management Feature Guide*.


Procedure:

- 1** Double-click the most recent version of the **SDM3000 Builder** icon on the desktop.
- 2** In the **SDM3000 Builder** window, depending on which device you are configuring, navigate to the desired **SDM3000 Builder Project** and click **Open**.
- 3** In the **SDM3000 Builder** window for your project, depending on which device you are configuring, perform one of the following actions:

If...	Then...
You are configuring SDM3000 RTU,	<p>perform one of the following actions:</p> <p>a In the Project window, select the desired zone .</p>

If...	Then...
	b From the Sites list in the main window, select the desired site. c In the Edit Site window, select the Network Servers tab.
You are configuring SNT,	perform one of the following actions: a In the Project window, select the desired site. b From the Devices and Equipment List Tabs in the main window, select the Equipment List tab. c From the desired site equipment list in the main window, select SNT . d In the Edit SNT window, select the Network Servers tab.

The Network Servers configuration settings appear in the **Edit Site** window.

- 4 Make sure that the **DNS Services** section and the **NTP servers** section are checked.
 - 5 Make sure that the RADIUS servers are configured as desired.
Add or remove a server, if required.
 - 6 Click the ... (three dots) button to configure the shared secret for the selected server.
 - 7 In the shared secret dialog box, enter the shared secret twice.
Assuming the same shared secret is applicable to all (primary, secondary or tertiary) RADIUS servers in the project, select this option to apply it to all relevant servers.
 - 8 Click **OK**.
The shared secret dialog box closes.
 - 9 Repeat [step 6](#) through [step 8](#) for all defined RADIUS servers.
 - 10 From the **Tools** menu, select **Operational Settings**, then select the desired device.
-  **NOTICE:** Verify that the Ethernet Port is connected.
- 11 In the **Select Operation** dialog box, select **RADIUS Settings**. Click **Next**.
 - 12 In the **Target Select** dialog box, depending on which device you are configuring, perform the following actions:

If...	Then...
You are configuring SDM3000 RTU,	perform the following actions: a Select the Select Sites option. Click Next . b In the Select Sites window, select the desired sites. Click Next .
You are configuring SNT,	perform the following actions: a Select the Select SNTs option. Click Next . b In the Select Sites window, select the desired SNTs. Click Next .

The SDM3000 Builder is ready to begin installing dialog box appears.

13 Click Install.

The installation begins.

14 In the Password field, type the <password> for SDM3000 Builder user and click Login.

The user name field is not editable. It shows the SDM3000 Builder user name. A different user name is not supported.

If messages appear stating that SDM host key is not cached in the known hosts list or that secure protocol service is unavailable, click **OK**.

The installation continues.

15 Click Next. Click Finish.

The **Installation complete** dialog box closes.

7.8.1

Disabling RADIUS on SDM3000 RTU and SNT

Procedure:

- 1 Perform [step 1](#) through [step 3](#) from [Configuring RADIUS on SDM3000 RTU and SNT on page 108](#).
- 2 Clear the **RADIUS Servers** section.
The RADIUS servers section becomes inactive.
- 3 Continue from [step 10](#) till the end of [Configuring RADIUS on SDM3000 RTU and SNT on page 108](#)

7.9

Configuring DNS for MCC 7500 Aux I/O with UNC

This is a **recommended** procedure for configuring DNS for the MCC 7500 Aux I/O Server. This procedure is performed in the Unified Network Configurator (UNC).

For more information, see “Aux I/O Servers” in the *Unified Network Configurator* manual.

Procedure:

- 1 Log on to the EMC Smarts™ Network Configuration Manager.
See “Logging On to the EMC Smarts Network Configuration Manager” in the *Unified Network Configurator* manual.
- 2 In the left pane of the **EMC Smarts Network Configuration Manager Dashboard** window, expand **Networks**→**Astro 25 Radio Network**→**Devices**.
- 3 In the list of devices in the left pane, right-click the FQDN of the Aux I/O. From the context menu, select **editor**→**configlet**.
- 4 In the **Configlet Editor** dialog box, locate the #<FilePath>Section Name</FilePath> section, #<FilePath>Domain Name Service</FilePath> subsection.
- 5 From the #<FilePath>Domain Name Service</FilePath> subsection, select and delete the existing configuration.
- 6 Perform one of the following actions:

If...	Then...
If the zone that contains the Aux I/O is not configured for DSR and the Aux I/O is not in a Tsub,	<p>In the #<FilePath>Domain Name Service</FilePath> subsection, type in the new configuration:</p> <p>a Hostname = <Aux I/O Hostname> Domain Name = <Aux I/O Domain Name></p> <p>b Primary Server = 10.<X>.233.163 Secondary Server = 10.0.0.226</p> <p>Where:</p> <p>The name of the device in the UNC consists of the Aux I/O Hostname and Domain Name in the form of: <Aux I/O Hostname>.<Aux I/O Domain Name></p> <p>For example, for a device with the name: rtul.site33.zone1, the <Aux I/O Hostname> is rtul and the <Aux I/O Domain Name> is site33.zone1.</p> <p><X> is the zone number of the Aux I/O. For Aux I/O devices located in a Conventional Subsystem, the zone number should be the set to the zone that is colocated with the ucs subnet.</p>
If the zone that contains the Aux I/O is configured for DSR and the Aux I/O is not in a Tsub,	<p>In the #<FilePath>Domain Name Service</FilePath> subsection, type in the new configuration:</p> <p>a Hostname = <Aux I/O Hostname> Domain Name = <Aux I/O Domain Name></p> <p>b Primary Server = 10.<X>.233.163 Secondary Server = 10.<X>.237.163 Tertiary Server = 10.0.0.226</p> <p>Where:</p> <p>The name of the device in the UNC consists of the Aux I/O Hostname and Domain Name in the form of: <Aux I/O Hostname>.<Aux I/O Domain Name></p> <p>For example, for a device with the name: rtul.site33.zone1, the <Aux I/O Hostname> is rtul and the <Aux I/O Domain Name> is site33.zone1.</p> <p><X> is the zone number of the Aux I/O. For Aux I/O devices located in a Conventional Subsystem, the zone number should be the set to the zone that is colocated with the ucs subnet.</p>
If the zone that contains the Aux I/O is not configured for DSR and the Aux I/O is in a Trunking Subsystem (Tsub),	<p>In the #<FilePath>Domain Name Service</FilePath> subsection, type in the new configuration:</p> <p>a Hostname = <Aux I/O Hostname> Domain Name = <Aux I/O Domain Name></p> <p>b Primary Server = 10.<X>.233.163 Secondary Server = 10.<X>+100.<rfsite>.126</p> <p>Where:</p> <p>The name of the device in the UNC consists of the Aux I/O Hostname and Domain Name in the form of: <Aux I/O Hostname>.<Aux I/O Domain Name></p> <p>For example:</p>

If...	Then...
	<ul style="list-style-type: none"> For a device deployed in a Tsub prime site with device name <code>rtu1.site64.zone1</code>, the <Aux I/O Hostname> is <code>rtu1</code> and the <Aux I/O Domain Name> is <code>site64.zone1</code>. For a device deployed in a Tsub RF subsite with device name <code>rtu1.site150.zone1</code>, the <Aux I/O Hostname> is <code>rtu1</code> and the <Aux I/O Domain Name> is <code>site150.zone1</code>. For a device deployed in a NM/Dispatch site within Tsub with device name <code>rtu1.nmd191.zone1</code>, the <Aux I/O Hostname> is <code>rtu1</code> and the <Aux I/O Domain Name> is <code>nmd191.zone1</code>. <p><X> is the zone number of the Aux I/O. <rfsite> is the Tsub ID, a number between 1 and 64</p>
If the zone that contains the Aux I/O is configured for DSR and the Aux I/O is in a Trunking Subsystem (Tsub),	<p>In the <code>#<FilePath>Domain Name Service</FilePath></code> subsection, type in the new configuration:</p> <pre> a Hostname = <Aux I/O Hostname> Domain Name = <Aux I/O Domain Name> b Primary Server = 10.<X>.233.163 Secondary Server = 10.<X>+100.<rfsite>.126 Tertiary Server = 10.<X>.237.163 </pre> <p>Where:</p> <p>The name of the device in the UNC consists of the Aux I/O Hostname and Domain Name in the form of: <Aux I/O Hostname>.<Aux I/O Domain Name> For example:</p> <ul style="list-style-type: none"> For a device deployed in a Tsub prime site with device name <code>rtu1.site64.zone1</code>, the <Aux I/O Hostname> is <code>rtu1</code> and the <Aux I/O Domain Name> is <code>site64.zone1</code>. For a device deployed in a Tsub RF subsite with device name <code>rtu1.site150.zone1</code>, the <Aux I/O Hostname> is <code>rtu1</code> and the <Aux I/O Domain Name> is <code>site150.zone1</code>. For a device deployed in a NM/Dispatch site within Tsub with device name <code>rtu1.nmd191.zone1</code>, the <Aux I/O Hostname> is <code>rtu1</code> and the <Aux I/O Domain Name> is <code>nmd191.zone1</code>. <p><X> is the zone number of the Aux I/O. <rfsite> is the Tsub ID, a number between 1 and 64</p>

7 Click **Schedule**.

8 In the **Schedule Job** window, type in the job name. Click **Approve & Submit**.

The job status can be viewed using the **Schedule Manager** available from the **Tools** menu in the EMC Smarts™ Network Configuration Manager main window.

7.10

Configuring NTP for MCC 7500 Aux I/O with UNC

This is a **recommended** procedure for configuring NTP for the MCC 7500 Aux I/O Server. This procedure is performed in the Unified Network Configurator (UNC).

For more information, see “Aux I/O Servers” in the *Unified Network Configurator* manual.

Prerequisites: Configure DNS. See [Configuring DNS for MCC 7500 Aux I/O with UNC on page 110](#).

Procedure:

- 1 Log on to the EMC Smarts™ Network Configuration Manager.
See “Logging On to the EMC Smarts Network Configuration Manager” in the *Unified Network Configurator* manual.
- 2 In the left pane of the **EMC Smarts Network Configuration Manager Dashboard** window, expand **Networks**→**Astro 25 Radio Network**→**Devices**.
- 3 In the list of devices in the left pane, right-click the FQDN of the Aux I/O. From the context menu, select **editor**→**configlet**.
- 4 In the **Configlet Editor** dialog box, locate the #<FilePath>Section Name</FilePath> section, #<FilePath>NTP Configuration</FilePath> subsection.
- 5 From the #<FilePath>NTP Configuration</FilePath> subsection, select and delete the existing configuration.
- 6 Perform one of the following actions:

If...	Then...
<p>Aux I/O resides in one of the following locations:</p> <ul style="list-style-type: none"> • Circuit Simulcast Subsite • IP Simulcast Dual LAN Subsite • IP Simulcast non-Dual LAN Subsite • Simulcast Prime Subsystem (DSR/non-DSR) 	<p>Type in <IP addresses> for NTP servers in the Primary Server field and Secondary Server field, if needed, in the following way:</p> <ul style="list-style-type: none"> • If this is a Simulcast Prime Subsystem: Status = on Primary server = ntp01.site<#>.zone<#> Secondary server = ntp02.zone<#> • If this is an IP Simulcast non-Dual LAN Subsite: Status = on Primary server = ntp01.ipss<#>.site<#>.zone<#> Secondary server = ntp01.site<#>.zone<#> • If this is an IP Simulcast Dual LAN Subsite: Status = on Primary server = ntp01.site<#>.zone<#> Secondary server = ntp02.zone<#> • If this is a Circuit Simulcast Subsite: Status = on Primary server = ntp01.ss<#>.site<#>.zone<#> Secondary server = ntp01.site<#>.zone<#>

If...	Then...
The Aux I/O Server resides in a non-DSR zone and a non-Simulcast site. This includes a non-Simulcast Tsub prime site,	Type in <IP addresses> for NTP servers in the Primary Server field and Secondary Server field, if needed, in the following way: Status = on Primary server = ntp02.zone<#> Secondary server = ntp03.zone<#>
The Aux I/O Server resides in a DSR zone and a non-Simulcast site. This includes a non-Simulcast Tsub prime site,	Type in <IP addresses> for NTP servers in the Primary Server field and Secondary Server field, if needed, in the following way: Status = on Primary server = ntp02.zone<#> Secondary server = ntp05.zone<#>

where <#> is the zone, site, or subsite number set to the ID of the location of the Aux I/O

7 Click **Schedule**.

8 In the **Schedule Job** window, type in the job name. Click **Approve & Submit**.

The job status can be viewed using the **Schedule Manager** available from the **Tools** menu in the EMC Smarts™ Network Configuration Manager main window.

7.11

Configuring RADIUS for MCC 7500 Aux I/O with UNC

This is a **recommended** procedure for configuring RADIUS for the MCC 7500 Aux I/O Server. This procedure is performed in the Unified Network Configurator (UNC).

For more information, see “Aux I/O Servers” in the *Unified Network Configurator* manual.

For updating the RADIUS passphrase, see “Updating the RADIUS Passphrase on the Aux I/O Server” in the *Unified Network Configurator* manual.

Prerequisites: Configure DNS. See [Configuring DNS for MCC 7500 Aux I/O with UNC on page 110](#).

Procedure:

- 1 Log on to the EMC Smarts™ Network Configuration Manager.
See “Logging On to the EMC Smarts Network Configuration Manager” in the *Unified Network Configurator* manual.
- 2 In the left pane of the **EMC Smarts Network Configuration Manager Dashboard** window, expand **Networks**→**Astro 25 Radio Network**→**Devices**.
- 3 In the list of devices in the left pane, right-click the FQDN of the Aux I/O. From the context menu, select **editor**→**configlet**.
- 4 In the **Configlet Editor** dialog box, locate the #<FilePath>Section Name</FilePath> section, #<FilePath>RADIUS Configuration</FilePath> subsection.
- 5 From the #<FilePath>RADIUS Configuration</FilePath> subsection, select and delete the existing configuration.
- 6 Perform one of the following actions:

If...	Then...
<p>The Aux I/O Server is in a non-DSR zone,</p>	<p>In the #<FilePath>RADIUS Configuration</FilePath> subsection, type in the following new configuration:</p> <pre> Radius Server 1 Server Hostname = z00<X>rad01.zone<X> Server Port = 1812 Timeout = 10 End Radius Server 2 Server Hostname = ucs-rad01.ucs Server Port = 1812 Timeout = 10 End </pre> <p>where <X> is the zone number of the Aux I/O. For Aux I/O devices located in a Conventional Subsystem, the zone number should be the set to the zone that is colocated with the ucs subnet</p>
<p>The Aux I/O Server is in a DSR zone,</p>	<p>In the #<FilePath>RADIUS Configuration</FilePath> subsection, type in the following new configuration:</p> <pre> Radius Server 1 Server Hostname = z00<X>rad01.zone<X> Server Port = 1812 Timeout = 10 End Radius Server 2 Server Hostname = z00<X>rad03.zone<X> Server Port = 1812 Timeout = 10 End Radius Server 3 Server Hostname = ucs-rad01.ucs Server Port = 1812 Timeout = 10 End </pre> <p>where <X> is the zone number of the Aux I/O. For Aux I/O devices located in a Conventional Subsystem, the zone number should be the set to the zone that is colocated with the ucs subnet</p>
<p>The Aux I/O Server is in a Trunking Subsystem (Tsub),</p>	<p>In the #<FilePath>RADIUS Configuration</FilePath> subsection, type in the following new configuration:</p> <p>Non-DSR:</p> <pre> Radius Server 1 Server Hostname = z00<X>rad01.zone<X> Server Port = 1812 Timeout = 10 End Radius Server 2 </pre>

If...	Then...
	<pre> Server Hostname = z00<X>s0<prime>rad01.site<rfSite>.zone<X> DSR: Radius Server 1 Server Hostname = z00<X>rad01.zone<X> Server Port = 1812 Timeout = 10 End Radius Server 2 Server Hostname = z00<X>s0<prime>rad01.site<rfSite>.zone<X> Server Port = 1812 Timeout = 10 End Radius Server 3 Server Hostname = z00<X>rad03.zone<X> Server Port = 1812 Timeout = 10 End </pre> <p>where:</p> <p><X> is the zone number of the Aux I/O located in a Tsub <rfsite> is the Tsub ID, a number between 1 and 64 <prime> is the zero padded Prime Site number between 01 and 64</p>

7 Click **Schedule**.

8 In the **Schedule Job** window, type in the job name. Click **Approve & Submit**.

The job status can be viewed using the **Schedule Manager** available from the **Tools** menu in the EMC Smarts™ Network Configuration Manager main window.

7.11.1

Disabling RADIUS for MCC 7500 Aux I/O with UNC

This is a **recommended** procedure for disabling RADIUS for the MCC 7500 Aux I/O Server. This procedure is performed in the Unified Event Configurator (UNC).

Procedure:

- 1 Log on to the EMC Smarts™ Network Configuration Manager.
See "Logging On to the EMC Smarts Network Configuration Manager" in the *Unified Network Configurator* manual.
- 2 In the left pane of the **EMC Smarts Network Configuration Manager Dashboard** window, expand **Networks**→**Astro 25 Radio Network**→**Devices**.
- 3 In the list of devices in the left pane, right-click the FQDN of the Aux I/O. From the context menu, select **editor**→**configlet**.
- 4 In the **Configlet Editor** dialog box, locate the #<FilePath>Section Name</FilePath> section, #<FilePath>RADIUS Configuration</FilePath> subsection.

- 5 From the #<FilePath>RADIUS Configuration</FilePath> subsection, select and delete the existing configuration.
- 6 Click **Save**→**Close**.

7.12

Configuring RADIUS for MCC 7500 Aux I/O on MCC 7500 Aux I/O Server

This is an **optional** procedure for configuring RADIUS for the MCC 7500 Aux I/O. This procedure is performed on the MCC 7500 Aux I/O Server.

Prerequisites: Obtain the following information from your system administrator:

- <IP address> of the MCC 7500 Aux I/O
- Web administrator's <password>

When and where to use: This procedure needs to be performed only when DNS and NTP services are enabled and configured properly.

Procedure:

- 1 Launch **Internet Explorer**.
- 2 In the Internet Explorer address bar, enter: <IP address>
where <IP address> is the IP address of the MCC 7500 AUX I/O
If a warning message appears, click **Yes**.
- 3 In the MCC 7500 AUX I/O splash screen, click **Go to home page**.
- 4 In the logon dialog box:
 - a In the **Username** field, type the web administrator's username.
The web administrator's username is `admin`.
 - b In the **Password** field, type the web administrator's <password>.
 - c Click **OK**.
- 5 On the MCC 7500 AUX I/O home page, select **Admin**.
- 6 On the Administrator page, select **Configuration**.
- 7 In the logon dialog box:
 - a In the **Username** field, type the web administrator's <username>.
where the web administrator's username is `admin`
 - b In the **Password** field, type the web administrator's <password>.
 - c Click **OK**.
- 8 On the Configuration page, select **RADIUS**.
- 9 On the RADIUS Configuration page, select **Support RADIUS**, then perform the following, depending on the site:

If...	Then...
This is a DSR site,	In the Hostname field: <ul style="list-style-type: none"> • For the primary server, type: <code>z00<z>rad01.zone<x></code>

If...	Then...
	<ul style="list-style-type: none"> For the secondary server, type: <code>z00<z>rad03.zone<x></code> For the tertiary server, type: <code>ucs-rad01.ucs</code> <p>where <z> is the zone number</p>
This is a non-DSR site,	<p>In the Hostname field:</p> <ul style="list-style-type: none"> For the primary server, type: <code>z00<z>rad01.zone<z></code> For the secondary server, type: <code>ucs-rad01.ucs</code> <p>where <z> is the zone number</p>
This is a Disaster Recovery situation,	<p>perform the following actions:</p> <ol style="list-style-type: none"> Type the primary server host name in the Host name field according to backed up data. Type the secondary server host name in the Host name field according to backed up data. <p>For Disaster Recovery, use the backed up data for the following:</p> <ul style="list-style-type: none"> If the tertiary server is used, type hostname in the Hostname field for the tertiary server. For the primary server, type the secret in the Secret field. For the primary server, retype the secret in the Secret Confirmation field. For the secondary server, type the secret in the Secret field. For the secondary server, retype the secret in the Secret Confirmation field. If the tertiary server is used, type the secret in the Secret field for the tertiary server. If the tertiary server is used, type the secret in the Secret Confirmation field for the tertiary server.
This is Trunking Subsystem (Tsub),	<p>In the #<FilePath>RADIUS Configuration</FilePath> subsection, type in the following new configuration:</p> <p>Non-DSR:</p> <pre>Radius Server 1 Server Hostname = z00<x>rad01.zone<x> Server Port = 1812 Timeout = 10 End Radius Server 2 Server Hostname = z00<x>s0<prime>rad01.site<rfsite>.zone<x></pre> <p>DSR:</p> <pre>Radius Server 1 Server Hostname = z00<x>rad01.zone<x> Server Port = 1812 Timeout = 10 End</pre>

If...	Then...
	<pre> Radius Server 2 Server Hostname = z00<X>s0<prime>rad01.site<rfsite>.zone<X> Server Port = 1812 Timeout = 10 End Radius Server 3 Server Hostname = z00<X>rad03.zone<X> Server Port = 1812 Timeout = 10 End where: <X> is the zone number of the Aux I/O located in a Tsub <rfsite> is the Tsub ID, a number between 1 and 64 <prime> is the zero padded Prime Site number between 01 and 64 </pre>

RADIUS is configured.

10 Click **Apply**.

A success message appears.

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

The desktop appears.

7.12.1

Disabling RADIUS on MCC 7500 Aux I/O Server

Follow these steps to disable previously enabled RADIUS authentication.

Procedure:

- 1 Perform [step 1](#) through [step 8](#) from [Configuring RADIUS for MCC 7500 Aux I/O on MCC 7500 Aux I/O Server on page 117](#).
- 2 Clear the **Support RADIUS** option to disable RADIUS on the MCC 7500 Aux I/O Server.
- 3 Click **Apply**.
A success message appears.
- 4 From the **File** menu, select **Close**.
The desktop appears.

7.13

RADIUS Configuration on PTP 600 and PTP 800 Devices

For systems that support fault management of PTP 600 and 800 devices, ensure that the list of PTP devices in your ASTRO® 25 system is established as a list of RADIUS clients in a .CSV file you can create and/or obtain from your system administrator. This file should include each PTP device and each new backhaul switches RADIUS clients with IP addresses which will need to be imported to the RADIUS server.

To import the file with the list of PTP devices as RADIUS clients to the RADIUS server, use [Batch Importing RADIUS Clients to the Primary RADIUS Server for a Zone on page 80](#).

To set up a PTP 600 and PTP 800 device to interface with the RADIUS Server in an ASTRO® 25 system, refer to the appropriate Cambium Networks PTP User Guide.

For information on PTP users and their assigned roles in the ASTRO® 25 system, see [Table 2: Roles in ASTRO 25 Active Directory on page 33](#).

For more information on RADIUS Authentication Sources for PTP devices, refer to the *Fault Management Reference Guide*.

7.14

Configuring RADIUS Shared Secret on Console Telephony Media Gateway

In an ASTRO® 25 system, the RADIUS authentication sources are already set up by Motorola Solutions in Console Telephony Media Gateway configurations. The only RADIUS configuration you need to perform on Console Telephony Media Gateway is to ensure that the shared secret in the Console Telephony Media Gateway configuration matches the shared secret entered for the Console Telephony Media Gateway RADIUS client on the RADIUS server.

There is a default shared secret in the Console Telephony Media Gateway configurations by Motorola Solutions.

Procedure:

- 1 To check current RADIUS server(s) configuration in the Console Telephony Media Gateway, enter: `show run | include radius`

The RADIUS server configuration appears. See the following example results. One or two RADIUS servers are configured.

```
radius-server host <radius server 1 IP address>auth-port 1812 acct-port 1813 key 7 <encrypted shared secret>
```

```
radius-server host <radius server 2 IP address>auth-port 1812 acct-port 1813 key 7 <encrypted shared secret>
```

- 2 To change the shared secret on the Console Telephony Media Gateway, in the configuration mode, enter:

```
radius-server host <radius server IP address>auth-port 1812 acct-port 1813 key <new shared secret>
```

where:

<radius server IP address> is the same radius server IP address you got from the [step 1](#)

<new shared secret> is the new shared secret you want to change to

The new shared secret is configured for this RADIUS server.

- 3 For additional RADIUS server(s), repeat [step 2](#).

For each server you can configure a different shared secret.

The new shared secret is configured for all RADIUS server(s).

- 4 To save the new configuration to startup configuration, enter: `write mem`

The new configuration is saved to startup configuration.

7.15

Configuring RADIUS Shared Secret on Terminal Servers

In the ASTRO® 25 system, RADIUS authentication sources are already set up in Terminal Server configurations provided by Motorola Solutions. The only RADIUS configuration to perform on LX-4008T, LX-4016T, and LX-4048T terminal servers is to ensure that the shared secret in the Terminal Server configuration matches the shared secret entered for the Terminal Server RADIUS client on the RADIUS server.

Prerequisites: Obtain the following from your system administrator:

- DB-9 Modular adapter and RJ-45 cable for serial connection to Terminal Server
- Terminal Server credentials with privilege password for Terminal Server account
- Primary and secondary shared secret

Procedure:

- 1 Establish Telnet or SSH connection to the terminal server.
Connection can be established using PuTTY. For more information, see “Logging On to the Terminal Servers” in the *Terminal Servers LX Series* manual.
- 2 Log on using the correct login and password.
- 3 To access privilege mode, at the prompt, enter: `enable <privilege password>`
- 4 Change the primary and secondary RADIUS server authentication passwords. At the prompt, enter:
 - a `config radius primary authentication server secret <primary secret>`
 - b `config radius secondary authentication server secret <secondary secret>`
- 5 Save configuration changes. Enter: `save config flash`

7.16

RADIUS Configuration on UNC

To configure RADIUS on the UNC, see “Configuring the RADIUS Server” in the *Unified Network Configurator* manual.

Chapter 8

Active Directory Server Operation

This chapter provides information about tasks that you can perform once the Active Directory and Domain Name Services (DNS) are installed and operational on your system.

8.1

Creating Active Directory User Accounts

Process:

- 1 Add user accounts to the domain.
See [Adding User Accounts to a Domain on page 122](#).
- 2 Enable user accounts in Active Directory.
See [Enabling User Accounts in Active Directory on page 125](#).
- 3 Modify the user account attributes for accessing Unix-based devices.
See [Modifying User Account Attributes for Accessing Unix-Based Devices on page 127](#).
- 4 Assign group membership to a user account (if the group is already created).
See [Assigning Group Membership to a User Account on page 124](#).

8.2

Adding User Accounts to a Domain

This procedure is **not** required for the administrator and guest accounts.

Prerequisites:

Log on to a Unix device joined to the domain automatically creates the user's home directory: `/home/username`. For a list of Unix-based devices, see [Active Directory Client Devices and Applications on page 36](#).

When and where to use:

When creating a user, use the UID that is populated by Active Directory. Do not try to change the UID of an existing user. Also, do not try to use the UID of a deleted user.



NOTICE: UID range varies from 10000 to 60000 (where 60000 is the maximum permitted UID in the Unix system). It is to be used for non-system user accounts (local or domain) created by the customer or Motorola Solutions support personnel after system installation and initial configuration. These are typically interactive accounts.

Since only a single domain exists by default, the same domain name is used for logging on to any device in any zone. For example, `<AD Domain Name>/user1` to log on to the system-level DC as well as the zone-level DC. For details see [Table 8: User Input Requirements – Domain Controller Configuration on page 75](#).

There is an association between user accounts created in Active Directory and some of the applications. In such situations, the user account that is created should have the same user name as that of the account used to log into the application. This makes it easier to administer this user and improves the overall performance of the server (for example, logging on and logging off).

Procedure:

- 1 From **Start**, open **Active Directory Users and Computers**:

- a From **Start**, click **Search**.
 - b In the search field, type in `administrative`
 - c Click **Administrative Tools**.
 - d In the **Administrative Tools** window, double-click **Active Directory Users and Computers**.
- 2 In the **Active Directory Users and Computers** window, right-click **Users** in the left pane and select **New→Users**.
- 3 In the **New Object - Users** window, enter the following information. Click **Next**:
 - a *<Full Name>*
 - b *<User login name>*

where *<Full Name>* and *<User login name>* are the AD domain name consisting of the following characters: a-z, A-Z, 0-9, _

Other fields are optional.
- 4 In the password dialog box, enter the same *<password>* for both **Password** and **Confirm password** fields.

Where *<password>* must meet the following criteria:

 - The minimum password length is 14 characters
 - The password must have at least two of the following: lowercase character, uppercase character, number
 - The password must have at least one of the following symbols: hyphen (-), underscore (_), dollar (\$), pound/hash (#)
 - The password must not be one of the last 24 passwords

If any of the criteria are not met, an error displays in the next step and the procedure needs to be repeated.
- 5 For a system account (as defined in [Active Directory Theory of Operations on page 31](#)), clear the **User must change password at next logon** check box and select the **Password never expires** check box.
- 6 On the account creation summary page, click **Finish**.

The **New Object** window closes. The user account appears in the user list in the right pane.
- 7 Optional: If an error occurs (for example, password of insufficient strength), a dialog box appears stating what the error is. Perform the following actions:
 - a Click **OK** to close the dialog box.
 - b Click **Cancel** to abort creating the user account.
 - c Repeat this procedure.
- 8 Right-click the newly created user.

To enable the user to log on to a specific device, the user has to be made member of the relevant user groups. If you want to enable RADIUS user, see [Setting Up User Accounts for RADIUS Authentication/802.1x on page 148](#).
- 9 From the drop-down menu, select **Properties**.
- 10 In the **User Properties** window, select the **Member Of** tab.
- 11 In the list of groups to which the user belongs, click **Add**.

For information about setting up group membership of Active Directory users so that they can perform specific administration menu procedures, contact your Active Directory administrator.

- 12 In the text area of the window that appears, type in the name of the group the user should become a member of. Click **OK**.

The new group appears in the list of groups to which the user belongs.

- 13 Repeat [step 11](#) and [step 12](#) for all the groups in which this user needs to be a member.
- 14 For Unix accounts, perform [Modifying User Account Attributes for Accessing Unix-Based Devices](#) on page 127.

Related Links

[Creating Active Directory User Accounts](#) on page 122

8.3

Adding Groups to a Domain

Procedure:

- 1 From **Start**, open **Active Directory Users and Computers**:
 - a From **Start**, click **Search**.
 - b In the search field, type in `administrative`
 - c Click **Administrative Tools**.
 - d In the **Administrative Tools** window, double-click **Active Directory Users and Computers**.
- 2 In the **Active Directory Users and Computers** window, right-click **Users** in the left pane and select **New→Group**.
- 3 In the **New Object - Group** window, enter the `<Group Name>`.**NOTICE:** Groups created by Motorola Solutions have roles by default. Any newly created groups should have roles assigned (by becoming a member of role groups) in order to be used in the system.
- 4 In the **Group Scope** field, select the **Domain local** radio button.
- 5 Click **OK**.

The **New Object - Group** window closes.
- 6 Double-click the group created and select the **Unix Attributes** tab.
- 7 Select domain name from the drop-down list for the **NIS domain**.

Use the GID that is auto-generated.
- 8 Click **OK**.

8.4

Assigning Group Membership to a User Account

When and where to use: Follow these steps to assign group membership to a user account that is a part of the Active Directory domain.



IMPORTANT: This procedure is **not** required for the administrator and guest accounts. Groups are provided by default. However, if there is a need for an extra group, it can be created using this procedure.

Procedure:

- 1 Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.

The account name set up by Motorola Solutions is “motosec”.

- 2 From **Start**, open **Active Directory Users and Computers**:
 - a From **Start**, click **Search**.
 - b In the search field, type in `administrative`
 - c Click **Administrative Tools**.
 - d In the **Administrative Tools** window, double-click **Active Directory Users and Computers**.
- 3 In the **Active Directory Users and Computers** window, select **Users** in the left pane.
- 4 In the list of users and groups in the right pane, double-click the desired user.
- 5 In the **User Properties** dialog box, select the **Member Of** tab.
- 6 In the list of groups to which the user belongs, perform one of the following actions:
 - To add users, click **Add...**
 - To remove users, click **Remove** and then **OK** twice.
- 7 In the **Select Groups** dialog box, enter the name of the group.
For information on Active Directory groups, contact your Active Directory administrator.
- 8 Perform one of the following actions:

If...	Then...
If the group is found and the group name that is entered becomes underlined,	in the Select Groups dialog box, click OK .
If the string entered is only a partial name and the Multiple Names Found dialog box appears showing all names found,	perform one of the following actions: <ol style="list-style-type: none">a Select the desired group.b In the Multiple Names Found dialog box, click OK.
If no match is found and the Name Not Found dialog box appears,	Click Cancel and repeat step 6 .

The dialog box closes. The group list is updated with the New Group.

- 9 Repeat [step 6](#) through [step 8](#) for all the groups in which this user needs to be a member.
- 10 Once all groups have been added, in the **User Properties** window, click **OK**.

The **User Properties** window closes.

- 11 Close the **Active Directory Users and Computers** window.

Related Links

[Creating Active Directory User Accounts](#) on page 122

8.5

Enabling User Accounts in Active Directory

Procedure:

- 1 Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.

The account name set up by Motorola Solutions is “motosec”.

The administrator’s desktop appears.

- 2 From **Start**, open **Active Directory Users and Computers**:
 - a From **Start**, click **Search**.
 - b In the search field, type in `administrative`
 - c Click **Administrative Tools**.
 - d In the **Administrative Tools** window, double-click **Active Directory Users and Computers**.
- 3 In the **Active Directory Users and Computers** window, select **Users** in the left pane.
- 4 In the list of users and groups in the right pane, right-click the desired user.
- 5 From the drop-down menu, select **Enable Account**.

A message window states that the user account has been enabled.
- 6 Click **OK**.

The message window closes and the user account is now enabled.

Related Links

[Creating Active Directory User Accounts](#) on page 122

8.6

Resetting User Passwords in Active Directory

Procedure:

- 1 Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.

The account name set up by Motorola Solutions is “motosec”.

The administrator’s desktop appears.
- 2 From **Start**, open **Active Directory Users and Computers**:
 - a From **Start**, click **Search**.
 - b In the search field, type in `administrative`
 - c Click **Administrative Tools**.
 - d In the **Administrative Tools** window, double-click **Active Directory Users and Computers**.
- 3 In the **Active Directory Users and Computers** window, select **Users** in the left pane.
- 4 In the list of users and groups in the right pane, right-click the desired user.
- 5 From the context menu, select **Reset Password**.
- 6 In the **Password Change** window:
 - a Type the `<new password>` twice.
 - b Clear the **User must change password at next login** check box. Click **OK**.

A message window states that the password has been changed successfully.
- 7 Click **OK**.

The message window closes.

8.7

Disabling User Accounts in Active Directory

If a user account is not needed anymore, it should first be disabled and only then deleted after 180 days.

This procedure applies only to Unix-based devices joined to the domain: once the user is deleted from Active Directory, home directory has to be deleted from each machine separately. The `delete_user_files` script can be invoked as root to delete all files belonging to a user including home directory of a user. For `delete_user_files` on Linux and Solaris devices, see the *Unix Supplemental Configuration* manual.

A Provisioning Manager or Elite console account needs to be deleted in both the Active Directory and the Provisioning Manager application. If an account is deleted from Active Directory, the user is no longer able to access the Provisioning Manager application with this account.

Procedure:

- 1 Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.
The account name set up by Motorola Solutions is “motosec”.
The administrator’s desktop appears.
- 2 From **Start**, open **Active Directory Users and Computers**:
 - a From **Start**, click **Search**.
 - b In the search field, type in `administrative`
 - c Click **Administrative Tools**.
 - d In the **Administrative Tools** window, double-click **Active Directory Users and Computers**.
- 3 From the **Active Directory Users and Computers** window, select **Users** in the left pane.
- 4 From the list of users and groups in the right pane, right-click the desired user.
- 5 From the drop-down menu, select **Disable Account**.
- 6 In the message window, click **OK**.
The message window closes and the user account is now disabled.

8.8

Modifying User Account Attributes for Accessing Unix-Based Devices

Follow these steps to enable Unix user accounts and specify the Unix-based devices that the account will be allowed to access.

Prerequisites: Contact your system administrator for the login group names of the devices this user will need to access. For a list of Unix devices, see [Active Directory Client Devices and Applications on page 36](#).

Procedure:

- 1 Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.
The account name set up by Motorola Solutions is “motosec”.
The administrator desktop appears.

- 2 From **Start**, open **Active Directory Users and Computers**:
 - a From **Start**, click **Search**.
 - b In the search field, type in `administrative`
 - c Click **Administrative Tools**.
 - d In the **Administrative Tools** window, double-click **Active Directory Users and Computers**.
- 3 In the **Active Directory Users and Computers** window, click the **Users** folder.
- 4 In the **Users** folder, right-click the user account and select **User Properties**.

User accounts have **User** as their **Type** in the **Active Directory Users and Computers** window.
- 5 In the **User Properties** window, select the **UNIX Attributes** tab. Perform the following actions:
 - a Select the domain in the **NIS Domain** field.
 - b Type in `3000` as the Group ID in the **Primary Group name/GID** field. Click **Apply**.

The Group ID changes to **domuser**.
- 6 Add group memberships for this user account in the following way:
 - a Click the **Member of** tab.
 - b Click **Add**.
 - c In the dialog box, type the name of the login group for the Unix device that this user will be permitted to access.

Click **Check Names** to verify correctness of the login group name.
 - d Click **OK**.

A warning message appears if you typed a group which had been already added to this user.
- 7 Add the **domuser** group membership in the following way:
 - a Click **Add**.
 - b In the dialog box, type the name of the login group for the Unix-based device that this user will be permitted to access.

Click **Check Names** to verify correctness of the login group name.
 - c Click **OK**.

A warning message appears if you typed a group which had been already added to this user.
- 8 Add role groups for each role the user belongs to.

This is required for successfully logging on to Unix-based devices.
- 9 Select the **domuser** account and click **Set Primary Group** to set the domuser as the primary group.
- 10 Optional: Perform one of the following actions:
 - If you want to remove one group membership for this user account, select a group. Click **Remove**.
 - If you want to remove multiple group memberships for this user account, select the groups you want to remove. Click **Remove**.



NOTICE: If you are asked if you want to remove the user from the selected group, select **Yes**.

11 Click OK.

The **User Properties** window closes.

12 Optional: If you are prompted with a **UID/GID Warning**, click **Yes**. If there is any User ID conflict, click **Generate Unique ID**.

UID range varies from 10000 to 60000 (where 60000 is the maximum permitted UID in the Unix system). It is to be used for non-system user accounts (local or domain) created by the customer or Motorola Solutions support personnel after system installation and initial configuration. These are typically interactive accounts.

Related Links

[Creating Active Directory User Accounts](#) on page 122

8.9

Adding a Unix-Enabled Group to the Active Directory Domain

Prerequisites: For a list of Unix devices, see [Active Directory Client Devices and Applications](#) on page 36.

Procedure:

- 1** Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.
The account name set up by Motorola Solutions is “motosec”.
The administrator desktop appears.
- 2** From **Start**, open **Active Directory Users and Computers**:
 - a** From **Start**, click **Search**.
 - b** In the search field, type in `administrative`
 - c** Click **Administrative Tools**.
 - d** In the **Administrative Tools** window, double-click **Active Directory Users and Computers**.
- 3** In the left pane of the **Active Directory Users and Computers** window, navigate to the **Users** folder.
- 4** In the left pane of the **Active Directory Users and Computers** window, right-click **Users**. Select **New→Group**
- 5** In the **New Object - Group** window, type the name of the group in the **Group Name** field. Click **OK**.
The **Group Name (pre-Windows 2000)** field is populated after the group name is entered. Keep the defaults for **Group Scope** and **Group Type** fields.
The **New Object - Group** window closes.
- 6** In the list of groups in the right pane of the **Active Directory Users and Computers** window, right-click the newly created group. Select **Properties**.
- 7** Select the **UNIX Attributes** tab.
- 8** On the **UNIX Attributes** tab:
 - a** Select the domain in the **NIS Domain** field.
 - b** Type the group ID in the **Group ID** field.

9 Click **OK**.

The **Properties** window closes.

8.10

MOSCAD NFM Operations Local to a Server

Procedures apply to the following MOSCAD NFM devices only:

- Graphical Master Computer (GMC)
- Graphical WorkStation (GWS)

8.10.1

Logging on to the Server with a Local Account

Procedure:

- 1 Press the CTRL+ALT+DEL keys simultaneously.



NOTICE: If the security is set up on this system, a dialog box presenting a legal description about the usage of this system appears. Press ENTER or click **OK**.

- 2 At the logon window, enter the user name and password to log on to the system.



NOTICE: If the system is part of an Active Directory domain, then the **Log on to** field appears. Ensure that the **local hostname** is selected and **not** an **Active Directory domain**.

The logon process takes place and the user's desktop appears.

8.10.2

Adding Users to a Local Server

Procedure:

- 1 Right-click the **My Computer** icon, and then select **Manage** from the drop-down menu.
- 2 In the **Computer Management** window, double-click **Local Users and Group**.



NOTICE: If **Local Users and Groups** is not visible, then Active Directory is installed in the system. Close the **Computer Management** window and proceed to [Adding User Accounts to a Domain on page 122](#).

The folder expands to list the user and group sub-folders.

- 3 Right-click the **Users** folder. From the drop-down menu, select **New User**.
- 4 In the **New User** dialog box, enter the following information:

- *<User name>*
- *<Full Name>*
- *<Description>*
- *<Password>*
- *<Confirm Password>*



NOTICE: **Full Name** and **Description** fields are optional.

- 5 Enter the password for the new user account, and reenter the password to confirm. The following options are provided:

- **User must change password at next logon**
- **User cannot change password**
- **Password never expires**

Select the appropriate check boxes, depending on the nature of the user account and click **Create**.

The account is created. The New User dialog box remains on the screen so that you can create additional accounts.

- 6 Click **Close** after creating the required user accounts.
- 7 Close the **Computer Management** window.

The administrator's desktop reappears.

8.10.3

Adding Groups to a Local Server

Procedure:

- 1 Right-click **My Computer**. From the drop-down menu, select **Manage**.
- 2 In the **Computer Management** window, double-click **Local Users and Groups**.
The folder expands to list the user and group sub-folders.
- 3 Right-click the **Groups** folder. From the drop-down menu, select **New Group**.
- 4 In the **New Group** dialog box, enter the following information and then click **Create**.
 - a **Group Name**
 - b Optional: **Description**

The group is created. The **New Group** dialog box remains on the screen so that you can create additional groups. The **New Object - Group** window closes.

- 5 On the **New Group** dialog box, click **Close**.
- 6 Close the **Computer Management** window.

8.10.4

Adding Groups to a User Account for a Local Server

Follow these steps to add groups to a user account that is local to a Windows-based device.

Procedure:

- 1 Right-click **My Computer**. From the drop-down menu, select **Manage**.
- 2 In the **Computer Management** window, double-click **Local Users and Group**.
The folder expands to list the user and group sub-folders.
- 3 Select the **Users** folder.
- 4 In the right pane, double-click the desired user.
- 5 In the properties window for that user, select the **Member Of** tab.
- 6 In the list of groups to which the account belongs, click **Add**.
- 7 In the **Select Group** dialog box, in the **Enter the object names to select** field, enter the name of the group. Click **Check Names**.

- 8 Perform one of the following actions:

If...	Then...
If the group name is entered correctly,	Click OK .
If the group name is entered incorrectly and the Name Not Found window appears,	perform the following actions: a Click Cancel . b Retype the name of the group. c Click OK .

The **Member Of** list changes to include the group.

- 9 Click **Apply**, and then click **OK**.

Once the user is added to the group, the **Computer Management** window appears.

- 10 Close the **Computer Management** window.

The administrator's desktop reappears.

8.11

Deleting a Computer Object from an Active Directory Domain

Perform this procedure to delete a computer object from the Active Directory if it is reinstalled or permanently removed. Otherwise, delete a computer from the primary Domain Controller in the domain. This disassociates it from the respective OU.

Reinstall the computer before joining it into the domain. Otherwise, the computer does not join the domain properly resulting in authentication problems. Delete the Domain Controller object from the Domain Controller in the Active Directory domain before reinstalling it.

Procedure:

- 1 Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.

The account name set up by Motorola Solutions is "motosec".

The administrator's desktop appears.

- 2 From **Start**, open **Active Directory Users and Computers**:

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

b In the search field, type in `administrative`

c Click **Administrative Tools**.

d In the **Administrative Tools** window, double-click **Active Directory Users and Computers**.

- 3 In the left pane of the **Active Directory Users and Computers** window, select the appropriate Organizational Unit (OU) from the **OU list**.

Double-click to expand the list.

Step example:Zone Controllers

- 4 From the list of Computers in the OU in the right pane, select and right-click the appropriate computer.

- 5 From the drop-down menu, select **Delete**.

- 6 In the confirmation dialog box, click **OK**.
The computer object is deleted.
- 7 Close the **Active Directory Users and Computers** window.

8.12

Adding/Removing a Standalone Backup Core Domain



IMPORTANT: This procedure is for the first system-level domain controller only.

When and where to use:

For a DSR system, follow these steps to add or remove standalone backup core DNS domains on the first system-level domain controller.

For more information on the standalone backup core, see the *Dynamic System Resilience Feature Guide*.

Procedure:

- 1 Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.
The account name set up by Motorola Solutions is “motosec”.
The administrator’s desktop appears.
- 2 Open PowerShell:
 - a From **Start**, click **Search**.
 - b In the search field, type in `powershell`
 - c Click **Windows PowerShell**.
- 3 At the PowerShell prompt, change the directory to `C:\Program Files\Motorola\AstroDC\dns\scripts`
- 4 Perform one of the following actions:
 - If you want to add a standalone backup core, enter: `.\AddPhantomDomain.ps1 -domain <zoneZ>`
where `<zoneZ>` is the standalone backup core domain to be added. For example, zone4.
 - If you want to remove a standalone backup core, enter: `.\RemovePhantomDomain.ps1 -domain <zoneZ>`
where `<zoneZ>` is the standalone backup core domain to be removed. For example, zone4.

If any of the scripts fail, rerun the script after a couple of minutes. The script could fail if the partition is locked for replication.

8.13

Modifying Active Directory Tombstone Lifetime

Perform this procedure on the system-level Domain Controller (DC) to determine how long a deleted object is retained in Active Directory. Once the value is modified on the system-level DC, it gets automatically replicated to the other DCs.

Procedure:

- 1 Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group (the account name set up by Motorola Solutions is “motosec”).
The domain administrator’s desktop appears.

- 2 Open PowerShell:

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

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

- c Click **Windows PowerShell**.

- 3 At the **PowerShell** prompt, change directory to: `C:\Program Files\Motorola\AstroDC\AD\scripts`

- 4 On the system-level DC, enter: `.\setTombstoneLifetime<int>`

where `<int>` is a number of tombstone lifetime days set on the AD



NOTICE: Once the DC has been deployed, the default tombstone lifetime value is set back to 180 days.

Chapter 9

Active Directory Client Operation

This chapter provides information about tasks that you can perform on Active Directory client devices after Active Directory and Domain Name Services (DNS) are operational on your system.

9.1

Adding Windows-Based Devices to an Active Directory Domain

Do **not** perform this process for Windows-based servers that function as Active Directory domain controllers.



NOTICE: The order of the tasks is significant and should be maintained as recommended in this process. All the tasks must be performed when the user is logged on using the administrator account.

Prerequisites: For a list of Windows-based devices, see [Active Directory Client Devices and Applications on page 36](#).

Process:

- 1 Install the devices within the system.

See procedures in the “Installation” chapter of the manuals for each device.

For devices already operating in the system, exit from applications as needed.

Step example: On the NM Client, exit from the Private Radio Network Management (PRNM) Suite applications, if any of these applications are open.

- 2 If required by your organization, create additional user and group accounts.

See [Adding User Accounts to a Domain on page 122](#).

Additionally, the local account structure may require modification (such as changing the local administrator password).

- 3 Log on to the Windows-based device using any local Windows account with administrative rights.

- 4 Enable necessary services.

The following services must be enabled and set to automatic:

- **DHCP Client**
- **DNS Client**
- **TCP/IP NetBIOS Helper**

- 5 Configure TCP/IP settings.

- 6 Configure time synchronization between the Windows-based device and the domain controller.



IMPORTANT: Maximum synchronization time is 5 minutes.

- 7 Validate host name and DNS domain name for the Windows-based device.

Do **not** proceed if unable to validate the NM client’s host name and DNS domain name.

Step example: For the NM client, see: [Configuring and Validating DNS on Windows-Based Devices on page 136](#).

- 8 Perform the [Joining and Rejoining a Windows-Based Device to an Active Directory Domain on page 140](#) procedure.
- 9 Perform the following in Active Directory for the Windows Service User account in Active Directory:
 - a [Enabling User Accounts in Active Directory on page 125](#)
 - b [Resetting User Passwords in Active Directory on page 126](#)

Both procedures must be performed after the device joins the Active Directory domain, before using the account to log on to that device.

9.2

Adding Hostname into DNS on Windows-Based Devices

Windows-based devices that need to be accessed from Active Directory and DNS domains must have DNS records. Among many different types of DNS records, the following are used in this procedure:

A (address)

Maps a hostname to an IP address.

PTR (pointer)

Maps an IP address to a hostname.

The PTR record creates a pointer to the host for reverse lookups. You can create address and pointer records at the same time or separately.

Follow these steps to add address and pointer records for devices that need to be added into DNS.

For a list of Windows-based devices, see [Active Directory Client Devices and Applications on page 36](#).

Procedure:

- 1 From **Start**, open **DNS**:
 - a From **Start**, click **Search**.
 - b In the search field, type in `administrative`
 - c Click **Administrative Tools**.
 - d In the **Administrative Tools** window, double-click **DNS**.
- 2 On the left pane of the DNS console, expand **DNS hostname**, then expand **Forward Lookup Zones** for the server you want to work with.
- 3 Select the DNS domain you want to add entry to.
Step example:For “host1.zone5” select a zone, right-click the zone, and select **New Host**.
- 4 In the **New Host** window, type the `<hostname>` and `<IP address>`.
- 5 Select the **Create Associated Pointer (PTR) Record** check box. Click **OK**.
- 6 Click **Add Host**. Repeat as necessary to add other hosts.
- 7 When finished, click **Done**.

9.3

Configuring and Validating DNS on Windows-Based Devices

The Windows-based devices must be configured with DNS, using the procedures in this section, before they join an Active Directory domain. DNS service is required for proper Kerberos authentication

with Active Directory. The client software must be able to resolve the DNS server host name for the zone in which the Windows-based device resides.



NOTICE: Before performing the following procedures, obtain from your system administrator the host names and IP addresses of the DNS servers, and the name of the domain where the Windows-based device resides.

For a list of Windows-based devices, see [Active Directory Client Devices and Applications on page 36](#).

See [DNS Theory of Operations on page 51](#) for detailed information about DNS servers in an ASTRO® 25 system.

9.3.1

Verifying the DNS Domain Name Configuration on Windows-Based Devices

Prerequisites: Obtain from your system administrator:

- Hostnames and IP addresses of the DNS servers
- Name of the domain where the Windows-based device resides

Procedure:

- 1 Access the command window.

Step example: Press the **Windows icon key+R** to open the **Run** dialog box. Enter: `cmd` in the text field. Click **OK**.

- 2 In the command prompt window, to check the domain name configuration for the DNS server, enter: `nslookup z<ZZZ>dc<NN>`

where:

`<ZZZ>` is the zone number

`<NN>` is the domain controller number

The IP address of the DNS primary server appears.

- 3 To check the domain name configuration:

- a At the DOS or command prompt, enter: `ipconfig`

The IP address appears.

- b At the DOS or command prompt, enter: `hostname`

The host name appears.

- c At the DOS or command prompt, enter, for example: `nslookup <NM Client hostname>.<DNS domain name>` to validate the DNS, where `<DNS domain name>` is the domain where NM Client resides.

Step example: `nslookup z003nmc01.ucs` or `nslookup nmclient1.ucs`

The IP address of the NM client you are configuring appears. The IP address should be the same as the IP address obtained using the `ipconfig` command.

9.3.2

Configuring DNS Suffix and DNS Server Addresses List on Windows-Based Devices



Prerequisites:

Obtain from your system administrator:

- Hostnames and IP addresses of the DNS servers
- Name of the domain where the Windows-based device resides

For a list of Windows-based devices authenticated in an ASTRO® 25 system, see the [Active Directory Client Devices and Applications on page 36](#) section.

Procedure:

- 1 Right-click **Local Area Connection**.
If the **User Account Control** dialog box appears, click **Continue** or type in the administrator password for the account displayed, depending on the prompt command and then click **Yes**.
- 2 On the pop-up menu, select **Properties**.
- 3 In the **Local Area Connection Properties** dialog box, select **Internet Protocol (TCP/IP)**. Click **Properties**.
The IP address varies depending on the NM client.
- 4 In the **Internet Protocol (TCP/IP) Properties** window, click **Advanced**.
- 5 In the **Advanced TCP/IP Setting** window, select the **DNS** tab.
- 6 In the **Advanced TCP/IP Settings** dialog box, under **DNS server addresses, in order of use**, remove the existing DNS server addresses.
The DNS server addresses disappear.
- 7 Under **DNS server addresses, in order of use**, click **Add**.
- 8 In the **TCP/IP DNS Server** dialog box, enter the server IP address. Click **Add**.
DNS server IP addresses for a DNS client device depend on where the client device resides.
For DNS server IP addresses, consult your system administrator.
The DNS server is added to the list.
 **NOTICE:** Repeat this step for each DNS server.
- 9 Use the arrow buttons to move the DNS servers to the correct order in the list.
- 10 Select the **Append these DNS suffixes (in order)** radio button.
- 11 From the **Append these DNS suffixes (in order)** field, remove all the previous DNS suffixes.
- 12 In the **Append these DNS suffixes (in order)** field, add all the DNS suffixes.
 **NOTICE:** Add DNS suffixes in the order specified in [DNS Suffixes on page 138](#). DNS suffix varies depending on where the client device resides.
- 13 Click **OK**.
Settings are applied and the **Advanced TCP/IP Setting** window closes.

9.3.2.1

DNS Suffixes

Use the following table to enter the appropriate DNS suffixes in the appropriate order, where:

- <Z> is the zone number
- <X> is the site number
- <Y> is the subsite number

or, for Conventional Subsystems:

<x> is the conventional subsystem number

<y> is the conventional location number



NOTICE: <y>, <x>, and <z> should be the device under configuration's subsite, site, and zone numbers. It ensures that the most local resource is used.

Table 14: DNS Suffixes

Site/Subsystem	Recommended Search Order
IP Simulcast Site	<ol style="list-style-type: none"> 1 site<x>.zone<z> 2 zone<z>
IP Simulcast Subsite	<ol style="list-style-type: none"> 1 ipss<y>.site<x>.zone<z> 2 site<x>.zone<z> 3 zone<z>
Other RF Sites	<ol style="list-style-type: none"> 1 site<x>.zone<z> 2 zone<z>
Other RF Subsites	<ol style="list-style-type: none"> 1 ss<y>.site<x>.zone<z> 2 site<x>.zone<z> 3 zone<z>
Network Management/Dispatch (NMD) Site	<ol style="list-style-type: none"> 1 nmd<x>.zone<z> 2 zone<z>
UCS	<ol style="list-style-type: none"> 1 ucs 2 zone<z> (colocated zone)
Zone core	zone<z>
Conventional Subsystem	<ol style="list-style-type: none"> 1 convloc<y>.csite<x>.ucs 2 zone<z> (colocated zone) 3 ucs
PTP devices	zone<z> (colocated zone)

9.3.3

Updating Zone Core LMP DNS Entries Manually

If the host name entry for the SmartConnect LMP or CriticalConnect LMP is not present or is present but contains wrong values in the Domain Name Server (DNS), you must add or update it manually before the device is joined to the domain.

Procedure:

- 1 Log on to the Domain Controller as an administrator.
- 2 From **Start**, launch **Administrative Tools**.

- 3 Open **DNS**.
- 4 On the navigation tree, expand the **Forward Lookup Zones** node.
- 5 Select the folder for the zone that you want to edit.
- 6 Click **Action, New Host (A or AAAA)**.
- 7 In the **New Host** window, type in the hostname and IP address of the CriticalConnect LMP on the tel0 subnet.
- 8 Select the **Create Associated Pointer** check box. Click **Add Host**.
- 9 If a message appears informing you that a new record was created, click **OK**.
- 10 If required, repeat [step 4](#) through [step 9](#) for other CriticalConnect LMP hosts.
- 11 Click **Done**.

9.4

Joining and Rejoining a Windows-Based Device to an Active Directory Domain

Join domain

The join domain operation automatically unjoins the device from any domain it may have been previously joined to.

Windows-based device

A Windows-based device is a platform running on a Windows OS for remote deployment and configuration of a virtual machine.

JoinADomain application

The application for joining a Windows client to the domain which automatically configures NTP, DNS, and OU for that client.



IMPORTANT: While rejoining a Windows-based device to an Active Directory Domain, do **not** use this application to move the Windows-based device from an Organization Unit (OU) to another OU.

Prerequisites:

Obtain from your system administrator the Organizational Unit for this Windows-based device, as well as the user name and password for the account that is used to join this Windows-based device to the Active Directory domain.

For a list of Windows-based devices, see [Active Directory Client Devices and Applications on page 36](#).

If the Windows-based device is a virtual machine, before performing this procedure, make sure that the virtual machine is connected to the DVD drive where you will insert the software media. For information about connecting DVD drives to virtual machines in ASTRO® 25 systems, see the *Virtual Management Server Software* manual.

Procedure:

- 1 If a Windows logon dialog box appears, enter the credentials for a Windows user account that is maintained locally on this Windows-based device.

If you are logging on with a local account, and you need to perform operations requiring Windows administrator privileges, log on with a local Windows administrator account.

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.

The administrator's desktop appears.

- 2 Insert the *Windows Supplemental* media in the drive.
- 3 Navigate to the `Motorola JoinADomain\OtherWindowsOS` folder on the *Windows Supplemental* media.
- 4 In the `Motorola JoinADomain\OtherWindowsOS` folder, double-click **JoinADomain.exe**.
- 5 Depending on the message displayed, perform the following actions:
 - a If a warning message appears stating that the application could not locate the AD domain, type in the **<AD Domain Name>** manually in the **AD Domain** field.
See [Table 8: User Input Requirements – Domain Controller Configuration on page 75](#).
 - b If a command prompt opens along with the **Join Active Directory Domain** window, do not close the command prompt. It will close after the **Join Active Directory Domain** window is closed.
 - c If a **User Account Control** window appears, click **Allow**, **Yes**, or **Continue**, depending on the prompt, then fill in the required fields for the account displayed and click **Yes**.
- 6 When prompted, log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.

The default domain administrator account is “motosec”.



NOTICE: If the **Organizational Unit** field does not update automatically, tab out of the password or **AD Domain Name** field or click the **Username** field.

The **Organizational Unit** field is updated with the information entered.

- 7 Select the correct Organizational Unit (OU) for the Windows-based device from the drop-down list.

The OU list reflects the information of the host type which could be either Client or Server. The corresponding prefixes identifying an OU name on the drop-down list are respectively **WinClient** or **WinServer** followed by the associated entity identifier and mentioned host types.

Step example:

- The OU for Network Management Clients is **WinClient Network Management Clients**
- The OU for Core Security Management Server (CSMS) is **WinServ Security Management Servers**

- 8 **For cohabited applications:** select the OU of the primary device on which the cohabited application is placed.

Step example: When joining a Authentication Center (AuC) Client cohabited with Network Management Clients to the domain, from the drop-down list, select **WinClient Network Management Clients**.

- 9 Click **Join**.

If a message window appears stating that Windows Firewall has blocked some features of the program, click **Allow Access**.

A message states that the Windows-based device has been successfully joined to AD in the INFO text area.



NOTICE: If an error message appears, repeat the procedure. If the error persists, contact the Motorola Solutions Support Center (SSC).

- 10 In the reboot window, click **Yes**.

Postrequisites:

If the device has problems joining the domain:

- Ensure the time is synchronized between the client and the AD/DNS.
- Verify the DNS server in the TCP/IP properties of the Network Interface Card (NIC) is set to the correct DNS Server IP.
- Verify the Network Connectivity is up and domain controllers are reachable.



NOTICE: After a device joins the domain, its applications that have Role Based Access Control in Active Directory may not be usable by the local Windows administrator or the domain administrator if that user account is not a member of the group associated with the application for that device.

In some cases, the administrator can access the application by entering its executable path and filename at the elevated Windows command line. The path and filename can be seen in the properties for the application shortcut on the desktop or the **Start** menu. For information how to run the elevated Windows command line, see [Starting the Windows Command Line as Administrator on page 142](#).



NOTICE: For Voice Card and Crypto Card-based consoles, after joining the device to the domain and rebooting the console, run `GPUpdate` or force it from a Windows command prompt.

9.5

Starting the Windows Command Line as Administrator

Perform this procedure to run the elevated Windows command line. Perform this procedure before you run an application that has Role Based Access Control in Active Directory as a local Windows administrator, or an Active Directory Domain Administrator account that is not a member of the group associated with the application.

Procedure:

- 1 If necessary, log on to the Windows-based device using your local administrator account or an Active Directory account.
- 2 Right-click **Start** and select **Command Prompt (Admin)**.
- 3 If the **User Account Control** window appears, click **Continue** or **Yes**, depending on the prompt you see.

The command prompt window appears.

9.6

Adding Unix-Based Devices to an Active Directory Domain

Prerequisites:

All devices should be installed in the system. To install the devices, see the “Installation” chapter of the manuals for each device.

For a list of Unix devices, see [Active Directory Client Devices and Applications on page 36](#).

Process:

- 1 Verify that the time between the domain controllers and the device you will join to the domain is synchronized.

The time must be synchronous within 2 minutes.

- 2 Join the device to an Active Directory domain using a domain administrator account.

See the list of specific devices in [Implementation of Centralized Authentication on Devices on page 143](#).



NOTICE: Ensure to re-enable the device after joining the domain, if required.

- 3 Verify that the join operation added a computer object for the device to the Active Directory database, in the appropriate Organizational Unit (OU).

9.7

Implementation of Centralized Authentication on Devices

Sections listed in the following table provide the procedures required to join Unix-based devices to an Active Directory domain, in order to implement centralized authentication for those devices.

Perform the correct procedure depending on the type of OS the device has.

Table 15: Procedures for Implementing Centralized Authentication on Devices

Device	Instructions for Implementing Centralized Authentication
Generic Application Server and all the individual server applications it hosts listed in Active Directory Client Devices and Applications on page 36	Joining Multiple Solaris-Based Servers to an Active Directory Domain on page 143
Linux-based Active Directory clients listed in Active Directory Client Devices and Applications on page 36	Joining a Linux-Based Device to the Domain on page 144

9.8

Joining Multiple Solaris-Based Servers to an Active Directory Domain

Prerequisites:

Ensure that the following conditions are met before performing this procedure:

- The Network Time Protocol (NTP) server, DNS server, and domain controllers must be operating.
- Validate the time between the Generic Application Server (GAS) and the domain controller. The time must be synchronous within 2 minutes before you proceed with the joining operation.
- Contact your System Administrator for the domain administrator account name and password that you need for the procedure.



NOTICE: For information about setting up Active Directory users so that they can perform specific administration menu procedures, contact your Active Directory administrator.



NOTICE: All Unix devices in the UCS subnet should be joined into the domain only after the colocated zone domain controller is installed. If the Unix devices in the UCS subnet are joined to the domain before the colocated zone domain controller is set up, they will not have domain controller redundancy.

When and where to use:

Follow these steps to enable centralized authentication for a GAS and for the Solaris-based server applications that it hosts. For a list of supported devices, see [Active Directory Client Devices and Applications on page 36](#).



NOTICE: If an ISSI.1 Network Gateway server application is added to a GAS after initial implementation, use the following procedure to join it to the domain, because the individual ISSI.1 Network Gateway administration menus do not provide a way to join an individual ISSI.1 Network Gateway server application to the domain. This is also true for the Public Safety LTE Push To Talk (PS PTT) Gateway server application.

Procedure:

- 1 Establish a terminal session with the GAS.
For instructions on using PuTTY, see the *Securing Protocols with SSH* manual.
- 2 Log on to the GAS with the root account.
- 3 At the root prompt, enter: `admin_menu`
The server application's administration menu and the menu prompt appears. There is a slight delay for the server to display the menu.
- 4 From the menu, enter the number for **Services Administration**.
- 5 From the **Services Administration** menu, enter the number for **Manage AAA Client Configuration**.
- 6 From the **Manage AAA Client Configuration** menu, enter the number for **Join All to the Domain**.
A list of all installed applications, including the GAS with the current domain status, is displayed, followed by a list of available domains.
- 7 Enter the number of the domain to be joined, and provide the domain administrator account and password.
A confirmation message appears.
- 8 Type: `y`
A success message appears, followed by the Manage AAA Client Configuration menu.
- 9 Type `q` to quit the server administration menus, then type `exit` to log off the server.

9.9

Joining a Linux-Based Device to the Domain

Prerequisites:

Validate the time between the Linux-based server and the Active Directory server. The time must be synchronous within 2 minutes.

If you are joining the Linux-based server to an Active Directory domain for the first time, close all open telnet and ftp sessions before attempting this procedure.

For information about setting up Active Directory users so that they can perform specific administration menu procedures, contact your Active Directory administrator.

For a list of Linux devices, see [Active Directory Client Devices and Applications on page 36](#).



NOTICE: All Unix devices in the UCS subnet should be joined into the domain only after the colocated zone domain controller is installed. If the Unix devices in the UCS subnet are joined to the domain before the colocated zone domain controller is set up, they will not have domain controller redundancy.

Procedure:

- 1 Log on to the Linux-based device using the root account.
- 2 At the root command prompt, enter: `admin_menu`
The administrative operations Main Menu appears for the Linux-based device.
- 3 Enter the number for the **Services Administration** option.
The Services Administration menu appears.
- 4 Enter the number for the **Manage AAA Client Configuration** option.
The Manage AAA Client Configuration menu appears.
- 5 Enter the number for the **Join Domain** option.
In most cases, there is only one domain.
A list of domains displays.
- 6 Enter the number for the appropriate domain name in the list.
You are prompted to enter the username and password for the domain administrator.
- 7 Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.
The account name set up by Motorola Solutions is “motosec”.
Numerous messages appear, concluding with a success confirmation message. The Manage AAA Client Configuration menu displays.
- 8 Enter the number for the **Display Domain Membership Status** option.
The Domain name displays, followed by the domain Membership Status for this Linux-based device.

9.10

Obtaining the IP Address Inventory from the Domain Controller

This procedure is performed only on the DC which is the DNS server.

Procedure:

- 1 From the menu, select **Start→Administrative Tools→DNS** to open the DNS Manager Snap-in.
- 2 Navigate to the appropriate domain. In most cases, this is the reverse domain of the site.
For more information, see the system IP plan.
- 3 With the appropriate domain selected, select **Action→Export List**.
- 4 Navigate to the appropriate directory to save the file, enter the appropriate filename, and select **(* .txt)** as the output format.

Chapter 10

RADIUS Service Operation

This chapter provides information about tasks that you can perform after Active Directory, Domain Name Services (DNS) and RADIUS services are operational on your system.

10.1

Adding RADIUS Clients Manually to a RADIUS Server

Follow these steps to manually add RADIUS clients to the Network Policy Server (NPS) on a zone-level domain controller.



IMPORTANT:

Changes made on one RADIUS server must be synchronized with the other RADIUS server(s) in the same zone.

Procedure:

- 1 Log on to the zone-level domain controller using your Active Directory account that is a member of the Domain Admins group.

The account name set up by Motorola Solutions is “motosec”.

The domain administrator’s desktop appears.

- 2 Open **Network Policy Server**:

- a From **Start**, click **Search**.
- b In the search field, type in `administrative`
- c Click **Administrative Tools**.
- d In the **Administrative Tools** window, double-click **Network Policy Server**.

- 3 In the left pane of the **Network Policy Server** window:

- a Double-click **RADIUS Clients and Servers**.
- b Right-click **RADIUS Clients** and select **New**.

- 4 In the **New RADIUS Client** window, **Settings** tab, enter the following information:

- a **<Name>**

where **<Name>** is the friendly name of the RADIUS client that must not contain spaces.

If a space is added it will cause issues with RADIUS replication and RADIUS batch import script.

- b **<IP Address>**

- c **<Shared Secret>**

where **<Shared Secret>** should be the same as the shared secret entered on the RADIUS client device and must consist of printable ASCII characters.

The RADIUS service supports up to 63 characters in a RADIUS shared secret key. In ASTRO® 25 systems, HP switches, Motorola Network Routers, and GGM 8000 gateways support up to 32 characters in a RADIUS shared secret key. The RF site and VPM-based devices support up to 63 characters. The character “?” is not supported by HP switches.

- d Repeat **<Shared Secret>**

- e Click **OK**.
- 5 After adding clients from the RADIUS server on the zone-level domain controller, trigger the replication to the system-level DCs by performing the following actions:
 - a Open PowerShell:
 - 1 From **Start**, click **Search**.
 - 2 In the search field, type in `powershell`
 - 3 Click **Windows PowerShell**.
 - b At the PowerShell prompt, change directory to `C:\Program Files\Motorola\AstroDC\RADIUS\scripts`
 - c Enter: `.\TriggerRADIUSReplication.ps1`

Once replication is triggered, it takes up to 30 minutes for the data to get replicated to the backup RADIUS servers.

Postrequisites:

Once you add a RADIUS client, for the centralized authentication to work, the following conditions must be met:

- User should be a member of the appropriate RADIUS group.
- Reverse encryption should be set on the user. See [Enabling Reverse Password Encryption on page 148](#).
- Shared Secret should match the secret on the RADIUS client.

10.2

Deleting a RADIUS Client from a RADIUS Server

Follow these steps to delete RADIUS clients from the Network Policy Server (NPS) on a zone-level domain controller.

Procedure:

- 1 Log on to the zone-level domain controller using your Active Directory account that is a member of the Domain Admins group.
The account name set up by Motorola Solutions is “motosec”.
The domain administrator's desktop appears.
- 2 Open **Network Policy Server**:
 - a From **Start**, click **Search**.
 - b In the search field, type in `administrative`
 - c Click **Administrative Tools**.
 - d In the **Administrative Tools** window, double-click **Network Policy Server**.
- 3 In the **Network Policy Server** window, expand **RADIUS Clients and Servers**.
- 4 Right-click the RADIUS client you want to delete.
- 5 From the context menu, select **Delete**.
- 6 At the confirmation prompt, click **Yes**.
The RADIUS client is deleted from NPS on this domain controller.
- 7 After adding clients from the RADIUS server on the zone-level domain controller, trigger the replication to the system-level DCs by performing the following:

- a Open PowerShell:
 - 1 From **Start**, click **Search**.
 - 2 In the search field, type in `powershell`
 - 3 Click **Windows PowerShell**.
- b At the PowerShell prompt, change directory to `C:\Program Files\Motorola\AstroDC\RADIUS\scripts`
- c Enter: `.\TriggerRADIUSReplication.ps1`

Once the replication is triggered, it takes up to 30 minutes for the data to get replicated to the backup RADIUS servers.

10.3

Setting Up User Accounts for RADIUS Authentication/802.1x

When and where to use:

An account set up in this procedure can be used for access through an 802.1x-enabled Ethernet port on an HP switch, GCP 8000 Site Controller, or GPB 8000 Reference Distribution Module, or for access through Secure Shell (SSH), telnet or the local serial port of any device that is enabled for centralized authentication in an ASTRO® 25 system.

For information about synchronizing RADIUS user names and passwords with global Account credentials in the VoyenceControl component of the Unified Network Configurator, see [RADIUS vs. Local Authentication for Sessions Between a Device and UNC on page 45](#).

For a detailed list of Active Directory groups, see [Roles in ASTRO 25 Active Directory on page 33](#).

Process:

- 1 Add the RADIUS users to Active Directory.
See [Adding User Accounts to a Domain on page 122](#).
- 2 Add the RADIUS users to one of the following groups:
 - `netwadm` (Network Administrators) group for administrative access
 - `configaud` (Configuration Auditor) group for read-only accessSee [Assigning Group Membership to a User Account on page 124](#).
- 3 For each RADIUS user account, perform [Enabling Reverse Password Encryption on page 148](#).

10.3.1

Enabling Reverse Password Encryption

Follow these steps to enable reverse password encryption on a user account.

Prerequisites: Reverse password encryption must be enabled on the user account before that user can be authenticated by RADIUS.

Procedure:

- 1 Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.
The account name set up by Motorola Solutions is “motosec”
The domain administrator’s desktop appears.
- 2 Open Active Directory Users and Computers:
 - a From **Start**, click **Search**.

- b** In the search field, type in **administrative**
- c** Click **Administrative Tools**.
- d** In the **Administrative Tools** window, double-click **Active Directory Users and Computers**.
In the left pane of the **Active Directory Users and Computers** window, select **Users**.
From the list of users and groups in the right pane, right-click the user for which you want to enable reverse password encryption.
From the context menu, select **Properties**.
In the **Properties** window, select the **Accounts** tab.
Select the **Store password using reversible encryption** check box. Click **OK**.
Reverse Password Encryption is enabled for the user.

Reset the user password in Active Directory.
See [Resetting User Passwords in Active Directory on page 126](#).

Adding a Remote Access Policy Manually

Procedure:

- Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.

The account name set up by Motorola Solutions is “motosec”.

The domain administrator's desktop appears.

- Open **Network Policy Server**:
 - a From **Start**, click **Search**.
 - b In the search field, type in `administrative`
 - c Click **Administrative Tools**.
 - d In the **Administrative Tools** window, double-click **Network Policy Server**.
- In the left pane of the **Network Policy Server** window:
 - a Double-click **Policies**.
 - b Right-click **Network Policies**.
 - c From the context menu, select **New**.

A **New Network Policy** wizard appears which can be used to create new policies.



NOTICE: Your organization is responsible for entering the values for the new policies.

10.5

Enabling 802.1x on the Technician Laptop

For detailed information on how to enable 802.1x on the technician's laptop, see the *802.1x Service Ports on Switches* manual.

10.6

Authenticating a User at an 802.1x Port on a Device

See [RADIUS Technical Overview on page 43](#) section for a summary. For details, see the *802.1x Service Ports on Switches* manual.

Chapter 11

AD/DNS/RADIUS Maintenance

This chapter is for periodic maintenance procedures relating to Active Directory, RADIUS, and Domain Name Services (DNS).

11.1

Performing AD/DNS/RADIUS Maintenance

Periodic maintenance should be performed on the Domain Controllers, including recommended maintenance in the following steps. Maintenance can be scheduled in accordance with the site's existing maintenance program.

See the “Troubleshooting” and “Reference” chapters if you are already aware of a problem that may involve the Domain Controllers.

Process:

- Patch the operating system.
See the `readme.txt` file on the *MOTOPATCH for Windows* media.
- Upgrade the VMware Tools on the virtual server.
See the *Virtual Management Server Software* manual.
- Verify that the Domain Controller is being backed up.
See [Domain Controller Disaster Recovery on page 189](#).
- Verify that the time on the Domain Controllers and its clients are synchronized, or if the time on the Domain Controller is no longer accurate.
See the following:
 - [Network Time Protocol \(NTP\) as the ASTRO 25 Time Source on page 32](#)
 - [Setting the Time Source on page 168](#)The time source is configured when the Domain Controller is initially set up.
- Periodically check the log files to see if there are any persistent errors:
 - For event logs on the Domain Controller, use Microsoft documentation to troubleshoot based on the Event ID.
 - For Centralized Event Logging, if that feature is implemented, see [Viewing Centralized Authentication Event Logs on page 184](#).
- Verify replication between domain controllers.
See [The Repadmin Tool Usage on page 167](#).
- Verify that the domain controllers are working properly. Enter: `dcdiag`
This includes interactions between domain controllers, interactions between AD and DNS, and with what is in AD itself.

Chapter 12

AD/DNS Troubleshooting

This chapter provides fault management and troubleshooting information relating to Active Directory and Domain Name Services (DNS).

This chapter provides fault management and troubleshooting information specific to ASTRO® 25 systems with centralized authentication for Solaris-based servers and Linux-based servers.



NOTICE: In order to perform Domain Controller troubleshooting, Active Directory administrator's knowledge is required.

12.1

General Troubleshooting for AD/DNS


Before troubleshooting Active Directory and DNS issues, perform validation checks to ensure that all configuration data is appropriately established for the following:



- Network settings
- IP address
- Subnet mask
- Default gateway
- DNS server addresses
- DNS search list
- Hostname(s)
- Computer name(s)
- DNS suffix information

Table 16: Troubleshooting Scenarios for Active Directory and DNS

Problem type	Actions to take
Motorola Solutions-provided users or groups have been corrupted or deleted in Active Directory.	<ul style="list-style-type: none">• Batch Importing ASTRO 25 System Users and Groups into Active Directory on page 156
Motorola Solutions-provided Organizational Units (OUs) (or their settings and links) have been corrupted or deleted in Active Directory.	<ul style="list-style-type: none">• Creating ASTRO 25 System Organizational Units on page 156• Reimporting ASTRO 25 System Group Policy Objects (GPOs) on page 159• Manually Linking a GPO to an OU on page 161
Motorola Solutions-provided Group Policy Objects (GPOs) (or their settings and links) have been corrupted or deleted in Active Directory.	<ul style="list-style-type: none">• Troubleshooting Group Policy Objects (GPOs) on page 157

Problem type	Actions to take
Failure in executing <code>customizedns.pl</code> scripts on system and zone-level domain controllers.	<ul style="list-style-type: none"> • Ensure that the TCP/IP properties on the DC are set correctly. • Examine log entries in Event Viewer DNS log for more information.
Failure in adding network computers to an Active Directory Domain (messages such as the following appear: <code>hostname lookup failure</code> or <code>access denied</code>)	<ul style="list-style-type: none"> • Ensure that the primary DNS server is available. Devices such as Windows-based computers are unable to join the domain if the primary DNS server is not available. • Ensure that all computers are on the network. • Check for any erroneous network settings on the devices involved. • Ensure that the computer is set to the same time as all other devices.
Failure in adding network computers to an Active Directory Domain. Messages such as: <code>duplicate hostnames already appear in Active Directory</code> appear.	<ul style="list-style-type: none"> • Check to ensure that there are unique hostnames within the same zone. Refer to Failure Due to Hostname and DNS Domain Name Misconfiguration on page 167. • For further assistance, contact the Motorola Solutions Support Center (SSC).
Unable to log on to a device using an Active Directory user account	<ul style="list-style-type: none"> • Ensure that the user is enabled on Active Directory. Refer to the Active Directory Server Operation on page 122 chapter for information about adding and enabling users. • Ensure that the user is allowed to access the device. • Ensure that the computer is part of the domain. • Ensure that the computer is on the network. • Ensure that the DC is on the network. • Ensure that there are no issues related to network connectivity between the computer and the domain controllers. For a zone-level environment, there should be network connectivity to both zone-level and system-level DCs. For a system-level environment, there should be network connectivity to the system-level DC. • Check the network settings. • Ensure that the computer is set to the same time as all other devices. Time should be synchronized between the Active Directory domain and clients for authentication to work properly. • If the Active Directory forest has been rebuilt after the client joined the domain, then rejoin the client to the domain. Refer to the troubleshooting section Joining and Rejoining a Windows-Based Device to an Active Directory Domain on page 140 for information on rejoining the client to the domain. • Check for DNS replication issues by looking at the event log in the DCs. DNS replication issues are related to network connectivity or zone core firewall configuration.

Problem type	Actions to take
	<ul style="list-style-type: none"> Delete the computer object from the appropriate zone-level domain controller. See: Deleting a Computer Object from an Active Directory Domain on page 132. Refer to Joining and Rejoining a Windows-Based Device to an Active Directory Domain on page 140 for information on unjoining and rejoining a Windows-based device to the domain. Verify that the join operation created the computer object for the device in the appropriate Organizational Unit (OU).
Failure to install the domain controllers	<ul style="list-style-type: none"> Verify network connectivity a couple of times. If the problem persists, contact the SSC. When installing additional domain controllers, check if the system is up (if the installation of the previous DC has finished, network connectivity is up).
Dcpromo failure	See Fixing Dcpromo Failure on page 157 .
Devices not placed into correct folders in UNC.	Verify that the Device DNS Domain Name was not misconfigured. See Fixing the DNS Misconfiguration in the DNS Server or UNC on page 176 .
Multiple devices with the same hostname discovered by UNC or UEM.	Verify that the device hostname was not reused. See DNS Misconfiguration on page 174 and the DNS-related procedures in RADIUS Client Configuration on page 83 .
Multiple devices with the same IP address.	<p>Verify that the device IP address was not reused. See DNS Misconfiguration on page 174. Additionally, depending on the device, see the appropriate manual from the following:</p> <ul style="list-style-type: none"> <i>GTR 8000 Base Radio</i> <i>GTR 8000 Expandable Site Subsystem</i> <i>HPD GTR 8000 Site Subsystem</i> <i>GCP 8000 Site Controller</i> <i>GCM 8000 Comparator</i> <p>and the Fixing the DNS Misconfiguration in the DNS Server or UNC on page 176 section.</p>
A DC is not replicated with other DCs. Replication failures from or to the DC.	Restart the domain controller.
 NOTICE: Only applicable where the ZCP firewall is implemented.	
DC installation appears to be paused for more than an hour.	<p>Inspect the log file at C:\Windows\Debug\DCInstall.log. Search for lines in the DCInstall.log that match a log entry such as: InstallDCPromo.ps1: Exit with 1641 or InstallRoles.ps1: Exit with 1641</p> <p>If either one of those lines is the last entry in the DCInstall.log file, it means that the DC Install scripts initiated a reboot of the</p>

Problem type	Actions to take
	DC but the DC is unable to reboot due to an unspecified transient condition. Restart the DC installation.
<p>Packets from the Network and Security Manager Client move from DC to DC (source and destination ports are both dynamic ports over 50152). One of the dynamic ports is at the low end around 50156.</p> <p> NOTICE: Only applicable where the ZCP firewall is implemented.</p>	Restart the domain controller.
<p>After running the <code>netstat -o</code> command, the result is not showing port 49280 being used in the "Local Address" column. Instead, it shows the same port that is the being seen in the NSM client.</p> <p> NOTICE: Only applicable where the ZCP firewall is implemented.</p>	Restart the domain controller.
Failure of the <Admin Restore password>	<p>If the <Admin Restore password> entered does not meet the default complexity rules, the installation will fail at <code>InstallADDCpromo.ps1</code> or <code>reinstallADDCpromo.ps1</code> with error code 43 in the log file <code>C:\windows\debug\dcinstall.log</code>.</p> <p>In such case, run the <code>C:\Program Files\Motorola\AstroDC\common\scripts\SetRestorePassword.ps1</code> script to reenter the passwords, and then click Retry on the WIF execution log window.</p>
Failure of the <AD domain admin password>	<p>If the <AD domain admin password> is entered wrong, the installation fails at <code>VerifyADDNDomainName.ps1</code>. In such case, run the <code>C:\Program Files\Motorola\AstroDC\common\scripts\SetDomainPassword.ps1</code> script to reenter the passwords, and then click Retry on the WIF execution log window.</p>

12.2

Batch Importing ASTRO 25 System Users and Groups into Active Directory

Perform this procedure to re-import Motorola Solutions-provided users and groups into Active Directory, if needed.



NOTICE: Importing users and groups must be executed only on the server with the DC hostname ucs-dc01.

For security reasons, all users are created in a disabled state. The appropriate accounts must be enabled and their passwords set before they can be used to log on to any system.

Prerequisites: This procedure assumes that, during Domain Controller installation, files for importing Motorola Solutions-provided users and groups were copied from the *Domain Controller Plugin Media* to the following location on the hard drive: `c:\program files\Motorola\Astro\AD\data`.



NOTICE: Space is not allowed in the friendly name when adding RADIUS client. If space is added it causes issues with RADIUS replication and RADIUS batch import scripts.

Procedure:

- 1 Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.
The account name set up by Motorola Solutions is “motosec”.
The domain administrator’s desktop appears.
- 2 Open PowerShell:
 - a From **Start**, click **Search**.
 - b In the search field, type in `powershell`
 - c Click **Windows PowerShell**.
- 3 At the PowerShell prompt, change directory to `C:\Program Files\Motorola\AstroDC\AD\scripts`.
- 4 Enter: `.\CreateGroups.ps1`
The Active Directory groups are created.
- 5 Enter: `.\CreateUsers.ps1`
The Active Directory users are created.

12.3

Creating ASTRO 25 System Organizational Units

Organizational Units (OUs) provided by Motorola Solutions are automatically created when installing the first system-level DC UCS-DC01. OUs are used to group computers into logical collections for easier administration.

This procedure assumes that the required scripts have been copied to the hard drive of the domain controllers during installation.

When and where to use:

Follow these steps to create all OUs in Active Directory, using a provided script.

Procedure:

- 1 Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.

The account name set up by Motorola Solutions is “motosec”.

The domain administrator’s desktop appears.

- 2 Open PowerShell:
 - a From **Start**, click **Search**.
 - b In the search field, type in `powershell`
 - c Click **Windows PowerShell**.
- 3 At the PowerShell prompt, change directory to: `C:\Program files\Motorola\AstroDC\AD\scripts`
- 4 Enter: `.\CreateOus.ps1`
The organizational units are now created.

12.4

Fixing Dcpromo Failure

Procedure:

- 1 Check the log file at `C:\windows\debug\DCInstall.log`.
- 2 Perform one of the following actions:

If...	Then...
The error in the log file says that the Restore Mode password did not meet the complexity requirements,	<p>perform the following actions:</p> <ol style="list-style-type: none"> a At the PowerShell prompt, enter: <code>C:\Program Files\Motorola\AstroDC\common\scripts\SetRestorePassword.ps1</code> b At the prompt, enter: <Admin Restore password> <p>See Table 8: User Input Requirements – Domain Controller Configuration on page 75.</p> <p>This error means that the password that was supplied at the beginning of the installation was not complex enough.</p>
The error in the log file is <code>dcpromo failed with return code 53</code> ,	<p>Wait for 30 minutes and, on the WIF window, click Retry.</p> <p>If the error persists:</p> <ol style="list-style-type: none"> a Power off the DC. b Delete the VM from the disk. c Redeploy the DC.

12.5

Troubleshooting Group Policy Objects (GPOs)

This section includes procedures for:

- Modifying Group Policy in an ASTRO® 25 system
- Restoring GPOs provided by Motorola Solutions and linking them to the Organizational Units (OUs) provided by Motorola Solutions
- Forcing GPO setting changes (if needed)

These procedures assume that the required scripts have been copied to the hard drive of the domain controllers during installation.

12.5.1

General Considerations for Modifying Group Policy in an ASTRO 25 System

This section describes Motorola Solutions' recommendations for modifying security policies in an ASTRO® 25 system. Before continuing, identify where your organization's settings reside in the Microsoft policies (that is, Computer/Machine Configuration or User Configuration). Once you have determined this, proceed to the appropriate section for guidance.

12.5.1.1

Modifying Your Organization's Computer/Machine Configurations

All Computer/Machine Configuration settings (such as password polices, services, security options, and event logging) can be managed or modified at either the device or domain level, depending on the situation.

- **If a Windows-based device is joined to the domain, then the settings should be managed/modified on the Domain Controller located in the same zone and site as the Windows-based device.** When managing or modifying Computer/Machine Configuration settings at the domain controller, Motorola Solutions recommends that you do not modify any of the Group Policy Objects (GPOs) provided by Motorola Solutions, unless expressly directed to do so by the Motorola Solutions documentation.

Motorola Solutions recommends to make the configuration changes of your organization by:

- 1 Creating a new GPO.
- 2 Linking that new GPO to the highest level in the Organizational Unit (OU) that you wish to affect.



NOTICE: GPOs are applied according to **Link Order**. The highest level is marked with the lowest number and is placed at the top of the list.

This ensures that the modifications are not overwritten when security is reapplied to the system.

- **If the Windows-based device is not joined to the domain, then the settings must be managed/modified at the local level using the Local Group Policy editor (`gpedit.msc`).**

See Microsoft documentation for detailed instructions on how to apply Computer/Machine Configuration settings.

12.5.1.2

Modifying Your Organization's User Configurations

The User Configuration settings of your organization (such as screen saver settings and IE Trusted Sites, and the permissions to alter these settings) must be managed/modified at the device level using the Local Group Policy editor (`gpedit.msc`).



NOTICE:

Domain-level changes to User Configuration settings do not take effect at the device level.

Ensure to document changes to User Configuration policies that are specific to your organization, for future reference. Your organization's settings will need to be re-applied each time after procedures from the ASTRO® 25 system *Windows Supplemental Configuration Setup Guide* are applied to the device.

See Microsoft documentation for detailed instructions on how to apply User Configuration settings.

12.5.1.3

Adding a Site to the Dynamic Trusted Sites Group Policy

Procedure:

- 1 Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.
- 2 From the administrator's desktop, open PowerShell:
 - a From **Start**, click **Search**.
 - b In the search field, type in powershell
 - c Click **Windows PowerShell**.
- 3 At the prompt, enter:
`cd "C:\Program Files\Motorola\AstroDC\common\scripts"`
- 4 At the prompt, enter: `addTrustedSite.ps1 -Hostname <protocol>://<site name>`

where:

`<protocol>` is "*" | "https" | "http"
`<site name>` is
`<ip address>` | `<hostname>` | `<dns domain>` | `<fqdn>`

where:

`<ip address>` is the IP Address of a network entity, for example 10.101.1.121
`<hostname>` is the name of a network entity, for example: z001s001ipcap01 or sz012301
`<dns domain>` is a DNS domain in the network, for example: *.site1.zone1
`<fqdn>` is `<hostname>.<dns domain>`, for example z001s001ipcap01.site1.zone1

12.5.2

Forcing GPO Setting Changes

If changes are made to the settings in any Group Policy Object (GPO), then the new settings take precedence during the next GPO refresh interval. The GPOs are refreshed every 90 - 120 minutes. For some settings, a restart is required for the changes to take effect.

Procedure:

To force all GPO changes in a given Organizational Unit (OU), at the root command prompt of all computers from that OU, enter: `gpupdate /force /boot`

Rebooting helps in downloading the new GPO settings.

12.5.3

Reimporting ASTRO 25 System Group Policy Objects (GPOs)

This procedure is only for recovering the Motorola Solutions-provided GPOs on the first Domain Controller (DC) for a system-level or zone-level Active Directory domain. Do **not** perform this procedure on any additional DCs.

When and where to use:

Follow these steps to re-import all of the Motorola Solutions-provided Group Policy Objects (GPOs) into Active Directory. GPOs are used to apply configuration settings to a collection of computers.



NOTICE: These GPOs are automatically imported and linked to OUs when installing the first system-level DC in the Active Directory domain.

Procedure:

- 1 Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.
The account name set up by Motorola Solutions is “motosec”.
The domain administrator’s desktop appears.
- 2 Open PowerShell:
 - a From **Start**, click **Search**.
 - b In the search field, type in `powershell`
 - c Click **Windows PowerShell**.
- 3 At the PowerShell prompt, change directory to: `C:\Program files\Motorola\AstroDC\AD\scripts`
- 4 At the command prompt, enter: `.\ReimportGPO.ps1`
The group policy objects are created.

12.5.4

Manually Reimporting Specific Domain Group Policy Object Settings

Prerequisites: Verify that:

- You know the Domain Group Policy Object (GPO) name to be reimported.
- The supplemental CD ISO image file is available for mounting to the virtual machine CD-ROM drive from the datastore or local drive.
- All domain controllers are in the correct state in Unified Event Manager (UEM) with no errors.
- The vSphere client is for A7.18 release or older. The browser is for A2019.1 release or newer.

Procedure:

- 1 Open the first system level DC virtual machine console.
- 2 Prepare the source data for the domain GPO reimport.
- 3 Mount the Supplemental CD ISO image to the virtual CD drive of the domain controller virtual machine.
The supplemental CD ISO is presented as an **E:** drive on the first system level DC.
- 4 Log on to the first system level DC with domain admin account (for example, **motosec**).
You can see the desktop of the first system level DC.
- 5 Open the Group Policy Management Console (GPMC).
- 6 Click **Search** and type: `gpmc.msc`
The **Group policy management** window opens.
- 7 Select the proper GPO.

- a Find in the left pane of GPMC tree: **domain** - *<your domain name>* (for example, **ucs.astro**)
 - b Open the **Group policy management objects** folder on your domain.
 - c Click the GPO object you want.
- 8 Import settings for this GPO.
 - a Right-click the GPO object and choose **Import Settings**.
 - b In the **Import Settings** wizard window, choose **Next**.
- 9 Optional: To back up the current GPO settings, perform the following actions:
 - a To choose the backup folder for the current GPO settings, click the **Backup** button.
 - b In the next window, click **Browse** and choose the folder to upload the settings.
 - c Fill in the **Description** field with a proper explanation of the backup, for example: *Previous state of test GPO settings*.
 - d Click the **Backup** button and **OK**.
- 10 Import the settings.



NOTICE: Double check that you are importing the right GPO, because every GPO import triggers the domain synchronization process. The process takes time and must be completed before the next attempt to import.

- a Click **Next** to continue.
A new window appears.
 - b Click **Browse**.
 - c Choose the **E:** drive to get GPO in the **Browse folder** window.
 - d Navigate to **E:\Active Directory\Data\GPO** and click **OK**.
 - e Click **Next**.
 - f From the GPO list, choose the right GPO and click **Next**.
 - g Wait until the wizard scans the backup folder, check the results and click **Next**.
 - h On the next screen, choose the migration table file by clicking the **Browse** button and selecting: **C:\Windows\Temp\updated.migtable**.
 - i Select the **Use migration table exclusively** flag. Click **Next**.
 - j Check the summary and click **Finish**.
- 11 Ensure that the import was done successfully. To close the import window, click **OK**.

12.5.5

Manually Linking a GPO to an OU

Follow these steps to manually link a Group Policy Object (GPO) to an Organizational Unit (OU) in the Active Directory domain. This procedure must be performed on a domain controller. Each GPO can be linked to multiple OUs and each OU can have multiple GPOs linked to it.

Procedure:

- 1 Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.

The account name set up by Motorola Solutions is "motosec".

The domain administrator's desktop appears.

- 2 From **Start**, select **Administrative Tools**→**Group Policy Management**.
- 3 In the left pane of the **Group Policy Management** window, right-click the appropriate Organizational Unit (OU) from the list.

Step example:WinClient Network Management Clients

- 4 From the context menu, select **Link an Existing GPO**.
- 5 From the list of GPOs in the **Select GPO** window, select the appropriate GPO. Click **OK**.

Step example:Network Management Clients

- 6 Optional: If needed, modify the **Link Order** of your new GPO.
See [Modifying Your Organization's Computer/Machine Configurations on page 158](#).
- 7 Perform one of the following actions:
 - Restart the client device (**not** the DC) to enable the changes.
 - **On a DC with Windows Server 2012:** Right-click your GPO and, from the context menu, select **Group Policy Update**.

12.6

Cohabitation Procedures

This section contains common procedures for configuring ASTRO® 25 system Active Directory domain controllers for cohabitation situations running on Windows clients. The procedures are not required for the proper operation of the system unless your organization is adding its own Organizational Unit (OU) and/or custom cohabitation scenario. In most cases, Motorola Solutions provides all the Organizational Units (OUs) that are necessary to properly configure certified system cohabitation.

This section only covers topics related to cohabitation OUs in Active Directory. Local supplemental configuration of applications cohabitating on the same Windows-based devices is addressed in the “Applying Device-Specific Settings Using the Windows Supplemental Media” in the *Windows Supplemental Configuration Setup Guide*.



NOTICE: The Dispatch Console cohabitation scenarios used in this section are examples. OUs for all certified console cohabitation configurations are provided by Motorola Solutions.

12.6.1

System/Device Specific Requirements Identification

In most cases, the cohabitation software does not exist on every instance of the host platform. For example, in a typical console site, only one or two dispatch consoles have cohabitation software installed. Therefore, each cohabitation permutation must be configured manually.

The following requirements need to be fulfilled before performing the cohabitation procedures:

- Identify the Windows devices hosting the cohabiting software and make note of the permutations needed and the hostnames of those Windows devices. Multiple instances of a specific cohabitation configuration need only one permutation.
- Using the Active Directory Users & Computers Console at the domain controller, identify the OUs in which the host devices currently exist and make a note of the OU.



IMPORTANT: Ensure that the software you want to install on the system is supported by Motorola Solutions. Failure to do so may void the warranty. For more information, contact the Motorola Solutions Support Center (SSC).

12.6.2

Creating New Organizational Units

When and where to use:

Follow these steps to create a new OU. Refer to the Microsoft documentation for specific procedures.

Procedure:

- 1 Log on to the domain controller using a valid domain administrator account.
- 2 Using the Active Directory Users & Computers Console, create a new OU for the cohabitation configuration. Be sure to name the new OU appropriately.

12.6.3

Linking Base Group Policy Objects to New Organizational Units

Procedure:

- 1 Using the existing OU of the host device as a reference, link all the applicable Group Policy Objects (GPOs) in exactly the same linking order as the OU of the host device.

See Microsoft documentation for specific procedures.



NOTICE: The linking order is critical. You must duplicate the host OU's GPOs and linking order exactly.

12.6.4

Creating a New Cohabitation GPO

This section is applicable only if a Group Policy Object (GPO) does not already exist for the application you want to cohabit. You can verify if an application GPO exists by using the Group Policy Management Console.

Procedure:

Perform one of the following actions:

- If a GPO exists, add a cohabitation GPO to a new OU. See [Adding a Cohabitation GPO to a New OU on page 163](#).
- If a GPO does not exist, create an application-specific GPO. When creating the application-specific GPO, be sure to only set those values that are required to enable the software to operate in the Motorola Solutions environment. Also, be sure to name the new application-specific GPO appropriately, so that the application name can be easily identified.

12.6.5

Adding a Cohabitation GPO to a New OU

Procedure:

- Using the Group Policy Management Console, link the cohabitation GPO to the new OU. Ensure that the cohabitation GPO is the last GPO to be applied to the OU of the Windows device.

See Microsoft documentation for specific procedures.

12.6.6

Merge Situations Configuration

Cohabitation applications require some user rights assignments in order to operate in the Motorola Solutions environment. In these cases, create a Merge GPO to ensure that the custom configuration is not lost during an upgrade or migration.



WARNING: Do **not** add the merge settings to existing GPOs as the existing values can be lost during an upgrade/migration. Always create a custom GPO for Merge values.

12.6.6.1

Identifying a Merge GPO

Follow these steps to identify if a Merge GPO is required for a device.

Procedure:

- 1 Using the Group Policy Management Console, check the User Rights Assignments sections of the application-specific GPO that are contained in the new OU.
Ignore the **DHT_ADM** and **BHT_ADM** GPOs.
- 2 Using the Active Directory Users & Computers Console, create an OU for the cohabitation configuration.
Be sure to name the new OU appropriately.
- 3 Perform one of the following actions:
 - If a merge GPO is needed, proceed to [Creating a Merge GPO on page 164](#).
 - Otherwise, proceed to [Moving Computer Objects \(CO\) to a New OU on page 165](#).

12.6.6.2

Creating a Merge GPO

Follow these steps to create a Merge GPO. See the Microsoft documentation for specific procedures.

Procedure:

- 1 Using the Group Policy Management Console, create a new GPO for the User Rights merge values.
Ensure to name the new GPO appropriately, so that the intended use can be easily identified by the name.
- 2 Using the Group Policy Management Console, edit the User Rights Assignments section to include the values from your list.
- 3 Using the list generated in [step 2 of Identifying a Merge GPO on page 164](#), hand-merge those values on paper.
- 4 Check if the values overlap with the DHT_ADM and BHT_ADM GPOs. If there is any overlap, then hand-merge those values into your list.
- 5 Add the created Merge GPO to the new OU.

12.6.6.3

Moving Computer Objects (CO) to a New OU

Procedure:

- 1 After the new OU is successfully created and tested, using the Active Directory Users & Computers Console, move the CO for the cohabitation computer(s) from the host OU to your new cohabitation OU.

Step example: Move the host computer.

See the Microsoft documentation for specific procedures.

- 2 Restart the moved computer.

12.7

Failure to Join an Active Directory Domain

Information provided in the following sections is generalized and is included here as an aid to troubleshooting.

The following actions need to be performed in order for a Windows system component to successfully join an ASTRO® 25 Active Directory domain:

- Enable necessary services
- Configure TCP/IP settings
- Configure time synchronization
- Check for hostname uniqueness
- Update System Properties
- Rejoin the Active Directory domain



NOTICE: For systems with the centralized authentication feature, see [Rejoining a Linux-Based Server to an Active Directory Domain on page 172](#) and [Rejoining a Solaris-Based Server to an Active Directory Domain on page 172](#) for information on troubleshooting the failure of a Linux or Solaris system to join an Active Directory domain.

12.7.1

Failure to Enable Services

The following services must be enabled and set to Automatic. Active Directory and DNS use these services to update their infrastructure. For example, the DHCP client is needed to update the hostname and IP address of this device in DNS.

The services that are set to Automatic are as follows:

- DHCP Client
- DNS Client
- TCP/IP NetBIOS Helper

12.7.2

Failure Due to TCP/IP Settings Misconfiguration

In order to connect a Windows-based device to an Active Directory domain, the network settings must be configured properly. The IP address, subnet mask, default gateway, DNS servers, and DNS search list must be set up correctly. Active Directory uses this information when joining the Windows-based device to an Active Directory domain.

[Configuring the IP Address on page 166](#) explains how to configure the IP address manually in case of a failure due to TCP/IP settings misconfiguration.

12.7.2.1

Configuring the IP Address

Follow these steps to configure the IP Address and related information for a Windows-based device in the Active Directory domain in case of a failure due to TCP/IP settings misconfiguration.

When and where to use: If a dialog box appears stating the system needs to be restarted in order for changes to take effect, click **No** in the dialog box. Then, once all of these procedures have completed, restart the system.

Procedure:

- 1 Right-click **Start**. From the context menu, select **Network Connections**.
- 2 In the **Network Connections** window:
 - a Right-click **Ethernet**.
 - b From the context menu, select **Properties**.
- 3 In the **Ethernet Properties** window, double-click **Internet Protocol Version 4 (TCP/IPv4)**.
- 4 In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box:
 - a Select **Use the following IP address**.
 - b Select **Use the following DNS server addresses**.
 - c Enter the correct information in all of the fields.

For more information on the fields, see the documentation provided with the system.
- 5 Click **Advanced**.
- 6 In the **Advanced TCP/IP Settings** dialog box, select the **WINS** tab.
- 7 In the **NetBIOS setting** area, select **Disable NetBIOS over TCP/IP**.
- 8 Select the **DNS** tab.
- 9 Select **Append these DNS suffixes**. Click **Add**.
- 10 In the **TCP/IP Domain Suffix** dialog box, enter the *<DNS Suffix>* associated with devices on this subnet. Click **Add**.

The DNS domain name appears in the list.
- 11 In the **Advanced TCP/IP Settings** dialog box, click **OK**.
- 12 In the **Internet Protocol Version 4 (TCP/IP) Properties** dialog box, click **OK**.
- 13 In the **Ethernet Properties** window, click **OK**.
- 14 Close the **Network Connections** window.

12.7.3

Failure Due to Improper Time Synchronization Configuration

The system time needs to be synchronized between the domain controller and devices in the radio network that communicate with the domain controller. The time must be synchronous within 2 minutes.

12.7.4

Failure Due to Hostname and DNS Domain Name Misconfiguration

In order to connect a device to an Active Directory domain, it must be configured properly. The hostname and DNS domain name must be properly set up. This must be done before the device can join the domain by altering the **Member Of** section of the **System Properties**.

The hostname of an Active Directory client must be unique within the Active Directory domain (that is, within the RNI zone). This is the short hostname of the Active Directory client, and not the Fully Qualified Domain Name.

For example, while `op1.nmd4.zone2` and `op1.nmd5.zone2` are unique, they are within the same Active Directory domain, `zone2`. Thus, the short hostname, `op1`, is not unique. The short hostname must be unique, or the most recent entry overwrites the older one.

For information regarding DNS Domain Name misconfiguration, see [DNS Misconfiguration on page 174](#).

12.8

Services Required for Active Directory Operation

The following services are required for normal operation of Active Directory in the ASTRO® 25 system:

- Active Directory Domain Services
- DFS Namespace
- DFS Replication
- DNS Server
- Intersite Messaging
- Kerberos Key Distribution Center
- Netlogon
- Network Policy Server
- Server For NIS
- Windows Time
- Workstation

12.9

The Repadmin Tool Usage

This section describes the use of the replication diagnostic utility (Repadmin) which is installed with Windows Server 2012 to resolve replication failure issues.

The Repadmin tool enables administrators to view the low-level status of Active Directory replication, force synchronization between domain controllers, view the topology in a graphical format, and monitor the status and performance of domain controller replication. You can use Replication Monitor to do the following:

- See when a replication partner fails.
- View the history of successful and failed replication changes for troubleshooting purposes.
- View the properties of directory replication partners.
- Create your own applications or scripts written in Microsoft Visual Basic Scripting Edition (VBScript) to extract specific data from Active Directory.
- View a snapshot of the performance counters on the computer, and the registry configuration of the server.

- Generate status reports that include direct and transitive replication partners, and detail a record of changes.
- Find all direct and transitive replication partners on the network.
- Display replication topology.
- Poll replication partners and generate individual histories of successful and failed replication events.
- Force replication.
- Trigger the Knowledge Consistency Checker (KCC) to recalculate the replication topology.
- Display changes that have not yet replicated from a given replication partner.
- Display a list of the trust relationships maintained by the domain controller being monitored.
- Display the metadata of an Active Directory object's attributes.
- Monitor replication status of domain controllers from multiple forests.

12.9.1

Checking Replication Status with Repadmin

Procedure:

- 1 Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.
The account name set up by Motorola Solutions is “motosec”.
The administrator’s desktop appears.
- 2 Press **Windows icon key+R** to open the **Run** dialog box.
- 3 In the **Run** dialog box, enter: `repadmin /replsummary`
- 4 Investigate the results of the replication output displayed. Check for failures in the summary.
- 5 If there are failures, enter: `repadmin /showrepl <name of the DC failing replication>`
The replication output is displayed.

12.10

Setting the Time Source

Prerequisites: For additional information regarding time sources, see [Network Time Protocol \(NTP\) as the ASTRO 25 Time Source on page 32](#).

Procedure:

- 1 Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.
The account name set up by Motorola Solutions is “motosec”.
The administrator’s desktop appears.
- 2 Open PowerShell:
 - a From **Start**, click **Search**.
 - b In the search field, type in `powershell`
 - c Click **Windows PowerShell**.

- 3 At the PowerShell prompt, change directory to: `C:\Program Files\Motorola\AstroDC\common\scripts.`
- 4 Enter: `.\ConfigNTPServerLists.ps1`
A message states what time sources will be used.
- 5 Click **OK**.
The message box closes.

12.11

Authentication Failure Troubleshooting

The following are possible Active Directory authentication failure scenarios:

- [Failure Between the User and Authenticating Server on page 169](#)
- [Failure Between a Device and Domain Controller on page 169](#)
- [RADIUS Authentication Failures on page 184](#)

12.11.1

Failure Between the User and Authenticating Server

The communication link between the central authentication server becomes unavailable if there is a link failure between the user-terminal/host and the server in the zone core.

If there is a failure of critical networking services required for authentication (for example, DNS or synchronized network time), the authentication protocol may fail resulting in an inability to authenticate a user.

12.11.2

Failure Between a Device and Domain Controller

If unable to authenticate an Active Directory user at a device, perform the following:

- Ensure that the device is part of the domain in the appropriate domain controller.
- Verify that there are no network connectivity issues between the device and the domain controllers. For a zone-level device, there should be network connectivity to both zone and system level domain controllers. For a system-level device, there should be network connectivity to the system-level domain controller.
- Ensure that the time is set to the correct value and the time is synchronized between the AD domain and clients for authentication to work properly.
- Ensure that the device is configured to be a member of the correct AD domain by logging on to the device as a local administrator or root user.
- Unjoin and rejoin the device if the Active Directory forest is rebuilt after the user has joined the domain.
- Check for any DNS replication issues by viewing the event log in the domain controllers. DNS replication issues are related to network connectivity issues or zone core firewall configuration.
- Delete the device from the appropriate domain controller, then rejoin the device to the domain.



NOTICE: For all devices (Windows, Solaris, and Linux-based), the unjoin operation is performed automatically when rejoining the device to the domain.

12.12

Authorization Failure Troubleshooting

When authorization failure is suspected, check the local Windows Event Viewer or Centralized Event Logging server for authorization events. For detailed information regarding Windows Event Viewer, see the *Centralized Event Logging* manual.

Authorization failure may be caused by the following:

- Account disabled in Active Directory
- Account does not have the required privilege (it is not a member of the appropriate Active Directory group for the operation being performed, or individual user account was not given the authorization needed for the operation)

For support, contact your domain administrator.

12.13

Troubleshooting Single-Sign On (SSO) on CAM

When and where to use: Follow these steps to perform initial troubleshooting if the single-sign on is failing and the user is being forced to log into the Console Alias Manager (CAM) application with a username and password. If performing the procedure does not solve the problem, contact the Motorola Solutions Support Center (SSC).

Procedure:

- 1 Verify the list of websites configured to be recognized as Intranet sites by the Internet Explorer:
 - a Open the Internet Explorer.
 - b Click **Tools**→**Internet Options**→**Security**.
 - c Click **Local Intranet**→**Sites**→**Advanced**.
 - d Ensure that the URL of the CAM server is in this list. If it is not, refer to the *MKM 7000 Console Alias Manager* manual for information how to add the CAM server to the appropriate Group Policy Object (GPO).
- 2 The user must be a member of the CAM application's login group.

See "Adding and Removing the CAM Group Names in the MKM 7000 CAM Configuration Utility" in the *MKM 7000 Console Alias Manager* manual. Note down each defined group name.

 - a Log on to the domain controller.
 - b Open the **Domain Users & Groups** window.
 - c Navigate to the **Users** folder and locate the user that the SSO is failing for.
 - d Double-click the username and go to the **Member Of** tab.
 - e Verify the CAM login group is present.
- 3 Verify that the Motorola Public Root certificate has been added to the Java keystore on the CAM server:
 - a Log on to the machine where the CAM server is installed.
 - b Open a command prompt with admin privileges. See [Starting the Windows Command Line as Administrator on page 142](#).
 - c Enter:
 - 1 `keytool -list -alias MOTOROLA_ROOT_CA_SHA1 -keystore "<DIRECTORY TO JAVA RUNTIME>\lib\security\cacerts"`

- 2 `keytool -list -alias MOTOROLA_ROOT_CA_SHA256RSA -keystore
"<DIRECTORY TO JAVA RUNTIME>\lib\security\cacerts"`
- d When prompted for a password, do **not** enter one. Press ENTER.
- e If a message appears stating that the certificate alias does not exist, contact the system administrator for instructions on how to import the root certificate.
- 4 Verify that the Service Principal Names (SPNs) are unique:
SPNs are associated with an application and registered with the Active Directory. They must be unique across the entire domain.
 - a Log on to the machine where the CAM server is installed.
 - b Open a command prompt with admin privileges.
See [Starting the Windows Command Line as Administrator on page 142](#).
 - c Enter the following to change the directory to AAA:
 - 1 `cd %AAA_HOME%`
 - 2 `cd conf`
 - d Verify that a `krb5.keytab` file exists.
 - If it does, continue with this procedure.
 - If it does not, verify that there is a file with the `.spn` extension and rejoin the machine to the domain to regenerate the needed `krb5.keytab` file.
 - e Open the file with the `.spn` extension and locate SPNs with the format: `HTTP/<server domain name>`
 - f For each SPN in the file, enter:
`"%AAA_HOME%\bin\callregsvc.bat" -searchSPN <SPN name> -U <username>
-P <password> -realm <domain name>`
 - If a message similar to the following appears, SPNs have been located:

```
SPN name :HTTP/PC-44-STM.zone1 Accounts  
-----  
SVC_PC-44-STM
```
 - If 0 `Accounts` message appears, make sure the `.spn` exists and join CAM to the domain. See [Joining and Rejoining a Windows-Based Device to an Active Directory Domain on page 140](#).

12.14

Failure of Application Access by Administrator on Windows-Based Device

After a device joins the domain, its applications that have Role Based Access Control in Active Directory may not be usable by the local Windows administrator or the domain administrator if that user account is not a member of the group associated with the application for that device. Active Directory account login is recommended, if available.

In some cases, the administrator can access the application by entering its executable path and filename at the elevated Windows command line. The path and filename can be seen in the properties

for the application shortcut on the desktop or the **Start** menu. For information how to run the elevated Windows command line, see [Starting the Windows Command Line as Administrator on page 142](#).



NOTICE: The administrator can run some applications, for example MOSCAD NFM applications, by using the **Run as administrator** option, without the need to open the command prompt window. For detailed information, see the logon section in the appropriate device manual.

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 for Windows 7 and Windows 10-based devices.

12.15

Failure Between the Domain Controller and a Device

A system-level domain controller becomes unavailable if there is a failure of the authentication protocol which may be caused by a link failure to the master zone or dropped packets. Any administrative or emergency access to the Solaris-based server or Linux-based server needs to be performed using a local administrator or root login account.

For Windows-based devices, when the central authority is not available, the user is alerted when logging on, and is informed if cached credentials are available. The user will be unable to access the device if the user was not previously authenticated by a successful domain logon.

12.16

Rejoining a Linux-Based Server to an Active Directory Domain

Perform [Joining a Linux-Based Device to the Domain on page 144](#) to rejoin a Linux-based server to an Active Directory domain.

12.17

Rejoining a Solaris-Based Server to an Active Directory Domain



NOTICE: The ISSI.1 feature is supported on a Generic Application Server (GAS) server platform. For detailed information regarding the GAS server and ISSI.1, see the following manuals:

- *Generic Application Server*
- *ISSI.1 Network Gateway Feature Guide*

Prerequisites:

For information about setting up Active Directory users so that they can perform specific administration menu procedures, contact your Active Directory administrator.



NOTICE: All Unix devices in the UCS subnet should be joined into the domain only after the colocated zone domain controller is installed. If the Unix devices in the UCS subnet are joined to the domain before the colocated zone domain controller is set up, they will not have domain controller redundancy.

Procedure:

- 1 Log on to the server with the root account.
- 2 At the command prompt, enter: `admin_menu`
- 3 At the **Servers Main Menu**, enter the number for the **Services Administration** option.
- 4 At the **Services Administration** menu, enter the number for the **Manage AAA Client Configuration** option.

- 5** At the **Manage AAA Client Configuration** menu, enter the number for the **Display Domain Membership Status** option.

Domain membership information appears, for example: Determining status - please wait. Domain: UCS.ASTRO Membership Status: Joined

- 6** Repeat the normal domain join procedure.

- 7** Select **Join Domain**.

A prompt appears with your organization's domain name listed as currently joined to the domain.



NOTICE: To join another domain, first unjoin this domain.

- 8** Enter: `y` to unjoin the domain.

- 9** Enter the domain administrator username and password.

- 10** Perform one of the following actions:

- If the unjoin operation was successful, proceed to [step 12](#).
- If not, the following prompt appears:

```
Error Detected
-----

1. Retry unjoin
2. Proceed to join

Please select an option (1-2, q):
```

- 11** Enter: `2`

- 12** Proceed with the normal domain join procedure.

12.18

Domain Controller Health Report in UEM

Domain Controller reports health of its critical services to UEM. It identifies if services are run properly or have any general problems. It may take up to 15 minutes to update the current state of the managed services.

[Table 17: Domain Controller Health Report in UEM on page 173](#) describes the meaning of states that can be reported to UEM.

Table 17: Domain Controller Health Report in UEM

State	Description	User Action
Enabled	Service is running normally.	N/A
Disabled	Service has been disabled by the user.	Verify that the affected service is running and start it, if necessary.
Enabling	Service is starting.	N/A
Malfunction	Service experienced some error condition. User intervention may be needed to recover from failure.	Wait for 15 minutes. If the state does not change, continue with the steps below:


State	Description	User Action
		<ol style="list-style-type: none"> 1 Every service has its own log file which can be checked for errors. See Table 18: Locations of Log Files on page 174. 2 Check for errors in the Windows Event Viewer. 3 Check the output of the <code>dcdiag</code> diagnostic tool. 4 Verify that there are no network connectivity issues between Domain Controllers. 5 Verify that there are no time synchronization problems between Domain Controllers and NTP servers. 6 Verify the replication status. See Checking Replication Status with Repadmin on page 168. Resolve all replication issues if they are reported by the <code>repadmin</code> tool. 7 Verify that Firewall rules are applied properly.
		 NOTICE: Search for resolutions of reported problems in the Microsoft Knowledge Base.

Table 18: Locations of Log Files

Type of Service	Log File Location
AD Service	C:\Program Files\Motorola\Motorola DC Fault Management\data\Check_DC_AD.log
DNS Service	C:\Program Files\Motorola\Motorola DC Fault Management\data\Check_DC_DNS.log
RADIUS Service	C:\Program Files\Motorola\Motorola DC Fault Management\data\Check_DC_RADIUS.log
Replication Service	C:\Program Files\Motorola\Motorola DC Fault Management\data\Check_DC_REPLICATION.log

12.19

DNS Misconfiguration

This section provides the troubleshooting and recovery information relating to DNS misconfiguration.

12.19.1

Interpreting Device DNS Misconfiguration

DNS maps the domain name to the IP address. A device registers its FQDN (hostname.domainname) in DNS with its IP address. This DNS data is stored as a collection of records known as Resource Records (RRs). An Address (A) resource record records an actual mapping between hostname and an IP address. A pointer (PTR) resource record records an actual mapping between an IP address and an FQDN.

As there are no restrictions on the number of A/PTR records that can be created, several such records can be created associating more than one IP address with a particular DNS name or more than one FQDN with a single IP address.

Some possible device misconfiguration scenarios are the following:

Incorrect DNS Hostname Example

Incorrect DNS hostname: cs321113cbr02
Device IP: 10.232.113.3
DNS Domain name: convloc113.csub32.ucs

where the correct DNS hostname should be:

Correct DNS hostname: cs321113cbr01

As a result, the following records have been created in DNS Server:

Forward lookup Zone:	
cs321113cbr01	10.232.113.3
cs321113cbr02	10.232.113.3
Reverse lookup zone:	
10.232.113.3	cs321113cbr01.con-vloc113.csub32.ucs
10.232.113.3	cs321113cbr02.con-vloc113.csub32.ucs

Incorrect Device IP Address Example

DNS hostname: cbr01
Incorrect Device IP: 184.61.96.45
DNS Domain name: ssl.site44.zone7

where the correct device DNS configuration should be:

Correct Device IP: 184.61.96.44

As a result, the following records have been created in the DNS Server:

Forward lookup Zone:	
cbr01	184.61.96.44
cbr01	184.61.96.45
Reverse lookup zone:	
184.61.96.44	cbr01.ssl.site44.zone7
184.61.96.45	cbr01.ssl.site44.zone7

12.19.2

Device DNS Misconfiguration State Verification

Unless removed manually, both incorrect and correct entries exist in DNS Server. Each time there is a forward/reverse DNS Lookup, DNS server sends all the IP addresses/FQDNs on the list back to the requester.

The server changes the order of the addresses supplied in the response, choosing the order randomly or in a sequence.

For devices with wrong DNS hostname, if the device was found in UNC already and the DNS hostname was corrected, the device still shows the incorrect folder name in the UNC. The folder name and the actual FQDN are mismatched.

The following are the results of this misconfiguration:

- An nslookup on the device IP address yields all the FQDNs (both the correct and incorrect ones):

```
Multiple FQDN pointing to same IP address.
```

```
nslookup 10.232.113.3  
cs321113cbr01.convloc113.csub32.ucs
```

```
nslookup 10.232.113.3  
cs321113cbr02.convloc113.csub32.ucs
```

- An nslookup on the FQDN yields all the device IP addresses (both the correct and incorrect ones):

```
Multiple IP addresses pointing to same FQDN.
```

```
nslookup cbr01.ss1.site44.zone7  
184.61.96.44
```

```
nslookup cbr01.ss1.site44.zone7  
184.61.96.45
```

12.19.3

Fixing the DNS Misconfiguration in the DNS Server or UNC

Procedure:

- 1 Delete the incorrect entries (both forward and reverse) from the primary DNS Server which holds the copy of the data for a zone.

For the procedure to delete incorrect DNS entries, see the Microsoft Windows online help.

The primary DNS Server for the Tsub is located on the zone-level Domain Controller.



NOTICE: Wait about 15 minutes before continuing to the next step, as secondary servers have copies of this data which they synchronize with the primary through zone transfers at intervals or when prompted by the primary.

- 2 Perform both forward and reverse lookup for the device on the system-level DNS Server to ensure a single mapping of Device IP address and FQDN exists for the device.

- 3 Delete the device from the UNC and rediscover it.

See “Deleting a Device” in the *Unified Network Configurator* manual.

- 4 Rediscover the device from the UNC.

Ensure that the device is discovered and placed in the correct folder. See “Performing Device Discovery with the UNCW Discovery Wizard” in the *Unified Network Configurator* manual.

12.20

Managing FSMO Roles

If the domain controller with the FSMO roles needs to be rebuilt for any reason, then the roles can be transferred and are assigned. The first system-level DC holds additional FSMO roles for the entire forest. If the first DC in a domain is damaged, the roles have to be transferred to the other DC in the domain. After the primary DC is rebuilt, then the FSMO roles have to be transferred back to it.

12.20.1

Determining the FSMO Role Owner

Procedure:

- 1 Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.
The account name set up by Motorola Solutions is “motosec”.
The administrator’s desktop appears.
- 2 To access the command window, press the **Windows icon key+R** to open the **Run** dialog box, then enter `cmd` in the text field. Click **OK**.
- 3 At the command prompt window, enter: `netdom query fsmo`
Schema owner and domain role owner are always present at the system-level DCs.
PDC role, RID Pool Manager, and Infrastructure owner roles are present at the system-level, zone-level, and site-level domains.
The Domain Controller computer names of the FSMO role owners are displayed.
- 4 In the command window, enter: `exit`
The command window closes.

12.20.2

Seizing FSMO Roles

Procedure:

- 1 Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.
The account name set up by Motorola Solutions is “motosec”.
The administrator’s desktop appears.
- 2 Press **Windows icon key+R** to open the **Run** dialog box. Type `Ntdsutil`, then click **OK**.
The command prompt window appears with the `Ntdsutil` prompt.
- 3 At the prompt, enter: `roles`
- 4 At the `fsmo maintenance` prompt, enter: `connections`
- 5 At the `server connections` prompt, enter: `connect to server <servername>`
where `<servername>` is the name of the server that assigns the roles
A few messages appear about connecting to the server.
- 6 At the `server connections` prompt, enter: `q`

- 7 At the fsmo maintenance prompt, enter: `seize <role>`

where **<role>** can be:

naming master (system-level domain only)
schema master (system-level domain only)
infrastructure master
PDC
RID master

A warning window appears prompting for confirmation for the seize operation.

- 8 Click **Yes**.

The role specified in [step 7](#) is seized.

- 9 Repeat [step 7](#) and [step 8](#) until all applicable roles are seized.

- 10 Enter: `q` until you exit from the `Ntdsutil` tool.

12.20.3

Transferring FSMO Roles

Perform this procedure when removing a Domain Controller in order to rebuild it.

Procedure:

- 1 Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.

Step example: If `ucs-dc01.ucs` is the FSMO role owner, log into the collocated zone `dc01`. The account name set up by Motorola Solutions is “motosec”.

The administrator’s desktop appears.

- 2 Open PowerShell:

- a From **Start**, click **Search**.
b In the search field, type in `powershell`
c Click **Windows PowerShell**.

- 3 At the prompt, enter:

```
Cd "c:\Program files\Motorola\AstroDC\common\scripts  
\" .\TransferFSMORoles.ps1
```

- 4 When prompted by the following script, enter: A

```
Move Operation Master Role
```

```
Do you want to move role 'PDCEmulator' to server 'z001dc01.zone1'
```

The server name displayed may vary, depending on the collocated zone.



NOTICE: When the same script is used to transfer the roles back to the first system-level DC, command line output may be slightly different (the server will be displayed as `ucs-dc01.ucs`).

The script is completed.

12.20.4

Seizing Active Directory Lightweight Directory Services (AD LDS) FSMO Roles

Procedure:

- 1 Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.
The account name set up by Motorola Solutions is “motosec”.
The administrator’s desktop appears.
- 2 Run `dsmgmt.exe`:
 - a From **Start**, click **Search**.
 - b In the search field, enter: `cmd`
 - c At the command prompt, enter: `dsmgmt.exe`
 - d Click **OK**.
- 3 At the `dsmgmt` prompt, enter: `roles`
- 4 At the `fsmo maintenance` prompt, enter: `connections`
- 5 At the `server connections` prompt, enter: `connect to server <servername:49281>`
where `<servername>` is the FQDN of the localhost server, for example: `z001dc01.zone1`
A few messages are shown about connecting to the server.
- 6 At the `server connections` prompt, enter: `q`
- 7 At the `fsmo maintenance` prompt, enter: `seize <role>`
where `<role>` can be one of the following:
`naming master`
`schema master`
A warning window appears prompting for confirmation for the seize operation.
- 8 Click **Yes**.
The role specified in [step 7](#) is seized.
- 9 Repeat [step 7](#) and [step 8](#) until all applicable roles, naming master and schema master are seized.
- 10 Enter `q` until you exit the **dsmgmt** tool.

12.21

Deleting a Domain Controller Server Object in a Domain

Procedure:

- 1 Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.
The account name set up by Motorola Solutions is “motosec”.
The administrator’s desktop appears.

- 2 Press **Windows icon key+R** to open the **Run** dialog box. Type `Ntdsutil`, then click **OK**.
The command prompt window appears with the `Ntdsutil` prompt.
- 3 At the prompt, enter: `metadata clean`
The `metadata cleanup` prompt appears.
- 4 At the prompt, enter: `connections`
The `server connections` prompt appears.
- 5 At the prompt, enter: `connect to server <server name>`
where **<server name>** is the name of the working domain controller.
Messages appear about connecting to the server, then the `server connections` prompt appears.
- 6 At the prompt, enter: `quit`
The `metadata cleanup` prompt reappears.
- 7 At the prompt, enter: `sel op target`
The `Select Operation Target` prompt appears.
- 8 At the prompt, enter: `list domains`
A numbered list of domains appears.
- 9 At the prompt, enter: `select domain <domain number>`
where **<domain number>** is the number of the domain that contains the domain controller server to be deleted.
The selected domain displays.
- 10 At the prompt, enter: `list sites`
A numbered list of sites appears.
- 11 At the prompt, enter: `select site <site number>`
where **<site number>** is the number of the site that contains the domain controller server to be deleted.
The selected domain and site display.
- 12 At the prompt, enter: `list server for domain in site`
A numbered list of servers appears.
- 13 At the prompt, enter: `select server <server number>`
where **<server number>** is the number of the domain controller server to be deleted.
The selected domain, site, and server are displayed.
- 14 At the prompt, enter: `q`
The `metadata cleanup` prompt reappears.
- 15 Enter: `Remove selected server`

16 At the confirmation prompt, click **Yes**.

The server object is deleted.

17 Enter `q` repeatedly to exit the `ntdsutil` tool.

The `ntdsutil` tool command prompt window closes.

12.22

Deleting an AD LDS Server Object in an AD LDS Configuration Set

Procedure:

1 Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.

the account name set up by Motorola Solutions is "motosec".

The administrator's desktop appears.

2 Run `dsmgmt.exe`:

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

b In the search field, enter: `cmd`

c At the command prompt, enter: `dsmgmt.exe`

d Click **OK**.

3 At the `dsmgmt` prompt, enter: `metadata clean`

4 At the `metadata cleanup` prompt, enter: `connections`

5 At the `server connections` prompt, enter: `connect to server <servername:49281>`

where `<servername>` is the FQDN of the localhost server, for example: `z001dc01.zone1`

A few messages are shown about connecting to the server.

6 At the `server connections` prompt, enter: `quit`

7 At the `metadata cleanup` prompt, enter: `sel op target`

8 At the `Select Operation Target` prompt, enter: `list sites`

A numbered list of sites appears.

9 Enter: `select site <site number>`

where `<site number>` is the number of the site that contains the domain controller server to be deleted. There should only be one site, so the site number should be 0.

10 Enter: `list servers in site`

A numbered list of servers appears.

11 Enter: `select server <server number>`

where `<server number>` is the number of the domain controller server to be deleted.

The selected domain, site, and server are displayed.

12 Enter: `q`

- 13 At the `metadata cleanup` prompt, enter: `Remove selected server`
A prompt asks you to confirm that you want the server object to be deleted.
- 14 Click **Yes**.
The server object is deleted.
- 15 Enter: `q` repeatedly to exit the **dsmgmt** tool.
The command prompt window closes.

12.23

Deleting an Active Directory Domain

Procedure:

- 1 Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.
The account name set up by Motorola Solutions is "motosec".
The administrator's desktop appears.
- 2 Perform the following actions:
 - a From **Start**, click **Search**.
 - b In the search field, enter: `cmd`
 - c At the command prompt, enter: `Ntdsutil`
 - d Click **OK**.
- 3 At the `Ntdsutil` prompt, enter: `metadata clean`
- 4 At the `metadata cleanup` prompt, enter: `connections`
- 5 At the `server connections` prompt, enter: `connect to server <server name>`
where **<server name>** is the name of the working domain controller.
Messages appear about connecting to the server.
- 6 At the `server connections` prompt, enter: `quit`
- 7 At the `metadata cleanup` prompt, enter: `sel op target`
- 8 At the `Select Operation Target` prompt, enter: `list domains`
A numbered list of domains appears.
- 9 Enter: `select domain <domain number>`
where **<domain number>** is the number of the domain to be deleted
The domain is selected.
- 10 Enter: `quit`
- 11 At the `metadata cleanup` prompt, enter: `remove selected domain`
- 12 At the confirmation prompt, enter: `yes`
The domain is deleted.

13 Enter: `q` repeatedly to exit the **ntdsutil** tool.

The command prompt window closes.

12.24

Transferring AD LDS FSMO Roles

Procedure:

1 Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.

The account name set up by Motorola Solutions is “motosec”.

The administrator’s desktop appears.

2 Run `dsmgmt.exe`:

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

b In the search field, enter: `cmd`

c At the command prompt, enter: `dsmgmt.exe`

d Click **OK**.

3 At the `dsmgmt` prompt, enter: `roles`

4 At the `fsmo maintenance` prompt, enter: `connections`

5 At the `server connections` prompt, enter: `connect to server <servername:49281>`

where `<servername>` is the FQDN of the localhost server, for example: `z001dc01.zone1`

A few messages are shown about connecting to the server.

6 At the `server connections` prompt, enter: `q`

7 At the `fsmo maintenance` prompt, enter: `transfer <role>`

where `<role>` can be:

`naming master` (system-level domain only)

`schema master` (system-level domain only)

A warning window appears prompting for confirmation for the seize operation.

8 Click **Yes**.

The role specified in [step 7](#) is transferred.

9 Repeat [step 7](#) and [step 8](#) until all applicable roles are seized.

10 Enter: `q` until you exit the **dsmgmt** tool.

Chapter 13

RADIUS Troubleshooting

This chapter provides troubleshooting information relating to the RADIUS functionality provided by Network Policy Server (NPS) in an ASTRO® 25 system.

13.1

RADIUS Authentication Failures

If the RADIUS server authentication is failing to authenticate a user, perform the following:

- Verify that the RADIUS client is configured with the correct IP address for the RADIUS server(s).
- Verify that the shared secret of the RADIUS client object on the RADIUS server matches the shared secret of the RADIUS client.
- Verify that the user account is enabled in Active Directory and that the user is part of either the `netwadm` (Network Administrators) group for administrative access or the `configaud` (Configuration Auditor) group for read-only access.



NOTICE: For a detailed list of Active Directory groups, see [Domain Groups on page 33](#).

- Verify that the “Control access through Remote Access Policy” option is selected on the Dial-In tab of the Properties for the user or user’s group in Active Directory.
- Verify that Reverse Password Encryption is enabled for the user account.
- Ensure that the password was reset after enabling reverse password encryption.
- Ensure that the authentication method used on the RADIUS client and the RADIUS server is the same.

If the 802.1x authentication is failing on the service laptop, check the following:

- The procedures for enabling 802.1x on the technician’s laptop have been performed. For detailed information, see the *802.1x Service Ports on Switches* manual.
- The RADIUS client is configured for 802.1x authentication.

13.2

Viewing Centralized Authentication Event Logs

If Centralized Event Logging is implemented, messages are generated for system events related to Centralized Authentication. Centralized Authentication event logs provide information on the following events:

- Logon Details (successful and unsuccessful)
- Security Configuration Events
- Switch Port Authentication Events
- Security Violations
- System Problems
- Audit Reports

This section provides information about accessing centralized authentication event logs. For details on implementing Centralized Event Logging, see the *Centralized Event Logging* manual.

13.2.1

Viewing Remote Access Logging Information

The local log files for the RADIUS server can be viewed in the `C:\windows\system32\logfiles` directory. The logon/logoff events can be viewed in the Event Viewer.

13.2.2

Centralized Authentication Log Information for RF Site and VPM Devices

When Centralized Event Logging is implemented on the following devices, system events related to centralized authentication are reported by these devices to the Centralized Event Logging server.

- **RF site devices:**
 - GTR 8000 Base Radio
 - GCM 8000 Comparator
 - GCP 8000 Site Controller
 - GPB 8000 Reference Distribution Module (RDM)
 - GPW 8000 Receiver
- **Voice Processor Module (VPM) devices:**
 - SmartX Site Converter
 - MCC 7500 Voice Processor Module (VPM)
 - Telephone Media Gateway (TMG)

The following types of system events related to centralized authentication are reported to the Centralized Event Logging server by the devices listed above:

- Logon/logoff events
- Authentication events
- Authentication service configuration events

These events are reported for all types of command line access, including local serial port access and network access with protocols such as serial command line, telnet, FTP, or (Secure Shell) SSH.

System event logs are not stored locally on RF site devices and VPM-based devices, because there is no persistent local storage.

13.3

Updating Syslog and RADIUS IP Addresses for RF Site and VPM Devices

When and where to use:

If the IP addresses of the Syslog or RADIUS services change, while the Syslog service name or the RADIUS service name in DNS remains the same, the RF site devices continue to use the IP address they previously looked up. This may result in unexpected feature operation until those service connections drop and are reconnected. A reconnection of those services may be forced in order to connect to new Syslog or RADIUS service IP addresses.



NOTICE: The DNS name lookups are cached on the RF site devices for a Time-to-Live period defined by the system DNS servers. Until the DNS Time-to-Live expires, even a RADIUS or Syslog service reconnection does not result in a connection to the updated service IP address.

Follow these steps to force an update to the Syslog and RADIUS IP addresses on an RF site device, after the DNS Time-to-Live has expired.

For additional DNS troubleshooting information, see [AD/DNS Troubleshooting on page 152](#).

Procedure:

- 1 Launch the **CSS** application.
- 2 Select **File**→**Read Configuration From Device**.
A message states that an Ethernet connection must be established.
- 3 Click **OK**.
- 4 In the **Connection Screen**, enter the **<IP address>** of the device you want to access. Click **Connect**.
If an authentication window appears, enter your credentials.
A message states that CSS successfully connected to this device, and that CSS successfully read the configuration data.
- 5 When prompted, click **OK**.
The device configuration displays in CSS.
- 6 Back up the configuration data from the device, as follows:
 - a Select **File** →**Save As** to create a backup of the configuration file.
 - b In the **Properties** dialog box, enter the required information, and a description for this file. Click **OK**.
 - c In the **Save** dialog box, enter a name for the file.
 - d In the **Look in** field, navigate to the directory in which you want to store the backup file.
 - e Click **Save**.
The file is saved as a **.cpl** file.
- 7 Expand the selections in the navigation pane on the left as needed, then select **Network Services Configuration**.
- 8 In the **Network Services Configuration** window, on the **SYSLOG** and **RADIUS** configuration tabs, set the following parameters to empty text fields:
 - SYSLOG service names (primary and backup).
 - RADIUS FQDNs
- 9 Select **File**→**Write Configuration to Device** to update the configuration changes on the device.
- 10 Select **File**→**Open**.
- 11 In the **Open** dialog box, navigate to the directory which contains the backup **.cpl** file that you created in [step 6](#), select it, and then click **Open**.
- 12 From the **File** menu, select **Write Configuration to Device**.
A success message appears after CSS writes the configuration data to the device. This will force a DNS lookup for the Syslog and RADIUS features, and ensure that the DNS changes take effect on the RF site device.

13.4

Disabling RADIUS on an HP Switch

When and where to use:

Follow these steps to disable RADIUS authentication on an HP switch that is connected and has its configuration maintained in the VoyenceControl component of the Unified Network Configurator (UNC).



NOTICE:

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

For additional information, see the *Unified Network Configurator* manual.

Procedure:

- 1 Log into VoyenceControl.

The VoyenceControl main window appears.

- 2 In the navigation pane on the left side of the window, double-click the name of the network that contains the switch you want to access.

The selected network tree expands to display the Devices node.

- 3 In the navigation pane on the left side of the window, double-click **Devices**.

The list of devices and associated properties are displayed in the pane on the right side of the screen.

- 4 Right-click the desired switch on the right side of the screen.

- 5 From the context menu, select **Properties**, then select the **Communication** tab. If needed, click **Update Credentials** to:

- Make sure that a Management Mechanism (protocol) appropriate for your organization's policies has been selected for this device.
- Make sure that the Management Account field is appropriately configured. Since RADIUS authentication is currently enabled on the device, make sure that the Management Account field is configured with a VoyenceControl global credential that matches the username and password for this device on the RADIUS server.

For information on adding and modifying credentials, see “EMC Smarts Network Configuration Manager Credential Modification” in the *Unified Network Configurator* manual.

- 6 Return to the Devices view, and right-click the switch again.

A context menu appears.

- 7 From the context menu, select **Editor→Configlet**.

- 8 At the top of the **Configlet Editor** window, click inside the **Common Configlet** text box.

The **Insert Template** icon becomes active in the tool bar of the **Configlet Editor** window.

- 9 Click the **Insert Template** icon.

- 10 Click the folder icon at the top of the **Select Item** dialog box, to the right of the **Look in** field.

- 11 In the **Look In** field, choose **Library Manager** from the drop-down list.

- 12 In the list of folders on the **Select Item** dialog box, double-click the **System** folder, then double-click the **Motorola** folder.

- 13 Double-click the **HP** subfolder.

A list of templates displays on the Select Item dialog box.

- 14 Double-click the template named **Disable RADIUS Server Authentication Source**.

- 15** In the **Template Variable Substitution** window, enter a RADIUS source (zone-level domain controller) IP address and click **OK**.

The **Configlet Editor** window displays the configuration commands generated by the template.



NOTICE: Although only one IP address appears in the commands, these commands effectively disable the use of any RADIUS source IP address existing in the configuration for this device.

- 16** Perform the following steps to push changes to the device:

- a** From the **Configlet Editor** window, click **Schedule**.
- b** On the **Schedule Job** tab, enter the job name in the relevant field.
- c** On the **Tasks** tab, make sure that the Mechanism is appropriate for your organization's policies. Keep the defaults of "running-configuration" and "Copy to Start" and "Pull Configs" in the other fields for this job.
- d** Click the **Approve & Submit** button or the **Submit** button, depending on your permissions.



NOTICE: If you select the **Run upon approval** option and then click the **Approve & Submit** button on the **Schedule Job** window, the job begins immediately. The operation may take a few minutes, before successful completion is reported on the **Schedule Manager** window.

- 17** After the job completes successfully in VoyenceControl, verify that you can log on to the switch with a local account.



NOTICE:
If you want to use VoyenceControl to verify logon, you must first make sure that the Account credentials are appropriately configured for this device. Since RADIUS authentication is no longer enabled on the device, make sure that the VoyenceControl global Account credentials for this device match the *local* username and password for this device, or make sure that no credential is selected, so that the device will prompt you to enter the username and password.

For example, if you want to verify logon using the Quick Command called Test Credentials, then make sure that the Management Account credential is appropriate. If you want to verify logon using Cut-Through, make sure that the Cut-Through Account credential is appropriate.

You can view and update credentials on the **Communications** tab in the **Properties** for the device. For information on adding and modifying credentials, see "EMC Smarts Network Configuration Manager Credential Modification" in the *Unified Network Configurator* manual.

Chapter 14

Domain Controller Disaster Recovery

This chapter provides references and information that will enable you to recover a domain controller in the event of a failure.

14.1

Recovering a Domain Controller

Process:

Perform one of the following actions, depending on the configuration and the disaster recovery scenario:

If...	Then...
If you are recovering a Domain Controller in a single-zone, non-redundant configuration (M1),	perform Recovering a Domain Controller Using Backup on page 189 . For example, when the ESXi-based server hardware failure causes both the domain controllers to go down.
If you are recovering a Domain Controller in a single-zone redundant configuration (M2) or a multizone capable configuration (M3),	perform one of the following actions: <ul style="list-style-type: none"> As the primary restore method, perform Recovering a Domain Controller Using Backup on page 189. As the secondary restore method, perform Recovering a Domain Controller Using Reinstall on page 192.

For more information on different types of configurations in an ASTRO® 25 system, see the *Master Site Infrastructure Reference Guide*.

14.1.1

Recovering a Domain Controller Using Backup

This process can be used to recover the Domain Controller when there is a recent backup of the Domain Controller in the BAR server.

Prerequisites:

Obtain the *Windows Supplemental* media.

Obtain *Microsoft Windows Server 2012 R2* media.

Ensure to delete the failed Domain Controller virtual machine from the virtual server.

Ensure that the ESXi-based virtual server hosting the Domain Controller virtual machine is working properly. See the *Virtual Management Server Software* manual.

For all user input information, such as passwords, see [Table 8: User Input Requirements – Domain Controller Configuration on page 75](#).

Process:

- 1 Import the Domain Controller virtual machine.
See [Importing the Domain Controller Virtual Machine on page 59](#).
- 2 Configure Virtual Machine resources.

- See [Configuring Virtual Machine Resources on page 61](#).
- 3 Apply supplemental configuration to the ESXi server-based Virtual Machine.
See [Applying Supplemental Configuration to Virtual Machines on page 62](#).
 - 4 **Only for systems with vCenter already installed:** Configure vCenter.
See [Configuring the vCenter for the Newly Deployed VM on page 63](#).
 - 5 Set the Virtual Machine startup and shutdown order.
See “Setting the Virtual Machine Startup and Shutdown Order” in the *Virtual Management Server Software* manual.
 - 6 Connect and power on a virtual machine.
See [Connecting and Powering on a New Virtual Machine on page 64](#).
 - 7 Apply OS-level identity.
See [Applying OS-Level Identity on the Domain Controller on page 65](#).
 - 8 Configure a Domain Controller virtual machine.
See [Activating a Domain Controller Virtual Machine on page 66](#).
 - 9 Install the Domain Controller MSI:
 - a Log on to the Domain Controller using the Local Administrator account (“Administrator”).
The administrator's desktop appears.
 - b Insert the *Domain Controller Plugin* media and navigate to the drive.
 - c Double-click **ADC_RXX.XX.XX.msi** to install the Domain Controller scripts to the following location: C:\Program Files\Motorola\AstroDC.

Domain controller MSI installation takes a couple of seconds. It does not require any user interaction.

If no window appears, the installation is successfully finished.
 - 10 Configure the Domain Controller for restore from the BAR server:
 - a Log on to the Domain Controller using the Local Administrator account (“Administrator”).
 - b Open PowerShell.
 - c In the **Windows PowerShell** window, change directory to C:\Program Files\Motorola\AstroDC\
 - d Insert the *Windows Supplemental* media to the CD/DVD drive.
 - e From the *Windows Supplemental* media, copy the `WindowsInstallFramework.exe` file to C:\Program Files\Motorola\AstroDC
 - f If prompted for administrator credentials or a confirmation, type the administrator credentials or click **Yes**.
 - g In the **Windows PowerShell** window, enter:

```
.\WindowsInstallFramework.exe /i /e common\data  
\Prepare_DC_For_Restore.xml
```


The script is executed.
 - h At the prompt, enter: `<DC hostname>`

where `<DC hostname>` is one of the following values:
For system-level DC in the primary core: `ucs-dc01`
For system-level DC in the backup core (DSR systems only): `ucs-dc03`

For zone-level DC in the primary core: z<zzz>dc01

For zone-level DC in the backup core (DSR systems only): z<zzz>dc03

For zone-level DC at a site: z<zzz>nmd<sss>dc<nn>

For Tsub prime site DC: z00<x>s<ppp>dc01

where:

<zzz> is the zone number

<sss> is the site number

<nn> is the Domain Controller number

<ppp> is the prime site number

i At the prompt, enter the path to the *Windows Supplemental* media.

j Wait for the execution to be completed. Log on, when prompted.

Reboots occur during the execution. Because auto-logon is not enabled, the user is required to log on for the installation to complete.

11 Transfer the SSH keys from the BAR server to the Domain Controller if the keys on the BAR server have been rotated.

See “Performing the Secure Transfer of the SSH Client Key to Windows-Based Backup Clients” in the *Securing Protocols with SSH* manual.

12 Register the BAR Client.

See “Registering and Enabling Windows-Based BAR Clients Manually” in the *Backup and Restore Services* manual.

13 Transfer the backup from BAR server to the Domain Controller.

See “Executing a BAR Client Data Restore” in the *Backup and Restore Services* manual.

This takes at least 1 hour to complete.

14 Recover the Domain Controller using the backup from the previous step in the following way:

a Log on to the Domain Controller that is prepared for restore using the Local Administrator account (“Administrator”).

b Cut the `WindowsImageBackup` folder from the `D:\restore\d\` location and paste it to `D:\`.

c Mount the *Microsoft Windows Server 2012 R2* media.

d Restart the Domain Controller and press **F8** while the virtual machine is booting.

The **Boot Manager** screen appears.

e In the **Boot Manager** screen, from the list of options, select **EFI VMware Virtual IDE (or SCSI) CDROM Drive**.

f When prompted, press any key.

Microsoft Windows Server 2012 R2 boots up and Windows Setup screen with localizations settings appears.


g Select **US** as the keyboard input method and click **Next**.

h Select **Repair your computer**.

Choose an option screen appears.

i Select **Troubleshoot**.

j Select **System Image Recovery**.

- k** Select the **Administrator** user.
 - l** In the **System Recovery Options** screen for selecting keyboard input, select **US** as the keyboard input method. Click **Next**.
 - m** In the **System Recovery Options** login screen, type in the *<Administrator account password>*. Click **OK**.
 - n** In the **Re-image your computer** screen, if the default date, time, and computer name are correct, click **Next**.
 If the recovery wizard fails to see the backup, the backup might be corrupted. If the backup is corrupted, proceed to the next step.
 If the backup was not copied to the root **D: ** drive from the restore folder, in the recovery wizard, click **Restart** or **Cancel** and repeat this step.
 - o** In the **Choose additional Restore Options** screen, click **Next**.
 - p** In the screen stating the date, time, computer name, and drives to restore to, keep the defaults and click **Finish**.
 - q** In the confirmation window, click **Yes**.
 A progress bar appears stating the status of the recovery. The server reboots after recovery and logon prompt appear.
- 15** If recovery from backup does not work, do the following, depending on the system configuration:
- If your configuration is **Single Zone Non-Redundant (M1)**, use the Domain Controller installation process to install from scratch. See [Domain Controller Installation on page 69](#).
- 

IMPORTANT: All the important custom configuration (users, computer objects) will be lost. Contact the Motorola Solutions Support Center (SSC) before taking this action.
- If your configuration is **Single-Zone Redundant (M2) or Multizone Capable (M3)**, recover the Domain Controller using reinstall. See [Recovering a Domain Controller Using Reinstall on page 192](#).
- 16** Log on to the Domain Controller using your Active Directory account that is a member of the Domain Admins group.
 The account name set up by Motorola Solutions is “motosec”.
 The domain administrator desktop appears.
- 17** Open PowerShell.
- 18** In the **PowerShell** window, enter:
- a** `cd C:\Program Files\Motorola\AstroDC\common\scripts`
 - b** `.\ConfigHostDefaultIPs.ps1`
 - c** `.\ConfigDNSSearchList.ps1`
 - d** When the script exits with 0, restart the Domain Controller.
- 19** Validate successful disaster recovery of the Domain Controller.
 See [Validating Successful Disaster Recovery on page 198](#).

14.1.2

Recovering a Domain Controller Using Reinstall

This is a secondary restore method.

During various stages of the installation, several reboots occur, prompting the user to log on. The user needs to repeatedly log on to the Domain Controller for the installation to be completed.

For troubleshooting information, see [General Troubleshooting for AD/DNS on page 152](#).

Prerequisites: Ensure to delete the failed Domain Controller virtual machine from the virtual server. For all user input information, such as passwords or hostnames, see [Table 8: User Input Requirements – Domain Controller Configuration on page 75](#).

Process:

- 1 If reinstalling the first system-level Domain Controller, see [Seizing FSMO Roles on page 177](#).
- 2 Clean up obsolete Domain Controller objects.
See [Deleting a Domain Controller Server Object in a Domain on page 179](#).
Cleans up objects related to the failed Domain Controller that might exist in the Domain Controllers that are online.
Step example: If the first zone-level Domain Controller fails, this procedure can be performed on the first system-level Domain Controller; if the system-level DC fails, it can be performed on zone-level DC.
- 3 Clean up Active Directory sites and services:
 - a Log on to the Domain Controller that is online using the “motosec” account.
 - b From **Start**, click **Search**.
 - c In the search field, type in `administrative`
 - d Click **Administrative Tools**.
 - e In the **Administrative Tools** window, double-click **Active Directory Sites and Services**.
 - f In the **Active Directory Sites and Services** window, expand **Sites**, then **Zone** (to which the failed Domain Controller belongs), and **Servers**.
 - g In the left pane, right click the server name of the failed Domain Controller and click **Delete**.
 - h In the confirmation window, click **Yes**.The Cleanup of Sites and Services is complete.
- 4 If reinstalling the first system-level Domain Controller, see [Seizing Active Directory Lightweight Directory Services \(AD LDS\) FSMO Roles on page 179](#).
- 5 Clean up obsolete AD LDS object. See [Deleting an AD LDS Server Object in an AD LDS Configuration Set on page 181](#).
Cleans up AD LDS instance object related to the failed Domain Controller that is referenced in the Domain Controllers that are online.
Step example: If the first zone-level Domain Controller fails, this procedure can be performed on the first system-level Domain Controller. If the system-level Domain Controller fails, it can be performed on zone-level Domain Controller.
- 6 Ensure that the ESXi-based virtual server hosting the Domain Controller virtual machine is working properly. See the *Virtual Management Server Software* manual.
- 7 Import the Domain Controller virtual machine.
See [Importing the Domain Controller Virtual Machine on page 59](#).
- 8 Configure Virtual Machine resources.
See [Configuring Virtual Machine Resources on page 61](#).
- 9 Apply supplemental configuration to the ESXi server-based Virtual Machine.

See [Applying Supplemental Configuration to Virtual Machines on page 62](#).

10 Only for systems with vCenter already installed: Configure vCenter.

See [Configuring the vCenter for the Newly Deployed VM on page 63](#).

11 Set the Virtual Machine startup and shutdown order.

See “Setting the Virtual Machine Startup and Shutdown Order” in the *Virtual Management Server Software* manual.

12 Connect and power on a virtual machine.

See [Connecting and Powering on a New Virtual Machine on page 64](#).

13 Apply OS-level identity.

See [Applying OS-Level Identity on the Domain Controller on page 65](#).

14 Configure a Domain Controller virtual machine.

See [Activating a Domain Controller Virtual Machine on page 66](#).

15 Install the Domain Controller MSI:

- a** Log on to the Domain Controller using the local administrator account (“Administrator”).

The administrator's desktop appears.

- b** Insert the *Domain Controller Plugin* media and navigate to the drive.

- c** Double-click **ADC_RXX.XX.XX.msi** to install the DC scripts to the following location:

C:\Program Files\Motorola\AstroDC.

Domain controller MSI installation takes a couple of seconds. It does not require any user interaction.

If no window appears, the installation is successfully finished.

16 Open PowerShell:

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

- b** In the search field, type in `powershell`

- c** Click **Windows PowerShell**.

17 In the **Windows PowerShell** window, enter one of the following commands:

If...	Then...
The Centralized Event Logging Server is not available in the system,	<p>Enter:</p> <pre>C:\Program Files\Motorola\AstroDC\common\scripts \ReinstallDC.ps1 -interactive -noSyslogCli -rootDC <DC- FQDN> -hostname <DC hostname></pre> <p>where:</p> <ul style="list-style-type: none"> <DC-FQDN> is the Domain Controller which takes the FSMO roles <DC hostname> is one of the following values: <ul style="list-style-type: none"> For system-level DC in the primary core: <code>ucs-dc01</code> For system-level DC in the backup core (DSR systems only): <code>ucs-dc03</code> For zone-level DC in the primary core: <code>z<ZZZ>dc01</code> For zone-level DC in the backup core (DSR systems only): <code>z<ZZZ>dc03</code>

If...	Then...
	<ul style="list-style-type: none"> For zone-level DC at a site: z<ZZZ>nmd<SSS>dc<NN> For Tsub prime site DC: z00<X>s<PPP>dc01 <p>where:</p> <p><ZZZ> is the zone number</p> <p><SSS> is the site number</p> <p><NN> is the Domain Controller number</p> <p><PPP> is the prime site number</p>
The Centralized Event Logging Server is available in the system,	<p>Enter:</p> <pre>C:\Program Files\Motorola\AstroDC\common\scripts \ReinstallDC.ps1 -interactive -rootDC <DC-FQDN> - hostname <DC hostname></pre> <p>where:</p> <p><DC-FQDN> is the Domain Controller which takes the FSMO roles</p> <p><DC hostname> is one of the following values:</p> <ul style="list-style-type: none"> For system-level DC in the primary core: ucs-dc01 For system-level DC in the backup core (DSR systems only): ucs-dc03 For zone-level DC in the primary core: z<ZZZ>dc01 For zone-level DC in the backup core (DSR systems only): z<ZZZ>dc03 For zone-level DC at a site: z<ZZZ>nmd<SSS>dc<NN> For Tsub prime site DC: z00<X>s<PPP>dc01 <p>where:</p> <p><ZZZ> is the zone number</p> <p><SSS> is the site number</p> <p><NN> is the Domain Controller number</p> <p><PPP> is the prime site number</p>

18 At the prompt, enter the *<Admin Restore password>*.

This is the Directory Service Restore password, set during installation/reinstallation, typically the same password as the “motosec” account password.

The password must be at least 14 characters long and must have three out of the following four characteristics:

- At least one upper case letter (A-Z)
- At least one lower case letter (a-z)
- At least one number (0-9)
- At least one of the following symbols: hyphen (-), underscore (_), dollar (\$), pound/hash (#)

19 Depending on the location of the Domain Controller, perform one of the following actions:

If...	Then...
If you are reinstalling the first system-level Domain	perform the following actions:

If...	Then...
<p>Controller or backup system-level Domain Controller,</p>	<p>a At the prompt, enter the <i><ucs colocated zone #></i> for the backup core where <i><#></i> is a number from 1 to 7.</p> <p>b At the prompt, enter the <i><AD domain admin password></i> AD domain administrator password was set while installing the first system-level Domain Controller. It is the password set for the local administrator in the system-level DC. The password must be at least 14 characters long and must have three out of the following four characteristics:</p> <ul style="list-style-type: none"> • At least one upper case letter (A-Z) • At least one lower case letter (a-z) • At least one number (0-9) • At least one of the following symbols: hyphen (-), underscore (_), dollar (\$), pound/hash (#) <p>c At the prompt, enter the local <i><administrator password></i> twice. If the password is wrong, you are prompted to click OK during every reboot and to reenter the local administrator password on the logon screen. Local administrator account is renamed from “Administrator” to “motosec”.</p> <p>d Wait for the DC to restart a few times.</p> <p>e Go to the dcinstall log at C:\Windows\debug and ensure that ReInstalldcpromo.ps1 exits with 1641. The 1641 message means that operation was successful.</p> <p>f Continue with step 20.</p>
<p>If you are reinstalling one of the following Domain Controllers:</p> <ul style="list-style-type: none"> • The first zone-level Domain Controller • The backup zone-level Domain Controller • The site-level Domain Controller • The Trunking Subsystem (Tsub) prime site Domain Controller 	<p>perform the following actions:</p> <p>a At the prompt, enter the <i><AD domain admin password></i> twice. AD domain administrator password was set while installing the first system-level Domain Controller. It is the password set for the local administrator in the system-level DC. The password must be at least 14 characters long and must have three out of the following four characteristics:</p> <ul style="list-style-type: none"> • At least one upper case letter (A-Z) • At least one lower case letter (a-z) • At least one number (0-9)

If...	Then...
	<ul style="list-style-type: none"> • At least one of the following symbols: hyphen (-), underscore (_), dollar (\$), pound/hash (#) <p>b At the prompt, enter the local <i><administrator password></i> twice.</p> <p>If the password is wrong, you are prompted to click OK during every reboot and to reenter the local administrator password on the logon screen.</p> <p>Local administrator account is renamed from “Administrator” to “motosec”.</p> <p>c Wait for the DC to restart a few times.</p> <p>d Go to the dcinstall log at C:\Windows\debug and ensure that ReInstallDcpromo.ps1 exits with 1641.</p> <p>The 1641 message means that operation was successful.</p> <p>e Continue with step 20.</p>

20 Depending on the location of the Domain Controller, perform the following actions:

- a** Launch the PowerShell command prompt.
- b** Change directory to: C:\Program Files\Motorola\AstroDC
- c** At the prompt, enter one of the following commands:
 - For the system-level DC:
WindowsInstallFramework.exe /e /i .\common\data\Reinstall_System_post_dcpromo.xml
 - For the zone-level DC:
WindowsInstallFramework.exe /e /i .\common\data\Reinstall_Zone_post_dcpromo.xml
 - For the site-level DC:
WindowsInstallFramework.exe /e /i .\common\data\Reinstall_Site_post_dcpromo.xml
 - For the Trunking Subsystem (Tsub) prime site DC:
WindowsInstallFramework.exe /e /i .\common\data\Reinstall_TSUB_post_dcpromo.xml
- d** On the UAC dialog box, enter the *<Domain Administrator account>*.
The domain administrator name is “motosec”.
- e** On the UAC dialog box, enter the *<AD domain admin password>*
The password must be at least 14 characters long and must have three out of the following four characteristics:
 - At least one upper case letter (A-Z)
 - At least one lower case letter (a-z)
 - At least one number (0-9)
 - At least one of the following symbols: hyphen (-), underscore (_), dollar (\$), pound/hash (#)

21 When the system reboots, log on for the installation to continue.

If installation of the dcpromo fails, it is possibly because some of the cleanup has not been synchronized to all the Domain Controllers in the system. Wait for 30 minutes to retry.

The post dcpromo installation continues. A message states that the Domain Controller installation finished.

22 Transfer FSMO roles.

See [Transferring FSMO Roles on page 178](#).

After the Domain Controller is reinstalled, some errors may appear until the synchronization is complete.

23 Transfer FSMO roles of AD LDS to UCS DC01.

See [Transferring AD LDS FSMO Roles on page 183](#).

24 Only when a zone-level Domain Controller is recovered by reinstall: Recover RADIUS configuration and data.

See [Recovering RADIUS Configuration on page 199](#).

The Active Directory data (that also contains the DNS data) is replicated to the Domain Controller that is reinstalled, but the RADIUS data is lost for a zone when a zone-level Domain Controller is rebuilt.

25 Re-deploy McAfee to the Domain Controller.

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

14.2

Validating Successful Disaster Recovery

Prerequisites: Depending on the date of the backup, replication of domain controllers might take from 1/2 hour to 1 hour, so it is required that ample time is allowed before going through this procedure.

Procedure:

- 1** Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.
The account name set up by Motorola Solutions is “motosec”.
The domain administrator desktop appears.
- 2** Validate that you are able to launch the users and computers without any errors and verify if the users and groups are present:
 - a** From **Start**, click **Search**.
 - b** In the search field, type in `administrative`
 - c** Click **Administrative Tools**.
 - d** In the **Administrative Tools** window, double-click **Active Directory Users and Computers**.
The **Active Directory Users and Computers** window appears.
- 3** Launch the **Network Policy Server** console to make sure that RADIUS clients are present:
 - a** From **Start**, click **Search**.
 - b** In the search field, type in `administrative`
 - c** Click **Administrative Tools**.

- d In the **Administrative Tools** window, double-click **Network Policy Server**.
The **Network Policy Server** window appears.
- 4 Launch the **DNS** console and validate if the DNS zones are loaded and running:
 - a From **Start**, click **Search**.
 - b In the search field, type in `administrative`
 - c Click **Administrative Tools**.
 - d In the **Administrative Tools** window, double-click **DNS**.
The **DNS Manager** window appears.
- 5 To validate that the DNS service is up, perform DNS lookups:
 - a From **Start**, click **Search**.
 - b In the search field, enter: `cmd`
 - c At the command prompt, enter: `nslookup <FQDN of the DC>`
 - d At the command prompt, enter: `nslookup <IP Address of the server>`
- 6 At the command prompt, perform the following actions:
 - a Enter: `dcdiag`
 - b Diagnose the result.
Success messages appear.
- 7 Perform the following actions:
 - a From **Start**, click **Search**.
 - b In the search field, type in `powershell`
 - c Click **Windows PowerShell**.
 - d At the PowerShell prompt, enter:

```
& 'C:\Program Files\Motorola\AstroDC\Common\scripts
\VerifyReplicationStatus.ps1'
```
 - e Diagnose the result.
Success messages appear.

Postrequisites:

NOTICE: If the script shows that the replication is not completed yet, wait another 30 minutes to run the script again.

14.3**Recovering RADIUS Configuration**

When and where to use: The procedure is required only if recovering a zone-level domain controller. To recover RADIUS data on a system-level DC, run `TriggerRADIUSREplication.ps1` on a zone domain controller in every zone.

Procedure:

- 1 Log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.

The account name set up by Motorola Solutions is “motosec”.

The domain administrator’s desktop appears.

2 In Windows Explorer, go to `C:\Windows\SYSVOL\domain\RADIUS_REPL.`

3 Copy the `.xml` file which matches the **<DC hostname>**.

Step example: If you are reinstalling the first zone-level domain controller, copy the `z001dc01.zone1.xml` file.

See [Table 8: User Input Requirements – Domain Controller Configuration on page 75](#) for DC hostname details.

4 Paste the `.xml` file to the `C:\` location.

5 Open PowerShell:

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

b In the search field, type in `powershell`

c Click **Windows PowerShell**.

6 In the **PowerShell** window, enter: `netsh nps import filename
="C:\<filename>.xml"`

where **<filename>** is the `.xml` file that matches the hostname of the domain controller, for example: `z001dc01.zone1`

A message states that the configuration was successfully imported to the NPS server.

7 Delete the file from the `C:\` location.

Appendix A

EMC Smarts Quick Reference

This chapter provides brief instructions for using the Configlet Editor in the EMC Smarts™ Network Configuration Manager component of the Unified Network Configurator (UNC) for modifying the configuration of devices in an ASTRO® 25 system.

For more information on EMC Smarts™, and for additional ways to use the Configlet Editor, see the *Unified Network Configurator* manual.

A.1

Config and Configlet Editors

Config and Configlet Editors are two possible ways to construct configuration files. The Config Editor is designed for editing a single, full configuration that affects one or more devices. The editor allows opening one or more instances of the Config Editor for multiple devices. Use the Configlet Editor to edit partial configurations that are pushed to the network. When selecting a single device, one editor window opens. When selecting more than one device, the single editor session contains the selected devices listed in the **Devices** column.

Access the editors from the menu bar (shown in the Devices View in table format). The other way is by right-clicking on any device on the EMC Smarts™ Network Configuration Manager dashboard, then selecting **Editor**.

Each editor is connected to the scheduler, allowing you to set the date and time, and the sequence of each job task.

The editors feature specific and common fields on their GUI. In most cases, first choice option is the **Specific** field. It lets you choose to which configuration units you want to send the data. A common configlet pushes the configuration down to all configuration units for a given device. An example where the common configlet might be used is a router that has startup and running configuration units whose configurations must be consistent.

The Config Editor:

- Provides an area for contextual editing of the device config file.
- Allows the comparison of device config.
- Opens with a selected device config in the editor, or opens multiple windows for selected devices simultaneously.
- Expands or collapses the editor area for additional real estate.
- Contains pre-defined locators in the navigation pane.
- Uses the Find and Replace feature to quickly locate single or string alphanumeric data.

The Configlet Editor:

- Allows taking pieces of configuration code or templates that are less than a complete configuration file, but equal to one or more commands.
- Allows scheduling configlets to be pushed to one or more devices in a network.
- Opens with no configuration displayed: enables making the same change to one or more devices; then scheduled for push at the same time.



NOTICE: In most cases, the Configlet Editor is the preferred method for editing device configuration files.

A.2

Updating the EMC Smarts Network Configuration Manager Credentials for a Device

When and where to use: Use this procedure to update the EMC Smarts™ Network Configuration Manager credentials for a device.

Procedure:

- 1 Log on to the EMC Smarts™ Network Configuration Manager as the network administrator.
- 2 On the left side of the EMC Smarts™ Network Configuration Manager main window, select **Networks**→**Astro 25 Radio Network**.
- 3 Double-click **Devices**.
A list of devices appears on the right side of the window.
- 4 Right-click a device from the device list. Select **Properties**.
- 5 From the **Properties** tab of the **Device Properties** window, select the **Communication** tab. Click **Update Credentials**.
- 6 Select the new credentials under **Management**.
- 7 Select the new credentials under the **Simple Network Management Protocol (SNMP)**.
- 8 Select the new credentials under the **Cut-Through**.
- 9 Save all the changes in the EMC Smarts™ Network Configuration Manager by clicking **Save Only**.

A.3

Scheduling Jobs

When and where to use: Use this procedure to schedule jobs.

Procedure:

- 1 Click **Schedule** at the bottom of an editor window.

Figure 12: Schedule Job Window



NOTICE: The **Schedule Job** tab permits setting the priority for the job and specifying when to perform the job.

The **Schedule Job** window appears.

- 2 Enter the job name in the relevant field.
- 3 In the **Job Details** section of the window, enter the following:
 - a Job Name.
 - b Job Owner. The Job Owner should reflect the name of the user who logged on.
 - c Description, if needed.
 - d Priority level. Select among Low, Medium, or High priority.
- 4 In the **Schedule Job** section of the window, perform the following actions:
 - a Select the run method. Choose between four options: **Run in the next maintenance window**, **Run upon approval**, **Run upon operator initiation**, or **Run at scheduled date/time**.



NOTICE: In the schedule job section, by default, all jobs are scheduled to run upon approval. With adequate permissions, click either the **Approve & Submit** button or the **Submit** button at the bottom of the window, depending on your permission level.



NOTICE: If the **Run upon operator initiation** option has been selected, and then **Submit for approval**, which keeps the job in a pending state after approval, any user with schedule permissions can then execute this job.

- b Select **Run as recurring series** to set a recurring schedule. The recurring setting options are then activated.
- c Set the following recurring options: **Frequency**, **Start and End Times**, and **Time Interval**.



NOTICE: When the recurring schedule is selected, the new time zone drop-down options are available. Make your selection from the drop-down options. The time zone selected must be the client's time zone. The new time zone field propagates with the client time zone automatically when creating a **Maintenance** window or a recurring scheduled job.

- 5 Click the **Tasks** tab.

Figure 13: Tasks Tab Fields

Schedule Job

Schedule Job **Tasks** Notification

☐ Preserve order ☒ Task Details

Task List

Device Name / Action	Destination	Mechanism	Post Operation	Pull After Push
2650		In-Band		Pull Configs
Push - Configlet (runni...	running-configur...	TELNET	Copy to Start	...

NOTE: Selected Mechanism affects only the push action, any pull will use the Primary Mechanism settings from the device.

Delete Up Down

Content: Configlet for running, Device Name: 2650

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17

Approve & Submit Submit Cancel

The Tasks tab appears.

- 6 Select the appropriate values.

Various choices are given in the **Destination**, **Post Operation**, and **Pull After Push** columns, depending on the device and the type of job, config or configlet.

Destination: Classification for how to process the configuration, typically as a full initialization or an incremental change. Values vary per device type and whether the job is a config or configlet.

For configlet operations which are the incremental variety, only one is selected by default.

For config operations which are full configuration variety, choose the startup configuration equivalent.

Mechanism: Communication protocol used for the job. The value of this setting is selected from the Device communication properties at the time of the job creation. If a device Mechanism is

changed after job creation, but before job execution, the job may fail due to stale mechanism. If this occurs, either update the job mechanism or re-create the job.

Post Operation: Tasks to perform after the push is completed.

- **Copy To Start** is a configlet job option designed for devices that support a running and startup configuration. If a device does not support this concept, then it is not configurable. If **Copy to Start** is selected, the change persists in the event the device is reset.
- **Reboot** is a config job option that varies by device type. If the option is checked, the device will reboot.



IMPORTANT: HP Procurve Switch automatically reboots when pushing to startup and there is no option to disable it.

Pull After Push: Controls what information is automatically pulled after the push job completes. It is recommended to keep the default setting to retain a meaningful history of operations.

- 7 Click either **Approve & Submit** or the **Submit**, depending on your permission level.



NOTICE:

- If clicking **Approve & Submit**, the Schedule Job window closes. The job status can be viewed using the Schedule Manager available from the **Tools** menu in the EMC Smarts™ Network Configuration Manager main window.
- If clicking **Submit**, the status of the job is Pending. Approve Pending jobs in the **Schedule Manager** window.

The system runs the updated configuration. If you clicked **Approve & Submit**, the **Schedule Job** window closes. The job status can be viewed using the Schedule Manager available from the **Tools** menu. If you clicked **Submit**, the status of the job is pending. Approve pending jobs in the **Schedule Manager** window.

Appendix B

Embedded Password Management

This chapter explains the embedded password management functionality in an ASTRO® 25 system.

B.1

Embedded Password Management Overview

Different ASTRO® 25 system applications and administrative scripts use embedded accounts to communicate with other applications, such as databases and LDAP servers. 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.

All write operations performed on the embedded passwords database require administrative privileges. The pwvadmin operations may be invoked by a root user or a domain user belonging to the secadm group on Unix and by a local administrator on Windows.



NOTICE: The command line interface is used for operations performed on the embedded passwords database.

Application groups may be specified for applications on a given device. If an application group is specified, the embedded passwords management commands need to include the application group parameter.



IMPORTANT: The procedures in this chapter are only recommended if your organization has higher assurance needs whose policies mandate regular maintenance of the passwords and keys.

B.2

Modifying the Embedded Password on a Device

Prerequisites: Obtain one of the following:

- Credentials for an account that is a member of the secadm group in the Active Directory (Windows or Unix-based devices)
- Password for the local root account (Unix-based devices)
- Password for the local administrator account (Windows-based devices)

For Key Management Facility (KMF) Server, KMF Client, and KMF CryptR: since KMF does not join the ASTRO® 25 system Active Directory domain, embedded passwords on the KMF can be modified by users who log on with the appropriate local account: “Administrator” or “motosec” for KMF Server and Client, and “admin” for KMF CryptR. See the *Key Management Facility User Guide* and the *KMF CryptR User Guide*.

For devices belonging to the STM application group: if the procedure is going to be performed on multiple interdependent devices belonging to the STM application group, see the details regarding STM application group considerations in [STM Application Group Considerations on page 224](#).

For MKM 7000 Console Alias Manager (CAM) Server: before performing the procedure on MKM 7000 Console Alias Manager (CAM) Server, stop the CAM Service using the CAM Configuration Utility. For more information refer to the *MKM 7000 Console Alias Manager* manual.

When and where to use: Modifying the embedded password on a device should be performed on the system according to your organization's specific operational policies.

For information regarding the procedure which need to be performed to modify the embedded password for an appropriate embedded account on a specific device, see [Embedded Password Management Variables and Procedures on page 209](#).

Modifying embedded passwords on some devices requires coordination across the impacted devices. The coordination is required due to one of the devices accessing password protected data or services on another device. The password synchronization is needed to prevent operational failure. See [Embedded Password Management Variables and Procedures \(Interdependent Devices\) on page 217](#) for a list of interdependent devices on which the password modification needs to be synchronized.

Procedure:

- 1 Run the command prompt window for the device.

- 2 Enter:

```
pwvadmin changeproperty -property <embedded account name> [-app
<application group name>]
```

No line breaks are needed in the command.

Information regarding the <embedded account name> and the <application group name> is provided in [Table 19: Embedded Password Management Variables and Procedures on page 209](#) and [Embedded Password Management Variables and Procedures \(Interdependent Devices\) on page 217](#).



IMPORTANT: If the application group name is not given, do not specify the -app variable (the default application group name is used).
For Unix, the full path to the command is needed.

If a command line user input value, for example, embedded account name or application group name contains special characters, the value should be placed in single quotation marks in Unix and in double quotation marks in Windows. In Unix, use `sudo`, rather than `esudo` with these user input values.

Step example:

- For Windows, see [Figure 14: Pwvadmin changeproperty Example on page 207](#).
- For Unix (root):
`/opt/Motorola/PWVault/bin/pwvadmin changeproperty -property AFFUSER -app STM`
- Unix (domain account - secadm):
`sudo /opt/Motorola/PWVault/bin/pwvadmin changeproperty -property '$ZONEWATCH' -app STM`

See the following figure for an example of modifying the embedded password.

Figure 14: Pwvadmin changeproperty Example



- 3 At the prompt, enter the new password.

For password strength guidelines, refer to your organization's policies. The password must have at least 8 characters and not exceed 1024 characters in length. For Windows-based devices, the password complexity needs to meet Microsoft default password complexity rules. For

information regarding password complexity rules on Linux and Solaris-based devices, see the sections “Changing the Root Account Password for a Linux-Based Device” and “Changing the Root Account Password for a Solaris-Based Device” in the *Unix Supplemental Configuration* manual.

- 4 At the confirmation prompt, reenter the password.

A message states that the value of property was modified successfully.

Postrequisites: After embedded passwords are modified, it is important to back them up to minimize system downtime in a recovery scenario. For information regarding backup and restore of embedded passwords, see [Embedded Password Backup and Restore on page 225](#).

B.3

Rotating the Encryption Keys

Encryption keys are used to secure the embedded passwords. This procedure is only recommended if your organization has higher assurance needs whose policies mandate regular maintenance of the passwords and keys.

Prerequisites: Obtain one of the following:

- Credentials for an account that is a member of the secadm group in the Active Directory (Windows or Unix-based devices)
- Password for the local root account (Unix-based devices)
- Password for the local administrator account (Windows-based devices)

For Key Management Facility (KMF) Server, KMF Client and KMF CryptR: since KMF does not join the ASTRO® 25 system Active Directory domain, embedded passwords on the KMF can be modified by users who log on with the appropriate local account: “Administrator” or “motosec” for KMF Server and Client, and “admin” for KMF CryptR. See the *Key Management Facility User Guide* and the *KMF CryptR User Guide*.

Procedure:

- 1 Run the command prompt window for the device.
- 2 Enter one of the following commands:
 - To create a new key for a specific application group: `pwvadmin rotateappkey [-app <application group name>]`
 - To create new keys for all application groups (a different key for each application group):
`pwvadmin rotateallkeys`

Information regarding the `<application group name>` for the account is provided in [Table 19: Embedded Password Management Variables and Procedures on page 209](#) and [Embedded Password Management Variables and Procedures \(Interdependent Devices\) on page 217](#).



IMPORTANT:

If the application group name is not given, do not specify this variable (the default application group name is used).

For Unix, the full path to the command is needed.

If the application group name contains special characters, it should be placed in single quotation marks in Unix and in double quotation marks in Windows.

Step example:

- For Windows: `pwvadmin rotateappkey -app ssl_client_group`
- For Unix (root): `/opt/Motorola/PWVault/bin/pwvadmin rotateappkey -app NM_CAM`

- For Unix (domain account - secadm): `sudo /opt/Motorola/PWVault/bin/pwvadmin rotateallkeys`

A message states that the key or keys were rotated successfully.

B.4

Embedded Password Management Variables and Procedures

The following table shows account names and application group names to be used with the pwvadmin command and provides links to procedures which should be applied to modify the embedded password on a single device.

For account names and application group names to be used on interdependent devices, see [Embedded Password Management Variables and Procedures \(Interdependent Devices\)](#) on page 217.


Table 19: Embedded Password Management Variables and Procedures

Device	Account Name	Application Group Name	Procedures to Modify the Embedded Passwords
Air Traffic Router (ATR)	AFFUSER	STM	Modifying the Embedded Password on a Device on page 206
ATR	AGNTUSER	STM	Modifying the Embedded Password on a Device on page 206
ATR	AGNTCERTUSER	STM	Modifying the Embedded Password on a Device on page 206
ATR	DSSAUSER	STM	Modifying the Embedded Password on a Device on page 206
ATR	EDDIAGT_CERT_USER	STM	Modifying the Embedded Password on a Device on page 206
ATR	EDDIAGT_DB_USER	STM	Modifying the Embedded Password on a Device on page 206
ATR	JMS_AFFSERV	STM	Before performing Modifying the Embedded Password on a Device on page 206 , disable the ATR. After changing the password, ATR can be enabled. See “Disabling PNM Server Applications” in the <i>Private Network Management Servers</i> manual.
ATR	JMS_ATRAGT	STM	Modifying the Embedded Password on a Device on page 206

Device	Account Name	Application Group Name	Procedures to Modify the Embedded Passwords
ATR	JMS_DSSA	STM	Before performing Modifying the Embedded Password on a Device on page 206 , disable the ATR. After changing the password, ATR can be enabled. See “Disabling PNM Server Applications” in the <i>Private Network Management Servers</i> manual.
ATR	JMS_EDDIAGT	STM	Before performing Modifying the Embedded Password on a Device on page 206 , disable the ATR. After changing the password, ATR can be enabled. See “Disabling PNM Server Applications” in the <i>Private Network Management Servers</i> manual.
ATR	JMS_NEMI	STM	Modifying the Embedded Password on a Device on page 206
ATR	JMS_RAPI	STM	Before performing Modifying the Embedded Password on a Device on page 206 , disable the ATR. After changing the password, ATR can be enabled. See “Disabling PNM Server Applications” in the <i>Private Network Management Servers</i> manual.
ATR	JMS_STATS	STM	Before performing Modifying the Embedded Password on a Device on page 206 , disable the ATR. After changing the password, ATR can be enabled. See “Disabling PNM Server Applications” in the <i>Private Network Management Servers</i> manual.
ATR	JMS_TEMPEST	STM	Before performing Modifying the Embedded Password on a Device on page 206 , disable the ATR. After changing the password, ATR can be enabled.

Device	Account Name	Application Group Name	Procedures to Modify the Embedded Passwords
			bled. See “Disabling PNM Server Applications” in the <i>Private Network Management Servers</i> manual.
ATR	LICHANDLER	STM	Modifying the Embedded Password on a Device on page 206
ATR	mcadi	STM	Modifying the Embedded Password on a Device on page 206
ATR	RAPI_PROXY_CERT_USER	STM	Modifying the Embedded Password on a Device on page 206
ATR	RCMCLEANUP	STM	Modifying the Embedded Password on a Device on page 206
ATR	STATMEASUSER	STM	Modifying the Embedded Password on a Device on page 206
ATR	STMAPPAUTH	STM	Modifying the Embedded Password on a Device on page 206
ATR	TEMPESTUSER	STM	Modifying the Embedded Password on a Device on page 206
ATR	WILDFLYDBUSER	STM	Before performing Modifying the Embedded Password on a Device on page 206 , disable the ATR. After changing the password, ATR can be enabled. See “Disabling PNM Server Applications” in the <i>Private Network Management Servers</i> manual.
ATR	WILDFLYJMSUSER	STM	Before performing Modifying the Embedded Password on a Device on page 206 , disable the ATR. After changing the password, ATR can be enabled. See “Disabling PNM Server Applications” in the <i>Private Network Management Servers</i> manual.

Device	Account Name	Application Group Name	Procedures to Modify the Embedded Passwords
Authentication Center (AuC) Server	ssl_agent_account	ssl_agent_group	Modifying the Embedded Password on a Device on page 206
AuC Server	ssl_server_account	ssl_server_group	Modifying the Embedded Password on a Device on page 206
Core Security Management Server (CSMS)	csmsadmin	CSMS_admin_group	Modifying the Embedded Password on a Device on page 206
CSMS	epoadmin	CSMS_admin_group	Modifying the Embedded Password on a Device on page 206
Key Management Facility (KMF) Server	cryptr_officer	kmf_server_group	“Changing KMF CryptR Embedded Passwords on the KMF Server and KMF Standby Server” in the <i>Key Management Facility User Guide</i> .
KMF Server	cryptr_usr	kmf_server_group	“Changing KMF CryptR Embedded Passwords on the KMF Server and KMF Standby Server” in the <i>Key Management Facility User Guide</i> .
KMF Server	ssl_server	kmf_server_group	“Changing KMF CryptR Embedded Passwords on the KMF Server and KMF Standby Server” in the <i>Key Management Facility User Guide</i> .
MKM 7000 Console Alias Manager (CAM) Server	cacertsPass	CAM	Modifying the Embedded Password on a Device on page 206
MKM 7000 CAM Server	cam.service.password	CAM	Modifying the Embedded Password on a Device on page 206
MKM 7000 CAM Server	camdbuser	CAM	Before performing Modifying the Embedded Password on a Device on page 206 , stop the CAM Service using the CAM Configuration Utility. See the <i>MKM 7000 Console Alias Manager</i> manual.
MKM 7000 CAM Server	javax.net.ssl.keyStore-Password	CAM	Modifying the Embedded Password on a Device on page 206

Device	Account Name	Application Group Name	Procedures to Modify the Embedded Passwords
Private Network Management (PNM) Client	AFFICIENT	STM	Modifying the Embedded Password on a Device on page 206 STM Application Group Considerations on page 224
PNM Client	java.cacerts.truststore	PNM	Modifying the Embedded Password on a Device on page 206
User Configuration Server (UCS)	activemqadmin	PM	Modifying the Embedded Password on a Device on page 206
UCS	astrocmuser	PM	Account used by ZDS to connect to the UCS database. Before performing Modifying the Embedded Password on a Device on page 206 , disable the ZDS. After changing the password, ZDS can be enabled. See “Disabling PNM Server Applications” in the <i>Private Network Management Servers</i> manual.
UCS	pmuser	PM	Modifying the Embedded Password on a Device on page 206  NOTICE: The UCS server has to be enabled while running the procedure. After changing the password, disable and re-enable the UCS server. For more information, see the <i>Private Network Management Servers</i> manual.
UCS	ucs_ads_eddiv2_link	PM	Modifying the Embedded Password on a Device on page 206

Device	Account Name	Application Group Name	Procedures to Modify the Embedded Passwords
Unified Network Configurator (UNC)	intloc-db-user	unc	Modifying the Embedded Password on a Device on page 206
UNC	keystorepass	ncr	Modifying the Embedded Password on a Device on page 206
UNC	tuc-db-user	unc	Modifying the Embedded Password on a Device on page 206
Zone Controller (ZC)	adsuser	ZC_NM_DB	Modifying the Embedded Password on a Device on page 206
ZC	jms_clientuser_pass	ZC_NM_DB	Modifying the Embedded Password on a Device on page 206
ZC	motoagt	ZC_NM_DB	Modifying the Embedded Password on a Device on page 206
Zone Database Server (ZDS)	ads_eddi	NMClassic	Before performing Modifying the Embedded Password on a Device on page 206 , disable the ZDS. After changing the password, ZDS can be enabled. See “Disabling PNM Server Applications” in the <i>Private Network Management Servers</i> manual.
ZDS	adsdbencryptionkey	NMClassic	Before performing Modifying the Embedded Password on a Device on page 206 , disable the ZDS. After changing the password, ZDS can be enabled. See “Disabling PNM Server Applications” in the <i>Private Network Management Servers</i> manual.
ZDS	adsdbpassword	NMClassic	Before performing Modifying the Embedded Password on a Device on page 206 , disable the ZDS. After changing the password, ZDS can be enabled. See “Disabling PNM Server Applications” in the <i>Private Network Management Servers</i> manual.

Device	Account Name	Application Group Name	Procedures to Modify the Embedded Passwords
ZDS	adsdbuser	NMClassic	Before performing Modifying the Embedded Password on a Device on page 206 , disable the ZDS. After changing the password, ZDS can be enabled. See “Disabling PNM Server Applications” in the <i>Private Network Management Servers</i> manual.
ZDS	auc	NMClassic	Before performing Modifying the Embedded Password on a Device on page 206 , disable the ZDS. After changing the password, ZDS can be enabled. See “Disabling PNM Server Applications” in the <i>Private Network Management Servers</i> manual.
ZDS	ddisynch	NMClassic	Before performing Modifying the Embedded Password on a Device on page 206 , disable the ZDS. After changing the password, ZDS can be enabled. See “Disabling PNM Server Applications” in the <i>Private Network Management Servers</i> manual.
ZDS	dr-dj	NMClassic	Before performing Modifying the Embedded Password on a Device on page 206 , disable the ZDS. After changing the password, ZDS can be enabled. See “Disabling PNM Server Applications” in the <i>Private Network Management Servers</i> manual.
ZDS	jddi_eddi	NMClassic	Before performing Modifying the Embedded Password on a Device on page 206 , disable the ZDS. After changing the password, ZDS can be enabled. See “Disabling PNM Server Applications” in

Device	Account Name	Application Group Name	Procedures to Modify the Embedded Passwords
			the <i>Private Network Management Servers</i> manual.
ZDS	keystore	NMClassic	Before performing Modifying the Embedded Password on a Device on page 206 , disable the ZDS. After changing the password, ZDS can be enabled. See “Disabling PNM Server Applications” in the <i>Private Network Management Servers</i> manual.
ZDS	report_ads_eddiv2_link	NMClassic	Before performing Modifying the Embedded Password on a Device on page 206 , disable the ZDS. After changing the password, ZDS can be enabled. See “Disabling PNM Server Applications” in the <i>Private Network Management Servers</i> manual.
ZDS	truststore	NMClassic	Before performing , disable the ZDS. After changing the password, ZDS can be enabled. See “Disabling PNM Server Applications” in the <i>Private Network Management Servers</i> manual.
ZDS	zc_ads_eddiv2_link	NMClassic	Before performing Modifying the Embedded Password on a Device on page 206 , disable the ZDS. After changing the password, ZDS can be enabled. See “Disabling PNM Server Applications” in the <i>Private Network Management Servers</i> manual.
ZSS	motostats	STM	This account is used by the ZSS to log into a Site Controller for Inbound RF Quality Metrics Collection file transfer. The Site Controller uses RADIUS to authenticate the ZSS.

Device	Account Name	Application Group Name	Procedures to Modify the Embedded Passwords
			Modifying the Embedded Password on a Device on page 206
ZSS	MotoZSS_auth	traces	Modifying the Embedded Password on a Device on page 206
ZSS	MotoZSS_encr	traces	Modifying the Embedded Password on a Device on page 206
ZSS	TRACESENCRYPTOR	STM_PERSISTENT	Modifying the Embedded Password on a Device on page 206

B.4.1

Embedded Password Management Variables and Procedures (Interdependent Devices)

The following tables show account names and application group names to be used with the `pwvadmin` command and provide links to procedures which should be applied to modify the embedded passwords on interdependent devices. On these devices, the embedded password modification needs to be synchronized.



NOTICE: The following tables represent **groups of devices** that have embedded password synchronization dependency. For each of the tables, when you are changing the embedded password for one device in a row, you also need to change the password for the other devices listed in this table.

Table 20: Embedded Password Management Variables and Procedures (Interdependent Devices)

Peer Devices	Account Names	Application Account Group Name	Procedures to Modify the Embedded Passwords
System Statistics Server (SSS)	SVRPTUSER	STM	Modifying the Embedded Password on a Device on page 206 STM Application Group Considerations on page 224
Air Traffic Router (ATR)	SVRPTUSER	STM	
Zone Statistics Server (ZSS)	SVRPTUSER	STM	
Private Network Management (PNM) Client	SVRPTUSER	STM	

Table 21: Embedded Password Management Variables and Procedures (Interdependent Devices)

Peer Devices	Account Names	Application Account Group Name	Procedures to Modify the Embedded Passwords
ATR	jbcliadm	STM	Modifying the Embedded Password on a Device on page 206 STM Application Group Considerations on page 224
ZSS	jbcliadm	STM	

Table 22: Embedded Password Management Variables and Procedures (Interdependent Devices)

Peer Devices	Account Names	Application Account Group Name	Procedures to Modify the Embedded Passwords
ATR	MAUSER	STM	Modifying the Embedded Password on a Device on page 206 STM Application Group Considerations on page 224
ZSS	MAUSER	STM	
SSS	MAUSER	STM	

Table 23: Embedded Password Management Variables and Procedures (Interdependent Devices)

Peer Devices	Account Names	Application Account Group Name	Procedures to Modify the Embedded Passwords
ATR	WILDFLYCERTUSER	STM	Modifying the Embedded Password on a Device on page 206 STM Application Group Considerations on page 224
ZSS	WILDFLYCERTUSER	STM	

Table 24: Embedded Password Management Variables and Procedures (Interdependent Devices)

Peer Devices	Account Names	Application Account Group Name	Procedures to Modify the Embedded Passwords
ATR	\$RCMUSER	STM	Modifying the Embedded Password on a Device on page 206 STM Application Group Considerations on page 224
UCS	\$RCMUSER	STM	

Table 25: Embedded Password Management Variables and Procedures (Interdependent Devices)

Peer Devices	Account Names	Application Account Group Name	Procedures to Modify the Embedded Passwords
ATR	atr_ads_eddiv2_link	STM	Modifying the Embedded Password on a Device on page 206
ZDS	atr_ads_eddiv2_link	NMClassic	Before performing Modifying the Embedded Password on a Device on page 206 , disable the ZDS. After changing the password, ZDS can be enabled. See “Disabling PNM Server Applications” in the <i>Private Network Management Servers</i> manual.

Table 26: Embedded Password Management Variables and Procedures (Interdependent Devices)

Peer Devices	Account Names	Application Account Group Name	Procedures to Modify the Embedded Passwords
ATR	SCHEDSERVICEUSER	STM	Modifying the Embedded Password on a Device on page 206
PNM Client	SCHEDSERVICEUSER	STM	

Table 27: Embedded Password Management Variables and Procedures (Interdependent Devices)

Peer Devices	Account Names	Application Account Group Name	Procedures to Modify the Embedded Passwords
AuC Server	ads_account	ads_group	Modifying the Embedded Password on a Device on page 206
ZDS	ads_account	NMClassic	Before performing Modifying the Embedded Password on a Device on page 206 , disable the ZDS. After changing the password, ZDS can be enabled. See “Disabling PNM Server Applications” in the <i>Private Network Management Servers</i> manual.

Table 28: Embedded Password Management Variables and Procedures (Interdependent Devices)

Peer Devices	Account Names	Application Account Group Name	Procedures to Modify the Embedded Passwords
ATR	\$ZONEWATCH	STM	Modifying the Embedded Password on a Device on page 206 STM Application Group Considerations on page 224
UCS	\$ZONEWATCH	STM	
NM Client	\$ZONEWATCH	STM	

Table 29: Embedded Password Management Variables and Procedures (Interdependent Devices)

Peer Devices	Account Names	Application Account Group Name	Procedures to Modify the Embedded Passwords
Dynamic Trans-coder	crypto_officer_password; crypto_user_password	kmf_server_group	Modifying the Embedded Password on a Device on page 206
MCC7100 IP Console	crypto_officer_password; crypto_user_password	kmf_server_group	
CryptR Micro SD Card	crypto_officer_password; crypto_user_password	kmf_server_group	“Changing KMF CryptR Embedded Passwords on the KMF Server and KMF Standby Server” in the <i>Key Management Facility User Guide</i> .
KMF CryptR	crypto_officer_password; crypto_user_password	kmf_server_group	

Table 30: Embedded Password Management Variables and Procedures (Interdependent Devices)

Peer Devices	Account Names	Application Account Group Name	Procedures to Modify the Embedded Passwords
Authentication Center (AuC) Server	admin_db_account	admin_db_group	Modifying the Embedded Password on a Device on page 206
Key Management Facility (KMF) Server	admin_db_account	admin_db_group	“Changing KMF CryptR Embedded Passwords on the KMF Server and KMF Standby Server” in the <i>Key Management Facility User Guide</i> .

Table 31: Embedded Password Management Variables and Procedures (Interdependent Devices)

Peer Devices	Account Names	Application Account Group Name	Procedures to Modify the Embedded Passwords
AuC Server	rdm_auth_client_account	rdm_auth_client_group	Modifying the Embedded Password on a Device on page 206
KMF Server	rdm_auth_client_account	rdm_auth_client_group	“Changing KMF CryptR Embedded Passwords on the KMF Server and KMF Standby Server” in the <i>Key Management Facility User Guide</i> .

Table 32: Embedded Password Management Variables and Procedures (Interdependent Devices)

Peer Devices	Account Names	Application Account Group Name	Procedures to Modify the Embedded Passwords
AuC Server	rdm_auth_account	rdm_auth_group	Modifying the Embedded Password on a Device on page 206
KMF Server	rdm_auth_account	rdm_auth_group	“Changing KMF CryptR Embedded Passwords on the KMF Server and KMF Standby Server” in the <i>Key Management Facility User Guide</i> .

Table 33: Embedded Password Management Variables and Procedures (Interdependent Devices)

Peer Devices	Account Names	Application Account Group Name	Procedures to Modify the Embedded Passwords
AuC Server	server_db_account	server_db_group	Modifying the Embedded Password on a Device on page 206
KMF Server	server_db_account	kmf_db_group	“Changing KMF CryptR Embedded Passwords on the KMF Server and KMF Standby Server” in the <i>Key Management Facility User Guide</i> .

Table 34: Embedded Password Management Variables and Procedures (Interdependent Devices)

Peer Devices	Account Names	Application Account Group Name	Procedures to Modify the Embedded Passwords
KMF Server	ssl_client	kmf_client_group	“Changing KMF CryptR Embedded Passwords on the KMF Server and KMF Standby Server” in the <i>Key Management Facility User Guide</i> .
KMF Client	ssl_client	kmf_client_group	

Table 35: Embedded Password Management Variables and Procedures (Interdependent Devices)

Peer Devices	Account Names	Application Account Group Name	Procedures to Modify the Embedded Passwords
System Statistics Server (SSS)	CSRPTUSER	STM	Modifying the Embedded Password on a Device on page 206 STM Application Group Considerations on page 224
Zone Statistics Server (ZSS)	CSRPTUSER	STM	
Private Network Management (PNM) Client	CSRPTUSER	STM	

Table 36: Embedded Password Management Variables and Procedures (Interdependent Devices)

Peer Devices	Account Names	Application Account Group Name	Procedures to Modify the Embedded Passwords
System Statistics Server (SSS)	SVBE	STM	Modifying the Embedded Password on a Device on page 206 STM Application Group Considerations on page 224
Zone Statistics Server (ZSS)	SVBE	STM	

Table 37: Embedded Password Management Variables and Procedures (Interdependent Devices)

Peer Devices	Account Names	Application Account Group Name	Procedures to Modify the Embedded Passwords
Authentication Center (AuC) Client	ssl_client_account	ssl_client_group	Modifying the Embedded Password on a Device on page 206
Authentication Center (AuC) Server	ssl_client_account	ssl_client_group	

Table 38: Embedded Password Management Variables and Procedures (Interdependent Devices)


Peer Devices	Account Names	Application Account Group Name	Procedures to Modify the Embedded Passwords
Zone Database Server (ZDS)	consoleapplplatform; ldapsecret	NMClassic	Modifying the Embedded Password on a Device on page 206
Consoles	consoleapplplatform; ldapsecret; platform_username	APP_GROUP_ RCSYNC	Modifying the Embedded Password on a Device on page 206  NOTICE: The new password will be used for future sessions, and existing sessions will not be impacted by password change.
Dynamic Trans-coder	consoleapplplatform; ldapsecret; platform_username	APP_GROUP_ RCSYNC	Modifying the Embedded Password on a Device on page 206
Group Data Gateway (GDG)	consoleapplplatform; ldapsecret; platform_username	APP_GROUP_ RCSYNC	Modifying the Embedded Password on a Device on page 206

Table 39: Embedded Password Management Variables and Procedures (Interdependent Devices)

Peer Devices	Account Names	Application Account Group Name	Procedures to Modify the Embedded Passwords
Private Network Management (PNM) Client	CERTKEYSTORE	STM	Modifying the Embedded Password on a Device on page 206 STM Application Group Considerations on page 224
MCC 7100 Consoles and MCC 7500 Consoles	CERTKEYSTORE	STM	

Table 40: Embedded Password Management Variables and Procedures (Interdependent Devices)

Peer Devices	Account Names	Application Account Group Name	Procedures to Modify the Embedded Passwords
MKM 7000 Console Alias Manager (CAM) Server	\$CAMHOSTNAME_SVCS	CAM	Modifying the Embedded Password on a Device on page 206

Peer Devices	Account Names	Application Account Group Name	Procedures to Modify the Embedded Passwords
Domain Controller (DC)	\$CAMHOSTNAME_SVCS	CAM	

Table 41: Embedded Password Management Variables and Procedures (Interdependent Devices)

Peer Devices	Account Names	Application Account Group Name	Procedures to Modify the Embedded Passwords
ZDS	svc_<{\$HOSTNAME}>*	DEFAULT_APP_GROUP_NAME	Modifying the Embedded Password on a Device on page 206
UNC	svc_{\$HOSTNAME}	DEFAULT_APP_GROUP_NAME	
UCS	svc_{\$HOSTNAME}	DEFAULT_APP_GROUP_NAME	
ATR	svc_{\$HOSTNAME}	DEFAULT_APP_GROUP_NAME	
DC	svc_{\$HOSTNAME}	DEFAULT_APP_GROUP_NAME	

* This account name is dynamically added to Active Directory during joining the domain to register the SPN of the application with Active Directory, where: <{\$HOSTNAME}> is the device hostname.

Table 42: Embedded Password Management Variables and Procedures (Interdependent Devices)

Peer Devices	Account Names	Application Account Group Name	Procedures to Modify the Embedded Passwords
Unified Network Configurator (UNC)	smc-user; mot-bat-user; mot-int-user; ncm-db-user;	unc	Modifying the Embedded Password on a Device on page 206
Unified Network Configurator Device Servers (UNCDS)	smc-user; mot-bat-user; mot-int-user; ncm-db-user;	unc	

B.4.2

STM Application Group Considerations

If embedded passwords need to be modified on multiple interdependent devices belonging to the STM application group, this is the recommended order of devices on which it should be executed:

- 1 System-level servers: SSS

2 Zone-level servers: ATR, ZSS

3 NM clients

If embedded passwords need to be modified on multiple interdependent devices belonging to the STM application group, it is recommended that the entire operation is executed as quickly as possible.

B.5

Embedded Password Backup and Restore

Devices that are centralized Backup and Restore (BAR) clients automatically include embedded passwords in that backup and restore functionality. For detailed information, see the *Backup and Restore Services* manual.

Devices that are not centralized BAR clients include embedded passwords in their device-specific backup and restore functionality. For detailed information, see the manual for the individual device.

B.6

Embedded Password Troubleshooting

Table 43: Embedded Password Troubleshooting

Problem type	Actions to take
User does not have privileges to manage embedded passwords	<ul style="list-style-type: none"> The user should be added to the <code>secadm</code> group in Active Directory, or local Windows administrator account, or use the root account for Unix. The user should be added to the embedded passwords administrator group <p>Contact the system administrator.</p>
Password management command fails if OpenSSL is not installed	<p>This error indicates a problem with the installation of the supported device. Refer to the “Troubleshooting” chapter for the individual device, in the appropriate device manual. For a list of peer devices for embedded passwords see the section Modifying the Embedded Password on a Device on page 206.</p>
Embedded password management admin operation fails with the following message: <code>Cannot lock Config file</code>	<ul style="list-style-type: none"> This message usually means that the user does not have read access to the embedded password management functionality. Contact the system administrator. Refer to the “Troubleshooting” and “Disaster Recovery” chapters for the individual device, in the appropriate device manual. For a list of peer devices for embedded passwords see the section Modifying the Embedded Password on a Device on page 206. If the error persists, contact the Motorola Solutions Support Center (SSC).
Embedded password management admin operation fails with the following messages: <code>Cannot open Context file, Cannot open Data file, Cannot open Data file</code> or similar.	<ul style="list-style-type: none"> These errors may mean that this user does not have read access to a specified application group. Contact the system administrator. Refer to the “Troubleshooting” and “Disaster Recovery” chapters for the individual device, in the appropriate device manual. For a list of peer devices for embedded passwords see the section Modifying the Embedded Password on a Device on page 206.

Problem type	Actions to take
	<p>tion Modifying the Embedded Password on a Device on page 206.</p> <ul style="list-style-type: none"> If the error persists, contact the SSC.
<code>changeproperty</code> command returns the following error: Invalid property value length	This error means that the password length is less than 8 characters. Run the command again and enter a password at least 8 characters long.
<code>changeproperty</code> command returns the following error: The values do not match	The password has been entered incorrectly the second time. Run the command again.
<code>changeproperty</code> or <code>rotateappkey</code> command returns the following error: Application group does not exist	The application group name is misspelled or not created yet. Use the correct application group name. To find the proper group name see Table 19: Embedded Password Management Variables and Procedures on page 209 and Embedded Password Management Variables and Procedures (Interdependent Devices) on page 217 .
<code>changeproperty</code> command returns the following error: Failed to execute pre-notified	Pre-change notify failure. Contact the SSC.
Local application or operation stops working because of embedded passwords mismatch – see also Table 44: Embedded Password Maintenance Failure on page 226	Refer to the “Troubleshooting” chapter for the individual device, in the appropriate device manual. For a list of peer devices for embedded passwords see the section Modifying the Embedded Password on a Device on page 206 .
An application group file is damaged	Use the <code>rmgroup</code> sub-command to remove the damaged group or the <code>rmallgroup</code> command to remove all groups.
A password management file is damaged	Contact the administrator. The file needs to be imported from a valid backup. If there is no backup, then the file needs to be deleted and re-generated manually.

B.7


Embedded Password Maintenance Failure

The following table displays information regarding the impact of embedded passwords mismatch or corruption (which may occur while performing embedded password maintenance) on particular applications and operations.

Table 44: Embedded Password Maintenance Failure

Account Name	Embedded Password Maintenance Failure
activemqadmin	The UCS server can operate normally but it is not possible to troubleshoot some of its components (ActiveMQ).
admin, CRYPTR_OFFICER	The Key Management Facility (KMF) starts but the connection to the KMF CryptR is down. The KMF CryptR management screen shows that there is a password mismatch and inform the user that the passwords must be synced with the KMF CryptR.

Account Name	Embedded Password Maintenance Failure
admin_db_account	Data restore is not possible.
AFFICIENT, JMS_AFF-SERV	Communication between Affiliation Display application (on Network Management Client) and Air Traffic Router (ATR) is not possible.
AFFUSER	No impact.
AGNTCERTUSER	Communication between Air Traffic Router (ATR) in primary zone core and Air Traffic Router (ATR) in backup zone core in DSR mode is not possible.
AGNTUSER, JMS_ATRAGT	The Air Traffic Router (ATR) server status cannot be read or changed. Statistics are not collected by statistical servers. The Dynamic Shared Services Algorithm (DSSA) stops working.
atr_ads_eddiv2_link	ATR does not receive any radio alias updates from ZDS. User is able to send radio command to new radios only by specifying the radio id.
astrocmuser	The UCS server can start but data synchronization between the UCS and ZDS server does not work.
auc, zds_account	Configuration updates are not propagated to AuC.
bar_app_account	Data backup is not possible.
bar_db_account	Data backup is not possible.
camdbuser	The MKM 7000 Console Alias Manager (CAM) Server cannot start. No services are available.
CERTKEYSTORE	Zone/System Historical Reports do not work.
consoleapplplatform	Configuration updates are not propagated to Console.
EDDIAGT_CERT_USER	ATR does not receive any radio alias updates from ZDS. User is able to send radio command to new radios only by specifying the radio id.
EDDIAGT_DB_USER	ATR does not receive any radio alias updates from ZDS. User is able to send radio command to new radios only by specifying the radio id.
ldapsecret	Configuration updates are not propagated to Console.
CRYPTR_USER, user	The KMF starts but the connection to the KMF CryptR is down. The KMF CryptR management screen shows that there is a password mismatch and inform the user that the passwords must be synced with the KMF CryptR.
CSRPTUSER	The Motorola Solutions Support Center (SSC) applications and Customer Reports on NM Client stop working.
ddisynch	Configuration updates are not propagated to ZDS.
DSSAUSER, JMS_DSSA	The Dynamic Shared Services Algorithm (DSSA) stops working.
dr-dj	ZDS upgrade is not possible.
jbcliadm	Changing audit levels for some of the processes on ATR is impossible.
JMS_EDDIAGT	Alias changes are not visible on the RCM application.
JMS_RAPI	Communication between Affiliation Display and ATR is not possible. The Dynamic Shared Services Algorithm (DSSA) stops working. Statistical data on ATR is not collected. RCM and CADI applications do not provide data. RCM and CADI commands stop working. The ZoneWatch application has limited or no functionality.

Account Name	Embedded Password Maintenance Failure
mcadi	Enhanced CADI applications do not provide data. Enhanced CADI commands stop working.
RAPI_PROXY_CERT_USER	Communication between Zone Controller and ATR is broken.
WILDFLYDBUSER, WILDFLYCERTUSER, WILDFLYJMSUSER	The RCM application on NM client/consoles has limited or no functionality.
LICHANDLER	ZoneWatch, Affiliation Display, CADI, and RCM applications may not be possible to launch.
MAUSER, JMS_NEMI	Configuration updates from UNC and PM are not propagated to ATR, SSS, or ZSS.
pmuser	The UCS server cannot start.
RCMCLEANUP	RCM and Computer Aided Dispatch Interface (CADI) display inaccurate data after Dynamic System Resilience (DSR) switchover.
server_db_account	Authentication Center (AuC) Server stops working.
sftpuser	If the accounts cannot be accessed at the time of UNC/UNCDS installation, the installation fails. After the installation is complete, there is no impact.
smc-user	If the accounts cannot be accessed at the time of UNC/UNCDS installation, the installation fails. After the installation is complete, there is no impact.
mot-bat-user	If the accounts cannot be accessed at the time of UNC/UNCDS installation, the installation fails. After the installation is complete, there is no impact.
mot-int-user	If the accounts cannot be accessed at the time of UNC/UNCDS installation, the installation fails. After the installation is complete, there is no impact.
ncm-db-user	If the accounts cannot be accessed at the time of UNC installation, the installation fails. After the installation is complete, there is no impact.
SSL_CLIENT, SSL_SERVER	The client is not able to connect to the server or one of the servers is not able to communicate with the other server.  NOTICE: The server to server SSL connection is used as part of the KMF redundancy feature.
ssl_client_account	AuC Client which is running continues to operate. An attempt to run a new AuC Client fails.
ssl_server_account	AuC Server which is running continues to operate. An attempt to restart the AuC Server fails.
STATMEASUSER, JMS_STATS	Statistical data on ATR are not collected.
SVBE	Statistical database is not updated. System/Zone Historical Reports do not provide accurate data.
SVRPTUSER	Zone/System Historical Reports do not work.

Account Name	Embedded Password Maintenance Failure
TEMPESTUSER, JMS_TEMPEST	RCM and CADI applications do not provide data. RCM and CADI commands stop working.
truststore	Configuration updates are not propagated to ZDS.
\$RCMUSER	The Tempest process is not able to retrieve data from the ATR database. Therefore, the RCM application on NM client/consoles reports that the database connection is broken. The RCM and CADI functionalities are reduced or stop working.
\$ZONEWATCH	The ZoneWatch application on NM client has limited or no functionality.
WILDFLYCERTUSER	On ATR, RCM and Enhanced CADI services are not accessible. On ZSS, Inbound RF Quality Metrics Collection interface is not accessible.
MotoZSS_auth	Default SNMPv3 credential for ZSS-Site Controllers communications. In case of failure, default credentials will be not updated for newly configured SCs on ZSS.
MotoZSS_encr	Default SNMPv3 credential for ZSS-Site Controllers communications. In case of failure, default credentials will be not updated for newly configured SCs on ZSS.