

SmartX Site Converter



Copyrights

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

© 2013 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 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, except for the normal nonexclusive, 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 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 trashbin label on the product (or the package in some cases).

As defined by the WEEE directive, this cross-out trashbin 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.

Document History

.....

Version	Description	Date
6871023P35-A	Original release of the <i>SmartX Site Converter</i> manual.	November 2012
6871023P35-B	<p>The following updates are available in this release:</p> <ul style="list-style-type: none">• Added the <i>Quick Guide for Replacing a Trunked 3600 QUANTAR with a GTR 8000 Base Radio</i> manual to the “Related Information” section.• Changed the name of the Service Support Center to the Solution Support Center.• Added notes where a GTR 8000 Base Radio can replace a QUANTAR® within a 3600 and SmartZone® system to:<ul style="list-style-type: none">◦ "How Does the SmartX Site Converter Fit into the System?"◦ "Supported Sites and Channels"◦ "ISSI 8000/CSSI 8000 Intersystem Gateways and 3600 Sites"• Clarified clocking source for the SmartX Site Converter in "SmartX Site Converter Connections to Remote Sites".• Updated step 5 in Process 4-2.	July 2013

This page intentionally left blank.

Contents

SmartX Site Converter

Chapter 1: SmartX Site Converter Description

What is the SmartX Site Converter?	1-1
Physical Description.	1-2
How Does the SmartX Site Converter Fit into the System?	1-3
Call Types Support	1-12
Audio Formats Support	1-13
Network Management Support	1-13
Information Assurance Features Support	1-14

Chapter 2: SmartX Site Converter Theory of Operation

SmartX Site Converter Operation in an ASTRO 25 System.	2-1
Supported Sites and Channels	2-2
Control Signaling and Audio Formats	2-6
NTP Services	2-21
Zone Core Protection and 3600 Sites	2-21
ISSI 8000/CSSI 8000 Intersystem Gateways and 3600 Sites	2-21
Network Management	2-22
Provisioning Manager	2-22
Configuration/Service Software	2-22
Unified Network Configurator	2-23
Unified Event Manager	2-23
ZoneWatch	2-24
Radio Control Manager	2-24
Call Processing	2-25
Operational Considerations	2-26
Talkgroups	2-26
Emergency Call.	2-26
Private Calls on ASTRO 25 System and a SmartZone 3600 System.	2-26
Secure Downgrade	2-27
Secure Upgrades	2-27
Conditions for Wide Trunking	2-27

Chapter 3: SmartX Site Converter Installation

SmartX Site Converter Installation Prerequisites.	3-1
Site Gateway Hardware Installation.	3-4
SmartX Site Converter Installation Process	3-5
SmartX Site Converter Component Mounting	3-6

SmartX Site Converter Power Distribution Installation	3-9
Using Software Download	3-10
SmartX Site Converter Initial Configuration	3-10
Enabling Secure Software Download	3-14
Performing an SNMPv3 Connection Verification Using CSS	3-23
Setting the Network Services Configuration Using CSS	3-24
Customizing the Login Banner Using CSS	3-25
SmartX Site Converter Network Connections	3-26
SmartX Site Converter Software Installation	3-26
Discovering the SmartX Devices with the UNC	3-27
Logging on to the UNC Server Application Using PuTTY	3-29
Loading the SmartX Site Converter OS Images to the UNC	3-29
Loading OS Software to SmartX Site Converter Devices	3-30

Chapter 4: SmartX Site Converter Configuration

SmartX Site Converter Configuration Process	4-1
SmartX Site Converter Network Management Configuration	4-2
Configuring the SmartX Site Converter Using the UNC	4-2
Network Management Configuration for the SMARTNET/SmartZone Devices	4-8
Adding and Configuring 3600 Sites and Channels	4-9
Monitoring SmartX Site Converter Faults	4-12
Discovering the SmartX Site Converter Devices with the UEM	4-12
Verifying System Installation with the UEM	4-13
SmartX Site Converter Connections to Remote Sites	4-15

Chapter 5: SmartX Site Converter Optimization

T1/E1 Optimization	5-1
Audio Optimization	5-1

Chapter 6: SmartX Site Converter Operation

Powering Up a SmartX Site Converter	6-1
Powering Down a SmartX Site Converter	6-2
Rebooting the SmartX Site Converter	6-2
Logging on to the SmartX Site Converter	6-4
Administering Accounts	6-5
Backing Up the SmartX Site Converter	6-6
Viewing Status	6-8
Viewing Status in the UEM	6-8
Viewing 3600 Site Status in ZoneWatch	6-9
Viewing Status in the UNC	6-10

Chapter 7: SmartX Site Converter Maintenance

Hardware Maintenance	7-1
Software Maintenance	7-1

Chapter 8: SmartX Site Converter Troubleshooting

General Troubleshooting for the SmartX Site Converter	8-1
Troubleshooting the Software Download to the SmartX Site Converter	8-1
Resetting SNMPv3 User Credentials to Defaults on Devices at a Remote Site	8-1
Resetting Passwords and SNMPv3 Passphrases	8-5
Troubleshooting with Local Tools	8-6

Troubleshooting the Serial Connection to the SmartX Site Converter	8-6
Troubleshooting the Ethernet Connection to the SmartX Site Converter	8-6
Troubleshooting with the Unified Event Manager	8-8
Troubleshooting Software Installation.	8-9
Troubleshooting Call Processing from the SmartX Site Converter Perspective	8-9

Chapter 9: SmartX Site Converter FRU/FRE

Field Replaceable Entity	9-1
FRE Parts List	9-1
Replacing the SmartX Site Converter	9-3
Replacing the Battery	9-4
Component Disposal	9-5

Chapter 10: SmartX Site Converter Reference

SmartX Site Converter Specifications.	10-1
SmartX Site Converter Connector Diagrams.	10-2
SmartX Site Converter Ports to Function Map	10-3
SmartX Site Converter LEDs.	10-4
Power LED.	10-4
Red on Reset	10-4
Ethernet Activity LED.	10-4
SmartX Site Converter Cable Connections	10-5

Chapter 11: SmartX Site Converter Disaster Recovery

Recovery Sequence for the SmartX Site Converter.	11-1
--	------

This page intentionally left blank.

List of Figures

Figure 1-1: Front View of the SmartX Site Converter	1-2
Figure 1-2: Rear View of the SmartX Site Converter — Power Connection and Ports in Use	1-3
Figure 1-3: SmartX Site Converter Power Supply	1-3
Figure 1-4: Circuit-based Simulcast Subsystem with SmartX Site Converter.	1-4
Figure 1-5: SmartX Site Converter at the Zone Core (with CSA)	1-5
Figure 1-6: SmartX Site Converter at the Zone Core (non-CSA)	1-7
Figure 1-7: SmartX Site Converter at the Remote Site (with CSA)	1-9
Figure 1-8: SmartX Site Converter at the Remote Site (non-CSA)	1-11
Figure 2-1: SmartZone 4.1 System	2-3
Figure 2-2: ASTRO 25 System with 3600 Sites and Gold Elite Consoles	2-5
Figure 2-3: 3600 RF Site to Zone Controller Data Path	2-7
Figure 2-4: 3600 Subscriber Radio Transmits on Analog Talkgroup	2-8
Figure 2-5: Radio TX on Analog TG, A25 — Console and 3600 Destinations	2-10
Figure 2-6: ASTRO 25 System Subscriber Radio Transmits on 3600 Analog Talkgroup	2-11
Figure 2-7: Radio TX on Digital 3600 TG, A25 — Console and 3600 Destinations.	2-13
Figure 2-8: A25 Radio TX on 3600 Digital TG — Console and 3600 Destinations	2-15
Figure 2-9: MCC 7500 Console Transmits on 3600 Analog Talkgroup	2-17
Figure 2-10: MCC 7500 Console Transmits on 3600 Digital Talkgroup	2-18
Figure 2-11: Console Takeover, Console, and 3600 Radio Transmit on 3600 Analog Talkgroup	2-19
Figure 2-12: Console Takeover, Console, and 3600 Radio Transmit on 3600 Digital Talkgroup	2-20
Figure 3-1: Site Converters in a Rack at the Zone Core.	3-7
Figure 3-2: A Site Converter in a Rack at the Remote Site	3-8
Figure 3-3: Password Configuration Window	3-16
Figure 4-1: SmartX Site Converter Discovery in the UEM	4-13
Figure 6-1: Rear View of the SmartX Site Converter	6-1
Figure 6-2: SmartX Site Converter Alarms in the UEM	6-9
Figure 6-3: 3600 Site Status in ZoneWatch	6-9
Figure 10-1: SmartX Site Converter T1/E1 Port Connector Pinout Diagram	10-2
Figure 10-2: SmartX Site Converter LEDs	10-4

This page intentionally left blank.

List of Tables

Table 2-1: Types of Calls Supported by the ASTRO 25 System	2-25
Table 6-1: SmartX Site Converter Accounts	6-5
Table 8-1: Local Password and SNMPv3 Passphrase Troubleshooting.	8-5
Table 8-2: SmartX Site Converter Troubleshooting Scenarios.	8-9
Table 9-1: Field Replaceable Entities	9-2
Table 9-2: Battery Replacement Time.	9-4
Table 10-1: SmartX Site Converter Hardware Specifications	10-1
Table 10-2: E1/T1 Connections	10-2
Table 10-3: SmartX Site Converter Serial Cable Connector Pinout	10-3
Table 10-4: Ethernet Activity LED	10-5

This page intentionally left blank.

List of Procedures

Procedure 3-1: How to Install the SmartX Site Converter Hardware.	3-9
Procedure 3-2: How to Provision the SmartX Site Converter Serial Connection Parameters.	3-11
Procedure 3-3: How to Configure the SmartX Site Converter Using CSS (Ethernet Connection)	3-12
Procedure 3-4: How to Set the SWDL Transfer Mode Using CSS.	3-14
Procedure 3-5: How to Set the SmartX Site Converter Local Password Configuration	3-15
Procedure 3-6: How to Set the Date and Time on the SmartX Site Converter	3-18
Procedure 3-7: How to Set the Serial Security Services	3-19
Procedure 3-8: How to Change SNMPv3 Configuration and User Credentials on the SmartX Site Converter.	3-20
Procedure 3-9: How to Add or Modify an SNMPv3 User.	3-23
Procedure 3-10: How to Verify SNMPv3 Credentials on the SmartX Site Converter	3-24
Procedure 3-11: How to Customize the Login Banner	3-25
Procedure 3-12: How to Attach the SmartX Site Converter to the Site Gateway	3-26
Procedure 3-13: How to Discover the Motorola SmartX Site Converter in the UNC	3-28
Procedure 3-14: How to Load the SmartX Site Converter OS Images to the UNC	3-29
Procedure 3-15: How to Enable FTP Service	3-30
Procedure 3-16: How to Transfer and Install the OS Image.	3-30
Procedure 3-17: How to Inspect Device Properties for Transferred and Installed Software	3-32
Procedure 3-18: How to Disable FTP Service	3-32
Procedure 4-1: How to Configure the SmartX Site Converter Using the UNC	4-3
Procedure 4-2: How to Configure the SmartX Site Converter Channels Using the UNC Wizard.	4-7
Procedure 4-3: How to Add a 3600 Site.	4-9
Procedure 4-4: How to Add a 3600 Channel.	4-11
Procedure 4-5: How to Define the Valid Trespass Protection ID List	4-12
Procedure 4-6: How to Discover the SmartX Site Converter in the UEM	4-13
Procedure 4-7: How to Verify SmartX Site Converter Operation with the UEM	4-14
Procedure 4-8: How to Connect the SmartX Site Converter and the Channel Bank	4-17
Procedure 6-1: How to Power Up the SmartX Site Converter.	6-1
Procedure 6-2: How to Power Down the SmartX Site Converter	6-2
Procedure 6-3: How to Reboot the SmartX Site Converter by Power Cycling the Hardware.	6-3
Procedure 6-4: How to Reboot the SmartX Site Converter on the CSS	6-3
Procedure 6-5: How to Reboot the SmartX Site Converter Using the UEM	6-3
Procedure 6-6: How to Restore the SmartX Site Converter Configuration from UNC.	6-6
Procedure 6-7: How to Verify the SmartX Site Converter is Compliant in the UNC	6-10
Procedure 8-1: How to Reset SNMPv3 User Credentials to Defaults on Devices at a Remote Site Locally through the CSS.	8-2
Procedure 8-2: How to Reset the SNMPv3 User Credentials to Defaults on Devices at a Remote Site Remotely through Telnet/SSH	8-3
Procedure 8-3: How to Access Log Files in the CSS	8-7
Procedure 8-4: How to Access the Software Version Information in the CSS	8-7
Procedure 9-1: How to Replace a SmartX Site Converter.	9-3
Procedure 9-2: How to Replace the Battery	9-4

This page intentionally left blank.

List of Processes

Process 3-1: Prerequisites for Initial SmartX Site Converter Installation and Configuration	3-2
Process 3-2: Installing the SmartX Site Converter	3-5
Process 3-3: Installing Software on the SmartX Site Converter	3-26
Process 4-1: Configuring the SmartX Site Converter	4-1
Process 4-2: Configuring the Trunked 3600 Sites and Channels on the Network Managers	4-9
Process 11-1: Recovering the SmartX Site Converter	11-1

This page intentionally left blank.

SmartX Site Converter

.....

The SmartX Site Converter interfaces with the SMARTNET® 3.1 and 3.2, SmartZone® 3.0, 3.5, and 4.1 Radio Frequency (RF) site to use those resources in a current ASTRO® 25 Integrated Voice and Data radio system.



CAUTION

All SMARTNET® 3.0 and 3.1 sites must be upgraded to a SmartZone® site before they can be interfaced through a SmartX Site Converter. Failure to upgrade the SMARTNET® sites results in loss of service to those subscribers.

The terms "3600 RF sites", "3600 sites", and "3600 subscriber radios" are used within this manual to designate SmartZone® RF sites and subscribers. The terms "9600 sites" and "ASTRO® 25" are used within this manual to designate ASTRO® 25 system sites. The numerical references 3600 and 9600 pertain to the control channel baud rate rather than the number of sites.

What Is Covered In This Manual?

This manual is organized into the following chapters:

- [Chapter 1, "SmartX Site Converter Description"](#) provides a high-level description of the SmartX Site Converter and the function it serves on your system.
- [Chapter 2, "SmartX Site Converter Theory of Operation"](#) explains how the SmartX Site Converter works in the context of your system.
- [Chapter 3, "SmartX Site Converter Installation"](#) details hardware and software installation procedures, as well as the initial configuration required for connectivity to the network for the SmartX Site Converter.
- [Chapter 4, "SmartX Site Converter Configuration"](#) details configuration procedures and fault management application discovery relating to the SmartX Site Converter.
- [Chapter 5, "SmartX Site Converter Optimization"](#) is for optimization procedures and recommended settings relating to the SmartX Site Converter.
- [Chapter 6, "SmartX Site Converter Operation"](#) is for tasks that are performed once the SmartX Site Converter is operational on your system.
- [Chapter 7, "SmartX Site Converter Maintenance"](#) describes maintenance instruction for the SmartX Site Converter.
- [Chapter 8, "SmartX Site Converter Troubleshooting"](#) provides fault management and troubleshooting information relating to the SmartX Site Converter.

- [Chapter 9, "SmartX Site Converter FRU/FRE"](#) describes Field Replaceable Units (FRU) and Field Replaceable Entities (FRE) relating to the SmartX Site Converter.
- [Chapter 10, "SmartX Site Converter Reference"](#) describes additional reference information on the Voice Processor Module (VPM) hardware ports, cabling, LEDs, and more when used as a SmartX Site Converter.
- [Chapter 11, "SmartX Site Converter Disaster Recovery"](#) provides references and information that enables you to recover a SmartX Site Converter in the event of a failure.

Helpful Background Information

Motorola 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

See the following documents for associated information about the radio system.

Related Information	Purpose
<i>Standards and Guidelines for Communication Sites</i> (6881089E50)	Provides standards and guidelines that should be followed when setting up a Motorola communications site. Also known as R56 manual. This document 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 Documentation Overview</i>	<p>For an overview of the ASTRO[®] 25 system documentation, open the graphical user interface for the ASTRO[®] 25 system documentation set and select the System Documentation Overview link. This action opens a file that includes:</p> <ul style="list-style-type: none"> • ASTRO[®] 25 system release documentation descriptions • ASTRO[®] 25 system diagrams • ASTRO[®] 25 system glossary <p>For an additional overview of the system, review the architecture and descriptive information in the manuals that apply to your system configuration.</p>
<i>Voice Processor Module</i>	Provides additional information on the VPM hardware platform, which is used for the SmartX Site Converter.
<i>System Routers - S6000/S2500</i>	Provides information on the S2500 router, which can be used with the SmartX Site Converter hardware to support SmartZone [®] sites.

Related Information	Purpose
<i>System Gateways - GGM 8000</i>	Provides information on the GGM 8000 gateways, which can be used with the SmartX Site Converter hardware to support SmartZone® sites.
<i>MCC 7500 Console Site with VPM</i>	Provides information about the VPM hardware as it is being used as the audio interface for the MCC 7500 console subsystem.
<i>Enhanced Telephone Interconnect</i>	Provides information about the Enhanced Telephone Interconnect feature, which is using the Voice Processor Module hardware for the Telephone Media Gateway (TMG).
<i>Authentication Services</i>	Provides information on CSS procedures used to set up Information Assurance features, such as Configuring DNS, Centralized Authentication, and RADIUS Authentication on the SmartX Site Converter using CSS.
<i>Centralized Event Logging</i>	Provides information on enabling the CEL feature on the SmartX Site Converter using CSS.
<i>Unified Network Configurator</i>	Provides information on the use of Unified Network Configurator (UNC), a sophisticated network configuration software that provides controlled and validated configuration management for system devices including routers, LAN switches, site controllers, and base radios, and is used to set up sites for the ASTRO® 25 IV&D system. UNC has two components: VoyenceControl and Unified Network Configurator Wizards (UNCW).
<i>Software Download</i>	Provides information on the SWDL application.
<i>ISSI 8000/CSSI 8000 — Intersystem Gateway</i>	Includes information required to understand, install, manage, and troubleshoot the ISSI 8000 ISGW and CSSI 8000 hardware to support the ISSI 8000/CSSI 8000 Intersystem Gateway feature, which provides an increased interconnectivity solution for P25 compatible systems.
<i>Motorola GGM 8000 Hardware User Guide</i>	Available on the Motorola Online (MOL) Web site (http://businessonline.motorola.com). To access the manual, select Resource Center > Product Information > Manuals > Network Infrastructure> Routers and Gateways .
<i>Motorola Network Router (MNR) 2500 Hardware User Guide</i>	
<i>Motorola Network Router (MNR) S6000 Hardware User Guide</i>	
<i>Quick Guide for Replacing a Trunked 3600 QUANTAR with a GTR 8000 Base Radio</i>	A supplemental document used to replace QUANTAR® base radios with new GTR 8000 base radio hardware at 3600 sites.

This page intentionally left blank.

SmartX Site Converter Description

This chapter provides a high-level description of the SmartX Site Converter and the function it serves on your system.

What is the SmartX Site Converter?

The SmartX Site Converter is a device designed to allow communication between subscriber radios at existing 3600 RF sites and an ASTRO[®] 25 Integrated Voice and Data system. It enables the continued use of 3600 RF sites and subscriber radios on an ASTRO[®] 25 release 7.7 or higher system, thus allowing the gradual replacement of equipment that is at or near the end of life with the newer technology and operational capabilities of an ASTRO[®] 25 system.

The SmartX Site Converter can be used to interface SmartZone[®] 3.0, 3.5, and 4.1 RF sites to a current ASTRO[®] 25 Integrated Voice and Data system. SMARTNET[®] 3.1 or 3.2 sites must be upgraded to a SmartZone[®] remote site, which can then be connected through the SmartX Site Converter to the ASTRO[®] 25 system.

The SmartX Site Converter performs the following tasks:

- Call control information
 - Bidirectional conversion between circuit-based 3600 call control packets and ASTRO[®] 25 IP-based call control protocol so calls can be managed through the ASTRO[®] 25 zone controller.
- Audio information
 - Conversion of analog audio from 3600 sites to G.728 packets that can be routed over the ASTRO[®] 25 IP network to the MCC 7500 consoles and to other 3600 sites.
 - Conversion of analog audio from 3600 sites to Advanced Multi-Band Excitation (AMBE) audio packets for routing over the ASTRO[®] 25 IP network to ASTRO[®] 25 RF sites.
 - Routing without conversion of digital Improved Multi-Band Excitation (IMBE) audio from the 3600 sites to other 3600 sites, MCC 7500 consoles, and ASTRO[®] 25 RF sites.
 - Conversion of AMBE audio from MCC 7500 consoles or ASTRO[®] 25 RF sites to analog or IMBE format for routing to analog or digital 3600 RF sites.
- System management
 - Converts 3600 site faults and diagnostics to enable management of the 3600 sites by the ASTRO[®] 25 network fault management system. It reports 3600 site states and faults to the fault manager using Simple Network Management Protocol version 3 (SNMPv3).

Physical Description

.....

The SmartX Site Converter is based on the Voice Processor Module (VPM) hardware platform. Specialized software allows the VPM to perform the tasks required for SmartX Site Converter operation. For details on the hardware see the *Voice Processor Module* manual.

Figure 1-1 shows the front view of the SmartX Site Converter.

Figure 1-1 Front View of the SmartX Site Converter

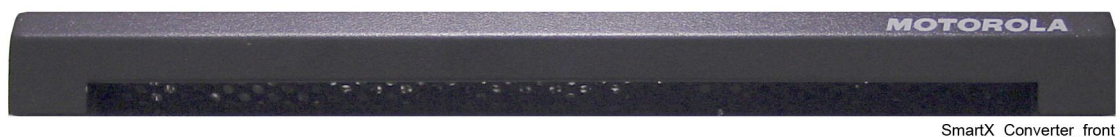


Figure 1-2 shows the rear view of the SmartX Site Converter. The power, serial, Ethernet, and E1/T1 ports are the only ones in use when the VPM functions as the SmartX Site Converter.

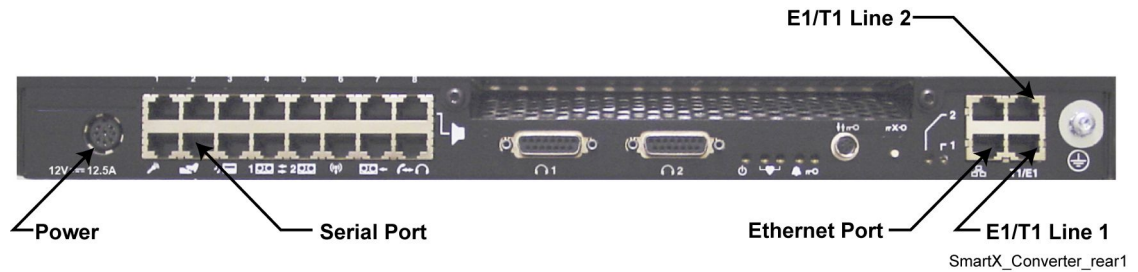
Figure 1-2 Rear View of the SmartX Site Converter — Power Connection and Ports in Use

Figure 1-3 shows the power supply, cable, and line cord.

Figure 1-3 SmartX Site Converter Power Supply

VPM_power_supply

How Does the SmartX Site Converter Fit into the System?

The SmartX Site Converter receives audio and control information from the 3600 RF sites through a T1/E1 link. The SmartX Site Converter transmits the processed information through a site gateway that serves as the link to the network transport facilities.

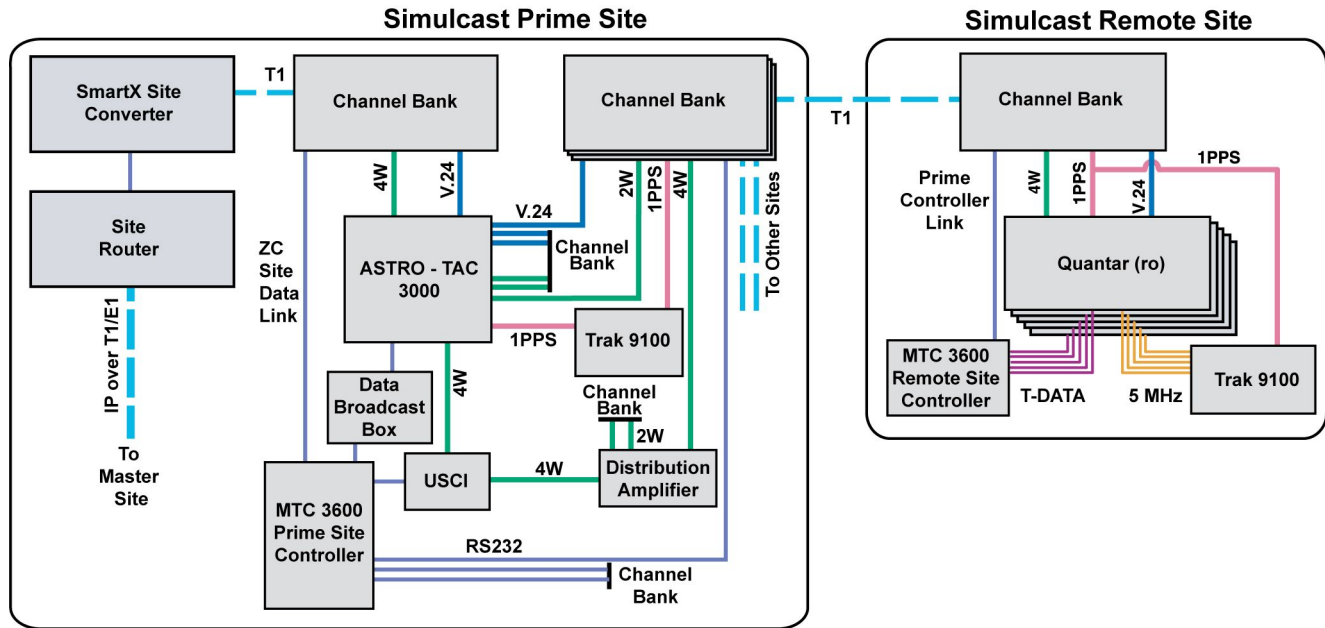


NOTE

The site gateway provides a preferred alternative solution for the site router. See the *System Gateways – GGM 8000* manual.

The SmartX Site Converter and its router/gateway can be physically at the 3600 RF sites or at the ASTRO[®] 25 system master site. Several factors enter into the decision for the physical location including transport links and bandwidth availability.

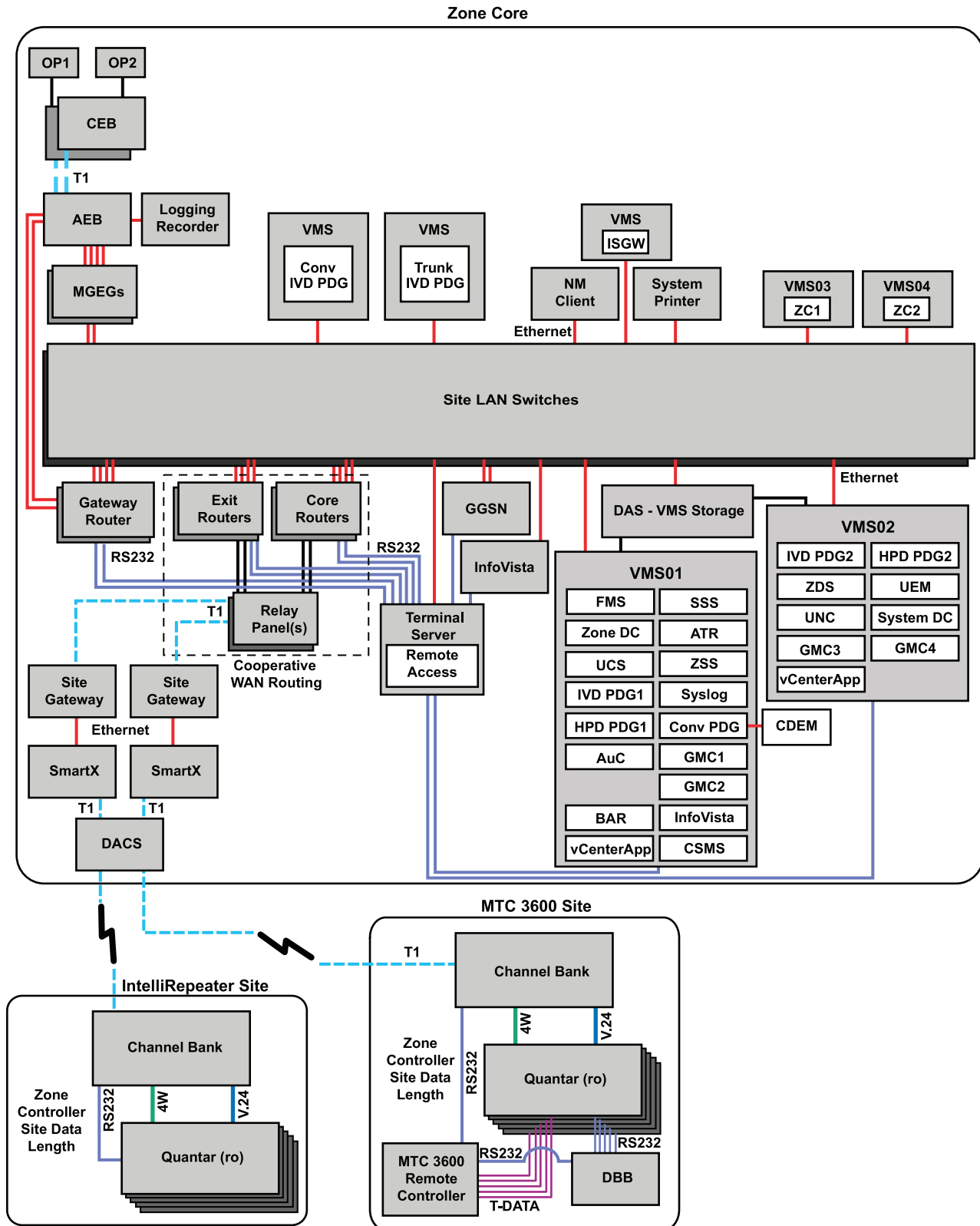
Figure 1-4 shows an example of a SmartX Site Converter and its site gateway installed at a 3600 RF site.

Figure 1-4 Circuit-based Simulcast Subsystem with SmartX Site Converter

Simulcast_3600_RF_Site_w_SmartX

Figure 1-5 shows an example of the SmartX Site Converter and its site gateway installed at the ASTRO® 25 zone core (master site) with a Common Server Architecture (CSA).

A GTR 8000 Base Radio can be implemented as a QUANTAR® replacement within a 3600 and SmartZone® system. The implementation details are in the *Quick Guide for Replacing a Trunked 3600 QUANTAR with a GTR 8000 Base Radio* manual.

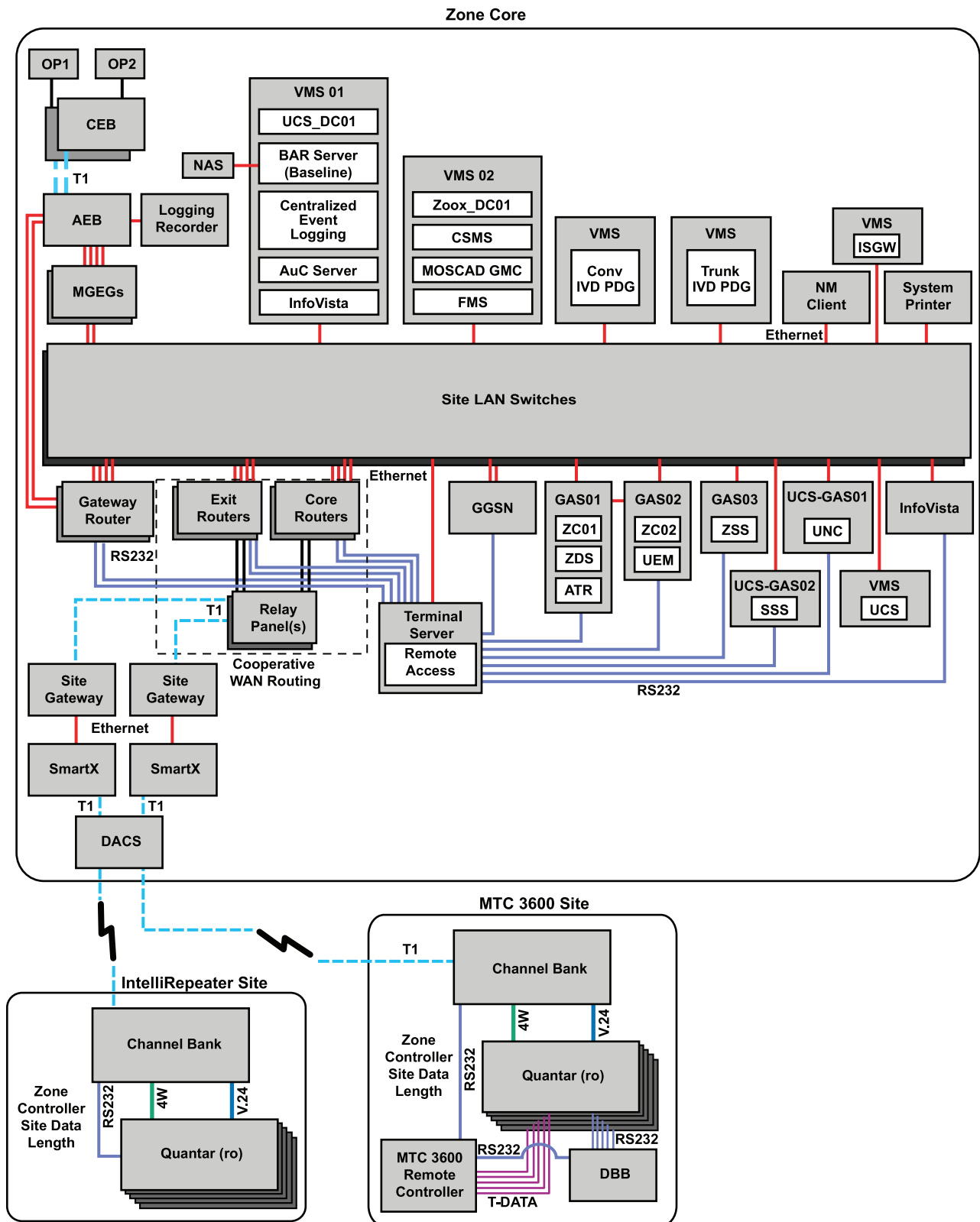
Figure 1-5 SmartX Site Converter at the Zone Core (with CSA)

S_SmartX_at_Zone_Core_CSA_A

**NOTE**

The site gateway provides a preferred alternative solution for the site router. See the *System Gateways – GGM 8000* manual.

[Figure 1-6](#) shows a SmartX Site Converter at the zone core (master site) in an ASTRO® 25 system with a non-CSA (Generic Application Server hardware) architecture.

Figure 1-6 SmartX Site Converter at the Zone Core (non-CSA)

S_SmartX_at_Zone_Core_NonCSA_A

**NOTE**

See the *Master Site Infrastructure* manual and *Generic Application Server* manual for network management server applications hosted on Solaris-based GAS servers.

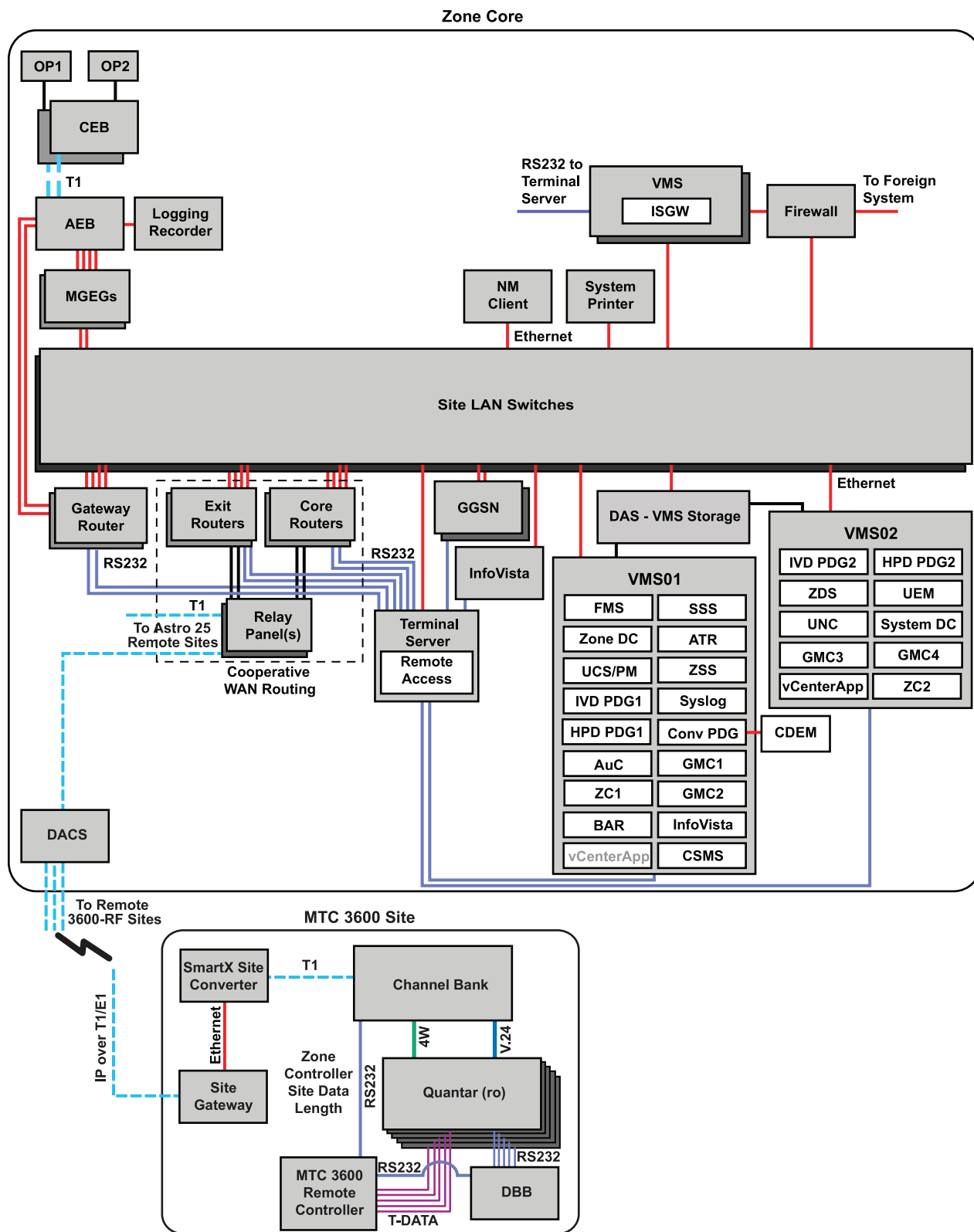
3600 RF sites operating in the VHF, UHF, 800 MHz, and 900 MHz bands can be interfaced to an ASTRO[®] 25 system through the SmartX Site Converter.

**NOTE**

This feature does not support 700 MHz operation because the 3.x/4.x system cannot support that band.

Figure 1-7 shows a SmartX Site Converter at a 3600 site in an ASTRO[®] 25 system with a Common Server Architecture (CSA).

A GTR 8000 Base Radio can be implemented as a QUANTAR[®] replacement within a 3600 and SmartZone[®] system. The implementation details are in the *Quick Guide for Replacing a Trunked 3600 QUANTAR with a GTR 8000 Base Radio* manual.

Figure 1-7 SmartX Site Converter at the Remote Site (with CSA)

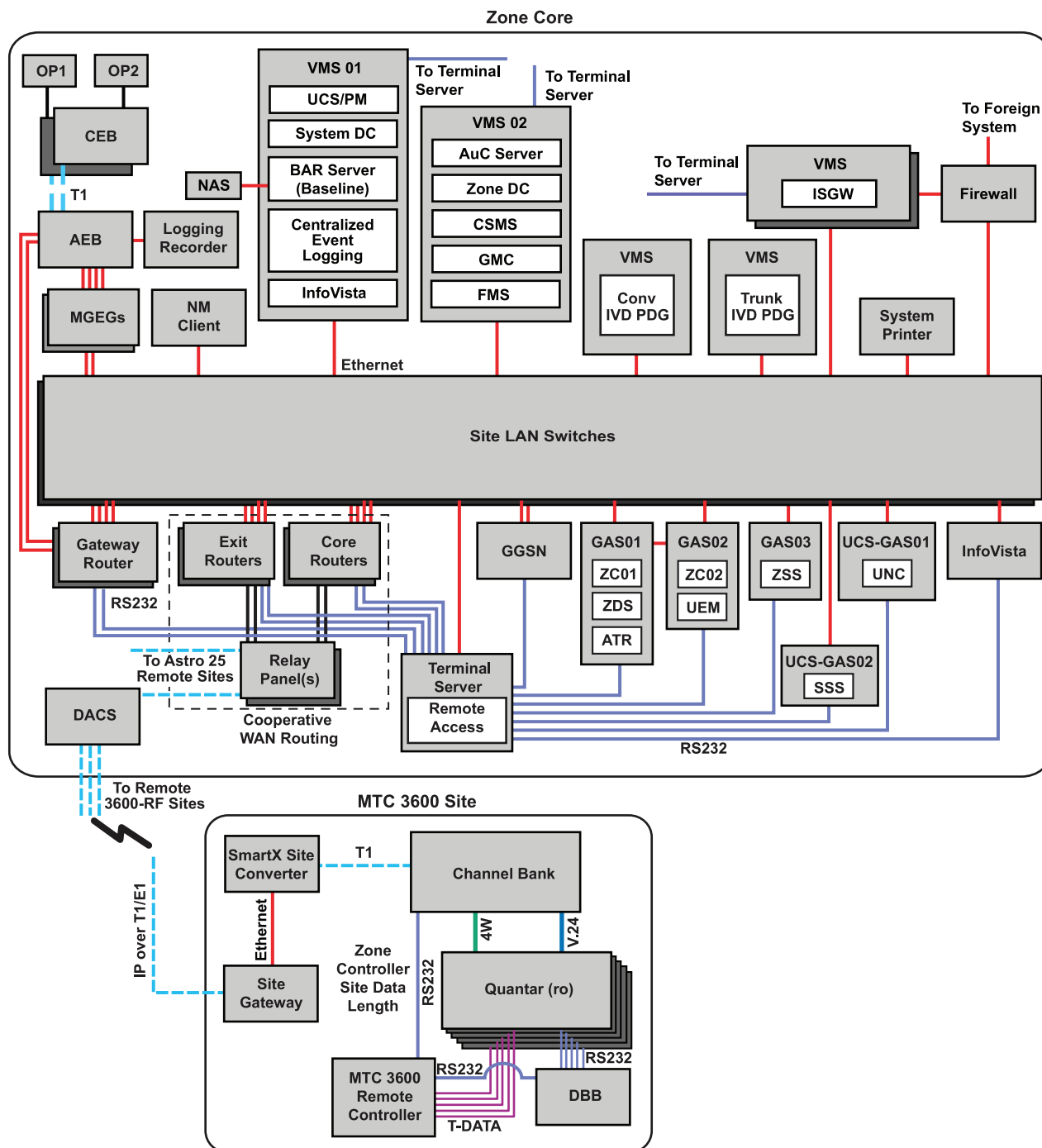
S_SmartX_at_Remote_Site_CSA_B

**NOTE**

The site gateway provides a preferred alternative solution for the site router. See the *System Gateways – GGM 8000* manual.

[Figure 1-8](#) shows a SmartX Site Converter at a 3600 site in an ASTRO® 25 system with a non-CSA (Generic Application Server hardware) architecture.

A GTR 8000 Base Radio can be implemented as a QUANTAR® replacement within a 3600 and SmartZone® system. The implementation details are in the *Quick Guide for Replacing a Trunked 3600 QUANTAR with a GTR 8000 Base Radio* manual.

Figure 1-8 SmartX Site Converter at the Remote Site (non-CSA)

S_SmartX_at_Remote_Site_NonCSA_B

Call Types Support

.....

.....

The SmartX Site Converter supports the following types of calls for sites connected to an ASTRO® 25 system:

- Talkgroup Call (clear)
- Talkgroup Call utilizing message trunking with PTT ID
- Talkgroup Call utilizing transmission trunking
- Talkgroup Call (ASTRO® 25) encrypted
- Emergency Call
- Emergency Alarm
- Multigroup Call
- Supergroup Call
- Priority Monitor (Scan)
- Enhanced Private Call
- Call Alert
- Console Priority
- Busy/Callback
- AllStart/Faststart Call Set-up

Audio Formats Support

The audio processing capabilities built into the SmartX Site Converter make it possible to support the following audio formats when interfacing 3600 RF sites to an ASTRO[®] 25 system:

- The existing analog solution utilizes the G.728 vocoder to accurately represent analog audio received over the air interface. This solution produces G.728 audio packets that are routed through the ASTRO[®] 25 network to MCC 7500 consoles and analog 3600 RF sites.
- MCC 7500 consoles and ASTRO[®] 25 RF sites source audio in AMBE format for all calls whether they are routed to analog or digital 3600 RF sites.
- The MCC 7500 console supports both the AMBE vocoder and the G.728 vocoder for trunking calls.
- When Gold Elite consoles are part of the system, the Motorola Gold Elite Gateway (MGEG) is equipped with both the AMBE vocoder and the G.728 vocoder for trunking calls.
- IMBE audio is supported in its native format.

Network Management Support

The following Network Management (NM) applications are used to configure and/or monitor the SmartX Site Converter:

- PM— The Provisioning Manager enables an administrator to enter and maintain related configuration information in the System, Subscribers, Security, and ZoneWatch configuration objects.
- UNC — The Unified Network Configurator provides support for the following:
 - OS and configuration updates for the SmartX Site Converter
 - Channel parameter configuration
 - System/site parameters
 - OS and configuration updates for the site gateway
- CSS — The Configuration/Service Software supports the initial network and authentication parameter configuration.
- UEM — The Unified Event Manager provides fault management and event monitoring of the 3600 sites as reported by the SmartX Site Converter.
- RCM — The Radio Control Manager application extends its monitoring and control capabilities to the 3600 subscriber radios.
- ZoneWatch — This application can be configured to monitor activity at the 3600 RF sites.

Information Assurance Features Support

.....

The SmartX Site Converter supports the following Information Assurance features:

- Password protection — The SmartX Site Converter supports passwords with configurable complexity requirements.
- SNMPv3 — The Simple Network Management Protocol is a set of rules that various end points in a network use when they communicate. It provides security through support for authentication with or without encryption.
- Centralized Authentication — The ASTRO[®] 25 Centralized Authentication feature uses Active Directory[®] (AD) and Remote Authentication Dial-In User Service (RADIUS) to provide identity management and authentication.
- SSH — Secure SHell (SSH) authenticates both ends of a connection, encrypts bearer traffic, and ensures the integrity of data. SSH uses a client-server model to secure traffic generated during remote login, remote file transfer, and remote command execution across a network. The optional Securing Protocols with SSH feature provides a secure alternative to the clear protocols that are used in an ASTRO[®] 25 communication system, including FTP, TFTP, Telnet, RLOGIN, RSH, and RCP.
- Centralized Event Logging — Centralized Event Logging is an optional security feature that captures Operating System (OS) events generated by most devices in the radio network in the form of event messages. Each device forwards event messages to a Centralized Event Logging server.

For more information about Information Assurance features, see the *Information Assurance Features Overview* and the manuals that document each specific feature.

SmartX Site Converter Theory of Operation

This chapter explains how the SmartX Site Converter works in the context of your system.

SmartX Site Converter Operation in an ASTRO 25 System

The SmartX Site Converter has two T1/E1 interfaces that can be used to interface to a 3600 RF site. Interface 1, interface 2, or both interface 1 and 2 may be used as required by the system configuration. The interfaces may be configured for standard T1 operation or E1 operation using the UNC. Configuration for T1 provides 24 slots, while the configuration of E1 provides 32 slots. The slots within the T1/E1 lines may be mapped to control signaling, analog voice signaling, and digital voice signaling as required by the system configuration. Note that a slot can be associated with digital voice or analog voice, but not both (no ADPCM support). The slot configuration is also performed using the UNC.

The SmartX Site Converter allows one or two slots to be configured, as control link transport. This provision allows redundant 6809 site configurations to be supported. In the redundant case, the control link from each site controller is mapped to a T1/E1 slot. Selection and configuration of the slots is performed through the UNC. The two T1/E1 connections share the external clock signal.

In addition to the control link slots, the SmartX Site Converter has capacity for 28 channels, 27 voice channels, and one active control channel. This capacity is sufficient to cover all sizes of certified SmartZone® RF sites.

The SmartX Site Converter has a single physical Ethernet interface that connects to a site gateway for connectivity to the ASTRO® 25 system.

Each 3600 RF site requires one SmartX Site Converter and a corresponding site gateway. SmartX Site Converter redundancy is not supported.



NOTE

The site gateway provides a preferred alternative solution for the site router. See the *System Gateways – GGM 8000* manual.

Supported Sites and Channels

The following 3600 RF site types are supported:

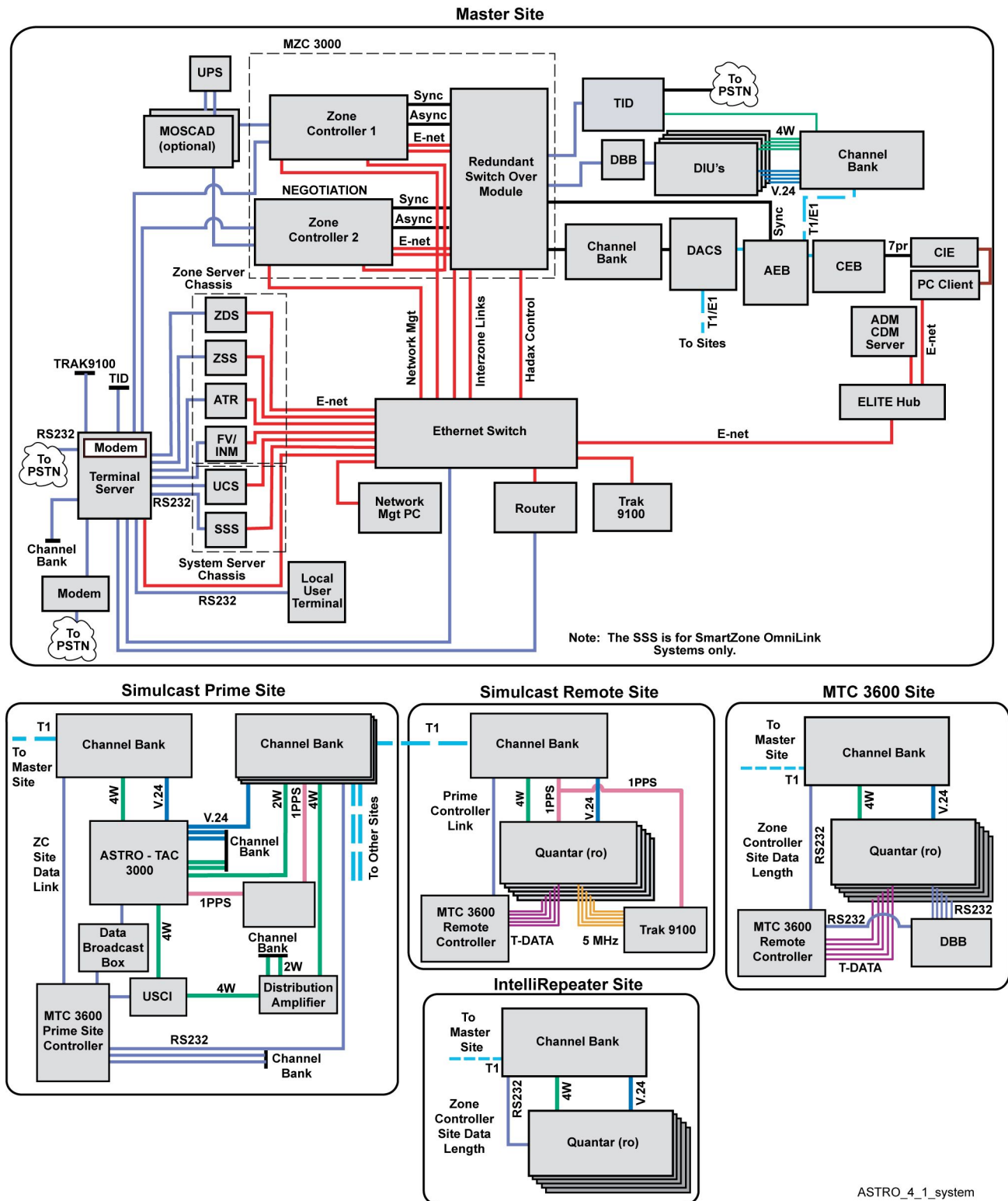
- 3600 IntelliRepeater remote site
- 3600 site controller-based remote site
- 3600 simulcast subsystem
- 3600 voting only subsystem (UHF, VHF)

The following channel types are supported on a 3600 RF site:

- 3600 analog only channel
- 3600 digital only channel (IMBE)
- 3600 mixed mode channel (3600 analog/3600 digital IMBE)

[Figure 2-1](#) shows a block diagram representation of a SmartZone® 4.1 system. The RF sites and Gold Elite consoles in this existing system can be integrated into an ASTRO® 25 system with the use of a SmartX Site Converter (see [Figure 2-2](#)).

A GTR 8000 Base Radio can be implemented as a QUANTAR® replacement within a 3600 and SmartZone® system. The implementation details are in the *Quick Guide for Replacing a Trunked 3600 QUANTAR with a GTR 8000 Base Radio* manual.

Figure 2-1 SmartZone 4.1 System

To deploy the SmartX Site Converter, the existing system must be modified. The impact to deploying the SmartX-based 3600 migration solution includes the following changes:

Removal of the following equipment:

- SmartZone[®] zone controller
- SmartZone[®] Manager
- DIUs
- Telephone interconnect components
- Pre-Gold Elite consoles
- Terminal server
- Redundant switchover module

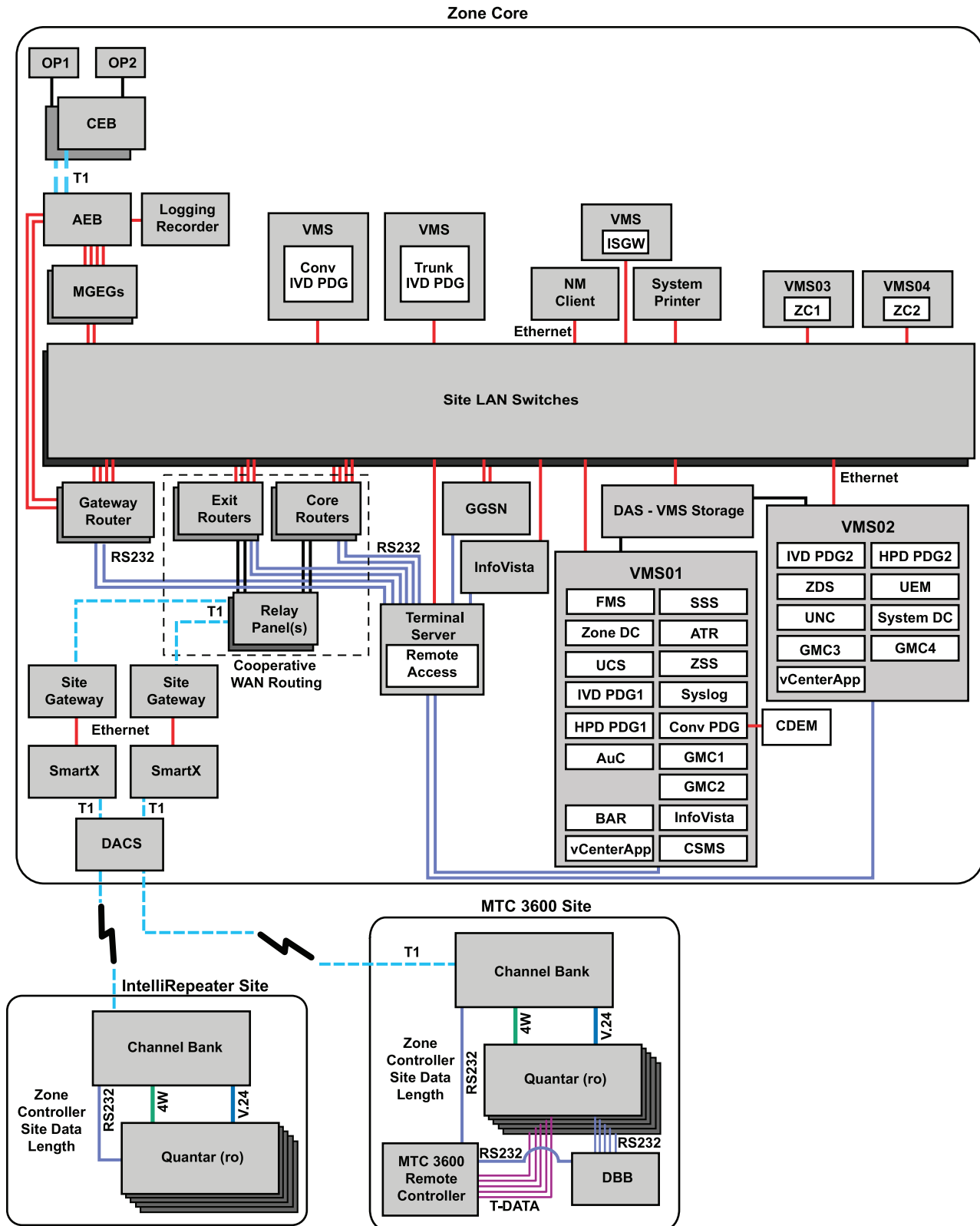
Reuse of the following:

- 3600 RF sites
- 3600 radios (both analog only and digital capable)
- Channel banks (may need updated modules)
- Gold Elite Dispatch positions (updated to ASTRO[®] 25 system)
- Ambassador Electronics Bank (AEB) – to enable use of Gold Elite consoles on system (updated to ASTRO[®] 25 system)
- Alias Database Manager (ADM)/Console Database Manager (CDM) server if it can be updated with ASTRO[®] 25 versions of the operating system and application software
- Digital Access Cross-connect Switch (DACS) depending on the system configurations

Addition of the following equipment based on options:

- Motorola Gold Elite Gateways (MGEs) – to enable use of Gold Elite consoles on system (if needed)
- Circuit-based logging equipment (if needed)
- Site gateways or routers for 3600 sites (one per site)
- SmartX Site Converters – one per RF site

Figure 2-2 shows an ASTRO[®] 25 system (featuring Common Server Architecture) with the addition of the 3600 RF sites and the Gold Elite console equipment that was migrated from the SmartZone[®] 4.1 system.

Figure 2-2 ASTRO 25 System with 3600 Sites and Gold Elite Consoles

S_SmartX_at_Zone_Core_CSA_A

**NOTE**

The site gateway provides a preferred alternative solution for the site router. See the *System Gateways – GGM 8000* manual.

**NOTE**

For the non-CSA version of the SmartX at the zone core, see [Figure 1-6](#).

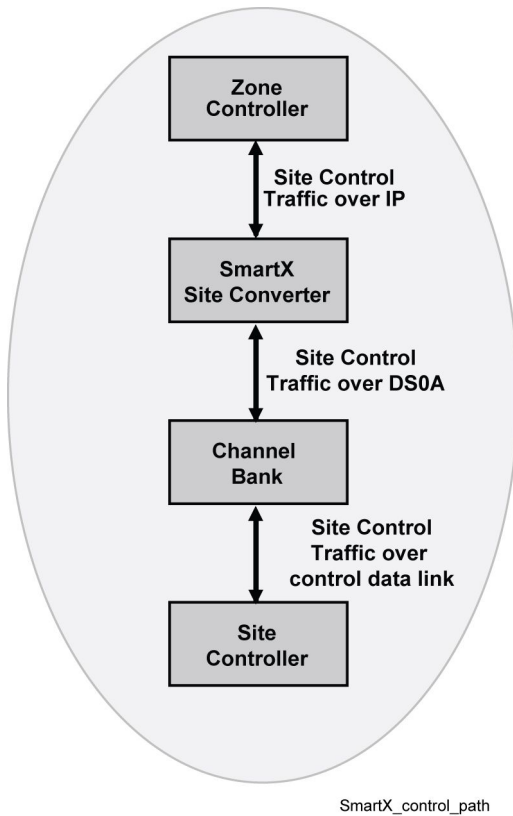
The following can be noted once the reused components from the SmartZone® 4.1 system have been interfaced to the ASTRO® 25 system through the SmartX Site Converter:

- The zone controllers in the ASTRO® 25 system manage all call processing functions for the 3600 sites and the ASTRO® 25 sites.
- MGEGs were added to provide the interface between the updated Gold Elite equipment and the IP-based ASTRO® 25 network. Once interfaced to the system, interoperability between the Gold Elite and the MCC 7500 console is available.
- The ASTRO® 25 Network Management applications provide the configuration, monitoring, and fault management capability for the 3600 and ASTRO® 25 infrastructure and subscribers.
- 3600 RF sites connect into the ASTRO® 25 master site in the same manner as the ASTRO® 25 sites, through their site gateway and the relay panels.

Control Signaling and Audio Formats

The SmartX Site Converter is responsible for managing the audio and control plane transition between the 3600 sites and ASTRO® 25 core. This means that the SmartX Site Converter, based on the received audio type from the 3600 site, must generate the necessary control and audio data packets to the ASTRO® 25 core for both analog and digital audio.

[Figure 2-3](#) shows the basic path and transitions for the control data between the ASTRO® 25 zone controller and the 3600 site controller.

Figure 2-3 3600 RF Site to Zone Controller Data Path

The SmartZone[®] 4.1 system uses a different call control protocol between its zone controller and the sites than is used between an ASTRO[®] 25 zone controller and the ASTRO[®] 25 sites. For the SmartZone[®] 4.1 sites to operate with an ASTRO[®] 25 system and ASTRO[®] 25 zone controller, the call control information must be converted between SmartZone[®] call control and ASTRO[®] 25 call control by the SmartX Site Converter.

The control plane information for a call request from a 3600 site is processed as follows:

- The 3600 site controller sends the data to an SRU interface in the channel bank.
- The channel bank routes data to the SmartX Site Converter over a T1/E1 interface.
- The 3600 control plane information is transformed by the SmartX Site Converter into the control plane format required by the ASTRO[®] 25 zone controller.
- The SmartX Site Converter sends the control plane information to the site gateway over an Ethernet interface.
- The site gateway sends the information over its T1/E1 interface to the zone controller.

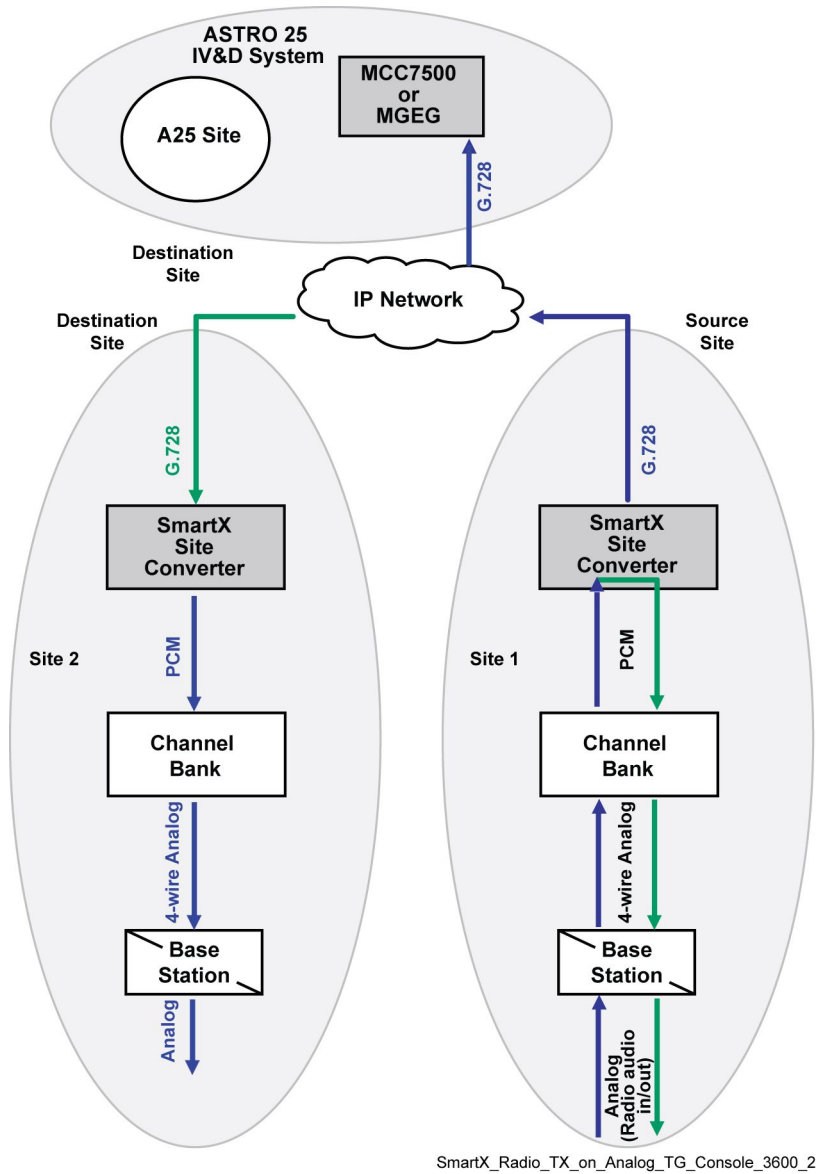
The SmartX Site Converter also provides the necessary conversion between the ASTRO[®] 25 control data format and the 3600 control data format when it receives the call grant information from the ASTRO[®] 25 zone controller.

See [Figure 2-4](#), [Figure 2-5](#), [Figure 2-6](#), [Figure 2-7](#), [Figure 2-8](#), [Figure 2-9](#), [Figure 2-10](#), [Figure 2-11](#), and [Figure 2-12](#), which provide some examples of audio processing in an ASTRO[®] 25 system with 3600 RF sites interfaced through the SmartX Site Converter.

Scenario 1:

- Source: Subscriber radio transmits on an analog talkgroup
- Destinations: 3600 sites, MCC 7500 consoles

Figure 2-4 3600 Subscriber Radio Transmits on Analog Talkgroup

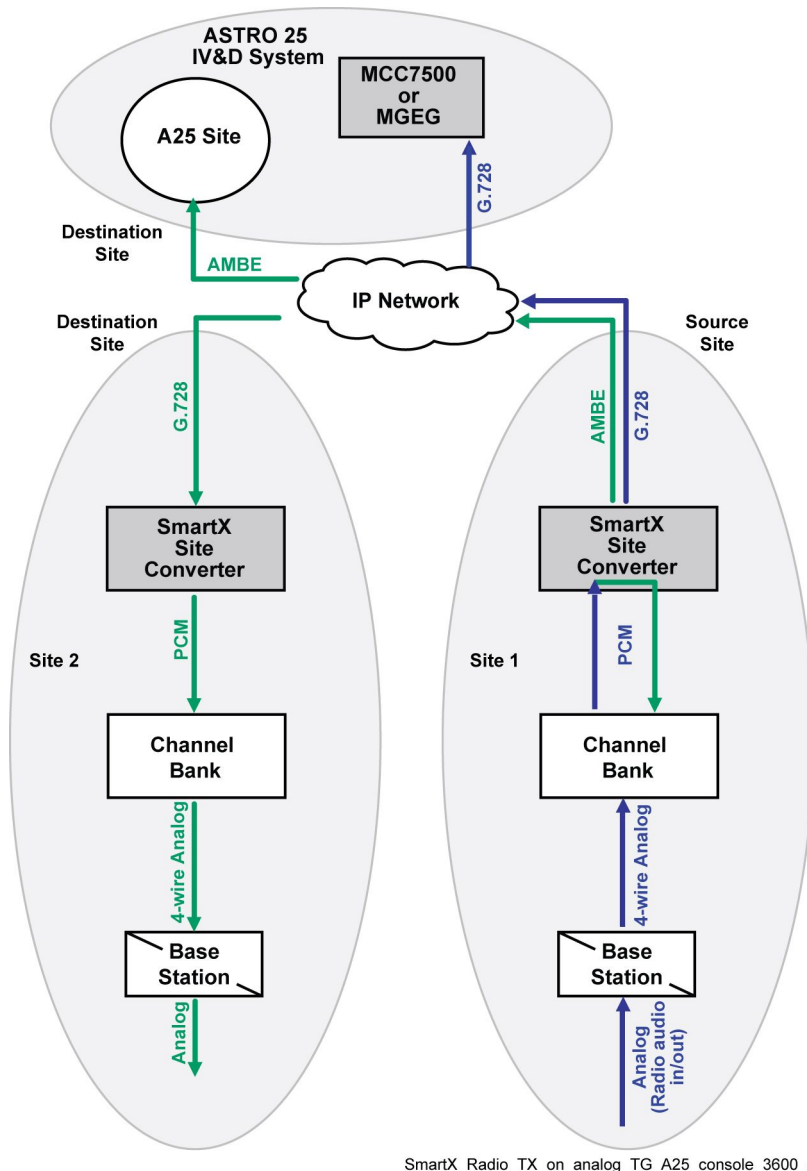


The following takes place when the source of audio is an analog subscriber from a 3600 site:

- The zone controller receives the request and assigns a multicast address to the call.
- The SmartX Site Converter generates G.728 audio packets in the format required by the ASTRO[®] 25 system. Once the G.728 audio packets are created, they are routed on the packet network through the assigned multicast address for G.728 audio.
- The channel bank transports digital voice in packet format.
- At the destination site, the SmartX device receives G.728 audio from the IP network and must enable the transmission of analog audio for the call at the 3600 RF site. This involves devocoding the G.728 audio and routing PCM audio on the DS0 for the channel assigned to the active call.

Scenario 2:

- Source: Subscriber radio transmit on an analog talkgroup
- Destinations: 3600 sites, ASTRO[®] 25 sites, MCC 7500 consoles

Figure 2-5 Radio TX on Analog TG, A25 — Console and 3600 Destinations

The following takes place when the source of audio is an analog subscriber from a 3600 site:

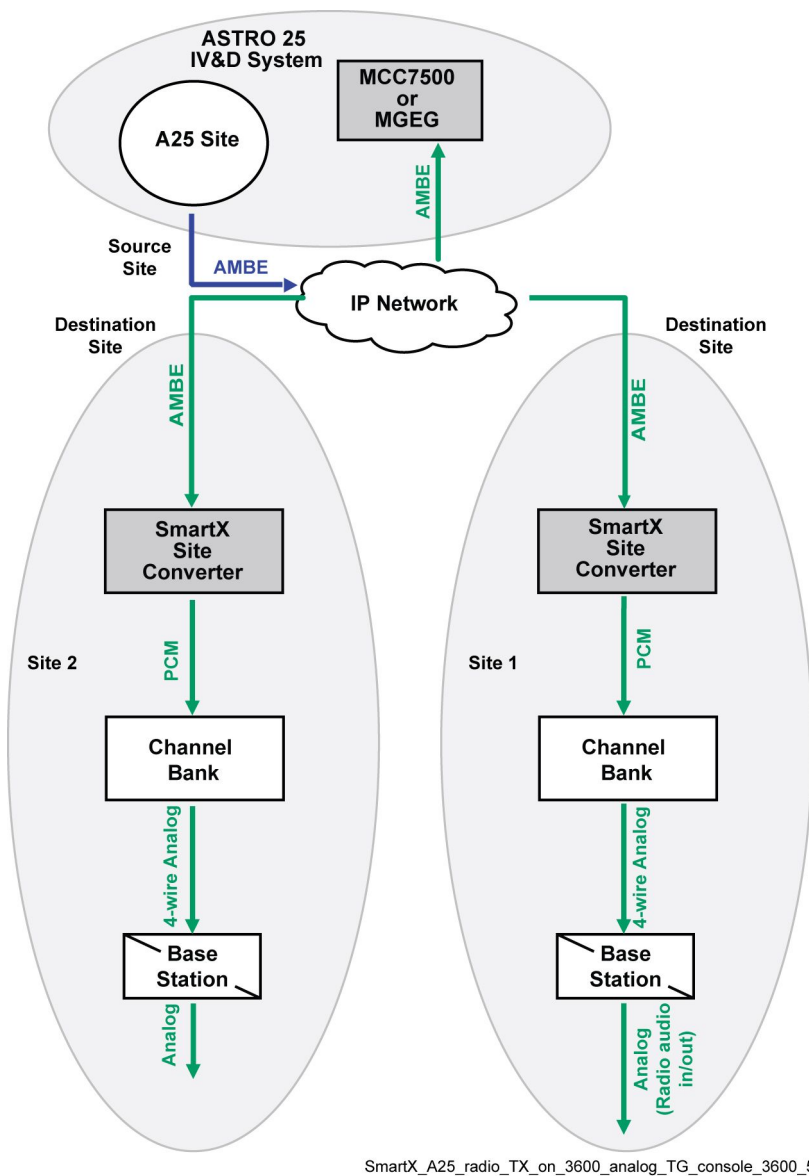
- Special audio routing is necessary to enable both 3600 sites/consoles, that need G.728 audio, and ASTRO[®] 25 sites, that need AMBE audio, to participate in the call.
- Two vocoded versions of the received analog audio must be created by the SmartX Site Converter, G.728, for routing to other 3600 sites and consoles, and AMBE for routing to ASTRO[®] 25 sites.
- The ZC must allocate two multicast addresses in order to route two versions of the audio, one for each version of audio.
- The ZC must inform the sourcing SmartX Site Converter device of the two multicast addresses along with the audio format to use on each multicast group.

- The ZC must also inform each destination in the call of the multicast address to obtain the correct version of audio (for example, the console and 3600 sites receive the multicast ID for G.728 audio and the ASTRO[®] sites receive the multicast ID for the AMBE audio).

Scenario 3:

- Source: ASTRO[®] 25 radio transmits on a talkgroup where all the subscriber radios at the 3600 sites are analog
- Destinations: 3600 site, MCC 7500 console

Figure 2-6 ASTRO 25 System Subscriber Radio Transmits on 3600 Analog Talkgroup

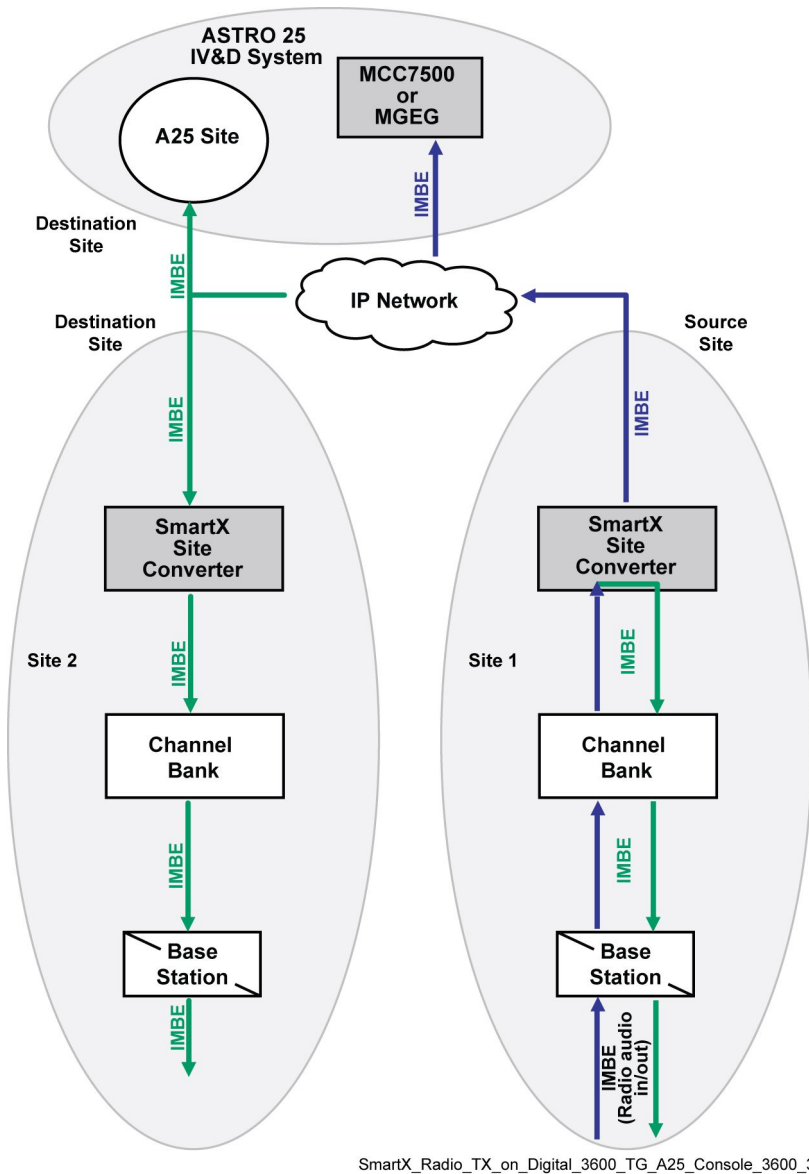


The following takes place when the source of audio is a radio at an ASTRO® 25 site and the destination is an analog talkgroup at the 3600 sites:

- The zone controller receives the request and assigns a multicast address to the call.
- The ASTRO® 25 radio transmits its audio over its assigned voice channel.
- The audio is received in its AMBE format at the destination MCC 7500 console sites.
- At a destination 3600 sites, the SmartX Site Converter receives the AMBE audio and sends the audio to the channel bank on a DS0 assigned to the call.
- The channel bank converts the PCM audio to 4-wire analog and sends it to the base station assigned to the call at the 3600 sites.

Scenario 4:

- Source: Subscriber radio transmits on a 3600 digital talkgroup (IMBE)
- Destinations: 3600 sites, ASTRO® 25 Sites, MCC 7500 consoles

Figure 2-7 Radio TX on Digital 3600 TG, A25 — Console and 3600 Destinations.

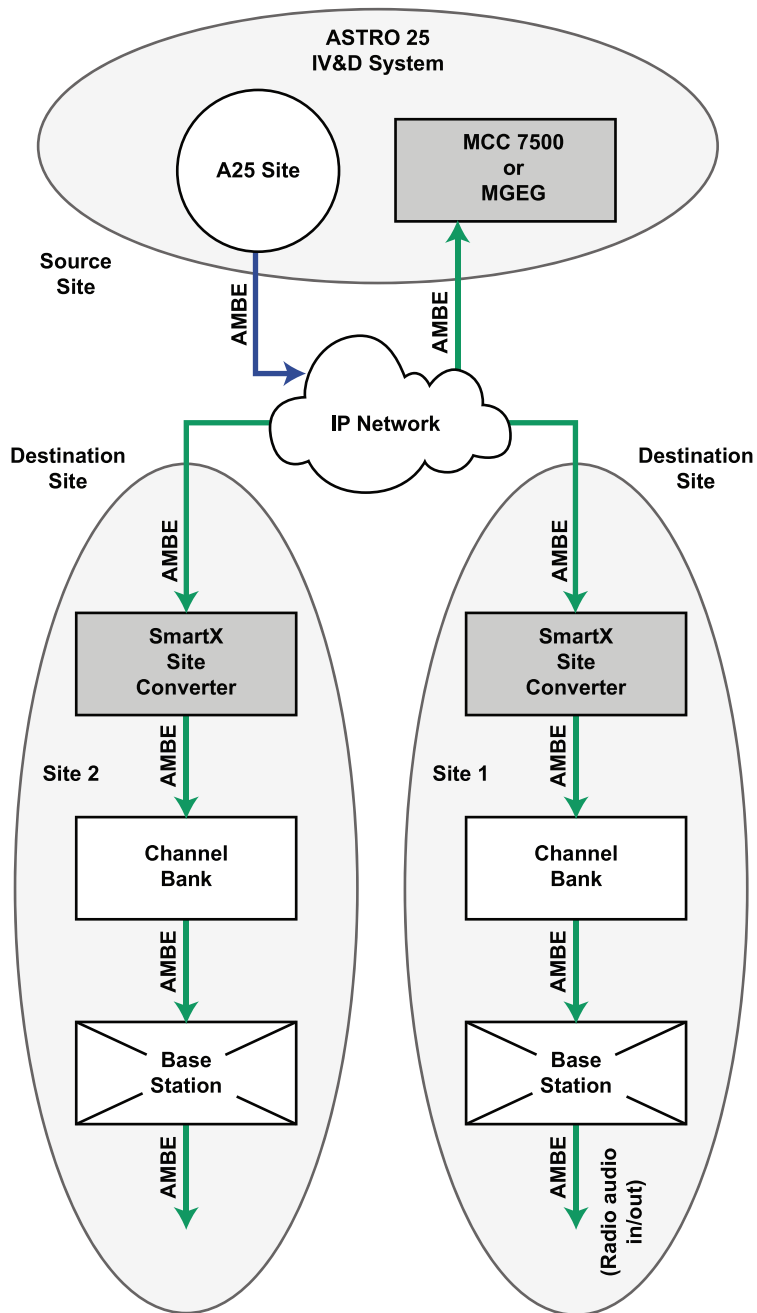
The following takes place when the source of audio is a digital subscriber from a 3600 site:

- The zone controller receives the request and assigns a multicast address to the call.
- At a source site, the SmartX Site Converter receives the audio on a DS0 assigned to the active analog call.
- The SmartX Site Converter repeats the audio back to the sourcing 3600 site to enable in the cabinet repeat. This is determined by the signaling in the call grant from the zone controller (destination flag).
- The SmartX Site Converter generates audio packets in the format required by the ASTRO[®] 25 system. Once the audio packets are created, they are routed on the packet network through the assigned multicast address.
- At the destination site, the SmartX device receives the audio packets from the IP network and must enable the transmission of IMBE audio for the call at the 3600 RF site.

There is no vocoding or devocoding of the IMBE packets transmitted by the source radio, they remain in their native format as they travel to their destination. The only conversion that takes place at the source and destination SmartX Site Converter is between the 3600 audio plane format and the ASTRO[®] 25 audio plane format.

Scenario 5:

- Source: ASTRO[®] 25 radio transmits on a talkgroup where all the subscriber radios at the 3600 sites are digital (IMBE)
- Destinations: 3600 site, MCC 7500 console

Figure 2-8 A25 Radio TX on 3600 Digital TG — Console and 3600 Destinations

SmartX_A25_radio_TX_on_3600_digital_TG_console_3600_A

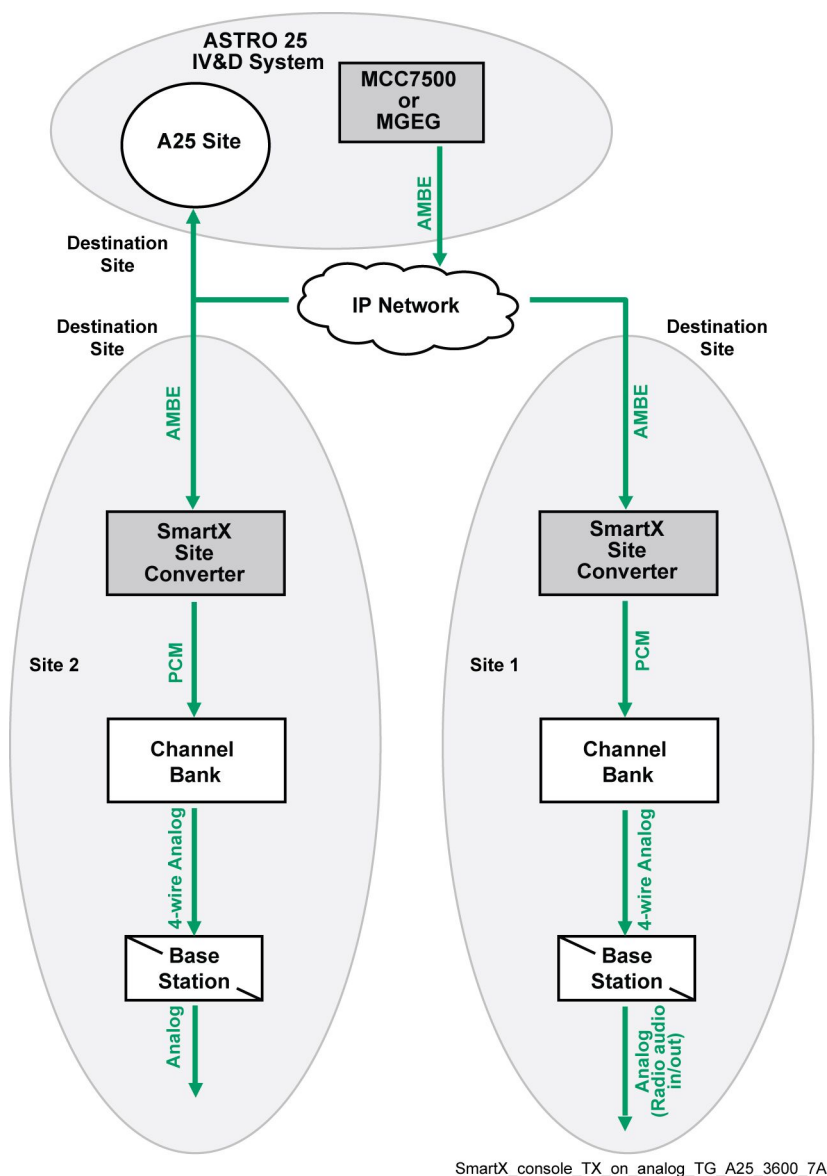
The following takes place when the source of audio is a radio at an ASTRO® 25 site and the destination is an analog talkgroup at the 3600 sites:

- The zone controller receives the request and assigns a multicast address to the call.
- The ASTRO® 25 radio transmits its audio over its assigned voice channel.
- The audio is received in its AMBE format at the destination MCC 7500 console sites.
- At a destination 3600 sites, the SmartX Site Converter receives the AMBE audio and sends the audio to the channel bank as packetized audio on a DS0 assigned to the call.
- The channel bank converts the IMBE audio to data and sends it to the base station assigned to the call at the 3600 sites.

Scenario 6:

- Source: MCC 7500 console transmits on a 3600 analog talkgroup
- Destinations: 3600 sites, ASTRO[®] 25 sites

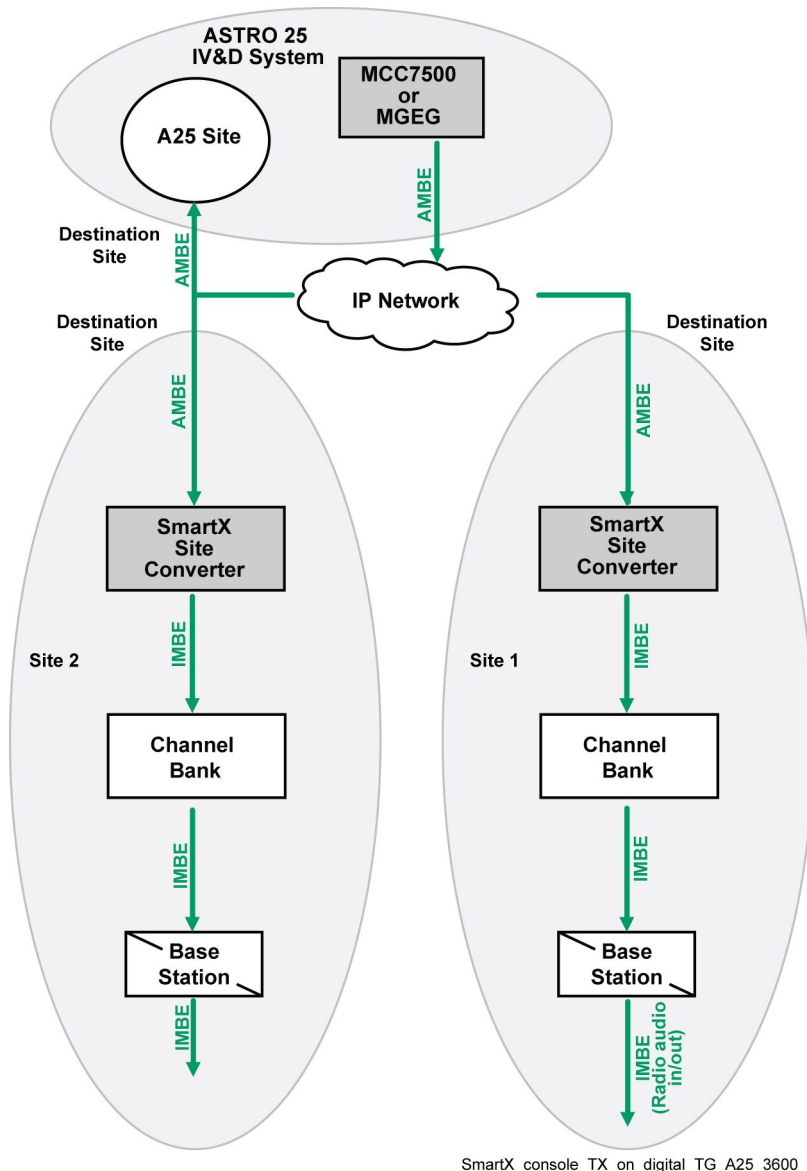
Figure 2-9 MCC 7500 Console Transmits on 3600 Analog Talkgroup



This is similar to Scenario 3 except that the audio originates at an MCC 7500 console instead of a radio at an ASTRO[®] 25 site.

Scenario 7:

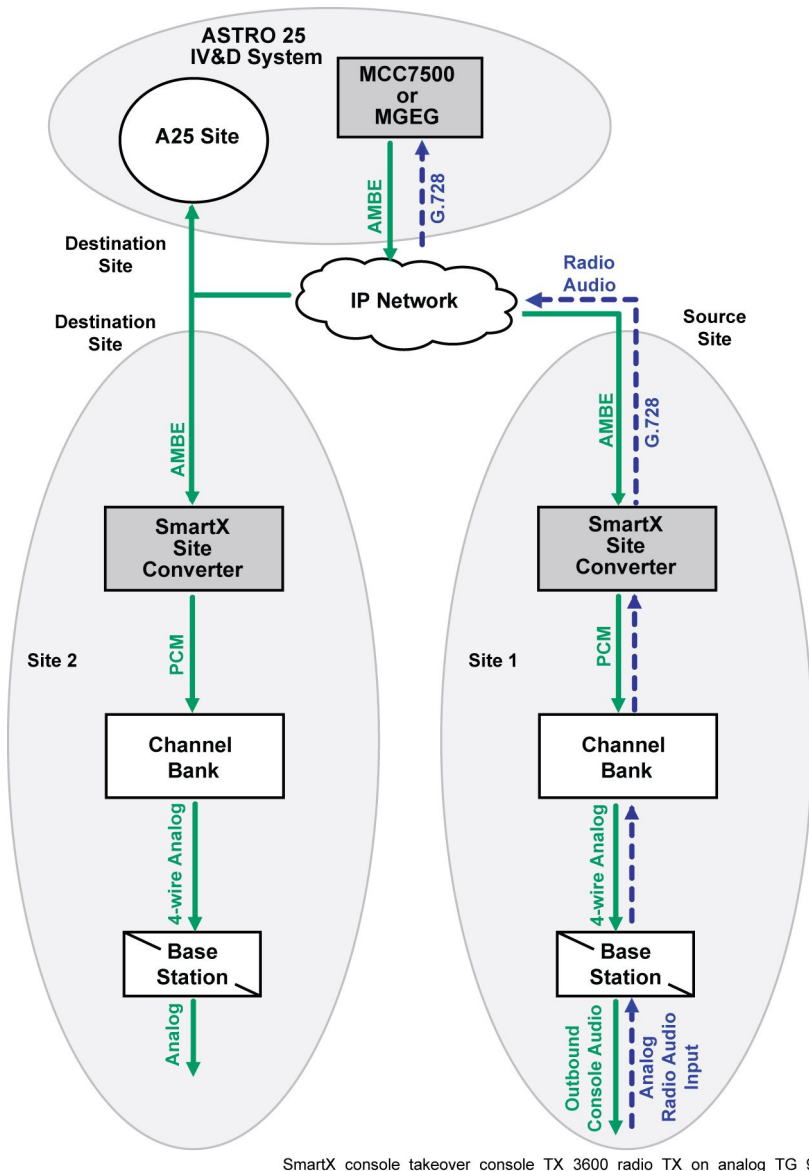
- Source: MCC 7500 Console transmits on a 3600 digital talkgroup
- Destinations: 3600 sites, A25 sites, console

Figure 2-10 MCC 7500 Console Transmits on 3600 Digital Talkgroup

This is similar to Scenario 5 except that the audio originates at an MCC 7500 console instead of a radio at an ASTRO® 25 site.

Scenario 8:

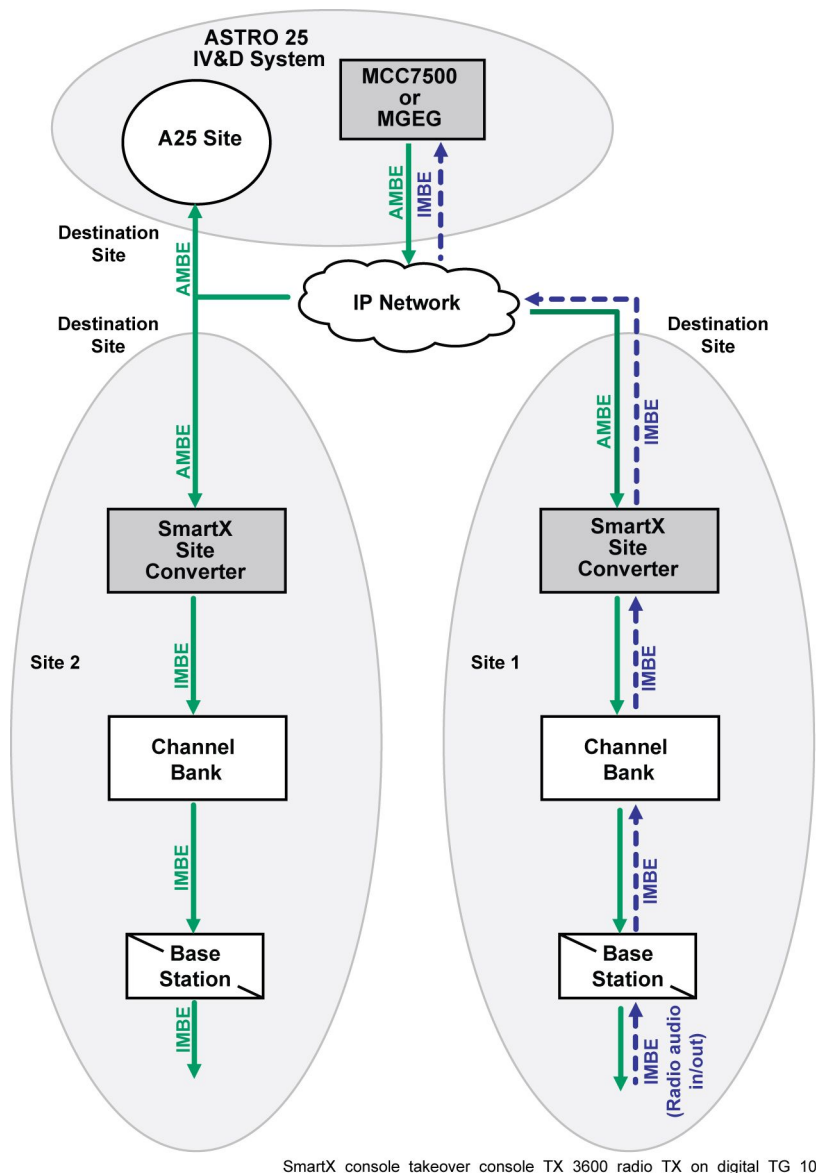
- Source: Radio on analog talkgroup at the source 3600 RF site
- Destinations: 3600 sites, ASTRO® 25 sites, console
- Console keys up on the same talkgroup

Figure 2-11 Console Takeover, Console, and 3600 Radio Transmit on 3600 Analog Talkgroup

Console transmissions have a higher priority in the system than those originating at subscribe radios. [Figure 2-11](#) and [Figure 2-12](#) show that if a console initiates a transmission on a currently active talkgroup, the console is given control of the call and its audio sent to the sites for transmission to the talkgroup. The audio from the radio that was transmitting at the time of the console takeover is routed only to the console. The dashed arrows in both figures indicate the path and conversions for the radio at the 3600 RF site.

Scenario 9:

- Source: Radio on a digital talkgroup at the source 3600 RF site
- Destinations: 3600 sites, ASTRO[®] 25 sites, console
- Console keys up on the same talkgroup

Figure 2-12 Console Takeover, Console, and 3600 Radio Transmit on 3600 Digital Talkgroup

NTP Services

Network Time Protocol (NTP) is a service used to provide time and date information to devices in the network. It is used in the system to synchronize all devices to the same time and date and allow those devices to include time stamps in error logs and SNMP fault information. The ASTRO® 25 system provides two sources of NTP information for the SmartX device. The primary source is ntp02.zone# and the secondary source is ntp03.zone#. Prior to system release 7.8, the primary source was ntp01.zone# with a secondary source of ntp02.zone#. The SmartX Site Converter does not support Dynamic System Resilience (DSR), so there are no additional NTP sources.

See the appendix in the *NTP Server* manual for more information.

Zone Core Protection and 3600 Sites

3600 sites utilizing the SmartX Site Converter and Zone Core Protection (ZCP) can coexist on the same ASTRO® 25 system. However, SmartX site links are in the clear while any other 7.x sites remain encrypted. For more information, see the *Router Encryption and Authentication* manual.

ISSI 8000/CSSI 8000 Intersystem Gateways and 3600 Sites

ISSI 8000/CSSI 8000 Intersystem Gateway does not offer roaming in QUANTAR® sites. Therefore, the 3600 Smart-X traffic does not pass over the P25 ISSI link, so users need to patch a P25 talkgroup to a Smart-X talkgroup. For more information, see the *ISSI 8000/CSSI 8000 – Intersystem Gateway* manual.



NOTE

A GTR 8000 Base Radio can be implemented as a QUANTAR® replacement within a 3600 and SmartZone® system. The implementation details are in the *Quick Guide for Replacing a Trunked 3600 QUANTAR with a GTR 8000 Base Radio* manual.

Network Management

.....

The information that used to be programmed using the specific network manager for the 3600 RF sites is now programmed at the ASTRO[®] 25 network managers. The sections that follow document the support provided by specific applications.

Provisioning Manager

The Subscriber Modulation Map object is programmed in the Provisioning Manager. The Subscriber Modulation Map object allows the system manager to map up to 32 sets of Radio and Talkgroup ID ranges to designated modulation types (ASTRO[®] 25 system or analog). This object is used when SmartZone[®] sites are connected to an ASTRO[®] 25 system through a SmartX Site Converter. The modulation ranges are used by the zone controller to determine the type of resources assigned to a radio or talkgroup operating in the sites that were interfaced to the ASTRO[®] 25 system through the SmartX Site Converter. For example, a radio or talkgroup ID that falls in an analog range is assigned analog resources at its site location.

For detailed information about the subscriber fields, see the *Provisioning Manager* manual or *Provisioning Manager Online Help*.

Configuration/Service Software

The following information is programmed through the CSS:

- Initial network configuration parameters
- NTP (date/time)
- SNMPv3 configuration
- DNS configuration and Centralized Event Logging services
- RADIUS service
- Set up the warning banner using the CSS
- Secure credentials
- Secure SHell (SSH) configuration
- Centralized authentication

Configure the SmartX Site Converter by completing the fields on the following screens:

- NTP Definition
- Site
- Network Services Configuration
- Remote Access Services

For components programmed through CSS, see the *CSS Online Help*.

Unified Network Configurator

The following tasks are performed through the UNC:

- Configuration of system parameters
- Configuration of site and zone parameters
- Configuration of channel parameters
- OS images (Operating System and applications)

The UNC views the SmartX Site Converter in the same way that it views an ASTRO[®] 25 site. Any information to/from a 3600 site must be routed through its attached SmartX Site Converter.

Unified Event Manager

When the 3600 site is moved to the ASTRO[®] 25 system, it is discovered by the UEM. The fault manager can display the current state information for the site. Faults, such as disconnecting a channel and dropping a site link generate a trap that can be displayed on the UEM.

UEM supports:

- **Remotely force a 3600 site into “Site Trunking”, “Wide Trunking”, “Site Failsoft” and “Site Off” state** — This is similar to what is done for A25 sites. See “Issuing commands” procedures in the “UEM Operation” chapter of the *Unified Event Manager* manual.
- **Remote Enable/ Disable Control of 3600 Site Channels** — To issue the diagnostic command, enter “SmartZone Site Equipment”. For the exact procedure, see “Issuing Commands” in the “UEM Operation” chapter of the *Unified Event Manager* manual.
- **Remote Enable/ Disable the SmartX Site Converter** — For the exact procedure see “Issuing Commands” in the “UEM Operation” chapter of the *Unified Event Manager* manual.

Once all the Gold Elite Console equipment has been interfaced to the ASTRO[®] 25 system, the site is discovered by the UEM to get the most current fault status from the site. The UEM monitors:

- **Board level fault events** — Reported from the SmartX Site Converter to the UEM include:
 - General state of the SmartX Site Converter — initializing, enabled, disabled, E1/T1 link synchronization malfunction
 - Site Control link state — up or down
 - Zone Controller Link state — up or down
 - Zone Controller Link redundancy state — active or standby
 - Misconfiguration
- **E-mail notification of supported fault events** — These events are supported by the UEM E-mail notification feature. For details, see “Event and Alarm Configuration Introduction” in the *Unified Event Manager* manual.

ZoneWatch

In addition to wide area call activity, the ZoneWatch application provides a degree of fault indication for an individual site. In the case of a 3600 RF site, channel indicates a “green” color if the UEM has detected no faults for the channel. The no fault indication of “green” are displayed even when the channel has been configured in the infrastructure through the UNC, but no physical channel infrastructure exists at the site for the configured channel. This behavior is due, in part, to the fact that the physical channel equipment does not have direct IP connectivity to the UEM.

Radio Control Manager

Support provided by Radio Control Manager (RCM) to the 3600 sites include the following:

- **Selective Radio Inhibit**— functionally disables selected radios that are currently affiliated to the system. The inhibited radios can still be powered on and off, but they can only accept a Cancel Inhibit command. No voice communications are possible, but the radio continues to listen to the control channel and re-affiliates to the system.
- **Dynamic Regrouping** — assigns an affiliated radio to a new talkgroup for communication purposes. This command allows radios to be reassigned over the air without the need for intervention by the radio user. If a 3600 radio is regrouped to a talkgroup that belongs to a multigroup, the radio does not hear the multigroup since the system does not generate the talkgroup to multigroup association to the target radio
- **Snapshot** — Displays the last status information for the radio. The Snapshot does not send a request to the radio. Instead, it reads the information from a database. For the 3600 radios, Snapshot database no longer update its regroup status on Dynamic Regroup or Cancel Dynamic Regroup command if the zone did not issue the command.
- **Status** — ASTRO[®] 25 system status (maximum of 16 statuses are supported in ASTRO[®] 25 system)
- **Message** — Messages from 3600 radios are converted and sent to the “Status display” on the ASTRO[®] 25 Radio Control Manager (RCM). Up to 16 messages are supported by the 3600 radios but only the first 8 messages are supported through the SmartX Site Converter to the ASTRO[®] 25 RCM.

Call Processing

From a call services perspective, [Table 2-1](#) lists the types of calls supported by an ASTRO® 25 system. Note that digital Vector Sum Excited Linear Prediction (VSELP) audio and analog 12KB SecureNet are not supported.

Table 2-1 Types of Calls Supported by the ASTRO 25 System

Type of Call	Supported
Talkgroup Call between 3600 Radios and 9600 Radios in Common Talkgroup	✓
Talkgroup Call (Clear)	✓
Talkgroup Call utilizing Message Trunking with PTT ID	✓
Talkgroup Call utilizing Transmission Trunking	✓
Talkgroup Call (ASTRO® Encrypted)	✓
Emergency Call	✓
Emergency Alarm	✓
Multigroup Call	✓
Supergroup Call	✓
Priority Monitor (Scan)	✓
Enhanced Private Call (uses ring sequence)	✓
Call Alert	✓
Console Priority	✓
Busy Queuing/Callback	✓
AllStart/Faststart Call Set-Up	✓
Trespass Protection (for multi-zone, OmniLink radios)	✓
Console Audio Logging Using LOMIs (upgraded to ASTRO® 25)	✓
MCC 7500-based IP Logging Solution	✓
MultiGroup Call (initiated by radio)	✓
MultiGroup Radio Scan within a Zone	✓
Console Talkgroup Call	✓
Console Multigroup Call	✓
Console Only Talkgroup Call	✓
Emergency Call/Alarm	✓
Console Secure Call (Trunked ASTRO® 25 Secure Only)	✓
Talkgroup Call between a 3600 user (at 3600 site) and a 9600 user in TDMA-mode	✗
Private Call II (does not use ring sequence to call another radio)	✗

Operational Considerations

Operational differences between 3600 systems and ASTRO® 25 systems require careful planning and coordination of radio and talkgroup IDs when interfacing 3600 sites and subscriber radios with an ASTRO® 25 system. It also requires an understanding of differences in the way some features operate.

The following sections represent only a partial description of the impact to 3600 radios when they operate in the ASTRO® 25 environment.

Contact Motorola for a more detail description of the impact to a specific system.

Talkgroups

Points to consider when creating talkgroups in an ASTRO® 25 system that includes 3600 sites:

- ASTRO® 25 systems allow the creation of a total of 16,000 talkgroups and multigroups. The assignable ID numbers can be anywhere in the range from 80000001 to 80065534.
- SmartZone® 3600 systems support a maximum of 4000 talkgroup/multigroups with IDs within the range of 800001 to 804094.
- Any talkgroup or multigroup communication that must include 3600 and ASTRO® 25 radios must have an ID in the 800001 to 804094 range.
- If an ASTRO® 25 site is a Dynamic Dual Mode site, 3600 sites/users cannot participate in a talkgroup that is assigned as TDMA-only in the Network Manager.

Emergency Call

Emergency group call operation functions the same between SmartZone® and ASTRO® 25 systems. The only difference is that SmartZone® sends an “emergency indication” message for logging devices to determine if this is the first time a radio has keyed in emergency mode. ASTRO® 25 systems do not support emergency indication and the message are not generated when a 3600 SmartZone® radio initiates an emergency call.

Private Calls on ASTRO 25 System and a SmartZone 3600 System

Private Call Enhanced has the following operational differences in ASTRO® 25 versus a SmartZone® 3600 system:

- SmartZone® Enhanced Private Calls operate slightly differently when utilized as part of an ASTRO® 25 system using SmartX Site Converter. In SmartZone®, Enhanced Private Calls work more like a dispatch call in that a channel is assigned for the PTT and is released after a short hang time expires. Subsequent PTTs while in Private Call (PC) mode result in a channel being reassigned and the call continuing. 3600 radios, when exiting Private Call mode do not signal the end of the call, they merely return to normal dispatch mode. The Private Call only ends when hang time expires and the radios no longer key up on the Private Call.
- In ASTRO® 25 systems, Private Calls operate similar to a telephone call in that channel resources are assigned for the length of the call. To end the ASTRO® 25 system Unit to Unit call, the hang time must expire or one of the call participants exits Private Call mode and signal the infrastructure to end the call.

- Since the SmartX Site Converter communicates with an ASTRO® 25 system zone controller and 3600 radios do not signal the termination of the enhanced private call; the system utilizes the expiration of the extended hang time to end the call (unless there is a console involved in the call which can terminate the PC). Therefore, the 3600 radios are assigned to the Private Call and stay on the voice channel for the entire length of the conversation. Once the extended hang time ends, the call is ended.
- Any new private call request from a radio in the recently ended private call requires the user to exit and re-enter Private Call mode before restarting the Private Call.

Secure Downgrade

SmartZone® systems do not allow users that are active in any type of secure call to downgrade the secure call to a clear call. ASTRO® 25 systems do allow radios to downgrade secure calls to a clear call. To maintain compatibility with SmartZone® operation, ASTRO® 25 systems with 3600 sites do not allow secure calls to be downgraded to clear calls if the talkgroup ID of the secure call is between 800001 and 804095. Also, private calls that include a 3600 radio user do not allow secure downgrades to clear. Talkgroups greater than 804095 and private calls between two ASTRO® 25 radio users are able to downgrade calls from secure to clear.

Secure Upgrades

In SmartZone® 3.0 systems, it is possible for a clear talkgroup call to be upgraded from clear to secure during the active clear talkgroup call. In SmartZone® 4.1, this feature was not allowed and the call must be clear throughout the length of the call. Since ASTRO® 25 systems allow for clear calls to be upgraded, with SmartX Site Converter, 3600 calls can now be upgraded if the system is configured to allow this capability.

Conditions for Wide Trunking

3600 RF sites connected to an ASTRO® 25 system through the SmartX Site Converter need to meet the following conditions to be considered in wide area trunking:

- ZC/site converter link established
- Site converter to 3600 circuit-based call control protocol link established
- 3600 site has one operational control channel capable channel
- 3600 site has one operational voice capable channel
- the user requested site state is Wide Trunking
- the ZC has been configured to match the operational channels previously mentioned
- at least one audio Gateway/Rendezvous Point (RP) router is in service.

This page intentionally left blank.

SmartX Site Converter Installation

This chapter details installation procedures relating to the SmartX Site Converter.

SmartX Site Converter Installation Prerequisites

The installation information in this chapter is based on two assumptions:

- The SMARTNET® 3.1/3.2 or SmartZone® 3.0/3.5/4.1 system has been upgraded to the appropriate level of hardware and software by Motorola's Field Services team.
- The ASTRO® 25 IV&D system is installed and operational.

The following prerequisites must be met before installing the SmartX Site Converter:

- Install new configuration files in the core routers.
- Install configuration files in the site gateway, which is installed with the SmartX Site Converter.
- Install channel banks at the master site. Also, an isolating device such as a Channel Service Unit (CSU), must be provided for the site converter connections if T1/E1 facilities from a Public Switched Telephone Network (PSTN) are used as transport between the remote sites and a site converter at the master site.

If the existing SmartZone® system includes Gold Elite consoles, migration is accomplished through Central Electronics Bank (CEB), Ambassador Electronics Bank (AEB), and Motorola Gold Elite Gateway (MGEG) links and not through the SmartX Site Converter.

[Process 3-1](#) provides a list of items you need to have access to before you can complete the installation and configuration procedures in this chapter.

Process 3-1 Prerequisites for Initial SmartX Site Converter Installation and Configuration

- 1 Make sure that the ASTRO® 25 system CDs and DVDs are available to you. Specifically, you need the Transport, Motorola SmartX Site Converter, and Motorola VPM OS Image CDs to perform [Procedure 3-14, "How to Load the SmartX Site Converter OS Images to the UNC,"](#) on [page 3-29](#).

Install applications, as needed, from the Windows Supplemental CD as follows:
Insert the Windows Supplemental CD, log on with administrator privileges, open the command window, change to \WIF directory on the CD/DVD drive, then execute the following command:
`WindowsInstallFramework.exe /e /i putty.xml`

This installs PuTTY, which can be used to initiate secure sessions with other devices that support secure protocols. You need the PuTTY application installed for SSH to the UNC server application, which you need to perform some of the procedures in [Process 3-3](#). See the *Securing Protocols with SSH* and *Unified Network Configurator* manuals.

A License Key CD is needed to install the VoyenceControl license key on the NM client for the UNC. See the *Unified Network Configurator* manual.

**NOTE**

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

Other system media that you need to install and configure the information assurance features are:

- Samba Winbind CD to install centralized authentication client software on the Generic Application Server.
- MOTOPATCH CD for the latest Windows OS updates.

- 2 Make sure that you have the user names, passwords and procedures you need to access the devices on the network. For specific user names and passwords to access devices on the network, contact your system administrator.

Set up the users in the IT Admin group in Active Directory Users and Computers. See the *Authentication Services* manual.

Process 3-1 Prerequisites for Initial SmartX Site Converter Installation and Configuration
(Continued)

- 3** Obtain the following values from the system administrator:
 - SmartX Site ID number
 - SmartX Site Converter IP address 1 and 2
 - Primary, secondary, and tertiary DNS IP addresses, as well as the DNS Domain Name
 - Primary and secondary NTP IP addresses
 - Primary and backup SYSLOG server Fully Qualified Domain Names (FQDN)
 - RADIUS FQDN parameter value
 - RADIUS Row Status parameter value
 - RADIUS Service Time Out (sec) parameter value
 - RADIUS Service Retransmits Attempts parameter value
 - RADIUS Service Dead Timer (min) parameter value
 - RADIUS Specific Key parameter value
 - RADIUS Service Global Key parameter value
 - SmartX Site Converter line interface number
 - ZC site link path 1 IP address
 - ZC site link path 2 IP address
 - ASYNC link number
 - Analog and digital slot numbers
 - Host name to access the UNC server application using SSH (<username>@<IP address> format)
- 4** Ensure that you have the default credentials (local accounts, central authentication, and SNMPv3) for the device being installed, as well as updated passwords for those types of accounts (so that you can change the password once you install the device). Contact your system administrator, if you do not have this information. See the *SNMPv3* manual for more information.

Process 3-1 Prerequisites for Initial SmartX Site Converter Installation and Configuration (Continued)

- 5** Ensure that the SmartX device is configured as a Remote Authentication Dial-In User Service (RADIUS) client on the RADIUS server. See the *Authentication Services* manual for more information.
- 6** To use the EMC Ionix Network Configuration Manager/VoyenceControl component of Motorola's centralized configuration application for any of the remote site device procedures, you need to set up the Unified Network Configurator (UNC). Depending on your organization's policies, you may also need to implement a secure protocol between the UNC and the remote site device. Before performing any procedures using VoyenceControl, you must discover the site converter in VoyenceControl and pull their configurations to the Unified Network Configurator's database. See the following ASTRO® 25 system documentation:
 - *Unified Network Configurator* manual
 - *Securing Protocols with SSH* manual
- 7** A variety of tools are needed to install and service the equipment. If information is needed regarding where to obtain any of the equipment and tools listed, contact the Motorola Solution Support Center (SSC). The following is a list of general recommended tools for installing and servicing the hardware:
 - ☐ 1 service laptop with the Configuration/Service Software (CSS) application installed. See the instructions in the CSS CD-ROM jewel box for instructions on loading the CSS application on a service laptop or computer.
 - ☐ 3 Rack Units (RUs) of space for the VPM hardware and power supply tray, plus 1 RU for the required site gateway.
 - ☐ 1 screwdriver
 - ☐ 1 Ethernet cross-over cable
 - ☐ 1 DB9F to RJ-45 VPM programming adapter
 - ☐ 1 RS232 cable

Site Gateway Hardware Installation

.....

The site gateway provides a preferred alternative solution for the site router. See the *System Gateways – GGM 8000* manual for the installation of the site gateway. For the site router information, see the *System Routers - S6000/S2500* manual for instructions on how to install the S2500 router.

SmartX Site Converter Installation Process

Follow [Process 3-2](#) to install the Voice Processor Module (VPM) hardware and configure it as a site converter.

Process 3-2 Installing the SmartX Site Converter

- 1 Install the Voice Processor Module (VPM) hardware. See [Procedure 3-1, "How to Install the SmartX Site Converter Hardware,"](#) on page 3-9.
- 2 Configure the startup parameters with the CSS. See [Procedure 3-2, "How to Provision the SmartX Site Converter Serial Connection Parameters,"](#) on page 3-11 and [Procedure 3-3, "How to Configure the SmartX Site Converter Using CSS \(Ethernet Connection\),"](#) on page 3-12.
- 3 Enable secure credentials.
 1. Set up the SWDL transfer mode using the CSS. See [Procedure 3-4, "How to Set the SWDL Transfer Mode Using CSS,"](#) on page 3-14.
 2. Set up the local Password Configuration using the CSS (optional). See [Procedure 3-5, "How to Set the SmartX Site Converter Local Password Configuration ,"](#) on page 3-15.
 3. Set the current date and time in CSS. See [Procedure 3-6, "How to Set the Date and Time on the SmartX Site Converter,"](#) on page 3-18.
 4. Set the serial security services. See [Procedure 3-7, "How to Set the Serial Security Services,"](#) on page 3-19.
 5. Change the SNMPv3 configuration and user credentials from CSS on a selected device in the remote site. See [Procedure 3-8, "How to Change SNMPv3 Configuration and User Credentials on the SmartX Site Converter,"](#) on page 3-20.
 6. Create, update, or delete an SNMPv3 user. See [Procedure 3-9, "How to Add or Modify an SNMPv3 User,"](#) on page 3-23.
- 4 Verify the SNMPv3 credentials. See [Procedure 3-10, "How to Verify SNMPv3 Credentials on the SmartX Site Converter,"](#) on page 3-24.
- 5 Set the Network Services Configuration using CSS.
 1. Configure DNS using the CSS. For instructions on using CSS to configure DNS on devices, search on "Network Services" in CSS Online Help. Also, see the *Authentication Services* manual.
 2. Configure the SmartX Site Converter for SSH. See the *Securing Protocols with SSH* manual's "Configuring SSH for RF Site Devices and VPMs Using CSS – Overview" section.
 3. Configure the local cache size for the SmartX Site Converter. See the *Authentication Services* manual.
 4. Enable Centralized Authentication using the CSS. See the *Authentication Services* manual.
 5. Customize the login banner text using CSS (optional). See [Procedure 3-11, "How to Customize the Login Banner,"](#) on page 3-25.
 6. Enable RADIUS Authentication using the CSS. See the *Authentication Services* manual.
 7. Enable Centralized Event Logging using the CSS (optional). See the *Centralized Event Logging* manual.

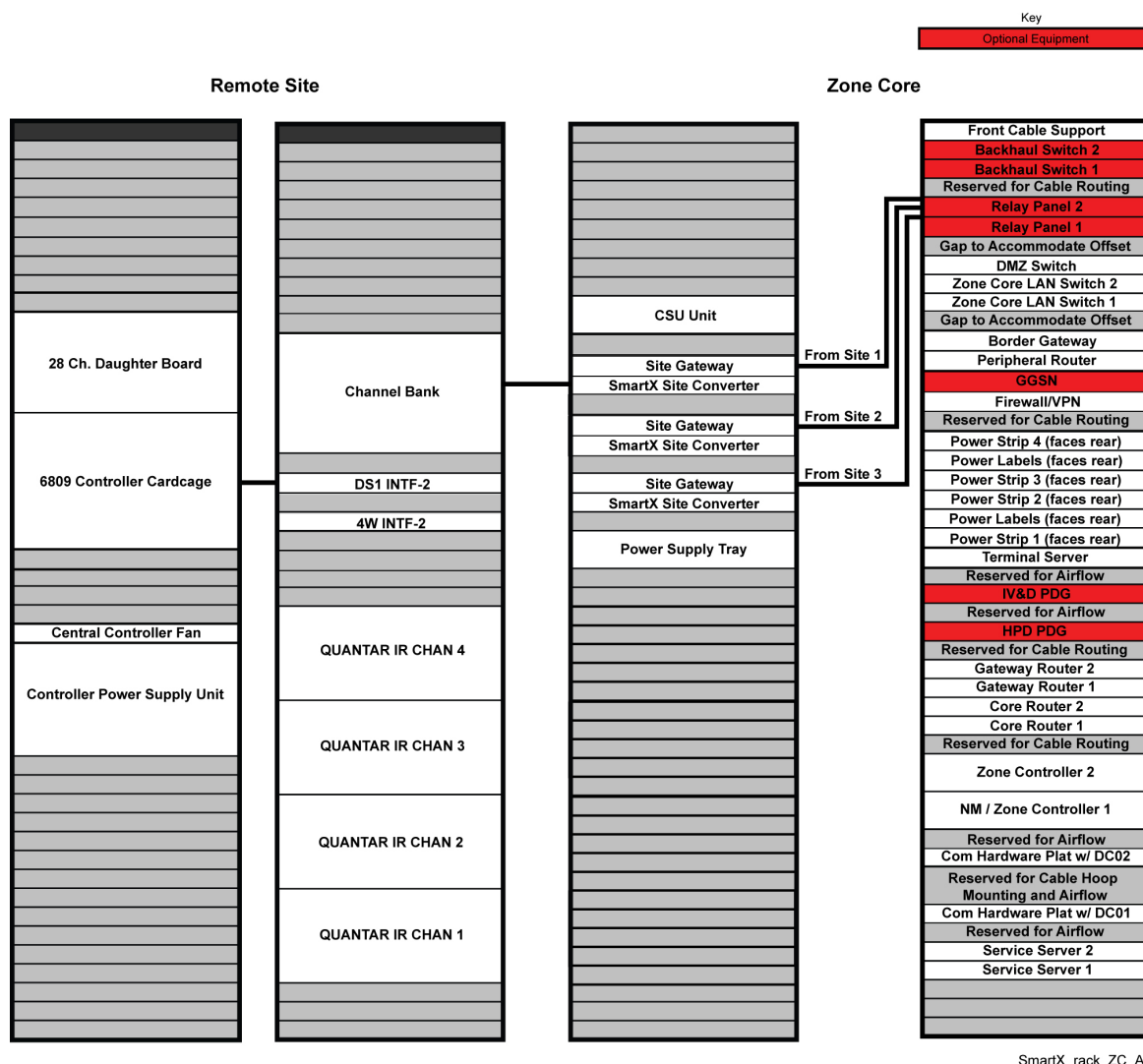
Process 3-2 Installing the SmartX Site Converter (Continued)

6	Connect the SmartX Site Converter to the site gateway. See Procedure 3-12, "How to Attach the SmartX Site Converter to the Site Gateway," on page 3-26.
7	Install the software on the SmartX Site Converter using the Unified Network Configurator (UNC). See Process 3-3, "Installing Software on the SmartX Site Converter," on page 3-26 for the procedures involved in the software installation on the site converter.
8	Configure the SmartX Site Converter. See Process 4-1, "Configuring the SmartX Site Converter," on page 4-1.

SmartX Site Converter Component Mounting

This section describes how to physically install the Voice Processor Module (VPM) hardware in the chassis. Before beginning this installation, verify that the power source, the site gateway, and the site equipment is located near the planned position of the SmartX Site Converter, and that there is adequate rack space.

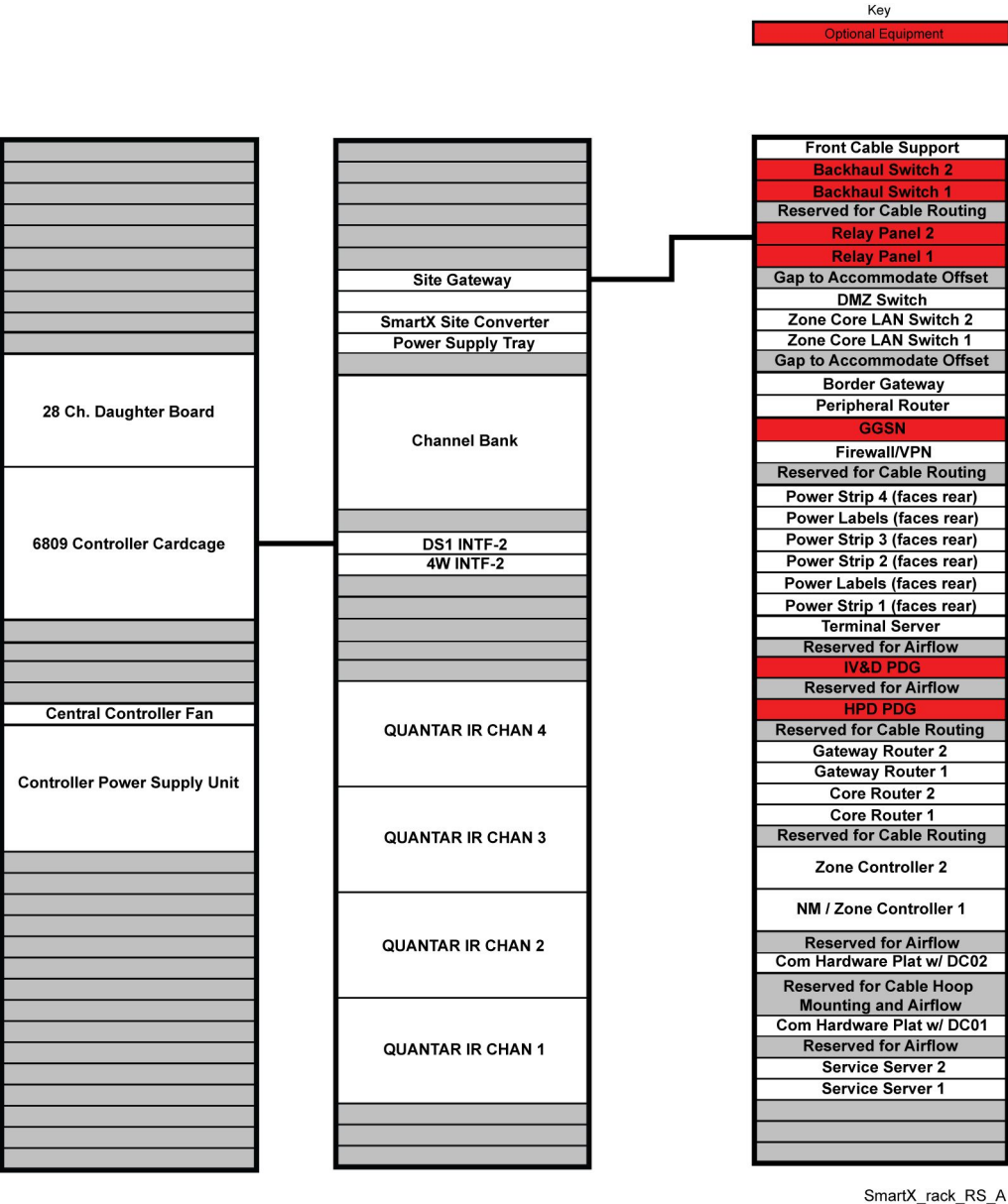
Each site converter uses one rack unit of space. The site converter uses a power supply, which sits on a 2–rack unit high tray. Each power supply tray can hold up to three power supplies. So, each site converter requires three rack units for the VPM hardware and power supplies, and three site converters would require five rack units of space (3 units for converters + 2 units for the power supply tray.) Additionally, one rack is needed for the site gateway, which is also connected to the SmartX Site Converter. See [Figure 3-1](#) for a typical zone core (master site) installation.

Figure 3-1 Site Converters in a Rack at the Zone Core**NOTE**

The site gateway provides a preferred alternative solution for the site router and resides in the same rack space. See the *System Gateways – GGM 8000* manual for a description of the hardware and installation.

See [Figure 3-2](#) for a typical remote site rack configuration. In another scenario, where the master site using leased T1/E1 circuits for connectivity to the remote 3600 sites, you must use an isolating device, such as a Channel Service Unit (CSU), so the SmartX Site Converter is protected against external transients in event of lightning strike or some other such event. However, if you are using microwave or fiber optics, this additional level of protection is not required.

Figure 3-2 A Site Converter in a Rack at the Remote Site




NOTE

The Site Gateway provides a preferred alternative solution for the site router. See the *System Gateways – GGM 8000* manual.

Install the Voice Processor Module (VPM) hardware installation as described in [Procedure 3-1](#) for use as a site converter. Once the VPM hardware is installed at the site, you can install the software and configure the device to function as a SmartX Site Converter within your ASTRO® 25 system.

Procedure 3-1 How to Install the SmartX Site Converter Hardware

1	Ensure that site gateway installation is complete.
2	Place the VPM hardware in the mounting rack.
	 <div style="background-color: #00AEEF; color: white; padding: 2px 5px; display: inline-block;">NOTE</div> <p>In order to easily access the ports and view the LEDS, Motorola recommends mounting the front of the SmartX Site Converter facing the rear of the rack.</p>
3	Fasten the grounding wire from the hardware to the rack, then tighten the grounding lug.
4	Connect the DC power cable to the round port on the chassis (left side) and the power supply.
5	Plug the AC power line cord to power supply and then into the AC power source.
6	Verify that the Power LED illuminates on the chassis (right side).

SmartX Site Converter Power Distribution Installation

.....

There is a single SmartX Site Converter for each site, so the configuration is quite simple. The basic power distribution is the site converter hardware, a power supply, and a power line cord. If there are multiple SmartZone[®] sites interfaced to the ASTRO[®] 25 system and all the site converters are installed in a rack at the master site, you should use a tray for the power supplies.

For more information on the hardware specifications, see the "SmartX Site Converter Component Mounting" section in this chapter, the "SmartX Site Converter Reference" chapter of this manual, and the *Voice Processor Module* manual for more information.

Using Software Download

The Software Download (SWDL) is an application that can transfer only, install only, or transfer and install new software to devices. The new software can be installed either locally at a site or on the Network Management subsystem. Individual devices not connected to the system can be downloaded using single device mode.

Data transfer can be performed by:

- **Clear SWDL** – transfer operations without security, based on the File Transfer Protocol (FTP)
- **Secure SWDL** – transfer operations are encrypted, based on the Secure File Transfer Protocol (SFTP)



NOTE

SWDL provisions the credentials for secure SWDL as part of initiating the SWDL operation. No user intervention is required. For a single device, secure or clear SWDL is configured by the user based on the SWDL transfer mode configuration within the CSS. The Unified Network Configurator (UNC) can be used to schedule and configure all devices in the system at once.



IMPORTANT

Before initiating transfer, SWDL connects to the site in the zone to discover all devices. The transfer mode of all devices displays in the SWDL window. It is important that all devices have the same SWDL transfer mode. Otherwise, the SWDL flags a mismatch of the SWDL transfer modes across site devices.

For information on how to configure the secure or clear SWDL transfer mode, see the *Unified Network Configurator* manual and “Device Security Configuration” in the *CSS Online Help*.

SWDL operation can be fault managed through UEM, syslog, local SWDL log files, user messages, and device reports. For further information on SWDL, see the *Software Download* manual.

SmartX Site Converter Initial Configuration

During the initial configuration, you must provide the IP addressing and enable the SNMP credentials, so that the Unified Network Configurator (UNC) can identify the SmartX Site Converter within the ASTRO[®] 25 system.

A laptop computer with the Configuration/Service Software (CSS) provides the VPM hardware with the necessary parameters to function as a site converter within an ASTRO[®] 25 radio system. [Procedure 3-2](#) describes how to set up the SmartX Site Converter start up parameters.

**NOTE**

The serial port uses the DB9F to RJ-45 VPM programming adapter and an RS232 cable.

Generally, there are two applications you can use to configure the SmartX Site Converters: CSS and UNC (not applicable for the serial port procedures which must be done using the CSS software). This manual focuses on the CSS procedures. If you want to configure the SmartX Site Converters using the UNC, see the *Authentication Services* manual or the *Unified Network Configurator* manual for the necessary procedures.

The CSS procedures in this manual assume CSS is loaded on your computer. See the *Private Network Management Client* manual, if necessary.


**IMPORTANT**

Changing the device IP Address causes the SNMPv3 configuration and user credentials to be reset.

Procedure 3-2 How to Provision the SmartX Site Converter Serial Connection Parameters

1	<p>Power on the VPM hardware.</p> <p>Result: The Power LED on the front of the SmartX Site Converter illuminates.</p>
2	<p>Connect the service laptop (with the CSS software) to the serial port on the SmartX Site Converter using an RJ-45 to female DB9 pin serial converter.</p> <div data-bbox="424 995 502 1081" data-label="Image"> </div> <div data-bbox="564 1017 651 1051" data-label="Section-Header">NOTE</div> <p>The serial port is designated by a footswitch icon on the Voice Processor Module (VPM) hardware. See Figure 1-2, "Rear View of the SmartX Site Converter — Power Connection and Ports in Use" on page 1-3 for the location of the serial port.</p> <p>Result: The laptop and VPM chassis are connected.</p>
3	<p>Launch the CSS application and connect to the device using a serial connection.</p> <div data-bbox="424 1287 502 1372" data-label="Image"> </div> <div data-bbox="564 1308 651 1342" data-label="Section-Header">NOTE</div> <p>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.</p> <p>Result: The Configuration Service Software main window appears.</p>
4	<p>To connect to the device using a serial connection, choose Tools, Connection Configuration.</p> <p>Result: The Connection Screen dialog box appears.</p>
5	<p>Set the following serial connection parameters, then click Connect.</p> <ul style="list-style-type: none"> • Select Serial from the Connection Type field. • Select a Baud rate of 19200. • Select the appropriate Com port (usually Com Port 1). <p>Result: A confirmation dialog box appears telling you that CSS has connected with the device.</p>
6	<p>Click OK. If authentication on the device is enabled, a login screen appears. Provide all required credentials. Click OK.</p>

Procedure 3-2 How to Provision the SmartX Site Converter Serial Connection Parameters (Continued)


7	<p>Select Tools, Set IP Address and Box Number.</p> <p>Result: The Set IP Address and Box Number dialog box appears.</p>
8	<p>Set the following parameters:</p> <ul style="list-style-type: none"> • Set the Device IP Address by entering the value, then press Set IP Address. • Set Device IP Address 2 by entering the value, then press Set IP Address 2. • Set the Netmask by entering the value, then press Set Netmask. • After setting the other values, press Reset to restart the hardware. <div data-bbox="395 644 662 719">  NOTE </div> <p>After a VPM device reset, the SNMPv3 user credentials and configuration are reset to defaults. You can reconfigure SNMPv3 user credentials or settings only after the device is reset.</p> <p>Result: The SmartX Site Converter restarts with the new IP address(es) and Netmask assignments. The SNMPv3 user credentials reset to their factory default values.</p>
9	<p>Proceed to Procedure 3-8, "How to Change SNMPv3 Configuration and User Credentials on the SmartX Site Converter," on page 3-20 to reconfigure the SNMPv3 credentials.</p>

Procedure 3-3 describes how to set the Site ID.





During initial installation this is done through an Ethernet cable connected directly to the Ethernet port of the SmartX Site Converter. After installation this procedure may be performed from a remote CSS.

Procedure 3-3 How to Configure the SmartX Site Converter Using CSS (Ethernet Connection)

1	<p>Connect the CSS Ethernet port to the SmartX Site Converter Ethernet port using a cross-over Ethernet cable.</p> <p>Result: The laptop and VPM chassis are connected.</p>
2	<p>Set the Ethernet to 100 MB full duplex on the CSS laptop.</p>
3	<p>Set the IP address of the CSS laptop to have an IP address on the same subnet as the site converter is configured. For example, if the site converter is configured with IP address 10.101.1.203, then an IP on the same subnet is 10.101.1.XXX.</p>
4	<p>Launch the CSS application and connect to the device using a serial connection.</p> <div data-bbox="395 1687 662 1761">  NOTE </div> <p>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.</p> <p>Result: The Configuration Service Software main window appears.</p>


Procedure 3-3 How to Configure the SmartX Site Converter Using CSS (Ethernet Connection) (Continued)

5	<p>To connect to the device using an Ethernet connection, choose Tools, Connection Configuration.</p> <p>Result: The Connection Screen dialog box appears.</p>
6	<p>Select Ethernet from the Connect Type field.</p>
7	<p>Enter the IP address of the device.</p>
8	<p>Click OK.</p> <p>Result: The SNMPv3 passphrase prompt appears. If the connection fails, a message appears.</p>
9	<p>Select appropriate security level. Click OK.</p> <ul style="list-style-type: none"> • NoAuthNoPriv – does not require authentication passphrase or encryption passphrase • AuthNoPriv – requires authentication passphrase • AuthPriv – requires authentication passphrase and encryption passphrase <div data-bbox="427 810 699 889">  <div data-bbox="523 827 699 868">NOTE</div> </div> <p>During initial installation, NoAuthNoPriv may be selected.</p>
10	<p>Choose File, Read Configuration From Device.</p> <p>Result: A message window states that an Ethernet connection must be established.</p>
11	<p>If Centralized Authentication is enabled, an FTP Login Screen opens. See "Device Security Configuration - Remote Access Login (Ethernet)" in the <i>CSS Online Help</i> for details. Provide the required credentials.</p> <div data-bbox="427 1144 699 1223">  <div data-bbox="523 1161 699 1202">NOTE</div> </div> <p>If Authentication Services is enabled in the Security Services Configuration window, enter a Username and Password. Also, enter an Elevated Privileges Password if the chosen security level requires these credentials. If Authentication Services is not enabled, enter any alphanumeric value for Username, Password, and Elevated Privileges Password, as they cannot be left blank.</p>
12	<p>Click OK.</p> <p>Result: The Connection Screen appears.</p>
13	<p>In the navigation pane, click the Site folder.</p> <p>Result: A Site dialog box appears.</p>
14	<p>Type the Site ID number.</p> <p>Result: A green mark appears indicating the Site ID has changed.</p>
15	<p>Save the configuration data to an archive file.</p>
16	<p>Choose File, Write Configuration to Device to download the configuration data to the SmartX Site Converter.</p> <p>Result: The Site ID is set for the SmartX Site Converter.</p>

Enabling Secure Software Download

[Procedure 3-4](#) describes how to set the SWDL transfer mode to FTP (clear) or SFTP (secure) for the device.




Procedure 3-4 How to Set the SWDL Transfer Mode Using CSS

1	Connect to the device using Configuration/Service Software (CSS) through an Ethernet port link. See Procedure 3-3, "How to Configure the SmartX Site Converter Using CSS (Ethernet Connection)," on page 3-12.
2	From the Security menu, select Device Security Configuration , and then select Remote Access/Login Banner (Ethernet) . Result: The Remote Access/Login Banner screen appears displaying the Remote Access Configuration tab.
3	In the Software Download Transfer Mode (Requested) field, choose either Ftp (clear) or Sftp (secure) . Click OK .  NOTE Secure Shell Service and Secure FTP service are automatically set to Enabled and grayed out when you choose Sftp.

[Procedure 3-5](#) describes how to set the complexity requirements and controls for the local service account password. The updated password criteria is enforced on the next password change for the device's local service account.

Password Configuration is an optional feature. For information, see "Password Configuration" in the *CSS Online Help*.

Procedure 3-5 How to Set the SmartX Site Converter Local Password Configuration

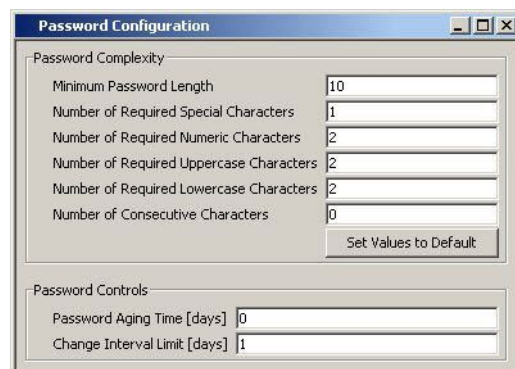
1	<p>Launch the CSS application.</p> <div data-bbox="443 357 523 442">  </div> <div data-bbox="539 378 719 414" style="background-color: #00AEEF; color: white; padding: 2px 5px; display: inline-block;">NOTE</div> <p>If Authentication Services are not enabled on a device, type any alphanumeric characters to populate the Username, Password, and Elevated Privileges Password fields, as they cannot be left blank.</p>
2	<p>Choose File, Read Configuration From Device.</p> <p>Result: A message window states that an Ethernet connection must be established.</p>
3	<p>If Centralized Authentication is enabled, an FTP Login Screen opens. See "Device Security Configuration - Remote Access Login (Ethernet)" in the <i>CSS Online Help</i> for details. Provide the required credentials.</p> <div data-bbox="443 783 523 868">  </div> <div data-bbox="539 804 719 840" style="background-color: #00AEEF; color: white; padding: 2px 5px; display: inline-block;">NOTE</div> <p>If Authentication Services is enabled in the Security Services Configuration window, enter a Username and Password. Also, enter an Elevated Privileges Password if the chosen security level requires these credentials. If Authentication Services is not enabled, enter any alphanumeric value for Username, Password, and Elevated Privileges Password, as they cannot be left blank.</p>
4	<p>Click OK.</p> <p>Result: The Connection Screen appears.</p>
5	<p>Enter the IP address of the site converter you want to access. Click Connect.</p> <div data-bbox="443 1215 523 1300">  </div> <div data-bbox="539 1236 719 1272" style="background-color: #00AEEF; color: white; padding: 2px 5px; display: inline-block;">NOTE</div> <p>If an authentication window appears, enter your credentials. A message window appears displaying the CSS Successfully Connected to this Device message.</p>

Procedure 3-5 How to Set the SmartX Site Converter Local Password Configuration (Continued)

- 6** In the navigation pane, click the **Password Configuration** element.

Result: The Password Configuration window appears.

Figure 3-3 Password Configuration Window



The screenshot shows a 'Password Configuration' dialog box with two main sections: 'Password Complexity' and 'Password Controls'. The 'Password Complexity' section includes fields for 'Minimum Password Length' (10), 'Number of Required Special Characters' (1), 'Number of Required Numeric Characters' (2), 'Number of Required Uppercase Characters' (2), 'Number of Required Lowercase Characters' (2), and 'Number of Consecutive Characters' (0). A 'Set Values to Default' button is located at the bottom right of this section. The 'Password Controls' section includes fields for 'Password Aging Time [days]' (0) and 'Change Interval Limit [days]' (1).

Password Complexity	
Minimum Password Length	10
Number of Required Special Characters	1
Number of Required Numeric Characters	2
Number of Required Uppercase Characters	2
Number of Required Lowercase Characters	2
Number of Consecutive Characters	0

Set Values to Default

Password Controls	
Password Aging Time [days]	0
Change Interval Limit [days]	1

Procedure 3-5 How to Set the SmartX Site Converter Local Password Configuration (Continued)

7	<p>Complete the following fields:</p> <ul style="list-style-type: none"> • Minimum Password Length— This field allows you to enter a value as the minimum length for the password. The minimum can be between 8 and 255 characters, with a default of 10 characters. • Number of Required Special Characters— This field allows you to enter a value for the required number of special characters which must be included in the password. The value can be between 0 and 255, with a default of 1. • Number of Required Numeric Characters— This field allows you to enter a value for the required number of numeric characters which must be included in the password. The value can be between 0 and 255, with a default of 2. • Number of Required Uppercase Characters— This field allows you to enter a value for the required number of uppercase alphabetic characters which must be included in the password. The value can be between 0 and 255, with a default of 2. • Number of Required Lowercase Characters — This field allows you to enter a value for the required number of lowercase alphabetic characters which must be included in the password. The value can be between 0 and 255, with a default of 2. • Number of Consecutive Characters — This field allows you to enter the maximum number of consecutive repeated characters that are permitted in the password. • Set Values to Default — This returns all fields to their system default values. • Password Aging Time [days] — This field allows you to enter a value between 0 and 65535 for the maximum number of days a device's local password will be valid. After the Password Aging Time has elapsed, the device's password must be changed. The default value is 0. • Change Interval Limit [days]— This field allows you to enter a value between 0 and 65535 for the number of days which must elapse before a device's local password can be changed. The default value is 1.
8	From the File menu, select Save to save the configuration changes.
9	Choose File, Write Configuration to Device to download the configuration changes on the SmartX Site Converter.

Procedure 3-6 provides the date and time to the SmartX Site Converter. In the event of a power outage, the site converter does not retain the date and time settings.

**NOTE**

During installation this is done through an Ethernet cable connected directly to the Ethernet port of the SmartX Site Converter. After installation this procedure may be performed from a remote CSS.

Procedure 3-6 How to Set the Date and Time on the SmartX Site Converter

1	Connect the laptop with CSS to the SmartX Site Converter through the Ethernet cross-over cable.
2	Set the Ethernet to 100 MB full duplex.
3	Set the IP address of the CSS laptop to have an IP address on the same subnet as the site converter is configured. For example, if the site converter is configured with IP address 10.101.1.203, then an IP on the same subnet is 10.101.1.XXX.
4	<p>Launch the CSS application.</p> <div data-bbox="389 559 464 640"></div> <div data-bbox="526 578 614 610">NOTE</div> <p>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.</p> <p>Result: The Configuration Service Software main window appears.</p>
5	<p>To connect to the device using an Ethernet connection, choose Tools, Connection Configuration.</p> <p>Result: The Connection Screen dialog box appears.</p>
6	Select Ethernet from the Connect Type field.
7	Set the IP address to the site converter's IP address. Choose Connect .
8	Choose Tools, Set Date and Time .
9	<p>Enter the current date and time. Click OK.</p> <p>Result: The date and time is reset.</p>

[Procedure 3-7](#) describes how to enable the secure services and change the device password. Perform these steps before changing the SNMPv3 configuration and user credentials from CSS on a selected device in the remote site.

Procedure 3-7 How to Set the Serial Security Services

1	<div data-bbox="424 336 502 421"></div> <div data-bbox="539 357 699 389">IMPORTANT</div> <p>Ensure that you have the required credentials information (local service account password and elevated privileges password) to configure the site devices before proceeding. The user credentials information includes both the current and new credentials. Without the current credentials, you cannot access the device and cannot change the user credentials.</p> <p>Changing to the incorrect user credentials may lead to not being able to access the device through CSS or SSH. See Chapter 8's "Resetting Passwords and SNMPv3 Passphrases" for troubleshooting information.</p> <p>Connect the CSS serial port to the SmartX Site Converter Serial port through an RJ-45 to female DB9 pin serial converter.</p>
2	<div data-bbox="424 857 502 942"></div> <div data-bbox="539 878 699 910">NOTE</div> <p>Launch the CSS application.</p> <p>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.</p> <p>Result: The Configuration Service Software main window appears.</p>
3	<p>To connect to the device using a Serial connection, choose Tools, Connection Configuration.</p> <p>Result: The Connection Screen dialog box appears.</p>
4	<p>Set the following serial connection parameters, then click Connect.</p> <ul style="list-style-type: none"> • Select Serial from the Connection Type field. • Select a Baud rate of 19200. • Select the appropriate Com port (usually Com Port 1). <p>Result: A confirmation dialog box appears telling you that CSS has connected with the device.</p>
5	<p>Click OK. If authentication on the device is enabled, a login screen appears. Provide all required credentials. Click OK.</p>
6	<p>Select Security, Device Security Configuration, Security Services (Serial) from the menu.</p> <p>Result: The Security Services Configuration dialog box opens.</p>
7	<p>Set the Authentication Services field to Enabled. This field enables local authentication services and must be enabled as a prerequisite for centralized authentication.</p>
8	<p>Set the Password Reset Mechanism field. This field allows a user to reset the passwords for two built-in device accounts to their default values.</p>

Procedure 3-7 How to Set the Serial Security Services (Continued)

9	To update the password for the device, select either Service Account or Elevated Privilege from the drop-down list. Click Update password . Result: A Change Account Password dialog box opens.
10	Enter the old password, then enter a new password and confirm the new password before clicking Change Password .
11	Click OK to save the new password. Result: The Change Account Password dialog box closes.

[Procedure 3-8](#) changes the SNMPv3 configuration and user credentials from CSS on a selected device in the remote site. For more information on this feature, see the *SNMPv3* manual.




**NOTE**

During installation this is done through an Ethernet cable connected directly to the Ethernet port of the SmartX Site Converter. After installation this procedure may be performed from a remote CSS.

Procedure 3-8 How to Change SNMPv3 Configuration and User Credentials on the SmartX Site Converter

1	<div data-bbox="223 974 300 1059" data-label="Image"> </div> <div data-bbox="336 995 485 1023" data-label="Section-Header">IMPORTANT</div> <p>Ensure that you have the required SNMPv3 credentials information (Authentication passphrase, Encryption passphrase, and Authoritative Engine ID) to configure the device before proceeding. The user credentials information includes both the current and new credentials. Without the current credentials, you cannot access the device and cannot change the user credentials. Changing to the incorrect user credentials may lead to not being able to access the device from the UNC or for the device to not be able to send alarms to the Unified Event Manager (for fault management).</p> <p>Connect the laptop with CSS to the SmartX Site Converter through the Ethernet cross-over cable.</p>
2	Set the Ethernet to 100 MB full duplex.
3	Set the IP address of the CSS laptop to have an IP address on the same subnet as the site converter is configured. For example, if the site converter is configured with IP address 10.101.1.203, then an IP on the same subnet is 10.101.1.XXX.
4	<p>Launch the CSS application.</p> <div data-bbox="223 1527 300 1613" data-label="Image"> </div> <div data-bbox="367 1549 450 1578" data-label="Section-Header">NOTE</div> <p>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.</p> <p>Result: The Configuration Service Software main window appears.</p>
5	<p>To connect to the device through an Ethernet connection, specifically for configuring the SNMPv3 User Credentials on the device, choose Security, SNMPv3 Configuration, then Configure SNMPv3 Users (Ethernet).</p> <p>Result: The SNMPv3 Login/Connection dialog box appears with MotoAdmin as the selected SNMPv3 user.</p>

Procedure 3-8 How to Change SNMPv3 Configuration and User Credentials on the SmartX Site Converter (Continued)



6	<p>Enter the appropriate authentication and encryption passphrases/passwords in the fields.</p> <div data-bbox="263 361 534 446">  <div data-bbox="359 378 534 421">NOTE</div> </div> <p>When accessing the device for the first time, if the default passphrases do not work, the passphrases may have been set to default values by a different system release of software. See the <i>CSS Online Help's</i> section "Reset SNMPv3 Configuration (Serial)" to reset the passphrases to the current software release defaults.</p>
7	<p>Enter the IP address.</p>
8	<p>Click OK.</p> <p>Result: A connection is made with the selected device, and the entered SNMPv3 admin passphrases/passwords are authenticated and the Configure SNMPv3 Users dialog box appears. If the connection fails, a message appears.</p>
9	<p>To choose the SNMPv3 user whose credentials are to be updated, select Username from the Username list in the User Information form of the Configure SNMPv3 Users dialog box.</p> <p>Result: The CSS retrieves the current credentials from the device for the selected user.</p> <div data-bbox="263 904 534 989">  <div data-bbox="359 921 534 963">NOTE</div> </div> <p>Depending on the user selected, some fields on this dialog box become Read-Only or disabled. Click Cancel on the Configure SNMPv3 Users dialog box at any time to discard changes made to the selected user.</p>
10	<p>To change or update the SNMPv3 security level for the selected user, select the security level from the Security Level list in the User Information form of the Configure SNMPv3 Users dialog box. The security level options are:</p> <ul style="list-style-type: none"> • NoAuthNoPriv: Neither the Authentication Password nor Encryption Password is needed for communicating with the device. • AuthNoPriv: Authentication Password is needed; but no Encryption Password is needed for communicating with the device. • AuthPriv: Both Authentication Password and Encryption Password are needed for communicating with the device. <p>Result: The security level of the selected user is set.</p> <div data-bbox="263 1489 534 1574">  <div data-bbox="359 1506 534 1549">NOTE</div> </div> <p>The User Status field on the Configure SNMPv3 Users dialog box reflects the current operational status of the selected SNMPv3 User. The Status Types include:</p> <ul style="list-style-type: none"> • Active: User configured on device; Update and Delete buttons are enabled. • Not in service: User configured on device; Update and Delete buttons are enabled. • Not ready: User configured on device; Update and Delete buttons are enabled. • Not present: Not present on the device; Create button is enabled.

Procedure 3-8 How to Change SNMPv3 Configuration and User Credentials on the SmartX Site Converter (Continued)

11	<p>To change the Authentication Password/Passphrase for the selected SNMPv3 user (if applicable to the selected security level), type the password into the Old Password Field in the Authentication Password form of the Configure SNMPv3 Users dialog box.</p> <div data-bbox="228 421 300 506"></div> <div data-bbox="320 442 497 480">NOTE</div> <p>If you do not know the password, click the I do not remember old password check box.</p>
12	<p>Type the new password/passphrase into the New Password field.</p> <div data-bbox="228 608 300 693"></div> <div data-bbox="320 629 497 668">NOTE</div> <p>Password must be between 8 and 64 characters in length and Password must consist of upper or lowercase alphanumeric characters (excluding the @ # \$ ^ or _ characters).</p>
13	<p>Type the same new password/passphrase into the Confirm New Password field.</p>
14	<p>To change the encryption password/passphrase for the selected SNMPv3 user (if applicable to the selected security level), type the old password/passphrase into the Old Password Field in the Encryption Password form of the Configure SNMPv3 Users dialog box.</p> <div data-bbox="228 927 300 1012"></div> <div data-bbox="320 949 497 987">NOTE</div> <p>If you do not know the password, click the I do not remember old password check box.</p>
15	<p>Type the new password/passphrase into the New Password field, then type the same new password/passphrase into the Confirm New Password field.</p>
16	<p>To change the Authoritative Engine Identifier (applicable to MotoInformA and MotorInformB users only), select the desired current engine ID from the Current Engine ID List in the Authoritative Engine ID Section of the Configure SNMPv3 Users dialog box.</p>
17	<p>Type the new engine ID into the New Engine ID field.</p> <div data-bbox="228 1293 300 1378"></div> <div data-bbox="320 1315 497 1353">NOTE</div> <p>The new engine ID must be between 1 and 27 characters and comply with the Engine ID Domain Name Syntax.</p> <p>Result: The authoritative engine ID is assigned.</p>
18	<p>To create, update, or delete SNMPv3 users, continue on with Procedure 3-9.</p>

[Procedure 3-9](#) describes how to create, update, or delete an SNMPv3 user from the Configure SNMPv3 Users Screen dialog box.

Procedure 3-9 How to Add or Modify an SNMPv3 User

1	In the CSS, log on using the appropriate credentials.
	NOTE
	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.
	Result: The Configure SNMPv3 Users dialog box appears.
2	To create, delete, or update the selected SNMPv3 user, use one of the following steps:
If...	Then...
If you want to add a user when the status is Not Present,	click Create .
If you want to modify an existing user,	click Update .
If you want to remove an existing user,	click Delete .
	Result: A confirmation dialog box appears and asks if you want to continue.
3	Click Yes .
	Result: The Processing Requests dialog box appears and processes the request. A green square indicates OK and a red square indicates failure.
4	After reviewing the processing status, click OK .
	NOTE
	If you encounter any errors, go back to the appropriate step and correct the information entered.
5	Repeat these steps for any SNMPv3 users you wish to create, update, or delete.
6	Select Cancel to exit the Configure SNMPv3 Users dialog box.
	Result: The Configure SNMPv3 Users dialog box closes, and the CSS main window returns.
7	Choose File, Exit . Click OK .
	Result: The CSS application closes.



Performing an SNMPv3 Connection Verification Using CSS

Once the SNMPv3 user credentials have been created, modified, or deleted, you can perform a sanity check to ensure the device is properly configured for SNMPv3. [Procedure 3-10](#) describes how to verify the SNMPv3 connection.

**IMPORTANT**

This procedure requires that you know the IP address or the Fully Qualified Domain Name (FQDN) for the device. If you do not, you can see the *SNMPv3* manual for more information on the **Fetch DNS** option.

Procedure 3-10 How to Verify SNMPv3 Credentials on the SmartX Site Converter

1	Connect a service laptop or NM client with CSS to the SmartX Site Converter, then launch the CSS application using an Ethernet connection.
2	When the passphrase prompt screen opens, select configured security level and enter the required passphrases.
	<div data-bbox="392 468 464 536"></div> <div data-bbox="483 485 662 521" style="background-color: #0070C0; color: white; padding: 2px 5px; display: inline-block;">NOTE</div> <p data-bbox="515 559 1401 649">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.</p> <p data-bbox="387 666 1369 723">Result: A confirmation dialog box appears indicating that the CSS has connected with the device.</p>
3	Click OK if the connection was successful. This indicates your SNMPv3 configuration is valid.
	<div data-bbox="392 819 464 887"></div> <div data-bbox="483 815 662 849" style="background-color: #0070C0; color: white; padding: 2px 5px; display: inline-block;">NOTE</div> <p data-bbox="515 883 1396 940">If you fail to connect or log on to the device in SNMPv3 mode, then the device is not properly configured for SNMPv3.</p>
4	On the main CSS window, select File, Exit . Click OK to confirm that you want to exit.
	Result: The CSS application closes.

Setting the Network Services Configuration Using CSS

The CSS is used to configure the Site, Network Services Configuration, and Password Configuration screens for the SmartX Site Converter. The Site screen is configured for the SmartX Site Converter in [Procedure 3-3](#) and the Password Configuration procedure is provided in [Procedure 3-5](#).

The Network Services Configuration window allows you to configure the network DNS, RADIUS, and SYSLOG services for this site converter, if part of a secure network. This window contains three tabs to configure all of the parameters. Each tab is its own procedure in this section; however, you do not need to launch CSS and save the configuration on each tab if you are performing all of these steps at the same time. You just need to fill in the fields on each tab, then save the file to the archive and write to the device once.

See the *CSS Online Help* and the following manuals for the CSS procedures to perform the following:

- Configuring DNS using the CSS. See the *Authentication Services* manual.
- Configuring the SmartX Site Converter for SSH. See “Configuring SSH for RF Site Devices and VPMs Using CSS – Overview” in the *Securing Protocols with SSH* manual.
- Configuring the local cache size for the SmartX Site Converter. See the *Authentication Services* manual.
- Enabling Centralized Authentication using the CSS. See the *Authentication Services* manual.
- Enabling RADIUS Authentication using the CSS. See the *Authentication Services* manual.

- Enabling Centralized Event Logging using the CSS (optional). See the *Centralized Event Logging* manual.



NOTE

You can also see the *CSS Online Help* in the software application to complete these tasks during the device configuration.

Customizing the Login Banner Using CSS

[Procedure 3-11](#) describes how to edit the login banner's security notice.

Procedure 3-11 How to Customize the Login Banner

1	Connect to the device using Configuration/Service Software (CSS) through an Ethernet port link. See Procedure 3-3, "How to Configure the SmartX Site Converter Using CSS (Ethernet Connection)," on page 3-12.
2	From the Security menu, select Device Security Configuration , and then select Remote Access/Login Banner (Ethernet) . Result: The Remote Access/Login Banner screen appears displaying the Remote Access Configuration tab.
3	Click on the Login Banner tab.
4	Edit the text of the banner.
5	Click one of the following: <ul style="list-style-type: none"> • Refresh: To re-read the original Login Banner text. • Apply: To save your changes and keep the screen open . • OK: To save your changes and close the screen. • Close: To close the screen without saving your changes.

SmartX Site Converter Network Connections

Once the SmartX Site Converter is installed in the mounting rack and the initial startup configuration and security credentials are set, you connect the site converter to the existing site gateway using [Procedure 3-12](#).

Procedure 3-12 How to Attach the SmartX Site Converter to the Site Gateway

1	Connect a cross-over Ethernet cable to the Ethernet port on the site gateway.
2	Connect the opposite end of the Ethernet cable into the Ethernet port on the SmartX Site Converter. Result: The SmartX Site Converter shares an Ethernet cable with the site gateway.
3	Verify the connection by accessing the site from the remote CSS.

SmartX Site Converter Software Installation

The Unified Network Configurator (UNC) is the Network Manager used to load Operating System software to the SmartX Site Converter devices. [Process 3-3](#) lists the basic steps involved in the software installation on the device.

Process 3-3 Installing Software on the SmartX Site Converter

1	Discover the SmartX Site Converter device in the UNC. See Procedure 3-13, "How to Discover the Motorola SmartX Site Converter in the UNC," on page 3-28.
2	Log on to the UNC Server Application Using PuTTY. See “How to Log In to the UNC Server Application Using PuTTY” in the <i>Unified Network Configurator</i> manual for more information on this procedure.
3	Load the Operating System images to the UNC. See Procedure 3-14, "How to Load the SmartX Site Converter OS Images to the UNC," on page 3-29.
4	Enable FTP services on the UNC. See Procedure 3-15, "How to Enable FTP Service," on page 3-30.

Process 3-3 Installing Software on the SmartX Site Converter (Continued)

- 5** Transfer and install the OS image to the SmartX Site Converter. See [Procedure 3-16, "How to Transfer and Install the OS Image,"](#) on page 3-30.
 - 6** Inspect the SmartX Site Converter and bank device properties for the transferred and installed software. See [Procedure 3-17, "How to Inspect Device Properties for Transferred and Installed Software,"](#) on page 3-32.
 - 7** Disable FTP services for the UNC. See [Procedure 3-18, "How to Disable FTP Service,"](#) on page 3-32.
-

**NOTE**

You can also use either the UNC or Software Download (SWDL) program to load software on the SmartX Site Converter.

Discovering the SmartX Devices with the UNC

The discovery process allows site devices to be managed by the Unified Network Configurator (UNC). Once the SmartX Site Converter is installed, configured through the CSS, and security parameters are enabled, use [Procedure 3-13](#) to discover the device and then you can update configuration information using this configuration management application.

The UNC network management solution consists of two applications, and both the UNC Wizard and the VoyenceControl applications are used in this procedure.

**NOTE**



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

Once the device is discovered in the UNC, the OS images and SmartX configuration files can be loaded to add a SmartX Site Converter to a 3600 site, which then connects the 3600 site to the current ASTRO® 25 zone core.

**NOTE**

To re-discover a replacement device in the system, you want to replace the previous SmartX Site Converter in the UNC. See Chapter 4, “Replacing a Device” in the *Unified Network Configurator* manual.

Procedure 3-13 How to Discover the Motorola SmartX Site Converter in the UNC

1	Ensure that DNS is functional on your system. DNS is supplied by a specific server application, which also needs to be operational before you can discover the SmartX Site Converter.
2	Log on to the UNC Wizard from the NM client, by double-clicking the Internet Explorer icon on the desktop. Result: The Internet Explorer browser opens.
3	Type http://ucs-unc0<Y>.ucs:9080/UNCW in the Address field, where <Y> is the number of the UNC server (01 for primary core UNC server, and 02 for backup core UNC server). Press Enter . Result: The UNC Wizard launches and a login dialog box appears.
4	Type the administrative username and password. Click OK . Result: The UNC Wizard appears.
5	From the list of available wizards on the left side, select Subnet Discovery . Result: The right side of the window is updated with the Subnet Discovery form.
6	Select RF Site by clicking on the Discovery Type drop-down list.
7	Type the Zone ID and Site ID . Click Submit . Result: An auto-discovery job is created in the UNC Schedule Manager. You are finished using the UNC Wizard at this point.
8	Log on to the UNC from the NM client, by typing http://ucs-unc0<Y>.ucs in the Address field, where <Y> is the number of the UNC server (01 for primary core UNC server, and 02 for backup core UNC server), then press Enter . Result: The UNC client launches and a login dialog box appears.
9	Type the administrative username and password. Click OK .  NOTE The names EMC Ionix Network Configuration Manager and VoyenceControl are used interchangeably for this product. Result: VoyenceControl launches.
10	Press F7 (Schedule Manager). Result: The Schedule Manager window appears in the UNC with the discovery jobs.
11	Verify that the Zone and Site containers include SmartX Site Converter device(s) just discovered.  NOTE No sites should be in the Lost and Found folder. If there are, see the <i>Unified Network Configurator</i> manual for troubleshooting guidance.
12	In the UNC Wizard, select RF Site Level Configuration, Channel to verify the SmartX Site Converter device(s). Choose Zone , if multiple zones exist. Result: The SmartX sites are listed, which means they are available for channel configuration.

Logging on to the UNC Server Application Using PuTTY


Log on to the UNC server application, using an SSH session and your Active Directory account that is a member of the user group with privileges to load new OS images and upgrade an OS. See “How to Log in to the UNC Server Application Using PuTTY” in the *Unified Network Configurator* manual for more information on this procedure.

Loading the SmartX Site Converter OS Images to the UNC

[Procedure 3-14](#) loads the Operating System (OS) images for the routers, gateways, switches, terminal servers, SmartX Site Converter, and VPM devices for distribution through the Unified Network Configurator (UNC). This procedure requires the Transport, Motorola SmartX Site Converter, and Motorola VPM OS Image CDs.

Once OS images are distributed to the UNC, you can update the site converter's configuration files to the UNC.

Procedure 3-14 How to Load the SmartX Site Converter OS Images to the UNC

1	Launch an SSH terminal server session in PuTTY to access the UNC Server Administration menu. Result: The UNC Server Administration menu appears.
2	Select Application Admin from the menu. Press Enter .
3	Select OS Images Administration from the menu. Press Enter . Result: The OS Images Administration menu appears.
4	Select Load new OS images from the menu. Press Enter . Result: A message appears indicating there are two methods for loading OS Images .
5	Insert the OS Images CD into the CD/DVD-ROM drive of the server. Result: The drive light starts blinking on the server.
6	When the drive light stops blinking, press Enter . Result: The OS images load on the UNC.
 <div style="background-color: #00AEEF; color: white; padding: 5px; display: inline-block;">NOTE</div> <p>The Transport OS Image media is packaged with the Network Management DVDs when an ASTRO® 25 system ships.</p>	
7	Select Eject CD from the menu. Press Enter . Result: The User Configuration Server Administration menu appears.
8	Remove the OS Image CD from the CD/DVD-ROM drive of the server.
9	Select quit . Press Enter . Result: The prompt appears.

Loading OS Software to SmartX Site Converter Devices



These procedures describe how to load software images onto UNC and download and install this software to the SmartX Site Converter. However, before you begin to install the software, you must enable FTP as described in [Procedure 3-15](#).

Procedure 3-15 How to Enable FTP Service






1	Launch an SSH terminal server session in PuTTY to access the UNC Server Administration menu. Result: The UNC Server Administration menu appears.
2	Select Unix Administration from the menu. Press Enter . Result: The Unix Administration menu appears.
3	Select FTP Services from the menu. Press Enter . Result: The FTP Services menu appears.
4	Select Enable FTP service from the menu. Press Enter . Result: The FTP Services are enabled and available for software transfer and install operations.

[Procedure 3-16](#) describes how to download the OS from the UNC to the SmartX Site Converter.

Procedure 3-16 How to Transfer and Install the OS Image

1	Log on to the UNC from the NM client, by typing http://ucs-unc0<Y>.ucs in the Address field, where <Y> is the number of the UNC server (01 for primary core UNC server, and 02 for backup core UNC server). Press Enter and log on using the admin account. Result: The UNC client launches and a login dialog box appears.
2	In the left navigation pane, expand Networks , Astro 25 Radio Network , then Views . Result: The list of options expands.
3	Double-click Motorola SmartX Site Converters from the navigation pane. Result: The view opens and all currently discovered SmartX Site Converter devices appear.
4	Select Tools , OS Inventory .  NOTE You can also press the F9 key to select the OS Inventory. Result: A list of the OS images appears.
5	Verify OS images loaded on the UNC server appear in the OS inventory.  NOTE These images were automatically created during the “How to Load OS Images to the UNC” procedure.

Procedure 3-16 How to Transfer and Install the OS Image (Continued)

6	<p>Under Networks in the navigation pane, select one or more devices from the same device class, right click the selections, then choose Update OS Image from the menu.</p> <p>Result: The Select OS Image window appears.</p>
7	<p>Select Software Image. Click Next.</p> <p>Result: The Update OS Image window appears.</p>
8	<p>Select each device that appears in the Selected Devices section.</p> <p>Result: This associates a version to a device instance.</p> <div data-bbox="427 591 699 666">  <div data-bbox="523 608 699 644">NOTE</div> </div> <p>In most cases, the “summary of device partitions” are already set up and you just need to verify the values in step 8 to step 11.</p>
9	<p>Select nvm partition from the Manage Partition for Device section.</p> <p>Result: This defines where the OS image is transferred.</p> <div data-bbox="427 857 699 932">  <div data-bbox="523 874 699 910">NOTE</div> </div> <p>This is the only choice for SmartX Site Converter device.</p>
10	<p>Select the image for this device from the Selected Image section.</p> <div data-bbox="427 1038 699 1112">  <div data-bbox="523 1055 699 1091">NOTE</div> </div> <p>You can ignore the Install and Copy check boxes.</p> <p>Result: This populates the Image Info tab and informs the application which image to use.</p>
11	<p>Select the Device Options section, Software Operations , then choose transfer, install, or both.</p> <p>Result: This indicates which operations occur when the job is executed.</p> <div data-bbox="427 1315 699 1389">  <div data-bbox="523 1332 699 1368">NOTE</div> </div> <p>If you choose transfer, you must select the install option later to complete the installation. If you choose both, the software is transferred and then installed. There are up to two resets of the SmartX Site Converter/VPM during installation.</p>
12	<p>Click Schedule.</p> <p>Result: The Schedule Push Job window appears.</p>
13	<p>Configure the schedule information and click Approve and Submit.</p> <p>Result: This approves the job and you can view it in the Schedule Manager window.</p> <div data-bbox="427 1698 699 1772">  <div data-bbox="523 1715 699 1751">NOTE</div> </div> <p>If you choose Submit, you are asked to approve the job later.</p>
14	<p>Verify the job status by pressing F7 (Schedule Manager).</p> <p>Result: The Schedule Manager window appears in the UNC with the discovery jobs.</p>

Once the software has been transferred and installed, use [Procedure 3-17](#) to inspect the device properties before assuming the installation was a success and disabling FTP service.

Procedure 3-17 How to Inspect Device Properties for Transferred and Installed Software

1	<p>From the Device view, right click the device, select Pull, then Pull Hardware Spec.</p> <p>Result: The current software version information is updated in the UNC.</p> <div data-bbox="391 485 464 570"></div> <div data-bbox="483 506 662 544">NOTE</div> <p>You can skip this step if a Pull All or Pull Hardware Spec has already occurred.</p>
2	<p>From the Device view, right click on the device, then choose Properties.</p> <p>Result: The Device Properties window appears.</p> <div data-bbox="391 719 464 804"></div> <div data-bbox="483 740 662 778">NOTE</div> <p>If you select the Properties icon, you can view the device properties appear directly within the Device view.</p>
3	<p>Choose the Configuration tab, then the Hardware tab.</p>
4	<p>Double-click the Chassis object from the Physical Hardware properties.</p> <p>Result: The Chassis property tree expands.</p>
5	<p>View the following properties and their values:</p> <ul style="list-style-type: none"> • Bnk1:SmartX_Converter: Transferred software in bank 1. • Bnk2:SmartX_Converter: Transferred software in bank 2. • SmartX_Converter: Installed and Running Software. <div data-bbox="391 1240 464 1325"></div> <div data-bbox="483 1261 662 1300">NOTE</div> <p>You can use the Table format (instead of the Diagram format) to view the Installed and Running Software in the Device view.</p>

After the transfer and installation of the software, the FTP service must be disabled. Follow [Procedure 3-18](#) to disable FTP service.

Procedure 3-18 How to Disable FTP Service

1	<p>Launch an SSH terminal server session in PuTTY to access the UNC Server Administration menu.</p> <p>Result: The UNC Server Administration menu appears.</p>
2	<p>Select Application Administration from the menu. Press Enter.</p> <p>Result: The Application Administration menu appears.</p>
3	<p>Select FTP Services from the menu. Press Enter.</p> <p>Result: The FTP Services menu appears.</p>

Procedure 3-18 How to Disable FTP Service (Continued)

4	Select Disable FTP service from the menu. Press Enter . Result: The FTP Services are disabled and unavailable for software transfer and install operations.
5	Back out of the menus by pressing q three times.
6	At the prompt, type exit to return to the previous menu.
7	Type exit again. Result: You have successfully logged out of the application.
8	Close the PuTTY connection.

This page intentionally left blank.

SmartX Site Converter Configuration

This chapter details configuration procedures relating to the SmartX Site Converter.

SmartX Site Converter Configuration Process

As with the installation of this feature, the configuration of the SmartX Site Converter has dependencies and there is a specific sequence of events you must follow when configuring the SmartX Site Converter. [Process 4-1](#) defines this configuration process.

Process 4-1 Configuring the SmartX Site Converter

- 1** Configure the SmartX Site Converter to transition the site to wide trunking using the UNC. See [Procedure 4-1, "How to Configure the SmartX Site Converter Using the UNC,"](#) on page 4-3.
- 2** Configure the channels using the UNC Wizard. See [Procedure 4-2, "How to Configure the SmartX Site Converter Channels Using the UNC Wizard,"](#) on page 4-7.
- 3** Configure the trunked 3600 sites and channels using the UNC Wizard. See [Process 4-2, "Configuring the Trunked 3600 Sites and Channels on the Network Managers,"](#) on page 4-9.
- 4** Monitor the SmartX Site Converter faults.
 - 1.** Discover the SmartX Site Converter device(s) in the UEM. See [Procedure 4-6, "How to Discover the SmartX Site Converter in the UEM,"](#) on page 4-13.
 - 2.** Verify SmartX Site Converter operation with the UEM. See [Procedure 4-7, "How to Verify SmartX Site Converter Operation with the UEM,"](#) on page 4-14.
- 5** Connect the SmartX Site Converter and the channel bank. See [Procedure 4-8, "How to Connect the SmartX Site Converter and the Channel Bank,"](#) on page 4-17.

SmartX Site Converter Network Management Configuration

.....

Network management of the SmartX Site Converter is performed using the Unified Network Configurator (UNC), Unified Event Manager (UEM), and the Configuration/Service Software (CSS) application. Much of the device's configuration is done in the initial installation of the SmartX Site Converter and is covered in that chapter.

Configuring the SmartX Site Converter Using the UNC

Once the SmartX Site Converter is discovered in the system and the OS and software are installed, follow [Procedure 4-1](#) to configure the site converter to transition the site from site trunking to wide trunking service within the ASTRO® 25 system. This procedure configures the site converter device objects in the UNC. Channels are configured using the Channel Wizard in the UNCW in [Procedure 4-2](#).

Configure the templates in the following order:

- Update Site Parameters
- Line Interface
- Site Controller Link
- ZC Site Link Path



IMPORTANT



You must use the *Configlet Editor* in the UNC to execute procedures involving templates. See the *Unified Network Configurator* manual for more information on the differences between the Configlet Editor and the Config Editor, as well as other nuances of the VoyenceControl application.



NOTE

Additional help for objects, parameter names, and valid values can be found at **`http://ucs-unc0<Y>.ucs:9080/HELP`**, where <Y> is the number of the UNC server (01 for primary core UNC server, and 02 for backup core UNC server).

Procedure 4-1 How to Configure the SmartX Site Converter Using the UNC

1	<p>Log on to the UNC from the NM client, by typing ucs-unc0<Y>.ucs , where <Y> is the number of the UNC server (01 for primary core UNC server, and 02 for backup core UNC server. Press Enter.</p> <p>Result: The UNC client launches and a login dialog box appears.</p>
2	<p>Type the administrative username and password. Click OK.</p> <div data-bbox="427 512 699 666">  <div data-bbox="523 534 699 570" style="background-color: #0070C0; color: white; padding: 2px 5px; display: inline-block;">NOTE</div> <p>The names EMC Ionix Network Configuration Manager and VoyenceControl are used interchangeably for this product.</p> </div> <p>Result: VoyenceControl launches.</p>
3	<p>Select the Network View tab.</p> <p>Result: The UNC window appears.</p>
4	<p>To open the list of available converter devices, select Networks, Astro 25 Radio Network , then Views in the navigation pane.</p> <p>Result: The list of options expands.</p>
5	<p>Double-click Motorola SmartX Site Converters from the navigation pane.</p> <p>Result: The list of options expands.</p>
6	<p>Right-click the desired SmartX device or devices.</p> <p>Result: A pop-up menu appears.</p>
7	<p>Select Properties, then select the Communications tab. If needed, use Update Credentials to:</p> <ul style="list-style-type: none"> • 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 VoyenceControl credentials, search on "Credentials Manager" in the <i>Unified Network Configurator</i> manual.
8	<p>Return to the Motorola SmartX Site Converters view and right-click the SmartX device or devices again.</p> <p>Result: A pop-up menu appears.</p>
9	<p>Select Editor from the menu.</p> <p>Result: A submenu appears.</p>
10	<p>Select Configlet from the menu.</p> <p>Result: The Configlet Editor appears.</p> <div data-bbox="427 1740 699 1906">  <div data-bbox="523 1761 699 1798" style="background-color: #FFD700; border: 1px solid black; padding: 2px 5px; display: inline-block;">CAUTION</div> <p>Do NOT choose the Config Editor, as it represents the absolute configuration of the device. Missing object instances configured through a Config Editor are deleted. This causes site trunking.</p> </div>

Procedure 4-1 How to Configure the SmartX Site Converter Using the UNC (Continued)

11	Click inside the Common Configlet section, then select the Insert Template icon from the menu bar. Result: A Select Item window appears.
12	Select System , Motorola , SmartX , then open the Template - Motorola SmartX Site Converter - Update Site Parameters template.

Procedure 4-1 How to Configure the SmartX Site Converter Using the UNC (Continued)

13 Configure the following fields. Click **OK**.

- NTP Server Address (Primary) – The primary NTP source is IP address corresponding to the hostname ntp02.zone#mit.
- NTP Server Address (Secondary) – The secondary NTP source is the IP address corresponding to the hostname ntp03.zone#.
- NTP_active – Set to **True**.

**NOTE**

If you do not set the ntp_active to **True**, the device fails the audit and is flagged as non-compliant.

- Site Type

**NOTE**

If the Site Type discovered is an IR site, set the Site Type to **IR**.

- IMBE Begin Encode Buffering Time (ms)
- G.728 Begin Encode Buffering Time (ms)
- IMBE Packet Transmission Holdoff Time (ms)
- G.728 Packet Transmission Holdoff Time (ms)
- IMBE Jitter Buffering Age (ms)
- G.728 Jitter Buffering Age (ms)
- Line Type
- Framing Parameter
- Line Build Out
- Level Idle Pattern

**NOTE**

If the SmartX Site Converter is set to "a-Law", then the connected channel bank must be set to "a-inv" (inverse a-Law). This configuration is done in the Line Idle Pattern field. For u-Law, both devices are configured the same.

- Line Length
- Line Impedance
- Site ID

Result: The Template Variable Substitution window closes and the configuration appears in the Common Configlet section of the Configlet Editor window.

Procedure 4-1 How to Configure the SmartX Site Converter Using the UNC (Continued)


14	Click inside the Common Configlet section, then select the Insert Template icon from the menu bar.
15	Select System, Motorola , SmartX , then open the Template - Motorola SmartX Site Converter - Add Line Interface template Result: The Template Variable Substitution window opens.
16	Configure the Line Interface_Index . Click OK . Result: The Template Variable Substitution window closes and the configuration appears in the Common Configlet section of the Configlet Editor window.
17	Select the Insert Template icon from the menu bar, then select System, Motorola , SmartX folder, then open the Template - Motorola SmartX Site Converter - Add Site Controller Link template. Result: The Template Variable Substitution window opens.
18	For the Site Controller Link , configure the Line_Interface and Slot_Number_For_ASYNC_Link fields. Click OK . Result: The Template Variable Substitution window closes and the configuration appears in the Common Configlet section of the Configlet Editor window.
19	Select the Insert Template icon from the menu bar, then select System, Motorola , SmartX , then open the Template - Motorola SmartX Site Converter - Add ZC Site Link Path template. Result: The Template Variable Substitution window opens.
20	Configure the ZC_Site_Link_Path_Index IP Address . Click OK . Result: The Template Variable Substitution window closes and the configuration appears in the Common Configlet section of the Configlet Editor window.
21	Click Schedule . Result: The Schedule Push Job window appears.
22	Configure the schedule information. Click Approve and Submit . Result: This approves the job and you can view it in the Schedule Manager window.  NOTE If you choose Submit, you are asked to approve the job later.
23	Press F7 (Schedule Manager). Result: The Schedule Manager window appears in the UNC with the discovery jobs.

Procedure 4-1 How to Configure the SmartX Site Converter Using the UNC (Continued)



24	<p>Verify that the Zone and Site containers include SmartX Site Converter device(s) just discovered.</p> <div data-bbox="427 331 502 417"></div> <div data-bbox="523 353 699 389">NOTE</div> <p>No sites should be in the Lost and Found folder. If there are, see the <i>Unified Network Configurator</i> manual for troubleshooting guidance.</p>
25	<p>Refresh the Network Device View to get the most accurate results, verify the site converter is compliant.</p> <div data-bbox="427 580 502 666"></div> <div data-bbox="523 602 699 638">NOTE</div> <p>Non-compliant devices show a red circle with a line through it.</p>
26	<p>If the site converter is not compliant, follow these steps:</p> <ol style="list-style-type: none"> 1. Right click the device, the choose Compliance Audit. 2. Select the appropriate Zone folder. 3. Select the appropriate Site folder. 4. Select the available Site Standard, and then the compliance results appear and contain any proposed remedies. 5. Choose Schedule to push the recommended changes to the device, otherwise examine and make corrections to configuration as necessary.

The SmartX Site Converter channels are configured using the UNC Wizard. [Procedure 4-2](#) describes how to define the channels.

Procedure 4-2 How to Configure the SmartX Site Converter Channels Using the UNC Wizard

1	Log on to the UNC Wizard from the NM client, by double-clicking the Internet Explorer icon on the desktop. Result: The Internet Explorer browser opens.	
2	Type http://ucs-unc0<Y>.ucs:9080/UNCW in the Address field, where <Y> is the number of the UNC server (01 for primary core UNC server, and 02 for backup core UNC server). Press Enter . Result: The UNC Wizard launches and a login dialog box appears.	
3	Type the administrative username and password. Click OK . Result: The UNC Wizard appears.	
4	Select Channel located within RF Site Level Configuration section.	
	If...	Then...
	If there here are multiple zones,	select a Zone ID .
	If there is a single zone,	select a Site .
		<div>NOTE</div> <p>A single zone automatically displays the available sites.</p>

Procedure 4-2 How to Configure the SmartX Site Converter Channels Using the UNC Wizard (Continued)

5	Select a Site ID . Result: The Channel Wizard appears.								
6	To add a new channel, click Add Row and enter the channel number and slot/line data.								
7	To edit the configuration of an existing channel, modify the channel row slot/line data.								
8	Click Submit . Result: Channel audit is run behind the scenes and a remedy is scheduled in the Schedule Manager to match the Channel Wizard data.  NOTE If invalid data is entered, you must correct the problem and resubmit the configuration.								
9	Approve or deny any new remedies in the Schedule Manager. <table> <tr> <th>If...</th><th>Then...</th></tr> <tr> <td>If a remedy is correct,</td><td>approve the job to configure the SmartX converter correctly.</td></tr> <tr> <td>If a remedy is incorrect,</td><td>deny the job and go back and edit the channel configuration.</td></tr> <tr> <td>If a remedy does not exist,</td><td>indicate the device configuration matches the Channel Wizard.</td></tr> </table> Result: Channel configuration is complete.  NOTE You can run site level audits to confirm compliance. Channel audits are formed based on the Channel Wizard configuration.	If...	Then...	If a remedy is correct,	approve the job to configure the SmartX converter correctly.	If a remedy is incorrect,	deny the job and go back and edit the channel configuration.	If a remedy does not exist,	indicate the device configuration matches the Channel Wizard.
If...	Then...								
If a remedy is correct,	approve the job to configure the SmartX converter correctly.								
If a remedy is incorrect,	deny the job and go back and edit the channel configuration.								
If a remedy does not exist,	indicate the device configuration matches the Channel Wizard.								
10	Verify the channel configuration by refreshing the device view and ensure the timestamp is accurate with the latest configuration.								

Network Management Configuration for the SMARTNET/SmartZone Devices

[Process 4-2](#) describes how to configure the 3600 sites and channels in the Unified Network Configurator (UNC) and Provisioning Manager (PM). This is done so that the zone controller can interface with these 3600 RF sites for call processing.

Process 4-2 Configuring the Trunked 3600 Sites and Channels on the Network Managers

- | | |
|----------|--|
| 1 | Add a 3600 site in the UNC. See Procedure 4-3, "How to Add a 3600 Site," on page 4-9. |
| 2 | Add a 3600 channel in the UNC. See Procedure 4-4, "How to Add a 3600 Channel," on page 4-11. |
| 3 | Define a valid trespass protection ID list in the UNC. See Procedure 4-5, "How to Define the Valid Trespass Protection ID List," on page 4-12. |
| 4 | Configure modulation mapping in the PM. See "Subscriber Modulation Map" in the <i>Provisioning Manager</i> manual for the parameters required. |
| 5 | Migrate the security groups from the 4.1 database to 7.x. Contact the Motorola Solution Support Center for assistance. |

Adding and Configuring 3600 Sites and Channels

When you add a 3600 site in the ASTRO® 25 7.x system, you must use both the Unified Network Configurator and the Provisioning Manager network managers to properly configure the new site. [Procedure 4-3](#) describes how to add a 3600 site using the UNC. For more information, see the *Unified Network Configurator* and *Provisioning Manager* manuals for more information on these network managers and the records that you need to configure for 3600 site operation.

Procedure 4-3 How to Add a 3600 Site

- | | |
|----------|--|
| 1 | Log on to the Unified Network Configurator Wizard .
Result: The UNC Wizard home page appears. |
| 2 | From the list of available wizards on the left side of the Unified Network Configurator Wizard, select Subnet Discovery .
Result: The right side of the window is updated with the Subnet Discovery form. |
| 3 | Select the RF Site Discovery Type from the drop-down list. |
| 4 | Select the Zone ID of the zone for the site you want to add.
Result: A table displays listing the previously configured sites for that zone. |
| 5 | Choose the Site ID for the site you want to configure. |
| 6 | Click Submit to send your changes to the UNC server. |
| 7 | Select the Site option under RF Site Level Configuration in the navigation tree.
Result: The Site Configuration Wizard screen appears. |

Procedure 4-3 How to Add a 3600 Site (Continued)

8	<p>In the Site Configuration Wizard, edit the following parameters for a 3600 channel:</p> <ul style="list-style-type: none"> • Site Alias • Carrier Timeout (sec) • Fade Timeout (sec) • Illegal Carrier/Carrier Malf (sec) • Link Timeout (sec) • Access Code Index Requested (hex) • Site Trunking Indication Holdoff Time (sec) • Message Trunk (sec) • 3600 Site Type • Recovery Timeout (sec) • Connect Tone <div data-bbox="391 840 470 925"></div> <div data-bbox="486 857 662 900">NOTE</div> <p>Any changes made to site parameters cause an update to the business rules stored in VoyenceControl.</p>
9	<p>Open the Schedule Manager and approve and submit any jobs that may have been created due to updates submitted here.</p>
10	<p>Configure the newly added 3600 site as an adjacent site in the Unified Network Configurator's System Wizard.</p> <div data-bbox="391 1159 470 1244"></div> <div data-bbox="486 1181 662 1223">IMPORTANT</div> <p>The 3600 sites can only be adjacent to other 3600 sites.</p> <div data-bbox="391 1298 470 1383"></div> <div data-bbox="486 1319 662 1361">NOTE</div> <p>Expanded Adjacent Site Broadcast (ASB) capable subscribers support an Adjacent Site Broadcast list of up to 15 adjacent sites. However, Expanded ASB capability only applies to the subscribers located in ASTRO® 25 sites. Subscribers from the sites connected through SmartX cannot be Expanded ASB capable and should leave the default setting of No.</p>
11	<p>Synchronize the data between the UNC and the Provisioning Manager by clicking the Publish Infrastructure Data link to transfer the new site information to the Provisioning Manager.</p> <p>Result: The site is fully operational on the system.</p>
12	<p>Add the 3600 site to the Radio Site Access Profile record. See “Radio Site Access Profile Parameters” in the <i>Provisioning Manager</i> manual.</p>
13	<p>Add the 3600 site to the TG/MG Site Access Profile record. See “TG/MG Site Access Profile Parameters” in the <i>Provisioning Manager</i> manual.</p>

[Procedure 4-4](#) describes how to add a 3600 channel in the ASTRO® 25 7.x system using the UNC.

Procedure 4-4 How to Add a 3600 Channel

1	Log on to the Unified Network Configurator Wizard . Result: The UNC Wizard home page appears.
2	From the list of available wizards on the left side of the Unified Network Configurator Wizard, select Channel under RF Site Level Configuration in the navigation tree. Result: The right side of the window updates.
3	Select the Zone ID of the zone in which you want to add the channel. Result: The available channels at the site are listed.
4	Select the Site ID of the SmartX site. Result: The Channel Configuration form appears displaying the list of available channels.
5	Click Add Row . Result: A new row appears in the table.
6	Edit the following parameter for a 3600 channel: <ul style="list-style-type: none"> • Home/Control Channel Capable • Home/Control Channel Preference level • BSI Enable • DFB Channel • Sub-Band • Allow All User Groups • Digital Voice Capable • Analog Voice Capable • Digital Line Interface • Digital Slot Number • Analog Line Interface • Analog Slot Number • Service Mode <div data-bbox="427 1449 502 1534"></div> <div data-bbox="564 1470 651 1502">NOTE</div> <p>Any changes made to channel parameters cause an update to the business rules stored in VoyenceControl.</p>
7	From the Tools menu, select Schedule Manager and approve and submit any jobs that may have been created due to updates submitted here. Result: The new channel record is created.
8	Synchronize the data between the UNC and the Provisioning Manager by clicking the Publish Infrastructure Data link to transfer the new channel information to the Provisioning Manager. Result: The channel is fully operational on the system.

Procedure 4-5 describes how to define the trespass protection IDs in the UNC. Since the SmartX Site Converter makes it possible to add older trunked 3600 sites to an ASTRO® 25 system, this can result in several system IDs appearing on the system. Since only one system ID is allowed in an ASTRO® 25 system, you need to inform the system of other possible IDs that are allowed.


You need to perform Procedure 4-5 when you have 3600 sites with multiple system IDs to enable subscriber radios to roam between the 3600 sites. If you have multiple 3600 sites that all have the same 3.x/4.x system ID, you do not need to perform this task.



The system ID parameter for the 3600 has four digits and the current 9600 is a three-digit value.

Procedure 4-5 How to Define the Valid Trespass Protection ID List

1	In the UNC Wizard, Select the Valid Trespass ID option under System Level Configuration in the navigation tree.
2	To add a valid system ID, click Add Row to add a row to the table displayed on the screen. Then
3	Enter the valid system ID (hex) for the 3600 site.
4	Click Submit to save your additions or changes to the UNC Server.



NOTE

To modify or delete IDs saved in the existing trespass ID list, see the UNCW online help.

See "Subscriber Modulation Map" in the *Provisioning Manager* manual for the parameters required to configure subscriber modulation mapping in the Provisioning Manager.

Monitoring SmartX Site Converter Faults



Once the SmartX Site Converter is on the network and fully configured, you can use the Unified Event Manager (UEM) application to monitor faults affecting these devices.

Discovering the SmartX Site Converter Devices with the UEM



Procedure 4-6 discovers the SmartX Site Converter and allows the Unified Event Manager to fault manage these devices.

Figure 4-1 shows the discovery of a Motorola SmartX Site Converter in the system.

Figure 4-1 SmartX Site Converter Discovery in the UEM

	Clear	Network - RF Site	X.X.X.X	X.X.X.X	
	Clear	Motorola SmartX Site Converter	X.X.X.X	X.X.X.X	X.X.X.X - Smartzone Site
	Clear	Smartzone Site	Site Alias		X.X.X.X - Smartzone Site
	Clear	Smartzone Site Equipment	Site Alias		X.X.X.X - Smartzone Site


Procedure 4-6 How to Discover the SmartX Site Converter in the UEM

1	To log on to the UEM from the NM client, double-click the Internet Explorer icon on the desktop. Result: The Internet Explorer window appears.
2	Type http://zxxxuem01:9090 in the Address field. Press Enter .  NOTE The xxx is where you need to identify the zone ID for the discovered devices. Result: The UEM window appears.
3	Enter the appropriate admin user name and password. Click OK . Result: The UEM main window appears.
4	Select Tools, Discovery Configuration .
5	On the Subnet Discovery tab, select RF Site from the Discovery Type list.
6	Type the site ID in the Site ID field, then click Start Discovery . Result: The Discovery Status dialog box appears with the job number for the discovery.
7	Click View Job Status . Result: The Job Status View window appears displaying the status of the discovery.
8	Verify that all SmartX Site Converter devices at the site appear in the log.  NOTE You can view the log to verify that all of the devices were discovered. The log ends with the following message: Job Status Success

Verifying System Installation with the UEM

Procedure 4-7 describes how to use the Unified Event Manager's Physical Detail View and Service Detail View maps to check for SmartX Site Converter alarms and confirm successful installation in the system. See the *Unified Event Manager* manual and online help for more information on using this fault management application.

Procedure 4-7 How to Verify SmartX Site Converter Operation with the UEM

1	To log on to the UEM from the NM client, double-click the Internet Explorer icon on the desktop. Result: The Internet Explorer window appears.
2	Type http://zxxxuem01:9090 in the Address field. Press Enter .  NOTE The xxx is where you need to identify the zone ID for the discovered devices. Result: The UEM window appears.
3	Enter the appropriate admin user name and password. Click OK . Result: The UEM main window appears.
4	Open the Physical Detail View map, and choose SmartX Site Network . Result: A pop-up menu appears.
5	Choose View Alarms .
6	Verify the health of the system, including that <ul style="list-style-type: none"> • wide trunking is enabled. • site converters enabled. • the site link up. • the ZC link up. • only clear, warning, and minor alarms appear.
7	Open the Service Detail View map. Choose SmartX Site ID . Result: A pop-up menu appears.
8	Choose View Group Alarms .
9	Verify the health of the system, including that <ul style="list-style-type: none"> • wide trunking is enabled. • site converters enabled. • the site link up. • the ZC link up. • only clear, warning, and minor alarms appear.

SmartX Site Converter Connections to Remote Sites

.....

The SmartX Site Converter devices may be installed at the master site or the remote site.

Master site location benefits:

- Easier to install, upgrade, maintain if all site converters are co-located.
- Keeps the RF remote site transport links unchanged.
- May save on labor costs if trips to remote sites are eliminated or minimized.

Remote site location benefits:

- Potential site link bandwidth savings
- Redundant links
- Potential lower equipment costs due to channel bank/network design considerations
- Use of Ethernet site links

There are additional remote site considerations:

1. ASTRO[®] 25 link specifications must be met if the SmartX Site Converter and site gateway are located at the RF remote site.
2. Temperature range of SmartX Site Converter is 5 to 40 °C.
3. The SmartX Site Converter requires AC power. If only DC is available at the site a converter is required.

At the master site, you must configure the channel bank to redirect the T1/E1 to the 7.x Master Site T1 patch panel instead of the SmartZone[®] zone controller for data links and the SmartZone[®] Ambassador Electronics Bank (AEB) for voice channels. This may require one or two T1 circuits depending on the number of channels to be connected and whether they are analog-only, digital-only, or mixed mode. Also, if the Master Site channel bank had previously been using ADPCM encoding and multiplexing of mixed mode channels, then the ADPCM card must be removed or disabled and each mixed mode channel must use a separate DS0 for the analog and ASTRO[®] digital channels.

At the remote site, the channel bank at the 3600 RF site needs to be configured if it has been replaced or if it had previously been using ADPCM encoding and multiplexing of mixed mode channels. The ADPCM card must be removed or disabled and each mixed mode channel must use a separate DS0 for the analog and ASTRO[®] 25 digital channels. It must be configured to connect voice channels and site data links to the T1/E1 circuit(s) connected to the Master Site.

The site converter is connected to the channel bank using one or two T1/E1 circuits depending on capacity needs for the number and type of channels supported by the 3600 RF site. If available, vacant T1/E1 interfaces on the channel bank are used first to avoid SmartZone[®] service disruption. The Ethernet port connects through an Ethernet crossover cable to the site gateway (100Mb full duplex – single physical connection). The only grounding that needs to be done is when the SmartX hardware is grounded to the rack using a grounding lug during the initial hardware installation.

The channel bank provides the clock source for the connection between the SmartX Site Converter and the channel bank. Further, the SmartX Site Converter uses a single clock input source for both T1/E1 interfaces internally. The implication is that if two T1/E1 interfaces are used, then they must be synchronized from a clocking perspective. The SmartX Site Converter cannot process two independently clocked T1/E1 links.


**WARNING**

Do not connect a SmartX Site Converter directly to the Public Switched Telephone Network (PSTN). A typical SmartX Site Converter connects to a channel bank, which provides FCC part 68 rated protection. If this is not the case, adequate protection, provided by a device such as a Channel Service Unit (CSU), must be provided for the site converter connections if T1/E1 facilities from a PSTN are used as transport between the remote sites and a site converter at the master site.

See the “Reference” chapter of this manual for the E1/T1 pinout and cabling information.

[Procedure 4-8](#) describes how to connect the site converter to the channel bank, which enables communication with the remote site.

Procedure 4-8 How to Connect the SmartX Site Converter and the Channel Bank

1	<p>Before connecting the SmartX Site Converter to the channel bank, verify the following:</p> <ul style="list-style-type: none">• the channel bank cabling and channel configuration match.• T1/E1 parameters and Async Link configuration is compatible with the physical hardware connectivity.• the number of T1/E1 connections that are necessary.• If the SmartX Site Converter is set to alaw, then the connected channel bank must be set to a-inv (inverse a-Law). This configuration is done in the Line Idle Pattern field, which is part of the RF Site object in the UNC. For u-Law, both devices are configured the same.
2	<p>Connect the E1/T1 lines to appropriate channel bank.</p> <div data-bbox="427 761 699 846"> NOTE</div> <p>E1/T1 line 1 is the lower-right port and E1T1 line 2 is upper-right port.</p>
3	<p>To confirm the connection: Log on to the Unified Network Configurator (UNC) and perform a discovery of the SmartX Site Converter.</p> <p>-OR-</p> <p>Log on to the Unified Event Manager (UEM), and verify the following:</p> <ul style="list-style-type: none">• the site link(s) come up.• the channels are not in an enabled state.• the site goes to wide trunking.

This page intentionally left blank.

SmartX Site Converter Optimization

This chapter contains optimization procedures and recommended settings relating to the SmartX Site Converter.

T1/E1 Optimization

The configuration in the channel bank equipment must map to the configuration in the SmartX Site Converter (as entered on the UNC). They are 1-to-1 mappings. Please see the mappings specified in the *Unified Network Configurator Online Help*.

Audio Optimization

There is no audio optimization specifically for the SmartX Site Converter. The deployment procedure assumes that your organization has followed the level setting procedures for the 3.x/4.x system.

This page intentionally left blank.

SmartX Site Converter Operation

This chapter details tasks to perform once the SmartX Site Converter is installed and operational on your system.

Powering Up a SmartX Site Converter

The SmartX Site Converter does not have an on/off switch. The device is activated by supplying power. Perform [Procedure 6-1](#) to power up the SmartX Site Converter and verify that it is working.

See the “Reference” chapter for descriptions of the LEDs on the SmartX Site Converter.

Procedure 6-1 How to Power Up the SmartX Site Converter

1

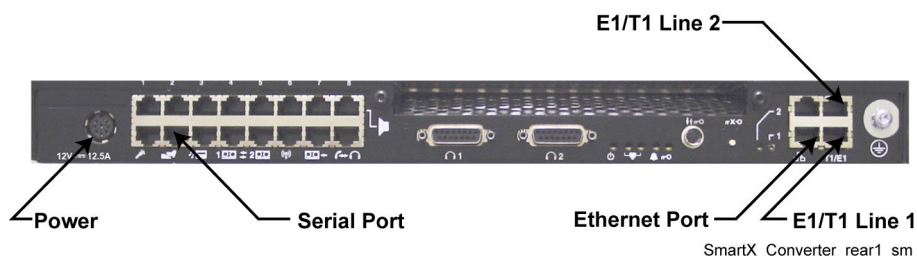


WARNING

Before performing this procedure, always make sure that power line cord is not connected to an AC source.

Connect the power supply 12V output line cord to the rear panel connector on the SmartX Site Converter.

Figure 6-1 Rear View of the SmartX Site Converter




2 Connect the opposite end of the power line cord to the AC power source.

3 Verify that the power LED is on. See the “SmartX Site Converter LEDs” section in the “Reference” chapter.

Powering Down a SmartX Site Converter

Perform [Procedure 6-2](#) to power down the SmartX Site Converter.

Procedure 6-2 How to Power Down the SmartX Site Converter

1	<div><div>CAUTION</div></div> <p>The site converter hardware contains low, safe, voltage levels but could cause arcing or damage to connected equipment when the cover is removed while the unit is powered. Unplug the power line cord from the site converter when preparing to service this equipment.</p> <p>Disconnect the power line cord from the AC source.</p>
2	<p>Disconnect the power supply 12V output cable from the rear of the SmartX Site Converter chassis.</p>

Rebooting the SmartX Site Converter

There are three ways to reboot the SmartX Site Converter hardware.

1. Power-cycling the hardware as described in [Procedure 6-3](#).
2. Issuing a command from the CSS as described in [Procedure 6-4](#).
3. Issuing a command from the UEM as described in [Procedure 6-5](#).

When the site converter is taken out of service for a reboot, the 3600 sites become out of service for the duration of the restart.

Procedure 6-3 How to Reboot the SmartX Site Converter by Power Cycling the Hardware

1	Trace the power line cord from the round power port on the left side of the device to the power source.
2	Disconnect the cable from the AC power source. Result: The SmartX Site Converter is off.
3	Verify the Power LED on back of the device is not lit.
4	Reconnect the power line cord to the AC source and verify the power LED is on. Result: The Power LED is green when reboot is complete.

An alternative method to powering down the hardware, is to reset the SmartX Site Converter using the CSS as described in [Procedure 6-4](#).

Procedure 6-4 How to Reboot the SmartX Site Converter on the CSS

1	Launch the CSS application using a serial connection (as described in the “SmartX Site Converter Installation” chapter).
2	Select Tools, Set IP Address and Box Number . Result: The Set IP Address and Box Number dialog box appears populated with the IP address for the site converter.
3	Click Reset .
4	Click OK in the confirmation box to proceed with the reset. Result: The Telephone Media Gateway restarts.
5	Proceed to Procedure 3-8, "How to Change SNMPv3 Configuration and User Credentials on the SmartX Site Converter," on page 3-20 to reconfigure the SNMPv3 credentials.

The Unified Event Manager also provides an option for resetting the SmartX Site Converter. See [Procedure 6-5](#).

Procedure 6-5 How to Reboot the SmartX Site Converter Using the UEM

1	Launch the Unified Event Manager .
2	From the Network Database link, right-click on the SmartX Site Converter device. Result:
3	Choose Command .
4	Select the entity associated with the device.
5	Choose Reset and click Apply . Result: The cursor changes into an hour glass when the process is initiated and it changes to normal when the process is completed.

Logging on to the SmartX Site Converter

.....

The SmartX Site Converter does have a default service account, and your system administrator has those credentials. You need to change the default credentials when the device is installed. You set the appropriate IP address, login, and password the first time you connect to the device, which is described in the “SmartX Site Converter Installation” chapter.

Administering Accounts

You can set up a local password for the SmartX Site Converter using CSS and that is described in the “Configuration” chapter.

Ensure that you have the required *user credentials information* (security level, authentication passphrase, and encryption passphrase) to configure the site devices before proceeding with changing or resetting a password.

The user credentials information includes both the current and new credentials. Without the current credentials, you are not able to access the device and cannot change the user credentials. Changing to the incorrect user credentials may lead to not being able to access the site converter from the Network Managers for the site devices or for the site devices to send alarms for fault management.

Table 6-1 provides the user accounts and the network management application that can be used to set or change them.



NOTE

Contact your system administrator for a list of all user accounts and passwords for your system.

Table 6-1 SmartX Site Converter Accounts

Type of Account	Description and Network Management Application Used
Local service account*	This account is used for setting IP addresses and can also be used to configure the SmartX device locally if it cannot connect to the rest of the system (e.g., site link failure). There are two privilege levels. The higher privilege allows for setting IPs and resetting the site converter. Credentials can be set or changed through CSS (serial connection).
Master admin account	Required for the configuration, fault management, and other SNMPv3 communications with the UNC, UEM, and CSS (Ethernet connection). Security is enabled by default.
Inform A account	Required for SNMPv3 inform event messages to UNC and UEM from devices (Ethernet connection).
Inform B account	Required for SNMPv3 inform event messages to UNC and UEM from devices (Ethernet connection).
CSS account	Used by CSS.
SNMPv3 user admin account	Used to administer the SNMPv3 Users (UEM). No other User Account is allowed to change the User Credentials.
* This account is not stored in the UNC, so changes are not backed up in the system.	

Backing Up the SmartX Site Converter

The Unified Network Configurator provides a backup and recovery mechanism for this device. A previously defined configuration can be pushed to the site converter using the audit and rollback provided in [Procedure 6-6](#). However, some user credentials and the IP address for the device are not stored, and would require a re-installation of the device in the event of a failure. See the “Replacing a Device” in the *Unified Network Configurator* manual for the process.





NOTE

The SmartX Site Converter can be used on a system with Dynamic System Resilience (DSR). However, if there is a switch to the backup zone core, the SmartX Site Converter is not switched. Any site connected through the SmartX Site Converter goes into Site Trunking mode.


Procedure 6-6 How to Restore the SmartX Site Converter Configuration from UNC

1	Log on to the VoyenceControl application.				
	<div><div></div><div>NOTE</div></div> <p>The names EMC Ionix Network Configuration Manager and VoyenceControl are used interchangeably for this product.</p> <p>Result: The VoyenceControl main window appears.</p>				
2	From the Devices View menu bar, select Device .				
3	Click on the Config icon. Result: The Configuration window opens.				
4	Make changes to the configuration and click Audit . Result: The Audit window opens.				
5	Select one or more devices you want to audit.				
6	Click Audit . Result: The Select the items window appears.				
7	Select the following items: 1. Select the Zone in which the device is located. 2. Select the Site ID in which your device is located. 3. Select the Site Standard.				
8	Click Select Item . Result: The Compliance Audit Results window appears.				
	<table><tr><th>If...</th><th>Then...</th></tr><tr><td>If the changes are valid,</td><td>the device appears in the Compliant pane. Close the Compliance Audit Results window.</td></tr></table>	If...	Then...	If the changes are valid,	the device appears in the Compliant pane. Close the Compliance Audit Results window.
If...	Then...				
If the changes are valid,	the device appears in the Compliant pane. Close the Compliance Audit Results window.				

Procedure 6-6 How to Restore the SmartX Site Converter Configuration from UNC (Continued)

	<p>If the changes are not valid, the device is listed in the Non Compliant pane.</p> <ol style="list-style-type: none"> 1. Select the device. 2. Select Preview. 3. In the Remedy Preview window, scroll the slider bar in the Test Results pane to find all red Xs. 4. Select the red X.
	<div>  <div> NOTE <p>The Remedy Configlets pane contains the lines of the configuration that need to be changed to bring the device into compliance.</p> </div> </div> <ol style="list-style-type: none"> 5. Make the changes in the configuration window and rerun the audit.
9	In the navigation pane, expand Networks and select Astro 25 Radio Network .
10	<p>Double-click Devices.</p> <p>Result: The Devices (view) appears showing a list of devices in the contents pane.</p>
11	Right-click the SmartX Site Converter whose configuration baseline you want to verify, then choose Properties from the pop-up menu.
12	<p>Click the History tab.</p> <p>Result: The list of Baselines appears.</p>
13	<p>On the right side in the History tab, select the Baseline tab.</p> <p>Result: The name of the baseline displays.</p>
14	<p>Select the revision to be used instead of the current one.</p> <div>  <div> NOTE <p>See “How to Determine Which Version Is Currently the Baseline” in the <i>Unified Network Configurator</i> manual if you are not sure how to determine the device's baseline.</p> </div> </div>
15	<p>Click the Roll Back icon.</p> <p>Result: The Schedule Job window appears.</p>
16	Type the job name and schedule the job.

Procedure 6-6 How to Restore the SmartX Site Converter Configuration from UNC (Continued)

17	Click Approve & Submit or click Submit , depending on your permissions.
	<div> NOTE</div> <ul style="list-style-type: none">• If you clicked Approve & Submit , the Schedule Job window closes and the job status can be viewed using Schedule Manager available from the Tools menu on the VoyenceControl main window.• If you clicked Submit , the status of the job is Pending. You can approve Pending jobs on the Schedule Manager window.
18	Close the Edit Network Properties window.
19	From the Tools menu, select Schedule Manager to view the pending rollback.

When you install and configure a SmartX Site Converter using the Configuration/Service Software application, you save the settings to an archive file. This file can be retrieved to restore a previous configuration. See the *CSS Online Help* for more information.

Viewing Status

The operational status of the SmartX Site Converter can be viewed using the network manager (UNC) and the fault manager (UEM).

Viewing Status in the UEM

The SmartX Site Converter reports the following information to the UEM:

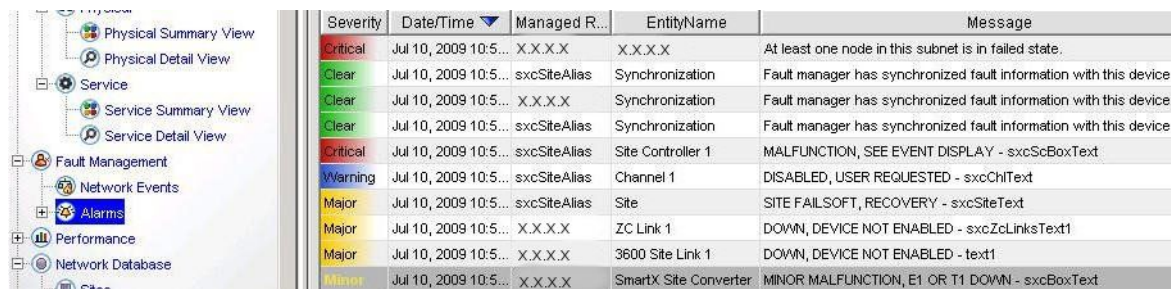
- **Motorola SmartX Site Converter** — SmartX Site Converter device state, SmartX - 3600 Site link state, and SmartX - ZC link state
- **SmartZone Site** — site and site communication state
- **SmartZone Site Equipment** — Site Controller equipment, communication, sub-site, and channel status

While the zone controller (ZC) reports the following information to the UEM:

- Site
- Channel

The primary difference in fault reporting is that 9600 sites are reported by the devices (base radio, site controller, and so forth) and 3600 site faults are reported by the SmartX Site Converter. Figure 6-2 depicts SmartX Site Converter alarms in the UEM.

Figure 6-2 SmartX Site Converter Alarms in the UEM

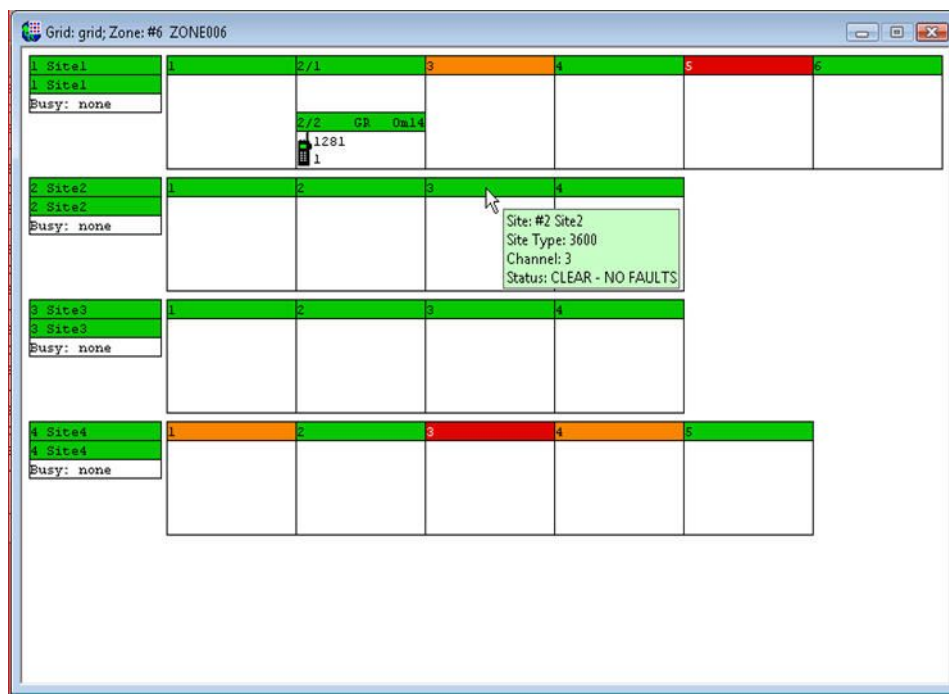


Severity	Date/Time	Managed R...	EntityName	Message
Critical	Jul 10, 2009 10:5...	X.X.X.X	X.X.X.X	At least one node in this subnet is in failed state.
Clear	Jul 10, 2009 10:5...	sxcSiteAlias	Synchronization	Fault manager has synchronized fault information with this device.
Clear	Jul 10, 2009 10:5...	X.X.X.X	Synchronization	Fault manager has synchronized fault information with this device.
Clear	Jul 10, 2009 10:5...	sxcSiteAlias	Synchronization	Fault manager has synchronized fault information with this device.
Critical	Jul 10, 2009 10:5...	sxcSiteAlias	Site Controller 1	MALFUNCTION, SEE EVENT DISPLAY - sxcScBoxText
Warning	Jul 10, 2009 10:5...	sxcSiteAlias	Channel 1	DISABLED, USER REQUESTED - sxcChlText
Major	Jul 10, 2009 10:5...	sxcSiteAlias	Site	SITE FAILSOFT, RECOVERY - sxcSiteText
Major	Jul 10, 2009 10:5...	X.X.X.X	ZC Link 1	DOWN, DEVICE NOT ENABLED - sxcZcLinksText1
Major	Jul 10, 2009 10:5...	X.X.X.X	3600 Site Link 1	DOWN, DEVICE NOT ENABLED - text1
Minor	Jul 10, 2009 10:5...	X.X.X.X	SmartX Site Converter	MINOR MALFUNCTION, E1 OR T1 DOWN - sxcBoxText

Viewing 3600 Site Status in ZoneWatch

The Unified Event Manager has no information on the channels configured at the 3600 site if there is no alarm on the channel. The UEM reports faults only when there is an active alarm for channel. For channels that do not have any alarms, the UEM does not report clear state. However, in ZoneWatch application, 3600 channels that are configured in the server application, but do not have necessary equipment at the site are reported as “CLEAR – NO FAULTS” as shown in Figure 6-3. The UEM can only send a “Clear” state for channels that had active alarms that are resolved. The difference in fault reporting terminology for 3600 sites instead of the CLEAR that is used in the 9600 sites is due to differences in infrastructure management.

Figure 6-3 3600 Site Status in ZoneWatch




Site	1	2	3	4	5	6
1 Site1	1	2/1	3	4	5	6
1 Site1		2/2 GP Data				
Busy: none		1281				
2 Site2	1	2	3	4		
2 Site2						
Busy: none						
3 Site3	1	2	3	4		
3 Site3						
Busy: none						
4 Site4	1	2	3	4	5	6
4 Site4						
Busy: none						

Viewing Status in the UNC

The VoyenceControl application contains auditing functionality. Standards and tests are created to ensure that the device configurations meet the ASTRO[®] 25 radio system operational rules. As part of the UNC Wizard functionality, the tests are run to determine any devices that are not compliant. In such cases remedy jobs are automatically created to resolve the issues. Please note that you have to schedule these remedy jobs manually.

[Procedure 6-7](#) describes how to verify if the SmartX Site Converter is compliant.

Procedure 6-7 How to Verify the SmartX Site Converter is Compliant in the UNC

1	<p>Log on to the VoyenceControl application.</p> <div data-bbox="391 619 464 704">  </div> <div data-bbox="483 640 662 678">NOTE</div> <p>The names EMC Ionix Network Configuration Manager and VoyenceControl are used interchangeably for this product.</p> <p>Result: The VoyenceControl main window appears.</p>
2	<p>In the navigation pane of the main Unified Network Configurator window, expand Networks and select the Astro 25 Radio Network.</p>
3	<p>Double-click Devices.</p> <p>Result: The diagram of devices appears in the right pane.</p>
4	<p>Change to a table view by clicking the Table icon in the right pane upper menu.</p> <p>Result: The list of devices is populated in a table.</p>
5	<p>Click the status column to sort devices by their status.</p>
6	<p>Scroll down to see SmartX Site Converter(s) compliance status.</p>

The “UNC Operation” chapter of the *Unified Network Configurator* manual also describes how to generate an audit report and make devices compliant.

SmartX Site Converter Maintenance

.....

.

.

.

.

This chapter provides information about maintenance procedures for SmartX Site Converter.

Hardware Maintenance

.....

.

.

There are no serviceable parts in the SmartX Site Converter that require maintenance or calibration. Exterior cleaning using a clean, lint-free cloth or soft brush is sufficient.

Software Maintenance

.....

.

.

There are no patches for the SmartX Site Converter. In the event the software needs to be altered, new software is transferred and installed on the software as a system upgrade.

This page intentionally left blank.

SmartX Site Converter Troubleshooting

This chapter provides fault management and troubleshooting information relating to the SmartX Site Converter.

General Troubleshooting for the SmartX Site Converter

This section describes potential scenarios and information on how to reset SNMPv3 user credentials.

Troubleshooting the Software Download to the SmartX Site Converter

The Unified Network Configurator (UNC) management software provide secure Software Download (SWDL) to the SmartX Site Converter. In the event that you are unable to download the software using secure SWDL, you can download in clear mode. See the *Unified Network Configurator* and *Software Download* manuals for more information.

Resetting SNMPv3 User Credentials to Defaults on Devices at a Remote Site



You only execute this procedure in the case where the primary admin user credentials are lost or forgotten on devices at a remote site. Execute [Procedure 8-1](#) if you are at the site and have direct access to the device. Execute [Procedure 8-2](#) if you are not at the site (remote), and do not have direct access to the device.




IMPORTANT

After resetting the SNMPv3 user credentials to factory defaults, you must restart the device. You must plan for the device to be out of service for the reboot period.

Procedure 8-1 How to Reset SNMPv3 User Credentials to Defaults on Devices at a Remote Site Locally through the CSS



1	Launch the CSS application using a serial connection (as described in the “SmartX Site Converter Installation” chapter).
2	Log on with the local service account username and password.
3	<p>Type the Elevated Privileges password for administrative level access in the appropriate field.</p> <div>  <div> NOTE <p>Administrative access is required to perform this procedure. If Central Authentication is enabled on the device, and is required to be used per the security policy rather than using the local service account to log on, you use the defined Central Authentication credentials (username and password). The Elevated Password Privileges password is not managed by Central Authentication Services, but locally managed on the device and is required for performing operations requiring administration level access. If you fail to elevate privileges, you cannot access or execute the mechanisms utilized to reset the SNMPv3 configuration and credentials.</p> </div> </div>
4	<p>Click OK.</p> <p>Result: A confirmation dialog box appears telling you that CSS has connected with the device.</p>
5	<p>Click OK.</p> <p>Result: The connection protocol status appears in the lower-right corner of the window and indicates that a serial connection is in use with the SmartX Site Converter.</p> <div>  <div> IMPORTANT <p>If you have provided the wrong user credentials, you need to go back to step 2 and try again. Per your organization's security policies, the device may limit the number of login attempts. If you fail to log on and exceed the maximum number of attempts, you may be locked out of the device for a period of time. The lockout time duration is defined by your policy (default is 15 minutes).</p> </div> </div>
6	<p>To reset the SNMPv3 user credentials to the factory default, select Security, SNMPv3 Configuration (serial), then select Reset SNMPv3 Configuration (serial).</p> <p>Result: The SNMPv3 Configuration dialog box appears.</p>
7	<p>Click Reset SNMPv3 Configuration, then choose Exit.</p> <p>Result: The Reset SNMPv3 Configuration dialog box closes.</p>
8	To reboot the device, select Tools on the main CSS window.
9	<p>Select Set IP Address/Box Number.</p> <p>Result: The Set IP Address/Box Number dialog box appears.</p>

Procedure 8-1 How to Reset SNMPv3 User Credentials to Defaults on Devices at a Remote Site Locally through the CSS (Continued)



10	Click Reset . Result: The device reboots.
11	On the main CSS window, select File, Exit . Click OK to confirm that you want to exit. Result: The CSS application closes.
12	Monitor the LEDs on the SmartX Site Converter to verify that the device reboots.  NOTE Once a SmartX Site Converter is reset, you must change the SNMPv3 configuration and user credentials on devices at a Remote Site and configure all SNMPv3 users for the device as described in this manual.

Procedure 8-2 requires that you know the SmartX Site Converter's FQDN or IP address to connect to the remote site. Also, see the “SSH Configuration” chapter in the *Securing Protocols with SSH* manual and the *CSS Online Help* for more information about using the CSS, Telnet, and SSH to configure RF site devices.

Procedure 8-2 How to Reset the SNMPv3 User Credentials to Defaults on Devices at a Remote Site Remotely through Telnet/SSH

1	To connect and log on to the device remotely over the network, use the PuTTY Terminal Services to connect to the device using SSH or Telnet.  NOTE Depending on security policy and site configuration of your system, SSH or Telnet may be enabled or disabled. Try SSH first, as that is the preferred secure remote access service. Obtain the IP address of the device to proceed with these steps. Result: A login warning banner appears prompting for a username.
2	Type the local service user login and password. Result: The device displays the CSS or J-O command prompt.  IMPORTANT If the username or password prompt appears again, you have entered the wrong credentials and must try again. If Central Authentication is enabled and is required to be used per the security policy rather than using the local service account to log on, use your defined Central Authentication username and password. Per the security policies for your organization, the device may limit the number of login attempts. If you fail to log on and exceed the maximum number of attempts, you may be locked out of the device for time. Your policy defines the lockout time duration (default is 15 minutes).
3	Type enablepriv -E . Press Enter to elevate the privileges to an administrative level. Result: The enablepriv command prompt appears for the elevated privileges password.

Procedure 8-2 How to Reset the SNMPv3 User Credentials to Defaults on Devices at a Remote Site Remotely through Telnet/SSH (Continued)

4	<p>Type the elevated privileges password. Press Enter to gain the administration level access.</p> <p>Result: The CSS or J-O command prompt appears.</p> <div data-bbox="387 414 464 500"></div> <div data-bbox="499 436 663 468">IMPORTANT</div> <p>If the username or password prompt appears again, you have entered the wrong credentials and must try again.</p> <p>If you fail to elevate privileges, you cannot view, access, or execute the commands utilized to reset the SNMPv3 configuration and credentials.</p>
5	<p>Type redefault_usm. Press Enter to reset the SNMPv3 user credentials to factory defaults.</p> <p>Result: The device displays the status message “USM Tables will have default values after box reset!” followed by the CSS or J-O command prompt.</p>
6	<p>Type reset. Press Enter to reboot the device.</p> <p>Result: The device reboots.</p>
7	<p>Close the PuTTY connection.</p>
8	<p>Monitor the LEDs on the SmartX Site Converter to verify that the device reboots.</p> <div data-bbox="387 953 464 1038"></div> <div data-bbox="531 974 616 1006">NOTE</div> <p>Once a SmartX Site Converter is reset, change the SNMPv3 configuration and user credentials on devices at a Remote Site and configure all SNMPv3 users for the device as described in this manual.</p>

Resetting Passwords and SNMPv3 Passphrases

You can enable/disable the password reset mechanism in the CSS application. See the *CSS Online Help's* “Device Security Configuration - Security Services (Serial)” screen for information. To obtain the keys for resetting either password or SNMPv3 passphrases for the device, contact the Motorola Solution Support Center.



NOTE

The default values for the local passwords and SNMPv3 passphrases, as well as the keys for the local password reset procedure, may vary by system release. These values are treated as sensitive information and are provided to you through secured communication.

Table 8-1 Local Password and SNMPv3 Passphrase Troubleshooting

Scenario	SNMPv3 Passphrase Known	Local Password Known	To Reset SNMPv3 Passphrase	To Reset Local Login Password
You are locked out of local login, but know SNMPv3 passphrases	✓	✗	See the <i>CSS Online Help's</i> “SNMPv3 User Configuration”.	See the <i>CSS Online Help's</i> “Resetting Device Passwords.”
You know the local login, but not the SNMPv3 passphrases	✗	✓	See the <i>CSS Online Help's</i> “Reset SNMPv3 Configuration (Serial)”.	See the <i>CSS Online Help's</i> “Device Security Configuration – Security Services (Serial)”
You know both passphrases and local service password	✓	✓	See the <i>CSS Online Help's</i> “SNMPv3 User Configuration”.	See the <i>CSS Online Help's</i> “Device Security Configuration – Security Services (Serial)”
You do not know SNMPv3 passphrase nor service account password	✗	✗	Contact the Solution Support Center.	Contact the Solution Support Center.

Troubleshooting with Local Tools

.....

.....

There are several troubleshooting techniques to employ when connected to the SmartX Site Converter using serial and Ethernet connections.

Troubleshooting the Serial Connection to the SmartX Site Converter

If you are unable to connect to the SmartX Site Converter using serial cable, troubleshoot the configuration in Windows by opening the com port through the Control Panel and unchecking the **Use FIFO buffer (requires 16550 compatible UART)** option in the **Advanced Settings** for the com port before clicking **OK**.




Troubleshooting the Ethernet Connection to the SmartX Site Converter

The first step in troubleshooting the SmartX Site Converter with the CSS is to retrieve the logs ([Procedure 8-3](#)) and software version table ([Procedure 8-4](#)). If the Unified Event Manager has not discovered the SmartX Site Converter, the CSS can be used to view the last 1,000 log events. These reports include information on how often T1/E1 synchronization issues have occurred. This issue may indicate some minor cabling issues and/or parameter mismatch between the site converter and channel bank. There is an entry in the log for every trap.

There are two types of log files:

- Technician log files — Contains time-stamped status and alarm messages that a service technician can use to troubleshoot the SmartX Site Converter.
- Engineering log files — Provides a detailed account of device operation. The SmartX Site Converter writes information about software health, as well as expected and unexpected software events. Motorola Development Engineers use this information to troubleshoot the software processes of a device.

Procedure 8-3 How to Access Log Files in the CSS

1	Connect the laptop with CSS to the SmartX Site Converter through the Ethernet cross-over cable.
2	Choose File, Read Configuration From Device . Result: A message window states that an Ethernet connection must be established.
3	If Centralized Authentication is enabled, an FTP Login Screen opens. See "Device Security Configuration - Remote Access Login (Ethernet)" in the <i>CSS Online Help</i> for details. Provide the required credentials. <div>  <div>NOTE</div> <p>If Authentication Services is enabled in the Security Services Configuration window, enter a Username and Password. Also, enter an Elevated Privileges Password if the chosen security level requires these credentials. If Authentication Services is not enabled, enter any alphanumeric value for Username, Password, and Elevated Privileges Password, as they cannot be left blank.</p> </div>
4	Click OK . Result: The Connection Screen appears.
5	Choose Service, Status Report Screen . Result: The Service Report Screen appears.
6	Click Refresh to see new messages that have occurred since the window was opened. <div>  <div>NOTE</div> <p>You can view the log by saving it to a text file and then viewing it using a text file editor. The Status Report screen also gives you the option to save and clear reports.</p> </div>
7	Save the log to a text file, then review the information. <div>  <div>IMPORTANT</div> <p>Do not attempt to download the logs consecutively with less than a 12-second interval between downloads as this action could lead to the following error: "FTP Error, Unable To Transfer Status Report File."</p> </div>

[Procedure 8-4](#) describes how to access the software version table for troubleshooting information.

Procedure 8-4 How to Access the Software Version Information in the CSS

1	Launch the CSS.
2	Choose Service, Version Screen from the main menu in the CSS.
3	Click the Software Version tab.
4	Review the status, location ID, activation date, and other data that may help you in troubleshooting the site converter.

If the hardware status LEDs indicate that the SmartX Site Converter is operational, you can begin troubleshooting the configuration. The initial configuration is done using a laptop with Configuration Service/Software (CSS), and any problems with accessing the device may require confirming the configuration with the CSS.

You need a laptop or NM Client with the CSS application and an RJ-45 to DB9 converter to begin re-configuring the site converter with a 1900-baud serial connection.

If a complete hardware failure or disaster occurs, the following fields are not retained in the UNC. Retrieve the configuration from the archive file or re-configure the fields in the CSS:

- IP address for the SmartX Site Converter
- Site ID
- Security credentials
- NTP/DNS settings

The ASTRO[®] 25 system provides two sources of NTP information for the SmartX device. The primary source is ntp02.zone# and the secondary source is ntp03.zone#. Prior to system release 7.8, the primary source was ntp01.zone# with a secondary source of ntp02.zone#. The SmartX Site Converter does not support Dynamic System Resilience (DSR), so there are no additional NTP sources. If a disaster occurs, see the appendix in the *NTP Server* manual for more information.

For more information on the configuration of the SmartX Site Converter, see the *Authentication Services*, *Securing Protocols with SSH*, *Information Assurance Features Overview* manuals, and the *CSS Online Help*.

When troubleshooting timing sources, see the appendix in the *NTP Server* manual for more information.

Troubleshooting with the Unified Event Manager

Once the SmartX Site Converter is discovered in the UEM, you can observe the following states:

- site converter
- site (must be in wide trunking mode)
- channel (6809)
- site link
- zone controller (ZC) link

The UEM can also be used to change the state of the site converter (enable/disable), site, and/or channel. If a low battery alarm appears in the UEM, perform the battery replacement procedure in the “FRU/FRE” chapter of this manual.

As with any RF site device, faults are reported as an alarm, or *trap*, in the UEM application. See “Verifying System Installation with the UEM” in the “Configuration” chapter for more information. Also, see the *Unified Event Manager* manual and online help for more information on alarms being generated for the site converter.

Troubleshooting Software Installation

Software download on the SmartX Site Converter is achieved through the Unified Network Configurator. If there is a problem with the installation, you can pull the known good software configuration from the UNC and load that configuration to the device. See “SmartX Site Converter Software Installation” in the “Installation” chapter for more information.

Troubleshooting Call Processing from the SmartX Site Converter Perspective

Table 8-2 provides general recovery actions and identifies which system application to use to re-establish service with the SmartX Site Converter. Other problems with the site and/ or network are beyond the scope of this manual, and you can consult other ASTRO® 25 system documentation.

Table 8-2 SmartX Site Converter Troubleshooting Scenarios


Problem	Recovery Action
ZC link(s) are down	<ul style="list-style-type: none">• Check connectivity between the site converter and network (example: discoverable in UNC and UEM, connect using CSS)• Check that ZC link IP addresses are configured correctly (UNC pull)• Check that the site converter is configured with the correct site ID (UNC pull)• Check that site converter requested state is “enabled” in the UEM
Site converter minor malfunction (indicates a T1/E1 is down)	<ul style="list-style-type: none">• Check that the E1/T1 configuration matches the cabling (UNC pull)• Check the E1/T1 parameters match those programmed in the channel bank (UNC pull, channel bank configuration)• Check the T1/E1 reports in the technician log (CSS).
<div> NOTE</div> <div>If only one T1 line is connected to the site converter, then only one should be configured.</div>	
Site converter state is disabled	Check that the site requested state is enabled in the UEM.

Table 8-2 SmartX Site Converter Troubleshooting Scenarios (Continued)

Problem	Recovery Action
Site link(s) are down or are periodically unstable	<ul style="list-style-type: none"> • Check that the site link configuration matches that in the channel bank (UNC pull) • Check the E1/T1 configuration (including the site type) is correct and matches the site type in the ZDS (UNC pull) • Check that the hardware cabling matches expected configuration (physical inspection) • Check that site converter requested state is “enabled” (UEM) • Check that the ZC link is functioning (UEM) • Check the SmartX Site Converter state (UEM) • Check the T1/E1 reports in the technician log (CSS) • If the 3600 site is an IR Site, verify that the UNC Wizard Site Type parameter is set to IR.
Site is not in Wide Trunking mode	<p>Check the following using the UEM:</p> <ul style="list-style-type: none"> • site requested state is “Wide Trunking” • ZC and site links are functioning • channel states are good • transient faults reported by Site • If the 3600 site is an IR Site, verify that the UNC Wizard Site Type parameter is set to IR.
Channel state not enabled	<p>Check the following in the UEM:</p> <ul style="list-style-type: none"> • Check that channel requested state is “enabled” • Check for transient faults indicating the issue <p>Check the following with a UNC Pull:</p> <ul style="list-style-type: none"> • Check that channel configuration matches that of the channel bank • Check T1/E1 parameters match those expected by the channel bank
Calls are failing	<p>Check the following in the UEM:</p> <ul style="list-style-type: none"> • Check the site state • Check the channel states and transient traps
Calls are established, but no voice	Check that the channel configuration at the site converter matches the channel bank (channel configuration and cabling) with a UNC pull.
Site is in Failsoft mode	Check to see if this has been user initiated in the UEM. If the 3600 site connection fails, you either have 0 control channels, 0 voice channels available, or neither.
Site is in Site Off mode	Change the site mode in the UEM. This setting can only be user initiated.
3600 sites are not set to Wide Trunking	Check that the site state is from SmartX Site Converter and ZC in the UEM.

Table 8-2 SmartX Site Converter Troubleshooting Scenarios (Continued)

Problem	Recovery Action
Site converter is not discovered in the UNC	See the “UNC Troubleshooting” in the <i>Unified Network Configurator</i> manual. This chapter provides scenarios and describes what to do if the site converter appears in the Lost and Found folder in the VoyenceControl application.
Site converter is not discovered in the UEM	See “UEM Troubleshooting” chapter in the <i>Unified Event Manager</i> manual.
Site audio distortion (unintelligible)	<p>Ensure that the Line Idle Pattern field for the RF Site object in the UNC conforms to the following guidelines:</p> <ul style="list-style-type: none"> • If the Line Idle Pattern field is set to alaw, then the connected channel bank must be set to a-inv (inverse a-Law). • If the Line Idle Pattern field is set to ulaw, then the connected channel bank must be set to ulaw.
"wide area analog link down" and "wide area digital link down" alarms in UEM or ZoneWatch	When a channel malfunction message is received from a configured channel at a 3600 site, the SmartX Site Converter notifies the zone controller that the channel is in the malfunction state. This may indicate that either a 4-wire link failure or V.24 link failure has occurred with the channel and the zone controller sends a malfunction alarm to the UEM and ZoneWatch. The link must be brought back up to clear the alarm.

This page intentionally left blank.

SmartX Site Converter FRU/FRE

This chapter lists the Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs) and includes replacement procedures applicable to the SmartX Site Converter.

Field Replaceable Entity

The SmartX Site Converter is a field replaceable entity. There are no FRUs associated with this hardware. If there is a failure, replace the module.

FRE Parts List

[Table 9-1](#) provides the FRE parts that are required for 3600 trunked sites to operate on an ASTRO[®] 25 radio system.

**NOTE**

Each site converter requires three racks for the SmartX Site Converter and power supplies. As an example, three site converters would require five rack units of space (three units for converters + 2 units for the power supply tray.) Additionally, one rack is needed for the site gateway, which must also be connected to the SmartX Site Converter.

Table 9-1 Field Replaceable Entities

Component	Part Number	Replacement Procedure
SmartX Site Converter Module	B1936A	See Procedure 9-1 .
3V coin cell Lithium battery	52858500100 (CR2450HR)	See Procedure 9-2 .
VPM Power Supply FRU	BLN1297A	See power up and power down procedures in the “SmartX Site Converter Operation” chapter.
Motorola SmartX Site Converter Voice Processor Module, includes the external power supply	T7599A	See Procedure 9-1 .
GPIOM/VPM Power Supply FRU	01009513001	See power up and power down procedures in the “SmartX Site Converter Operation” chapter.
DC Cable (connects 12V DC)	30009351001	See power up and power down procedures in the “SmartX Site Converter Operation” chapter.
Power Supply Tray	1575395h01_revD	Not applicable.
Power Supply Velcro Fastener (for use with tray)	42009052001_revB	Not applicable.
DB9F/RJ-45 VPM Programming Adapter	58009256065	Not applicable.
S2500 Router	ST2500	See the <i>System Routers - S6000/S2500</i> manual.
GGM 8000	TYN4001A	See the <i>System Gateways - GGM 8000</i> manual.

There are also two cables, a serial programming and a cross-over Ethernet cable, which are used to access the CSS from the SmartX Site Converter. They are available through Motorola or may be supplied by your organization.

Replacing the SmartX Site Converter

Procedure 9-1 describes how to replace the SmartX Site Converter in the event of a hardware failure.



IMPORTANT

Before replacing the site converter, pull the configuration and hardware information from the device into the Unified Network Configurator by performing the “Pull All” procedure. For instructions on how to perform a “Pull All” procedure, see the *Unified Network Configurator* manual. This step may not be possible if communication is severed between the SmartX Site Converter and the UNC. If this happens, perform any one of the following:

- Use the last known good configuration files from the UNC.
- Extract the configuration files from the site converter directly.
- Use files provided by Motorola when your system was commissioned.

Regardless of the source, copy the configuration file to the service PC with 3com® TFTP software enabled.

Locate the following information before performing this procedure:

- IP address for the site converter
- Account usernames and passwords for (types of accounts)
Contact your system administrator to obtain this information.

Procedure 9-1 How to Replace a SmartX Site Converter

1	<div data-bbox="422 1234 507 1304"></div> <div data-bbox="539 1251 699 1287">CAUTION</div> <p>The SmartX Site Converter contains low, safe voltage levels, but could cause arcing or damage to connected equipment when the cover is removed while the unit is powered. Unplug the power supply 12 V cable from the SmartX Site Converter when preparing to service this equipment.</p> <p>Disconnect the SmartX Site Converter power supply line cord from an AC source.</p>
2	Disconnect the power supply 12V cable from the rear of the SmartX Site Converter chassis.
3	<p>Remove the existing site converter:</p> <ol style="list-style-type: none"> 1. Label and disconnect all communication cabling from the site converter. 2. Disconnect the ground cable from the rear of the chassis. 3. Remove the screws securing the site converter to the rack. 4. Pull out the site converter through the front of the rack.

Procedure 9-1 How to Replace a SmartX Site Converter (Continued)

4	Remove the mounting brackets from the existing site converter and install the brackets on the replacement site converter.
5	Install the replacement site converter: <ol style="list-style-type: none"> 1. Install the replacement site converter in the rack and secure it with the screws that were previously removed. 2. Secure the ground cable to the ground location on the rear of the chassis. 3. Attach all communication cabling to the site converter.
6	Proceed to “How to Install the SmartX Site Converter Hardware” in the “SmartX Site Converter Installation” chapter and proceed with the installation and configuration procedures in this manual to install a new site converter.

Replacing the Battery

.....

There is a 3V coin cell battery on the Motorola Advanced Crypto Engines (MACE) digital circuitry that is provided for future feature enhancement in the SmartX Site Converter. However, the battery does require periodic replacement.

Table 9-2 lists the recommended time table for replacing the MACE's coin cell battery.

Table 9-2 Battery Replacement Time


Hardware State	Replacing Time
Installed in the system	Every two years
Stored	Once a year

Procedure 9-2 describes how to replace the battery.

Procedure 9-2 How to Replace the Battery

1	Unplug the site converter power line cord from the AC source.
2	Disconnect all power and data/control connections to and from the site converter.
3	Dismount the hardware from the equipment rack.
4	Remove the cover screws and the chassis cover from the site converter.
5	Unpack the replacement battery.

Procedure 9-2 How to Replace the Battery (Continued)

6	Lift an exposed edge of the battery until it "pops" out of the holder and put the old battery aside.  <div data-bbox="523 351 699 389" style="background-color: #00AEEF; color: white; padding: 2px 5px; display: inline-block;">NOTE</div> <p>When replacing the battery, make sure that its wider side is at the top.</p>
7	Place the new battery carefully on top of the holder and with a slight rocking action, push it downward into the holder. Result: The battery clicks into place.
8	Reinstall and secure the site converter's chassis cover.
9	Reconnect all data/control and power connections to the site converter.
10	Reconnect the power supply 12V cable.
11	Reconnect the power line cord to an AC source.
12	Verify the LEDs status and restore the proper operation of the site converter within the system.
13	Properly dispose of the old (Lithium) battery.

Component Disposal

.....

The Motorola Solution Support Center (SSC) provides technical support, return material authorization (RMA) numbers, and confirmations for troubleshooting results. Call the SSC for information about returning faulty equipment or ordering replacement parts. North America: 1-800-221-7144 / International: 302-444-9800.

After removing a failed SmartX Site Converter, it must be shipped to the Motorola Infrastructure Depot Operations (IDO) for further troubleshooting and repair. You must return any failed units to the Motorola IDO at 2214 Galvin Dr, Elgin, IL 60123. The field shop contacts the Solution Support Center to request a replacement or repair, and the Depot ships out a replacement FRE. Included in the packaging is paperwork with instructions on how to return the failed unit.

Properly dispose of any replaced Lithium batteries.



CAUTION

Do not attempt to repair or service subcomponents in the SmartX Site Converter.

This page intentionally left blank.

SmartX Site Converter Reference

This chapter provides supplemental hardware information about the SmartX Site Converter.

SmartX Site Converter Specifications

Table 10-1 provides hardware specifications.

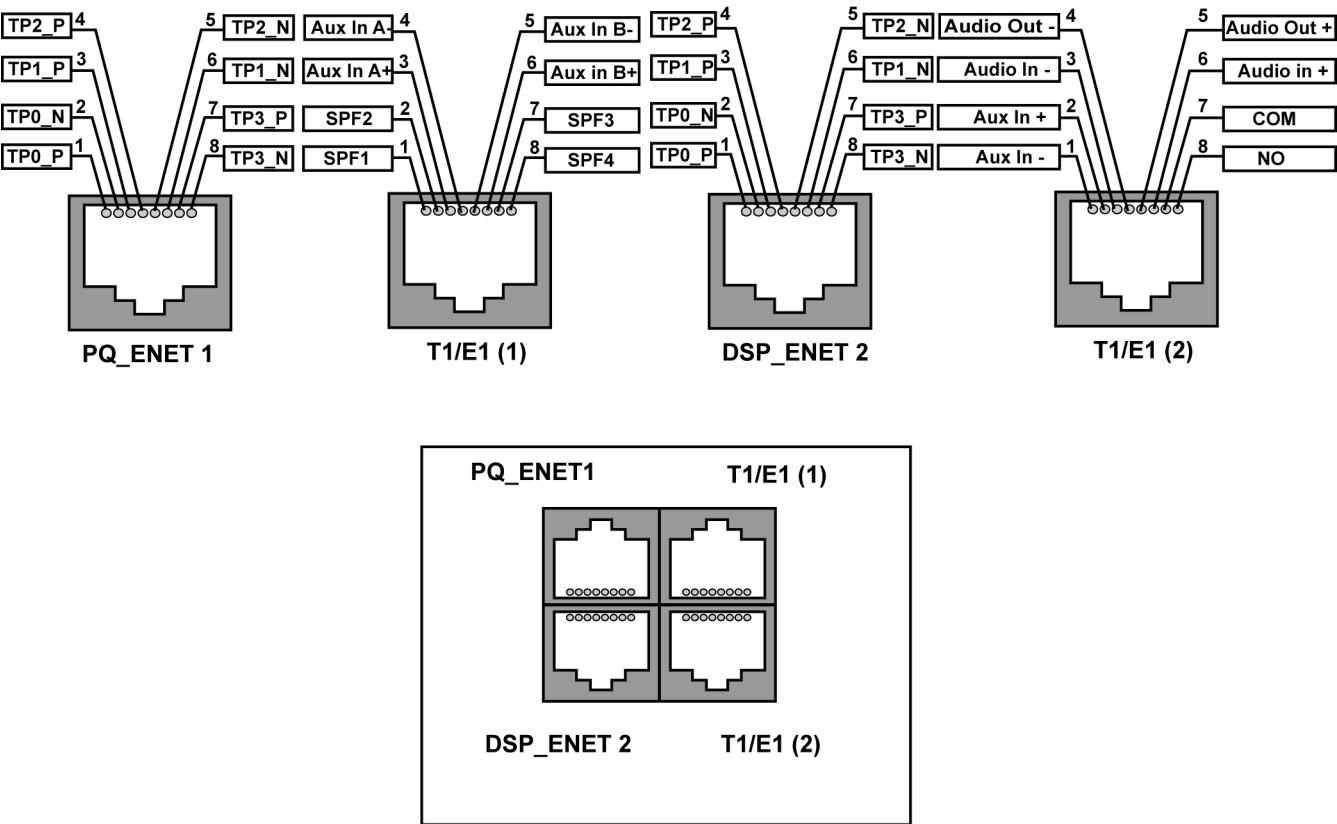
Table 10-1 SmartX Site Converter Hardware Specifications

SmartX Site Converter	Specifications
Environmental Operating Range	<ul style="list-style-type: none">Meets the temperature and humidity storage requirements of ETSI EN-300-019-2-1 Class T1.2 (Weather protected, not temperature-controlled storage locations, -25 °C to 70 °C).Is capable of being continuously operated over an ambient temperature range of 5 °C to 40 °C.Is capable of being continuously operated over an ambient range of 0 to 90% relative humidity (non-condensing) at 40 °C with no degradation in performance at any point in that humidity range.
Voltages	Power is provided by an AC-powered 12 VDC output, 108 W external regulated power supply. AC operating power 96 VAC -264 VAC (47 -63 Hz).
Amperage	0.4A at 120 VAC and 0.2A at 240 VAC
Converter Operating Power	18W
OS version	OSE
Shock and Vibration	The device and power supply tray solution (with the supplies installed) are capable of surviving vibration per ETS 300 019-2-3 (V2.2.2) class T3.3 without damage, deformation, loosening, or dislodging of any parts.
Ventilation Requirements	Maximum air temperature at the vent openings cannot exceed 40 °C. Provide 6 inches of ventilation on the sides, front and back, and 0 on top and bottom. Do not operate the SmartX Site Converter in a closed cabinet due to heat buildup.

SmartX Site Converter Connector Diagrams

Figure 10-1 shows the pinout connections for the SmartX Site Converter.

Figure 10-1 SmartX Site Converter T1/E1 Port Connector Pinout Diagram



SmartX_E1_T1_pinout

Table 10-2 shows the E1/T1 connections for the SmartX Site Converter.

Table 10-2 E1/T1 Connections

Port	Function							
DSP_T1-E1 Port (1)	C1	C2	C4	C5	C3	C6	C7	C8
	Receive pair		Transmit pair		Not used		Not used	
DSP_T1-E1 Port (2)	D1	D2	D4	D5	D3	D6	D7	D8
	Receive pair		Transmit pair		Not used		Not used	

[Table 10-3](#) describes the serial cable connector, which is used to configure the device using the Configuration/Service Software (CSS) application.

Table 10-3 SmartX Site Converter Serial Cable Connector Pinout

DB9	RJ45
1	
2	8
3	1
4	
5	2
6	
7	
8	
9	

SmartX Site Converter Ports to Function Map

The applicable ports include:

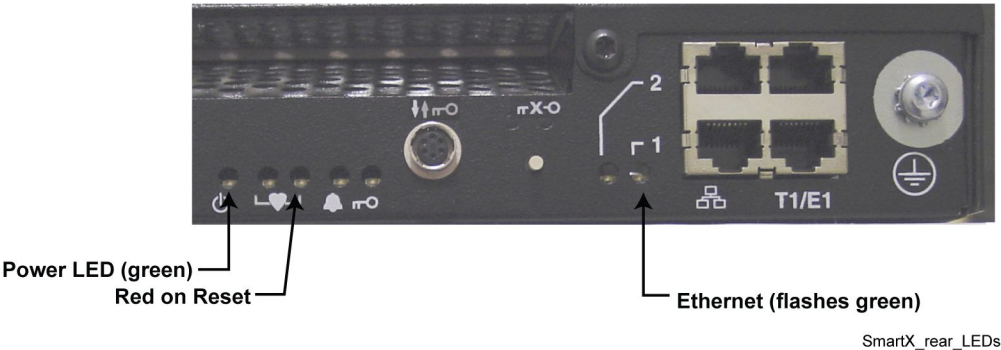
- AC power connection
- Serial port for connection to CSS
- Ethernet connector
- Two E1/T1 Line connectors

See [Figure 1-2, "Rear View of the SmartX Site Converter — Power Connection and Ports in Use"](#) on [page 1-3](#) for location of these ports on the device.

SmartX Site Converter LEDs

The SmartX Site Converter has five types of LEDs indicating the general conditions for the device and its Ethernet activities. See [Figure 10-2](#).

Figure 10-2 SmartX Site Converter LEDs



All types of SmartX Site Converter LEDs and their definitions are described in the following sections.

Power LED

The Power LED is on (solid green) if the power is supplied to the device from the external power supply.

Red on Reset

The Red on Reset LED is on (solid red) until the SmartX Site Converter software completes initialization. When the initialization is complete, it turns off.

Ethernet Activity LED

There are two Ethernet Activity LEDs, but only the one marked with "1" is functional.

Table 10-4 explains the definitions for the SmartX Site Converter Ethernet Activity LED.

Table 10-4 Ethernet Activity LED

State	Activity LED (Green)	Description
Link Inactive	Off	The link is not established.
Link Established	On	The link is established but there is no current activity.
Link Active	Flashing	Ethernet activity

SmartX Site Converter Cable Connections

The cross-over Ethernet cable connecting the SmartX Site Converter and site gateway and the T-line connections between SmartX Site Converter and the channel bank should comply with industry specifications. The lengths vary based on each organization's floor layout for their equipment.

When the SmartX Site Converter is at the Master Site and connects to the remote 3600 site over an external PSTN line, connect to the external PSTN circuit by an intervening Channel Service Unit (CSU), Motorola part number CDN6637. This CSU is needed to provide necessary protection to the SmartX Site Converter and the telco equipment. The SmartX Site Converter must never be connected to an external circuit directly.

When the SmartX Site Converter is at the Master Site, connect the T1/E1 cable from the SmartX Site Converter to the channel bank.

This page intentionally left blank.

SmartX Site Converter Disaster Recovery

This chapter provides references and information that enables you to recover a SmartX Site converter in the event of a failure.

Recovery Sequence for the SmartX Site Converter

Follow the steps in [Process 11-1](#) to replace an entire SmartX Site Converter.

Process 11-1 Recovering the SmartX Site Converter

- 1** Remove the old SmartX Site Converter hardware. Install the new SmartX Site Converter hardware. See “How to Install the SmartX Site Converter Hardware” in the *SmartX Site Converter Manual*.
- 2** Perform basic device configuration using the serial port. See Chapter 3's "How to Provision the SmartX Site Converter Serial Connection Parameters" in the *SmartX Site Converter manual*.
- 3** Perform basic device configuration using the Ethernet port. See Chapter 3's "How to Configure the SmartX Site Converter Using CSS (Ethernet Connection)" in the *SmartX Site Converter manual*.
- 4** Enable secure credentials.
 - 1.** Set the SWDL transfer mode using CSS. See Chapter 3's “How to Set the SWDL Transfer Mode Using CSS” in the *SmartX Site Converter manual*.
 - 2.** Set the local password configuration. See Chapter 3's “How to Set the SmartX Site Converter Local Password Configuration” in the *SmartX Site Converter manual*.
 - 3.** Set the date and time in CSS. See Chapter 3's “How to Set the Date and Time on the SmartX Site Converter” in the *SmartX Site Converter manual*.
 - 4.** Set the serial security service in Chapter 3's “How to Set the Serial Security Services” in the *SmartX Site Converter manual*.

Process 11-1 Recovering the SmartX Site Converter (Continued)

- 5** Complete the configuration of the Information Assurance features using CSS, as follows:
- 1.** Create, update, or delete an SNMPv3 user. See Chapter 3's "How to Add or Modify an SNMPv3 User" in the *SmartX Site Converter* manual.
 - 2.** Verify the SNMPv3 credentials. See Chapter 3's "How to Verify SNMPv3 Credentials on the SmartX Site Converter" in the *SmartX Site Converter* manual.
 - 3.** Configure DNS using the CSS. See Chapter 7's "Configuring DNS Using CSS" in the *Authentication Services* manual.
 - 4.** Configure for SSH. See Chapter 4's "Configuring SSH for RF Site Devices and VPMs Using CSS – Overview" in the *Securing Protocols with SSH* manual.
 - 5.** Configuring the local cache size for the SmartX Site Converter. See Chapter 7's "Setting the Local Cache Size for Centralized Authentication Using CSS" in the *Authentication Services* manual.
 - 6.** Enable RADIUS authentication using the CSS. See Chapter 7's "Configuring RADIUS Sources and Parameters Using CSS" in the *Authentication Services* manual.
 - 7.** Enable Centralized Authentication using the CSS. See Chapter 7's "Enabling/Disabling Centralized Authentication Using CSS" in the *Authentication Services* manual.
 - 8.** Optionally, enable Centralized Event Logging using the CSS. See Chapter 6's "Enabling/Disabling Centralized Event Logging on Devices Using CSS" in the *Centralized Event Logging* manual.
 - 9.** Customize the Login Banner using CSS. See Chapter 3's "How to Customize the Login Banner" in the *SmartX Site Converter* manual.

**NOTE**

You can also see the *CSS Online Help* in the software application to complete these tasks during the device configuration.

- 6** Connect the SmartX Site Converter to the Site Gateway. See Chapter 3's "How to Attach the SmartX Site Converter to the Site Gateway" in the *SmartX Site Converter* manual.
- 7** Replace the SmartX Site Converter in the UNC. See Chapter 4, "Replacing a Device" in the *Unified Network Configurator* manual.
- 8** Perform a software download (SWDL) from the Unified Network Configurator (UNC). See "How to Transfer and Install the OS Image" in the *SmartX Site Converter* manual.
- 9** Set up the SmartX Site Converter. See Chapter 4's "Configuring the SmartX Site Converter" in the *SmartX Site Converter* manual.