System Release 7.17
ASTRO® 25
INTEGRATED VOICE AND DATA

# SmartX Site Converter Feature Guide

NOVEMBER 2016

MN003356A01-A

# Copyrights

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



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

## Disclaimer

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

## Trademarks

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

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

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

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

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

This page intentionally left blank.

# Contact Us

## Motorola Solutions Support Center

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

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

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

## North America Parts Organization

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

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

## Comments

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

Provide the following information when reporting a documentation error:

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

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

This page intentionally left blank.

# Document History

| Version | Description | Date |
|---|---|---|
| MN003356A01-A | Original release of the *SmartX Site Converter Feature Guide* manual. | November 2016 |

This page intentionally left blank.

# Contents

# List of Figures

This page intentionally left blank.

# List of Tables

This page intentionally left blank.

# List of Processes

This page intentionally left blank.

# List of Procedures

# About 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:

- SmartX Site Converter Description on page 25 provides a high-level description of the SmartX Site Converter and the function it serves on your system.
- SmartX Site Converter Theory of Operation on page 33 explains how the SmartX Site Converter works in the context of your system.
- SmartX Site Converter Installation on page 55 details hardware and software installation procedures, as well as the initial configuration required for connectivity to the network for the SmartX Site Converter.
- SmartX Site Converter Configuration on page 79 details configuration procedures and fault management application discovery relating to the SmartX Site Converter.
- SmartX Site Converter Optimization on page 93 is for optimization procedures and recommended settings relating to the SmartX Site Converter.
- SmartX Site Converter Operation on page 95 is for tasks that are performed once the SmartX Site Converter is operational on your system.
- SmartX Site Converter Maintenance on page 103 describes maintenance instruction for the SmartX Site Converter.
- SmartX Site Converter Troubleshooting on page 105 provides fault management and troubleshooting information relating to the SmartX Site Converter.
- SmartX Site Converter FRE on page 115 describes Field Replaceable Units (FRU) and Field Replaceable Entities (FRE) relating to the SmartX Site Converter.
- SmartX Site Converter Reference on page 119 describes additional reference information on the Voice Processor Module (VPM) hardware ports, cabling, LEDs, and more when used as a SmartX Site Converter.
- SmartX Site Converter Disaster Recovery on page 123 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 |
|---|---|
| *Standards and Guidelines for Communication Sites* (6881089E50) | Provides standards and guidelines that should be followed when setting up a Motorola communications site. Also known as the R56 manual. This manual may be purchased on CD 9880384V83 by calling the North America Parts Organization at 800-422-4210 (or the international number: 302-444-9842). |
| *System Overview and Documentation* | Describes the manuals that comprise the ASTRO® 25 IV&D system documentation set, a list of new features for this release, system diagrams, and system-level disaster recovery information. |
| *Voice Processor Module* | Provides additional information on the VPM hardware platform used for the SmartX Site Converter. |
| *S6000 and S2500 Routers* | Provides information on the S2500 router, which can be used with the SmartX Site Converter hardware to support SmartZone® sites. |
| *GGM 8000 System Gateway* | Provides information on the GGM 8000 gateways, which can be used with the SmartX Site Converter hardware to support SmartZone® sites. |
| *MCC 7500 Console Site with VPM* | Provides information about the VPM hardware as it is being used as the audio interface for the MCC 7500 console subsystem. |
| *Enhanced Telephone Interconnect Feature Guide* | Provides information about the Enhanced Telephone Interconnect feature using the Voice Processor Module hardware for the Telephone Media Gateway (TMG). |
| *Authentication Services* | Provides information about Configuration/Service Software (CSS) application procedures used to set up Information Assurance features, such as Configuring DNS, Centralized Authentication, and RADIUS Authentication on the SmartX Site Converter in the CSS application. |
| *Centralized Event Logging* | Provides information on enabling the CEL feature on the SmartX Site Converter in the Configuration/Service Software (CSS) application. |
| *Unified Network Configurator* | 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 IVD system. UNC has two components: EMC Smarts™ Network Configuration Manager and Unified Network Configurator Wizards (UNCW). |
| *Software Download Manager* | Provides information on the SWDL application. |

*Table continued...*

| Related Information | Purpose |
|---|---|
| *ISSI 8000/CSSI 8000 Intersystem Gateway Feature Guide* | 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. |
| *Motorola GGM 8000 Hardware User Guide*<br>*Motorola Network Router (MNR) 2500 Hardware User Guide*<br>*Motorola Network Router (MNR) S6000 Hardware User Guide* | Available on the Motorola Online (MOL) Web site. To access the manual from the **Resource Center**, select **Product Information** → **Manuals** → **Network Infrastructure** → **Routers and Gateways**. |
| *Conventional QUANTAR Replacement Guide* | A supplemental document used to replace QUANTAR® stations with new GTR 8000 base radio hardware at 3600 sites. |

This page intentionally left blank.

Chapter 1

# SmartX Site Converter Description

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

## 1.1 SmartX Site Converter Introduction

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 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:

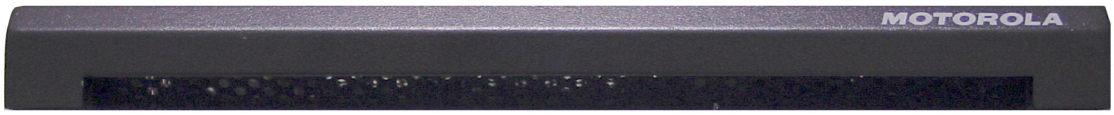
- Call control information
  - Bidirectional conversion between circuit-based 3600 call control packets and ASTRO® 25 IP-based call control protocol so calls can be managed through the ASTRO® 25 zone controller.
- Audio information
  - Conversion of analog audio from 3600 sites to G.728 packets that 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 Multiband Excitation (AMBE) audio packets for routing over the ASTRO® 25 IP network to ASTRO® 25 RF sites.
  - Routing without conversion of digital Improved Multiband 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).

## 1.2 SmartX Site Converter 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.

The following figure shows the front view of the SmartX Site Converter.

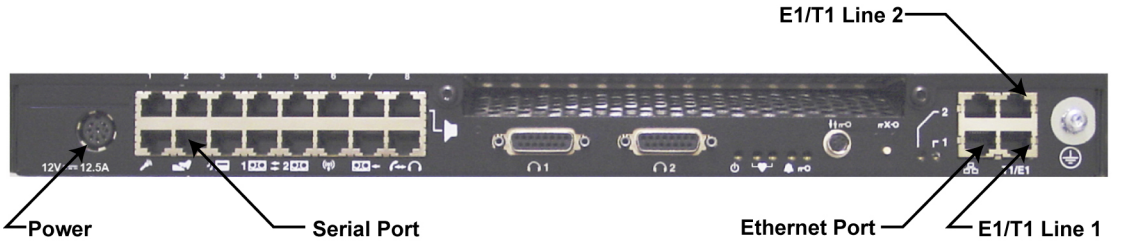
**Figure 1: Front View of the SmartX Site Converter**




SmartX_Converter_front

The following figure 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 2: Rear View of the SmartX Site Converter — Power Connection and Ports in Use**




SmartX_Converter_rear1

The following figure shows the power supply, cable, and line cord.

**Figure 3: SmartX Site Converter Power Supply**

VPM_power_supply

## 1.3 SmartX Site Converter and the ASTRO 25 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.

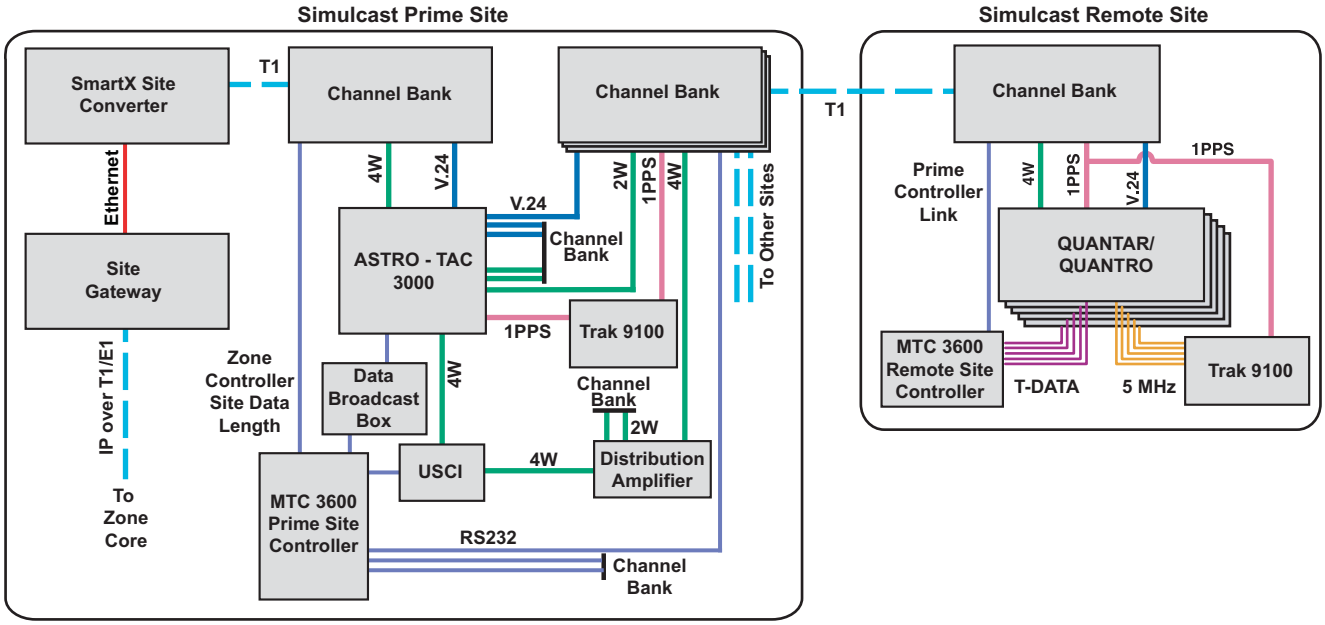
**NOTICE:** The site gateway provides a preferred alternative solution for the site router. See the *GGM 8000 System Gateway* manual.

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.

The exception to installing the SmartX Site Converter at a remote site is with the L core configuration, which does require the SmartX Site Converter and its router/gateway at the ASTRO® 25 master site. The L core does not support T1 site link connections. The T1 connection is from the 3600 RF site to the SmartX Site Converter in the master site. The connection from the SmartX Site Converter to the site router and the site router to the core gateway (router) are Ethernet connections.

The following figure shows an example of a SmartX Site Converter and its site gateway installed at a 3600 RF site.

**Figure 4: Circuit-based Simulcast Subsystem with SmartX Site Converter**



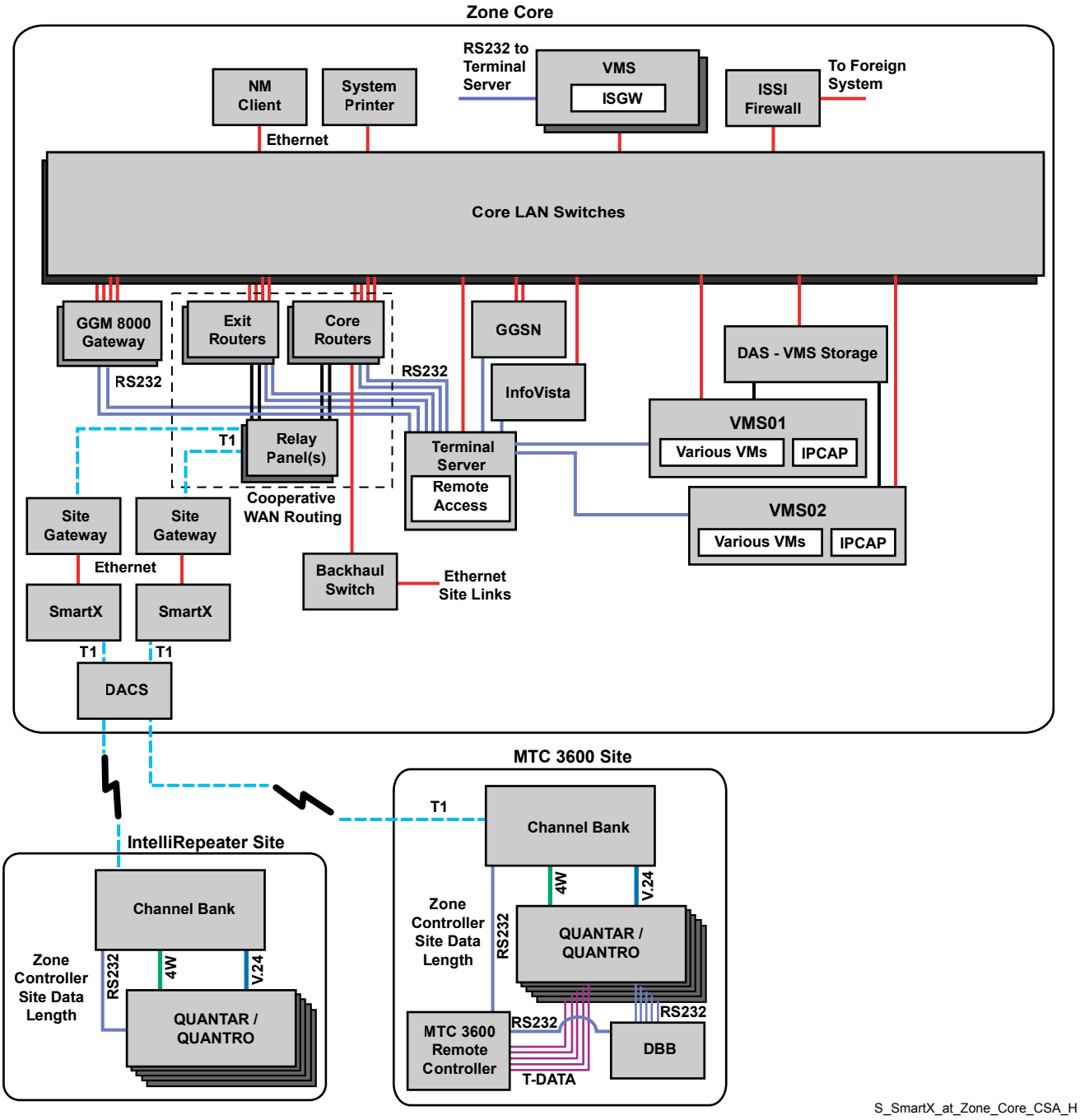

Simulcast_3600_RF_Site_w_SmartX_B

The following figure 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).

**NOTICE:** An Ethernet site link connection is used for the interface between the L core backhaul switch and site gateway.

A GTR 8000 Base Radio can be implemented as a QUANTAR® station replacement within a 3600 and SmartZone® system. The implementation details are in the *Conventional QUANTAR Replacement Guide* manual.

**Figure 5: SmartX Site Converter at the Zone Core (with CSA)**




S_SmartX_at_Zone_Core_CSA_H

**NOTICE:** The site gateway provides a preferred alternative solution for the site router. See the *GGM 8000 System Gateway* manual.

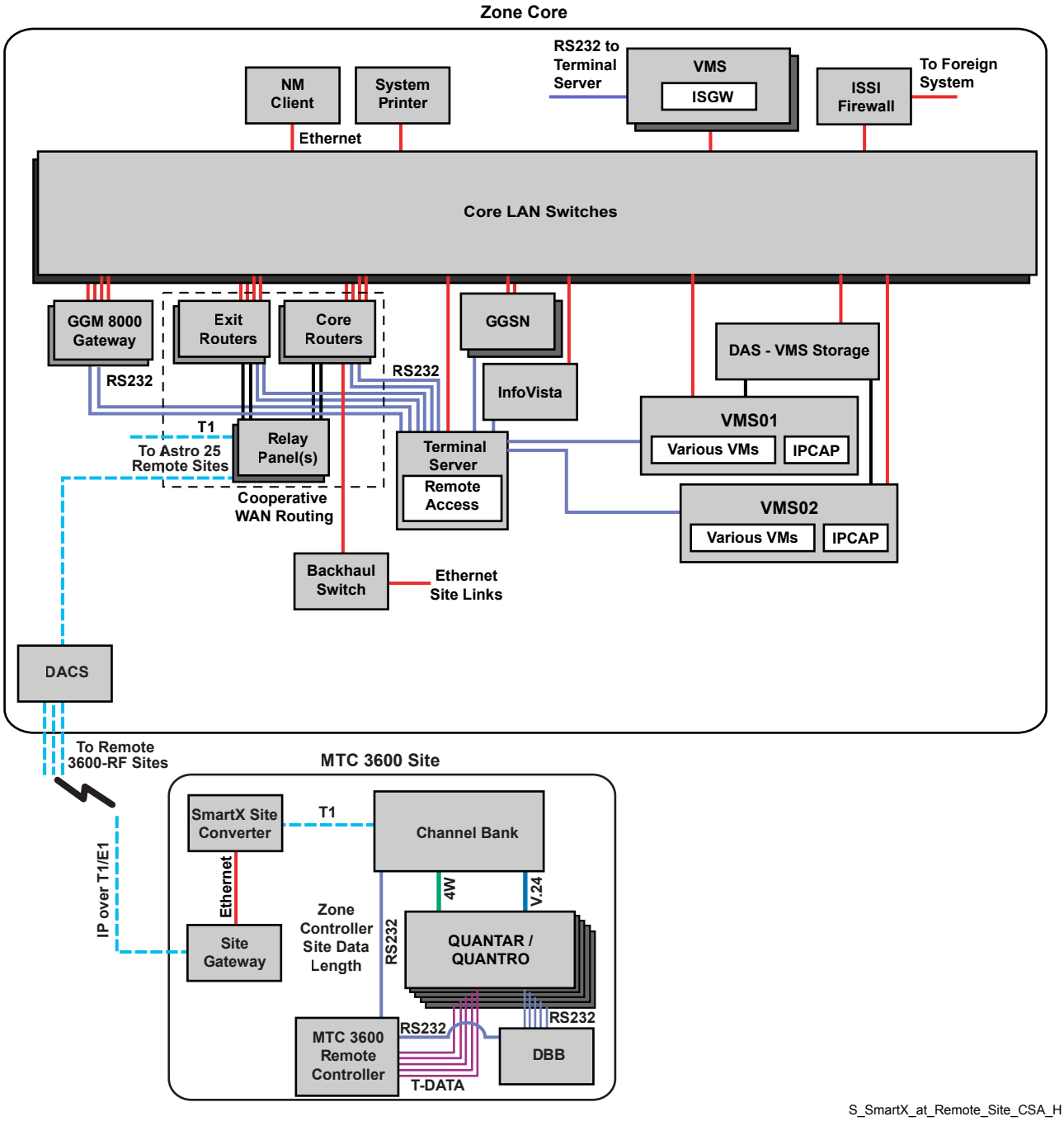
3600 RF sites operating in the VHF, UHF, 800 MHz, and 900 MHz bands can be interfaced to an ASTRO® 25 system through the SmartX Site Converter.

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

The following figure 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® station replacement within a 3600 and SmartZone® system. The implementation details are in the *Conventional QUANTAR Replacement Guide* manual.

**Figure 6: SmartX Site Converter at the Remote Site (with CSA)**




S_SmartX_at_Remote_Site_CSA_H

**NOTICE:** The site gateway provides a preferred alternative solution for the site router. See the *GGM 8000 System Gateway* manual.

Dynamic Transcoding allows FDMA-only subscriber radios on a talkgroup to communicate with TDMA radios on a 700 MHz site while preserving the FDMA and TDMA modes of operation at each respective site. The SmartX Converter creates two audio streams from the analog transmission

received by the SmartZone site. The converter creates a G.728 stream for the consoles and the parallel 3600 sites and a full-rate IMBE stream for the parallel 9600 sites.

The G.728 stream to and from the SmartX sites is not transcoded. The full-rate IMBE stream has to be transcoded for destination 9600 sites that have been granted in TDMA mode. Likewise, half-rate audio from a 9600 site has to be transcoded to full-rate for participating SmartX sites. If the console receives half-rate audio from a 9600 site, and a SmartX radio keys up on analog talkgroup during hangtime, the console ends the half-rate audio session, and start a new session for the G.728. See the *Dynamic Transcoder User Guide* manual for details.

## 1.4 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

## 1.5 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.
- IMBE audio is supported in its native format.

## 1.6 Network Management Support

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

**Provisioning Manager (PM)**
Enables an administrator to enter and maintain related configuration information in the System, Subscribers, Security, and ZoneWatch configuration objects.

**Unified Network Configurator (UNC)**
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

**Configuration/Service Software (CSS)**
Supports the initial network and authentication parameter configuration.

**Unified Event Manager (UEM)**
Provides fault management and event monitoring of the 3600 sites.

**Radio Control Manager (RCM)**
Extends its monitoring and control capabilities to the 3600 subscriber radios.

**ZoneWatch**
Monitors activity at the 3600 RF sites.

## 1.7 Information Assurance Features Support

The SmartX Site Converter supports the following Information Assurance features.

**Password protection**
Supports passwords with configurable complexity requirements.

**Simple Network Management Protocol (SNMPv3)**
Provides security through support for authentication with or without encryption through a set of rules that various end points in a network use when they communicate.

**Centralized Authentication**
Uses Active Directory® (AD) and Remote Authentication Dial-In User Service (RADIUS) to provide identity management and authentication.

**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 the remote logon, 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**
Captures Operating System (OS) events that most devices generate 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.

This page intentionally left blank.

Chapter 2

# SmartX Site Converter Theory of Operation

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

## 2.1 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 depending on the system configuration. The interfaces may be configured for standard T1 operation or E1 operation in 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 depending on the system configuration. A slot can be associated with digital voice or analog voice, but not both (no ADPCM support). Perform slot confguration with 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.

**NOTICE:** The site gateway provides a preferred alternative solution for the site router. See the *GGM 8000 System Gateway* manual.

### 2.1.1 3600 Site and Channel Types Support

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:

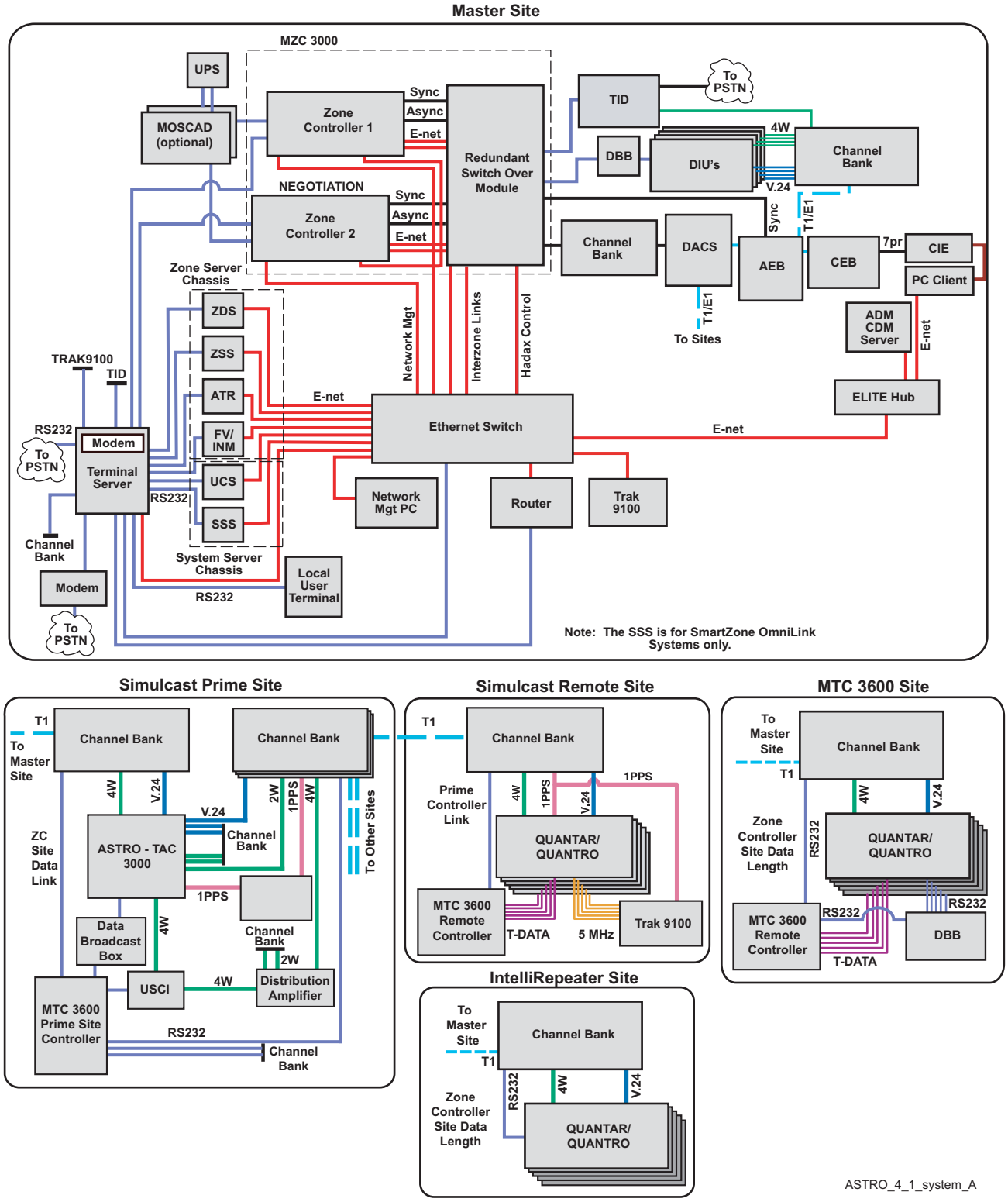
- 3600 analog only channel
- 3600 digital only channel (IMBE)
- 3600 mixed mode channel (3600 analog/3600 digital IMBE)

The following figure shows a block diagram representation of a SmartZone® 4.1 system. The RF sites in this existing system can be integrated into an ASTRO® 25 system with the use of a SmartX Site Converter.

**NOTICE:** The use of Gold Elite consoles and Motorola Gold Elite Gateways (MGEGs) in ASTRO® 25 systems is discontinued. System owners must replace their Gold Elite consoles and MGEGs with MCC 7100/7500 consoles.

A GTR 8000 Base Radio can be implemented as a QUANTAR® station replacement within a 3600 and SmartZone® system. The implementation details are in the *Conventional QUANTAR Replacement Guide* manual.

**Figure 7: 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
- Gold Elite Dispatch positions (updated to ASTRO® 25 system)
- Ambassador Electronics Bank (AEB) to enable use of Gold Elite consoles on the 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

Reuse of the following:

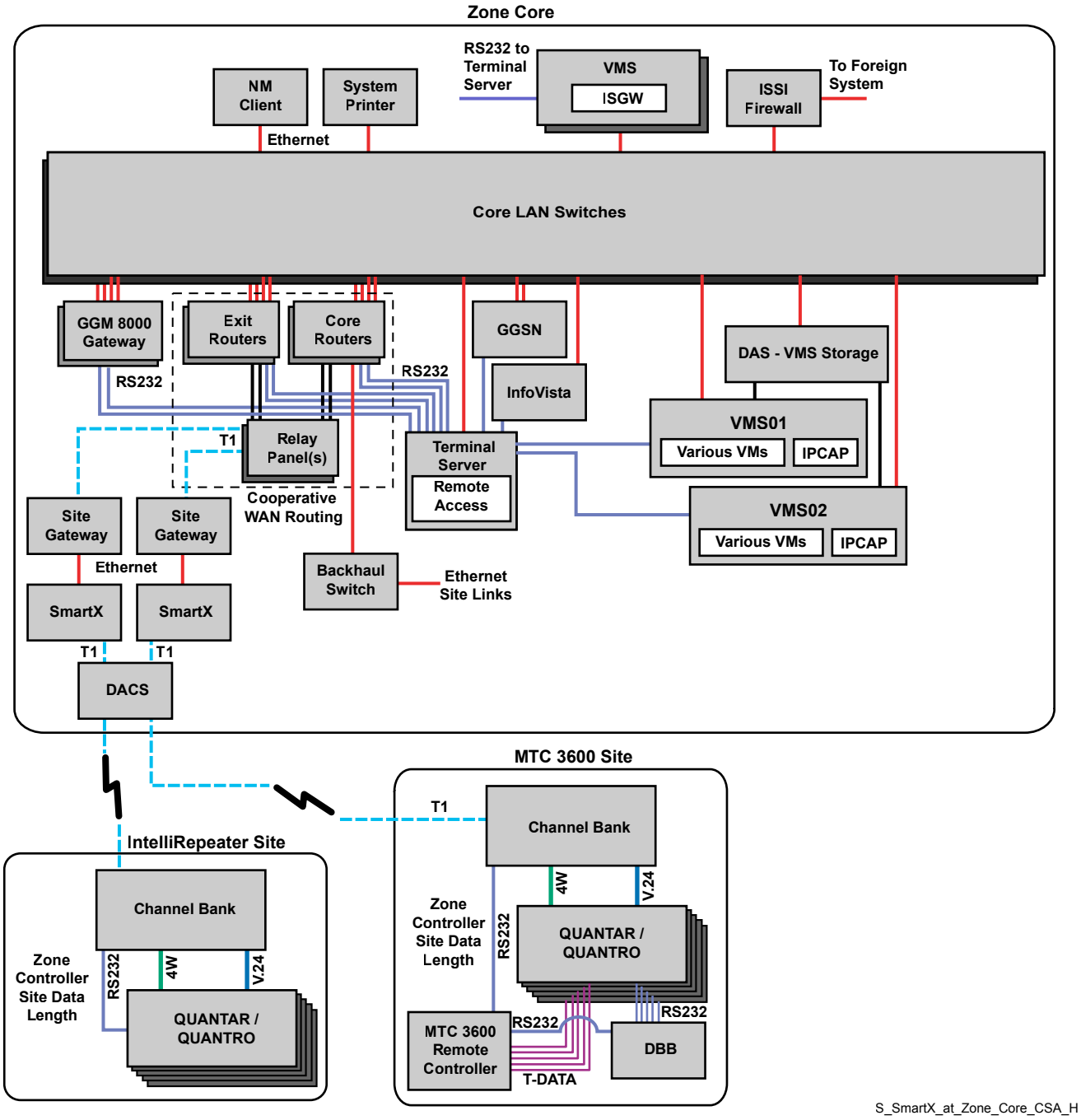
- 3600 RF sites
- 3600 radios (both analog only and digital capable)
- Channel banks (may need updated modules)
- Digital Access Cross-connect Switch (DACS ) depending on the system configurations

Addition of the following equipment based on options:

- Site gateways or routers for 3600 sites (one per site)
- SmartX Site Converters – one per RF site
- MCC 7100 or MCC 7500 dispatch consoles

The following figure shows an ASTRO® 25 system (featuring Common Server Architecture) with the addition of the 3600 RF sites that were migrated from the SmartZone® 4.1 system.

**Figure 8: ASTRO 25 System with 3600 Sites**




S_SmartX_at_Zone_Core_CSA_H

**NOTICE:** The site gateway provides a preferred alternative solution for the site router. See the *GGM 8000 System Gateway* manual.

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.
- The ASTRO® 25 Network Management applications provide the configuration, monitoring, and fault management capability for the 3600 and ASTRO® 25 infrastructure and subscribers.

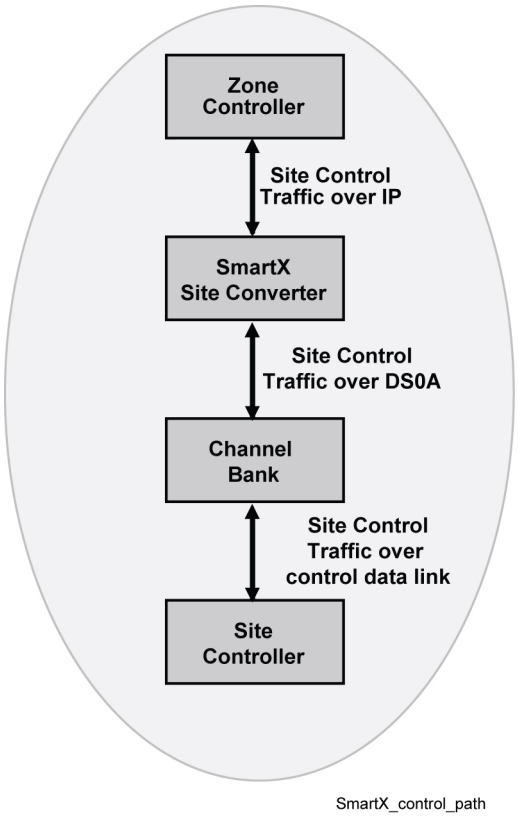
- 3600 RF sites connect into the ASTRO® 25 master site in the same manner as the ASTRO® 25 sites, through their site gateway and the patch panels.

### 2.1.2
## SmartX Site Converter 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.

The following figure shows the basic path and transitions for the control data between the ASTRO® 25 zone controller and the 3600 site controller.

**Figure 9: 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 SmartX Site Converter transforms the 3600 control plane information into the required control plane format for 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.

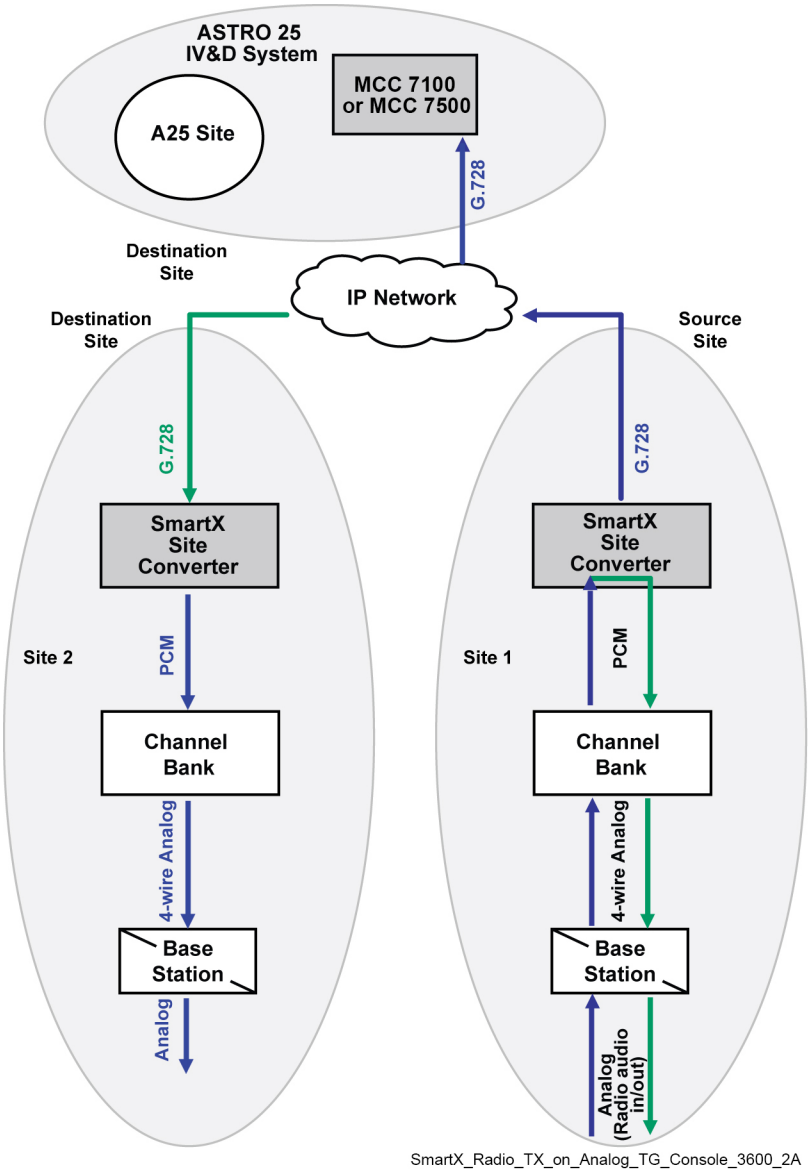
The SmartX Site Converter also provides the necessary conversion between the ASTRO® 25 control data format and the 3600 control data format when it receives the call grant information from the ASTRO® 25 zone controller.

See Figure 10: 3600 Subscriber Radio Transmits on Analog Talkgroup on page 40, Figure 11: Radio TX on Analog TG, A25–Console and 3600 Destinations on page 41, Figure 12: ASTRO 25 System Subscriber Radio Transmits on 3600 Analog Talkgroup on page 42, Figure 13: Radio TX on Digital 3600 TG, A25–Console and 3600 Destinations on page 43, Figure 14: A25 Radio TX on 3600 Digital TG–Console and 3600 Destinations on page 44, Figure 15: MCC 7500 Console Transmits on 3600 Analog Talkgroup on page 45, Figure 16: MCC 7500 Console Transmits on 3600 Digital Talkgroup on page 46, Figure 17: Console Takeover, Console, and 3600 Radio Transmit on 3600 Analog Talkgroup on page 47, and Figure 18: Console Takeover, Console, and 3600 Radio Transmit on 3600 Digital Talkgroup on page 48, 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 10: 3600 Subscriber Radio Transmits on Analog Talkgroup**



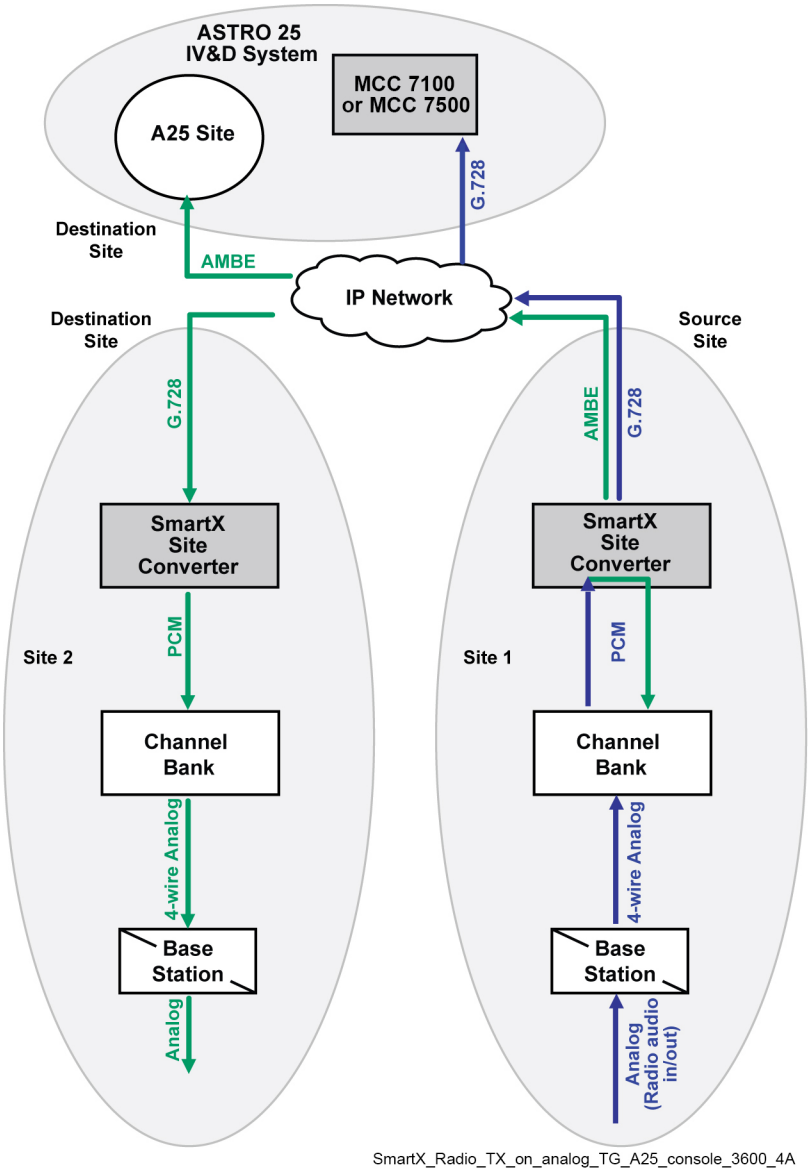

The following takes place when the source of audio is an analog subscriber from a 3600 site:

- 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 require format for 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 transmission 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 11: Radio TX on Analog TG, A25–Console and 3600 Destinations**



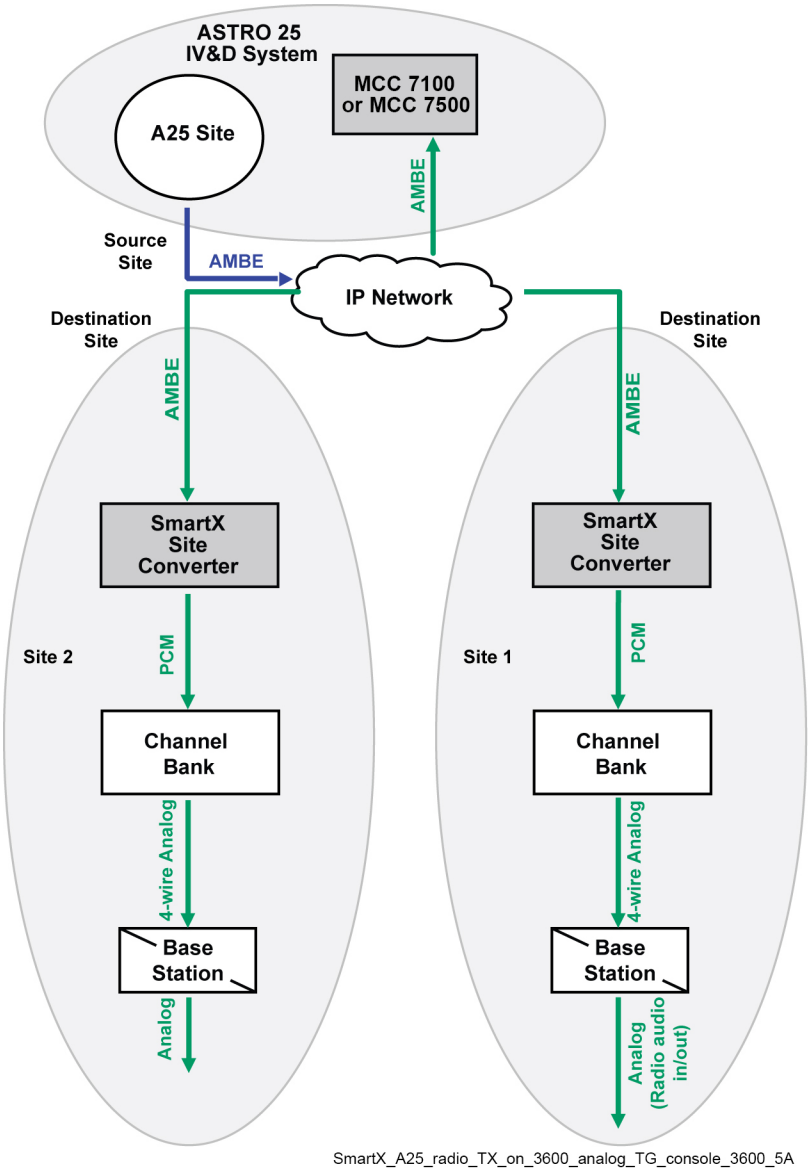

The following takes place when the source of audio is an analog subscriber from a 3600 site:

- 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.
- The SmartX Site Converter must create two vocoded versions of the received analog audio: 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 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 12: ASTRO 25 System Subscriber Radio Transmits on 3600 Analog Talkgroup**



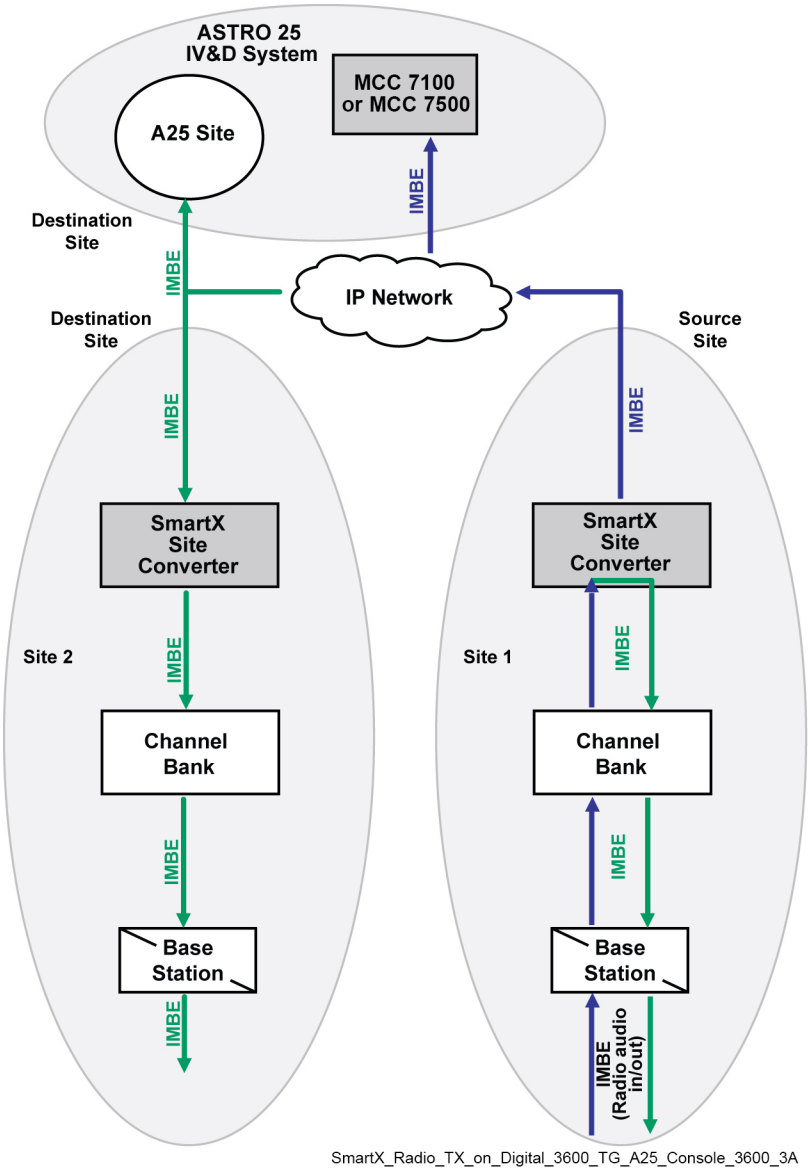

The following takes place when the source of audio is a radio at an ASTRO® 25 site and the destination is an analog talkgroup at the 3600 sites:

- 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 13: 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 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.

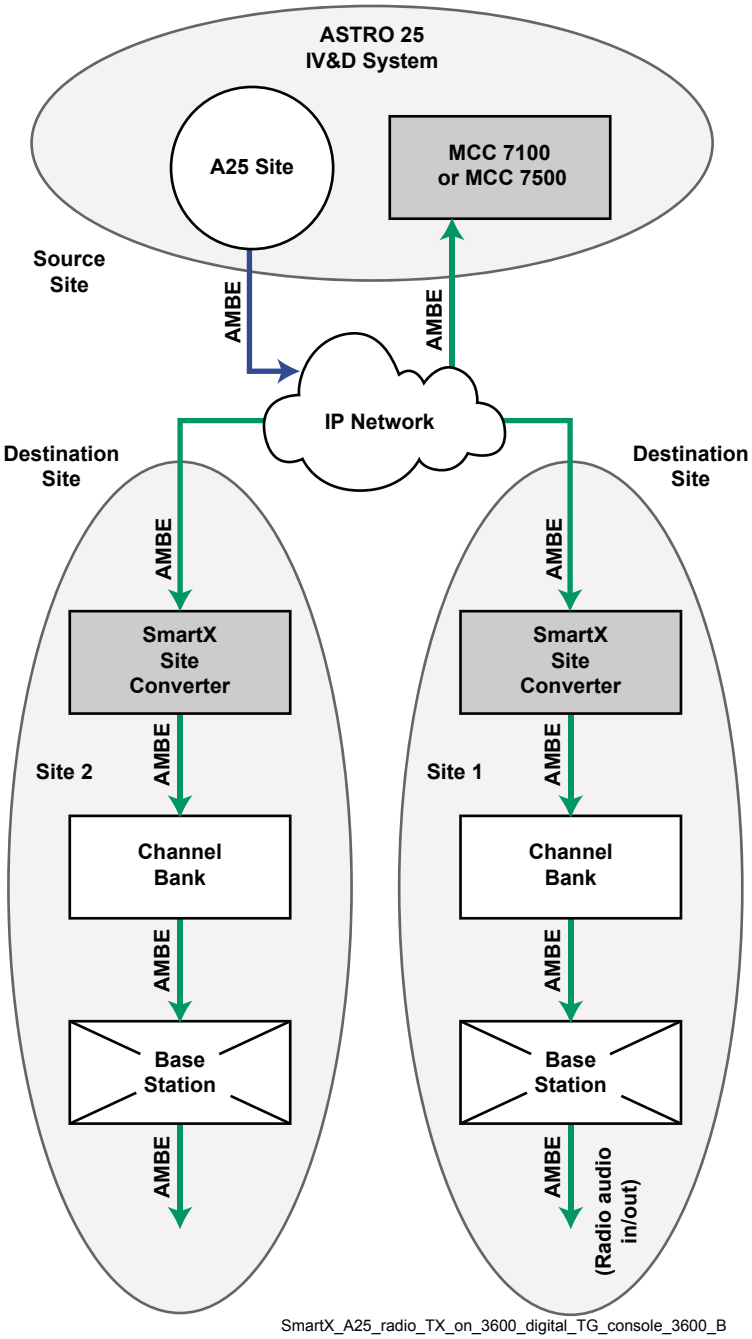
- At the destination site, the SmartX device receives the audio packets from the IP network and must enable the transmission of IMBE audio for the call at the 3600 RF site.

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 14: A25 Radio TX on 3600 Digital TG–Console and 3600 Destinations**



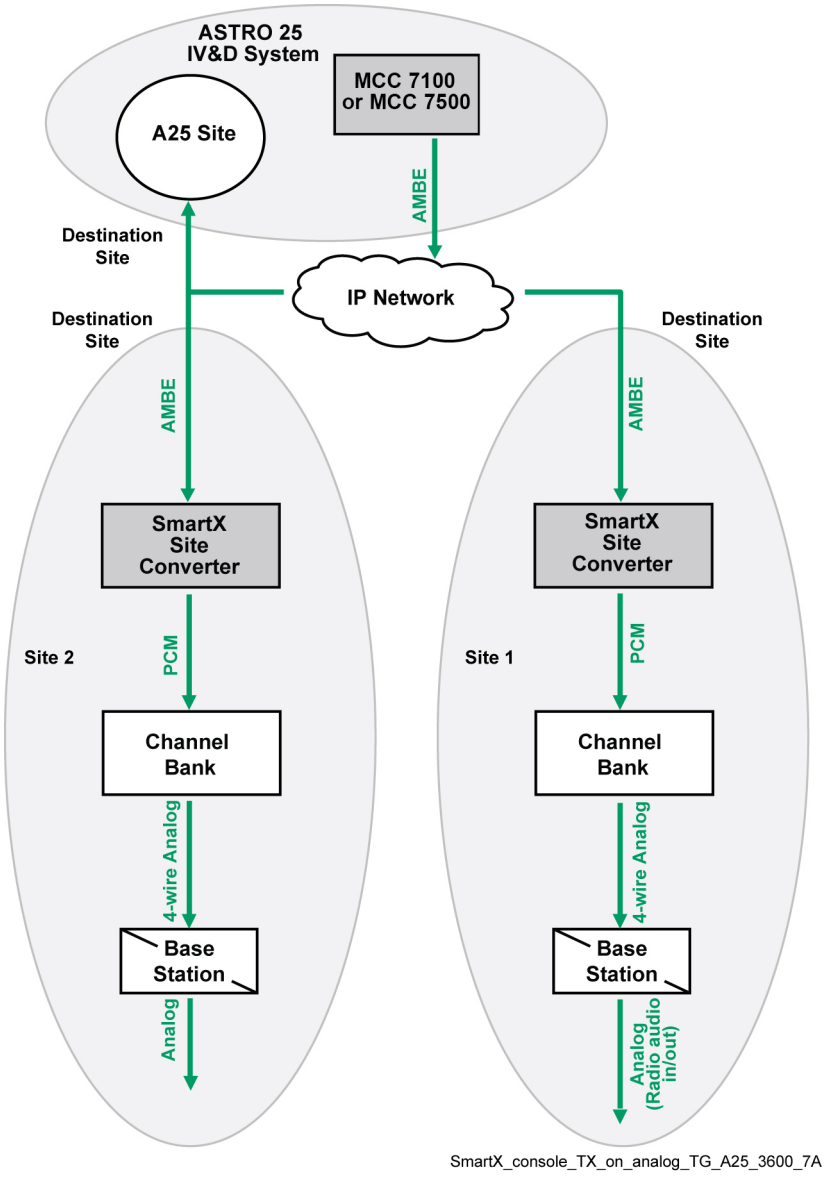
The following takes place when the source of audio is a radio at an ASTRO® 25 site and the destination is an analog talkgroup at the 3600 sites:

- 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 15: MCC 7500 Console Transmits on 3600 Analog Talkgroup**

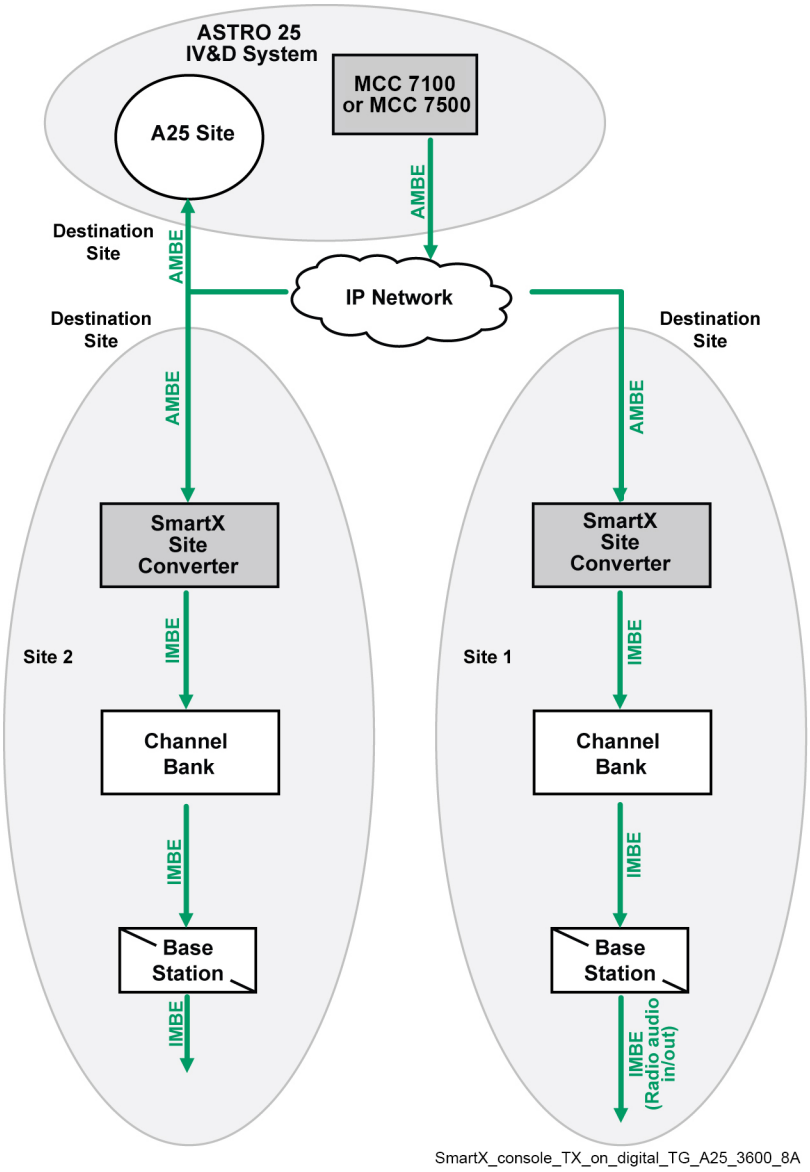


This example is similar to Scenario 3 except that the audio originates at an MCC 7500 console instead of a radio at an ASTRO® 25 site.

Scenario 7:

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

**Figure 16: MCC 7500 Console Transmits on 3600 Digital Talkgroup**

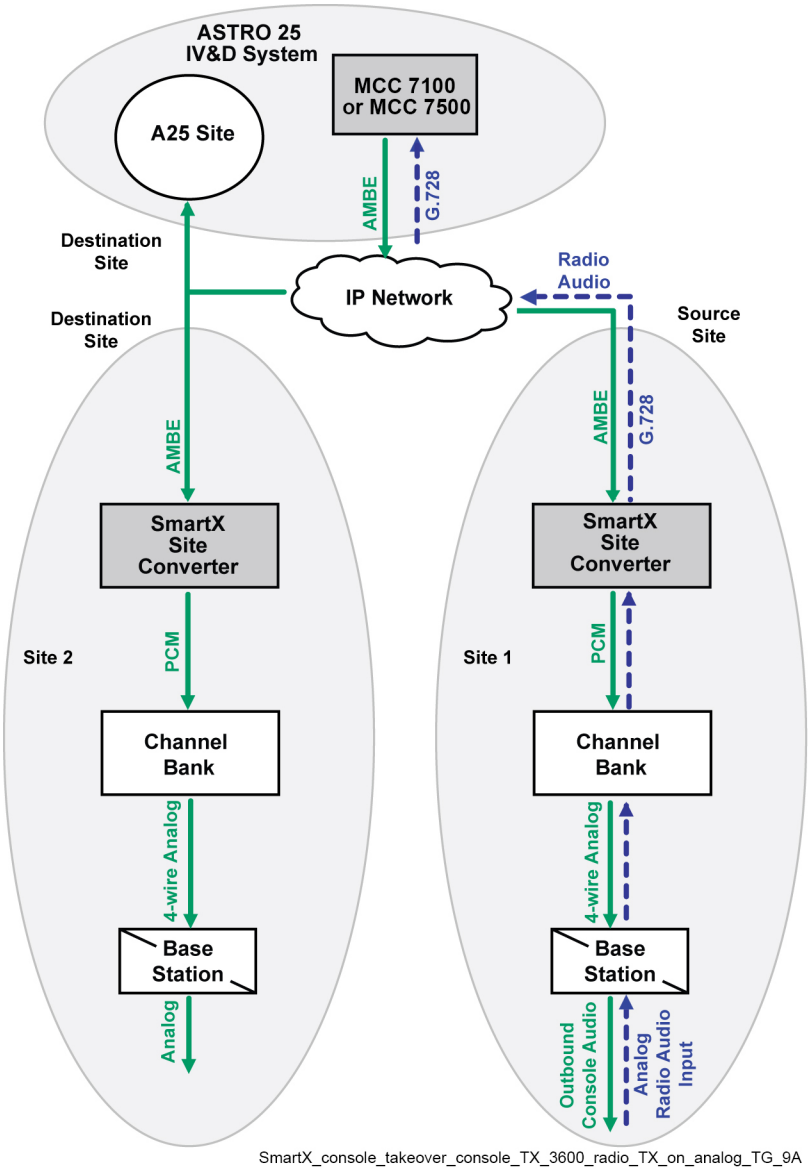



This example is similar to Scenario 5 except that the audio originates at an MCC 7500 console instead of a radio at an ASTRO® 25 site.

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 17: Console Takeover, Console, and 3600 Radio Transmit on 3600 Analog Talkgroup**

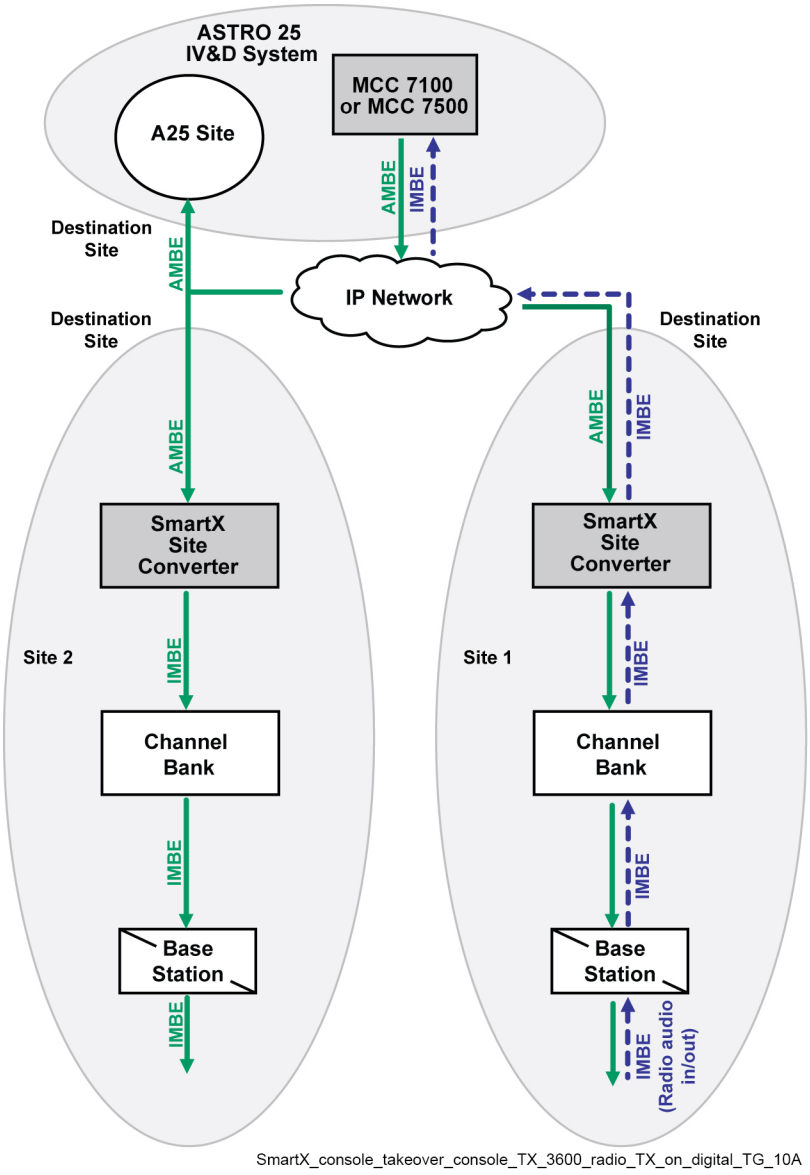



Console transmissions have a higher priority in the system than those originating at subscribe radios. Figure 17: Console Takeover, Console, and 3600 Radio Transmit on 3600 Analog Talkgroup on page 47 and Figure 18: Console Takeover, Console, and 3600 Radio Transmit on 3600 Digital Talkgroup on page 48 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 18: Console Takeover, Console, and 3600 Radio Transmit on 3600 Digital Talkgroup**




## 2.2
# NTP Services for the SmartX Site Converter

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#. Before 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 *Network Time Protocol Server* manual for more information.

2.3
## Zone Core Protection and the 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.

2.4
## ISSI 8000/CSSI 8000 Intersystem Gateways and the 3600 Sites

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

**NOTICE:** A GTR 8000 Base Radio can be implemented as a QUANTAR® station replacement within a 3600 and SmartZone® system. The implementation details are in the *Conventional QUANTAR Replacement Guide* manual.

2.5
## Network Management and the 3600 Sites

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.

2.5.1
### Provisioning Manager Programming for Subscribers

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*.

2.5.2
### Configuration/Service Software for the SmartX Site Converter

The following information is programmed through the Configuration/Service Software (CSS):

- Initial network configuration parameters
- NTP (date/time)
- SNMPv3 configuration
- DNS configuration and Centralized Event Logging services
- RADIUS service
- Set up the warning banner in 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 Configuration/Service Software (CSS), see the *CSS Online Help*.

### 2.5.3
## Unified Network Configurator Configuration for the SmartX Site Converter

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.

### 2.5.4
## Unified Event Manager Support for 3600 Sites

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.

The following features support 3600 site monitoring:

- Remotely force a 3600 site into “Site Trunking,” “Wide Trunking,” “Site Failsoft,” and “Site Off” state: This action 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.” See “Issuing Commands” in the “UEM Operation” chapter of the *Unified Event Manager* manual.
- Remote Enable/ Disable the SmartX Site Converter: For the procedure, see “Issuing Commands” in the “UEM Operation” chapter of the *Unified Event Manager* manual.

Once all the 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.

### 2.5.5
## ZoneWatch Support for 3600 Sites

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” displays 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.

### 2.5.6
## Radio Control Manager Support for 3600 Sites

The Radio Control Manager (RCM) provides support to the 3600 sites with the following options:

**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**
Provides ASTRO® 25 system status (maximum of 16 statuses are supported in ASTRO® 25 system).

**Message**
Provides 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.

2.6

# Call Processing for 3600 Radios in the ASTRO 25 System

From a call services perspective, the following table lists the types of calls supported by an ASTRO ® 25 system. Digital Vector Sum Excited Linear Prediction (VSELP) audio and analog 12KB Securenet are not supported.

Table 1: Call Types 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 (radio initiated) | ✓ |
| 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 radio (at 3600 site) and a 9600 radio in TDMA mode | x |
| Private Call II (does not use ring sequence to call another radio) | x |

2.6.1

## Operational Considerations for 3600 Sites

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.

**NOTICE:** When a 3600 radio subscriber initiates a call and the subscriber manually terminates the call before it is answered, the ASTRO® 25 system continues processing the call until the ring timer expires (60 seconds by default).

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.

2.6.1.1

### Talkgroups with 3600 Sites

Consider the following items 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/radios cannot participate in a talkgroup assigned as TDMA only in the Network Manager.

2.6.1.2

### Emergency Calls in 3600 Sites

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.

2.6.1.3

### Private Calls on an 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 hangtime 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 hangtime 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 hangtime 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 hangtime 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 hangtime ends, the call is ended.
- Any new private call request from a radio in the recently ended private call requires you to exit and re-enter Private Call mode before restarting the Private Call.

#### 2.6.1.4
### 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.

#### 2.6.1.5
### 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.

## 2.7
# Wide Area Trunking for 3600 Sites

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

- 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 that 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

Chapter 3

# SmartX Site Converter Installation

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

## 3.1 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 is upgraded to the appropriate level of hardware and software by the Motorola Field Services team.
- The ASTRO® 25 IVD system is installed and operational.

### 3.1.1 Preparing for the Initial SmartX Site Converter Installation and Configuration

This process provides a list of items to obtain before you can complete the installation and configuration procedures required to install the SmartX Site Converter.

**Prerequisites:**

- Install new configuration files in the core routers.
- Install configuration files in the site gateway (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.

**When and where to use:**
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 system.

**Process:**

1. Make sure that the ASTRO® 25 system CDs and DVDs are available to you. Specifically, obtain the *Transport*, *Motorola SmartX Site Converter*, and *Motorola VPM OS Image* media to perform Loading the SmartX Site Converter OS Images to the UNC on page 75.

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

   PuTTY is the utility certified for initiating interactive sessions. Install the PuTTY application for Secure SHell (SSH) to the UNC server application. SSH is necessary in Installing the SmartX Site Converter Software on page 73. See the *Securing Protocols with SSH* and *Unified Network Configurator* manuals.

   A License Key media to install the EMC Smarts™ Network Configuration Manager license key on the NM client for the UNC. See the *Unified Network Configurator* manual.

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

Other system media for installation and configuration of the information assurance features are:

- *Samba Winbind* media to install centralized authentication client software on the server.
- *MOTOPATCH for Windows* media for the latest Windows OS updates.

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

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

4 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)

5 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.

6 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.

7 To use the EMC Smarts™ Network Configuration Manager/VoyenceControl component of the Motorola centralized configuration application for any of the remote site device procedures, set up the Unified Network Configurator (UNC). Depending on the policies of your organization, you may be required to implement a secure protocol between the UNC and the remote site device. Before performing any procedures using this application, discover the site converter in EMC

Smarts™ Network Configuration Manager and pull the device configurations to the Unified Network Configurator database. See the following ASTRO® 25 system documentation:

- *Unified Network Configurator* manual
- *Securing Protocols with SSH* manual

8 You need various tools to install and service the equipment. If you need information 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:

- one service laptop with the Configuration/Service Software (CSS) application installed. See the instructions in the CSS media jewel box for instructions on loading the CSS application on a service laptop or computer.
- three Rack Units (RUs) of space for the VPM hardware and power supply tray, plus 1 RU for the required site gateway.
- one screwdriver
- one Ethernet cross-over cable
- one DB9F to RJ-45 VPM programming adapter
- one RS232 cable

## 3.2 Site Gateway Hardware Installation

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

## 3.3 Installing the SmartX Site Converter

**When and where to use:**
Follow this process to install the Voice Processor Module (VPM) hardware and configure it as a SmartX Site Converter.

**Process:**

1 Install the Voice Processor Module (VPM) hardware. See Installing the SmartX Site Converter Hardware on page 60.

2 Configure the startup parameters with the Configuration/Service Software (CSS) application. See Performing the Initial Configuration for the SmartX Site Converter on page 61 and Configuring the SmartX Site Converter in the CSS (Ethernet Connection) on page 63.

3 Enable secure credentials.

**a** Set up the SWDL transfer mode in the CSS. See Enabling Secure Software Download on page 64.

**b** Optional: Set up the local Password Configuration in the CSS. See Setting the SmartX Site Converter Local Password Configuration on page 65.

**c** Set the current date and time in the CSS. See Setting the Date and Time on the SmartX Site Converter on page 66.

**d** Set the serial security services. See Setting the Serial Security Services on page 67

**e** Change the SNMPv3 configuration and user credentials from CSS on a selected device in the remote site. See Changing SNMPv3 Configuration and User Credentials on the SmartX Site Converter on page 68.

**f** Create, update, or delete an SNMPv3 user. See Adding or Modifying SNMPv3 Users on page 70.

**4** Verify the SNMPv3 credentials. See Performing an SNMPv3 Connection Verification in the CSS on page 71.

**5** Set the Network Services Configuration in the CSS.

**a** Configure DNS in 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.

**b** Configure the SmartX Site Converter for SSH. See the “Configuring SSH for RF Site Devices and VPMs Using CSS – Overview” section in the *Securing Protocols with SSH* manual.

**c** Configure the local cache size for the SmartX Site Converter. See the *Authentication Services* manual.

**d** Enable Centralized Authentication in the CSS. See the *Authentication Services* manual.

**e** Optional: Customize the login banner text in the CSS. See Customizing the Login Banner in the CSS on page 72.

**f** Enable RADIUS Authentication in the CSS. See the *Authentication Services* manual.

**g** Optional: Enable Centralized Event Logging in the CSS. See the *Centralized Event Logging* manual.

**6** Connect the SmartX Site Converter to the site gateway. See Connecting the SmartX Site Converter to the Site Gateway on page 72.

**7** Install the software on the SmartX Site Converter in the Unified Network Configurator (UNC). See Installing the SmartX Site Converter Software on page 73 for the procedures involved in the software installation on the site converter.

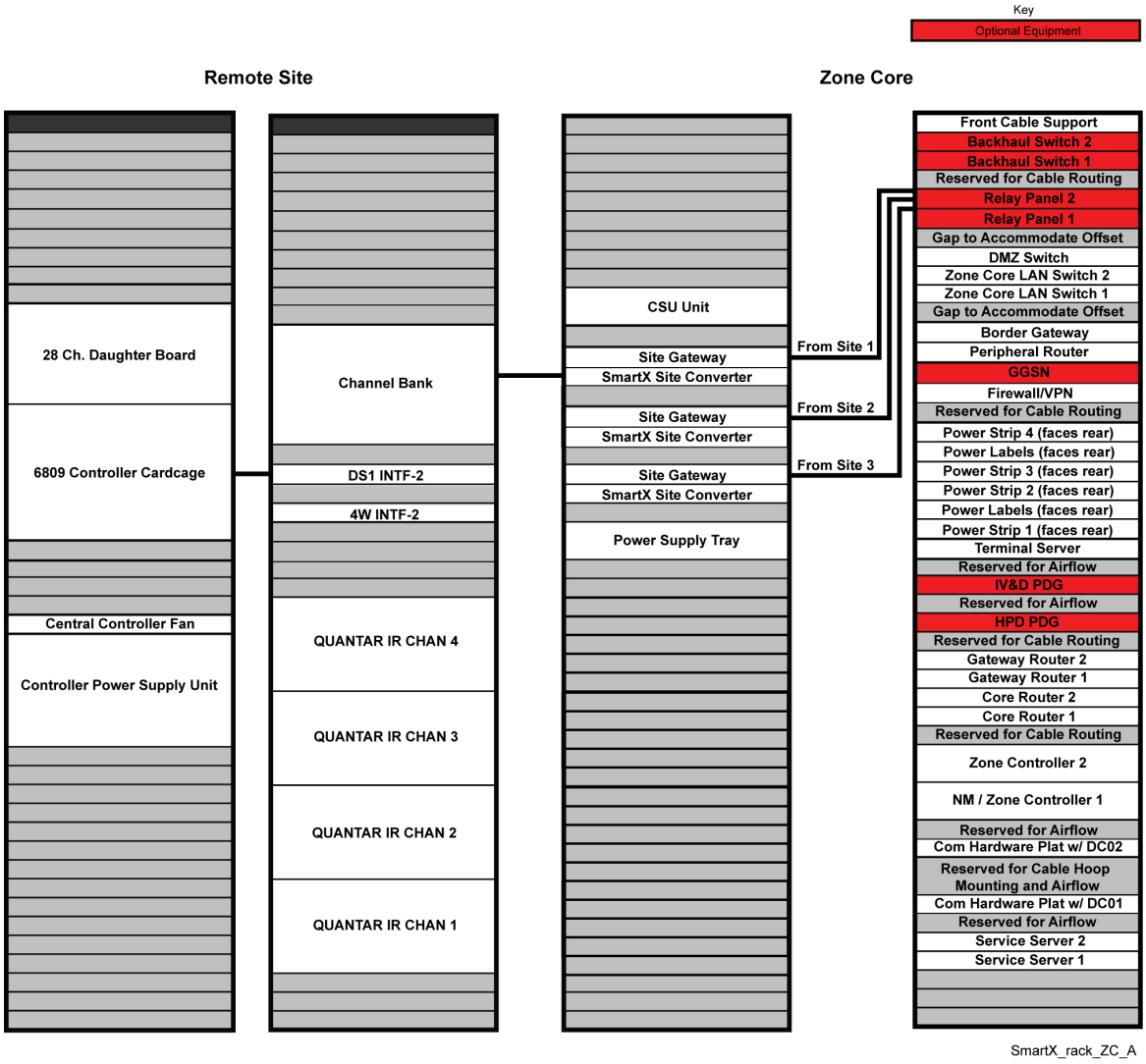
**8** Configure the SmartX Site Converter. See Configuring the SmartX Site Converter on page 79.

## 3.4 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 (three units for converters + 2 units for the power supply tray.) Additionally, one rack is needed for the site gateway, which connects to the SmartX Site Converter. See Figure 19: Site Converters in a Rack at the Zone Core on page 59 for a typical zone core (master site) installation.

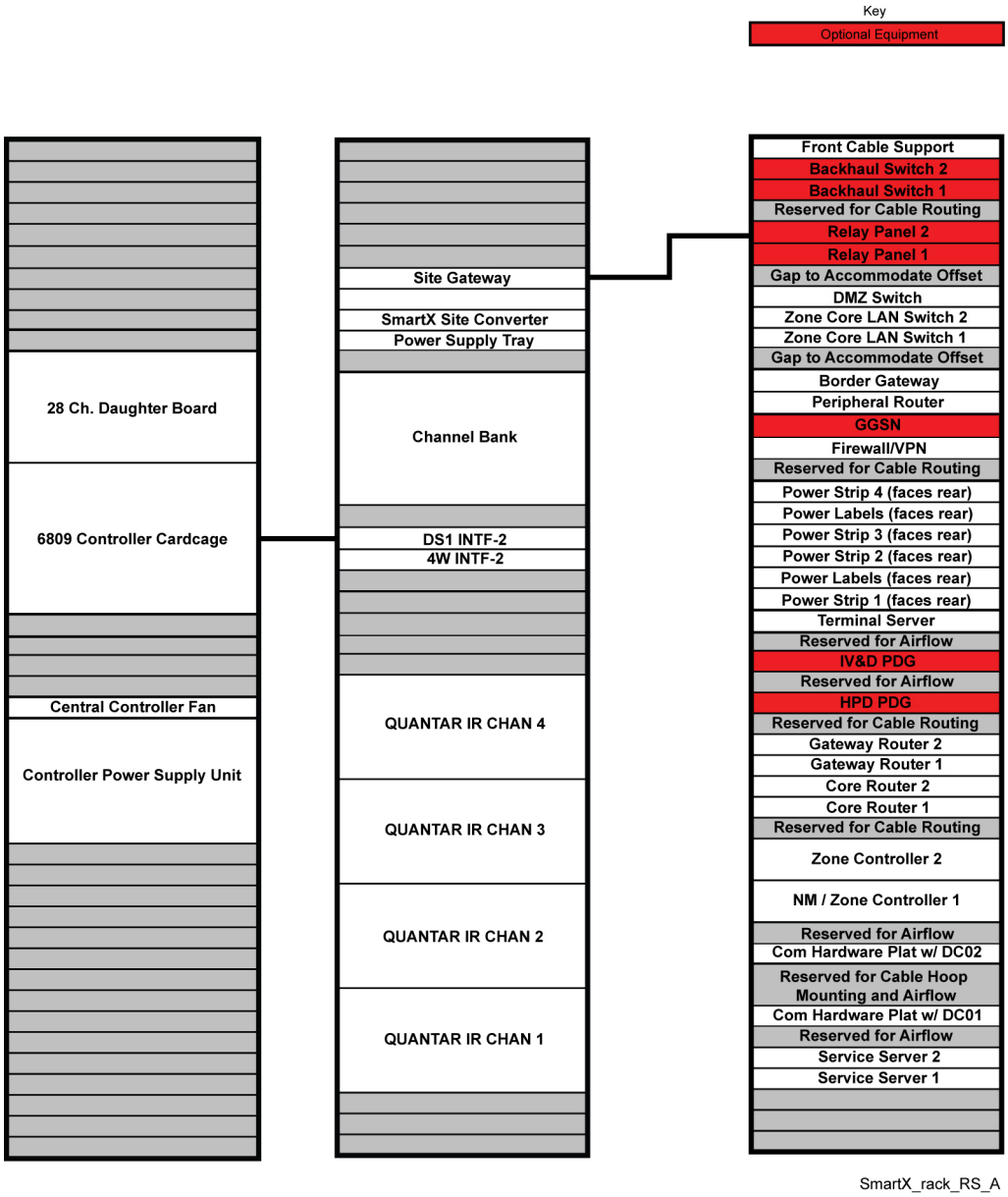
**Figure 19: Site Converters in a Rack at the Zone Core**




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

The following diagram shows 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 the event of a lighting strike or some other event. However, if you are using microwave or fiber optics, this additional level of protection is not required.

**Figure 20: A Site Converter in a Rack at the Remote Site**




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

3.5

## Installing the SmartX Site Converter Hardware

Once the Voice Processor Module (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:**

1. Ensure that site gateway installation is complete.
2. Place the VPM hardware in the mounting rack.

**NOTICE:** 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.

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).

## 3.6 SmartX Site Converter Power Distribution Installation

There is a single SmartX Site Converter for each site, so the configuration is 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, 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.

## 3.7 Software Download Manager Installation and Data Transfer

The Software Download Manager (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.

SWDL performs two types of data transfer.

**Clear SWDL**
Performs transfer operations without security, based on the File Transfer Protocol (FTP)

**Secure SWDL**
Performs transfer operations are encrypted, based on the Secure File Transfer Protocol (SFTP)

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 Configuration/Service Software (CSS). Schedule and configure all devices in the system at once in the Unified Network Configurator (UNC)

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 Manager* manual.

## 3.8 Performing the Initial Configuration for the SmartX Site Converter

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. This procedure describes how to set up the initial SmartX Site Converter parameters.

**Prerequisites:**
A laptop computer with the Configuration/Service Software (CSS) application.

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

**When and where to use:**
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 in the CSS application). This manual focuses on the CSS procedures. If you want to configure the SmartX Site Converters in the UNC, see the *Authentication Services* manual or the *Unified Network Configurator* manual for the necessary procedures.

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

**Procedure:**

1. Turn on the VPM hardware.

   The Power LED on the front of the SmartX Site Converter illuminates.

2. Connect the service laptop (with the Configuration/Service Software application) to the serial port on the SmartX Site Converter using an RJ–45 to the female DB9 pin serial converter.

   **NOTICE:** The serial port is designated by a footswitch icon on the Voice Processor Module (VPM) hardware. See Figure 2: Rear View of the SmartX Site Converter — Power Connection and Ports in Use on page 26 for the location of the serial port.

   The laptop and VPM chassis are connected.

3. Launch the CSS application and connect to the device using a serial connection.

   **NOTICE:** If Authentication Services are not enabled on a device, type any alphanumeric characters to populate the user name, Password, and Elevated Privileges Password fields, as they cannot be left blank.

   The **Configuration/Service Software** main window appears.

4. To connect to the device using a serial connection, choose **Tools** → **Connection Configuration**.

   The **Connection Screen** dialog box appears.

5. Set the following serial connection parameters, then click **Connect**.
   - Select **Serial** from the Connection Type field.
   - Select a Baud rate of **19200**.
   - Select the appropriate Com port (usually Com Port 1).

   A confirmation dialog box appears telling you that CSS has connected with the device.

6. Click **OK**. If authentication on the device is enabled, a login screen appears. Provide all required credentials. Click **OK**.
7. Select **Tools** → **Set IP Address and Box Number**.

   The **Set IP Address and Box Number** dialog box appears.

8. Set the following parameters:
   - 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.

**NOTICE:** 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.

The SmartX Site Converter restarts with the new IP address(es) and Netmask assignments. The SNMPv3 user credentials reset to their factory default values.

**Postrequisites:** Proceed to Changing SNMPv3 Configuration and User Credentials on the SmartX Site Converter on page 68 and reconfigure the SNMPv3 credentials.

3.8.1

## Configuring the SmartX Site Converter in the CSS (Ethernet Connection)

This procedure describes how to set the Site ID.

**Prerequisites:**
A laptop computer with the Configuration/Service Software (CSS) application.

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

**When and where to use:** During the initial installation, this procedure is done through an Ethernet cable connected directly to the Ethernet port of the SmartX Site Converter. After installation, you can perform this procedure from a remote Configuration/Service Software (CSS) session.

**Procedure:**

1. Connect a cross-over Ethernet cable to the CSS Ethernet port and the SmartX Site Converter Ethernet port.

   The laptop and VPM chassis are connected.

2. Set the Ethernet to 100 MB full duplex on the CSS laptop.
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. Launch the CSS application and connect to the device using a serial connection.

   **NOTICE:** If Authentication Services are not enabled on a device, type any alphanumeric characters to populate the user name, Password, and Elevated Privileges Password fields, as they cannot be left blank.

   The **Configuration/Service Software** main window appears.

5. To connect to the device using an Ethernet connection, choose **Tools** → **Connection Configuration**.

   The **Connection Screen** dialog box appears.

6. Select **Ethernet** from the **Connect Type** field.
7. Enter the IP address of the device.
8. Click **OK**.

   The SNMPv3 passphrase prompt appears. If the connection fails, a message appears.

9. Select appropriate security level. Click **OK**.
   - **NoAuthNoPriv** – does not require authentication passphrase or encryption passphrase
   - **AuthNoPriv** – requires authentication passphrase

- **AuthPriv** – requires authentication passphrase and encryption passphrase

**NOTICE:** During initial installation, you can select **NoAuthNoPriv**.

10 Choose **File** → **Read Configuration From Device**.

A message appears and informs that an Ethernet connection must be established.

11 If Centralized Authentication is enabled, an FTP Login Screen opens. See “Device Security Configuration - Remote Access Login (Ethernet)” in the *CSS Online Help* for details. Provide the required credentials.

**NOTICE:** If Authentication Services is enabled in the Security Services Configuration window, enter a user name 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 user name, Password, and Elevated Privileges Password, as they cannot be left blank.

12 Click **OK**.

The **Connection Screen** appears.

13 In the navigation pane, click the **Site** folder.

A **Site** dialog box appears.

14 Type the **Site ID** number.

A green mark appears indicating the Site ID has changed.

15 Save the configuration data to an archive file.

16 Choose **File** → **Write Configuration to Device** to download the configuration data to the SmartX Site Converter.

The Site ID is set for the SmartX Site Converter.

### 3.8.2
## Enabling Secure Software Download

The following procedure describes how to set the SWDL transfer mode to FTP (clear) or SFTP (secure) for the device.

**Procedure:**

1 Connect to the device using the Configuration/Service Software (CSS) through an Ethernet port link.

2 From the **Security** menu, select **Device Security Configuration** → **Remote Access/Login Banner (Ethernet)**.

The **Remote Access/Login Banner** screen appears displaying the **Remote Access Configuration** tab.

3 In the **Software Download Transfer Mode (Requested)** field, choose between:

- **Ftp (clear)**
- **Sftp (secure)**

4 Click **OK**.

**NOTICE:** Secure Shell Service and Secure FTP service are automatically set to Enabled and grayed out when you choose Sftp.

3.8.2.1

## Setting the SmartX Site Converter Local Password Configuration

The following procedure 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 devices local service account. Password Configuration is an optional feature. For information, see “Password Configuration” in the *CSS Online Help*.

**Procedure:**

1 Launch the **CSS** application.

**NOTICE:** If Authentication Services are not enabled on a device, type any alphanumeric characters to populate the user name, Password, and Elevated Privileges Password fields, as they cannot be left blank.

2 Choose **File** → **Read Configuration From Device**.

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 *CSS Online Help* for details. Provide the required credentials.

**NOTICE:** If Authentication Services is enabled in the Security Services Configuration window, enter a user name 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 user name, Password, and Elevated Privileges Password, as they cannot be left blank.

4 Click **OK**.

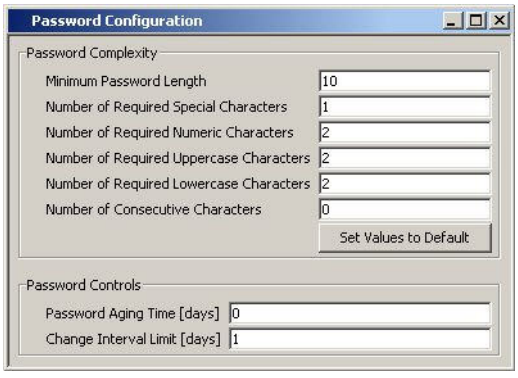
The **Connection Screen** appears.

5 Enter the IP address of the site converter you want to access. Click **Connect**.

**NOTICE:** If an authentication window appears, enter your credentials. A message window appears displaying the **CSS Successfully Connected to this Device** message.

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

**Figure 21: Password Configuration Window**




The **Password Configuration** window appears.

7 Complete the following fields:

- **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 devices local password is valid. After the Password Aging Time has elapsed, the devices 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 devices local password can be changed. The default value is 1.

8 Choose **File** → **Save** to save the configuration changes.

9 Choose **File** → **Write Configuration to Device** to download the configuration changes on the SmartX Site Converter.

### 3.8.2.2
## Setting the Date and Time on the SmartX Site Converter

The following procedure provides the date and time to the SmartX Site Converter. If a power outage occurs, the site converter does not retain the date and time settings.

**NOTICE:** 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 Configuration/Service Software (CSS) session.

**Procedure:**

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 Launch the **CSS** application.

**NOTICE:** If Authentication Services are not enabled on a device, type any alphanumeric characters to populate the user name, Password, and Elevated Privileges Password fields, as they cannot be left blank.

The **Configuration/Service Software** main window appears.

5 To connect to the device using an Ethernet connection, choose **Tools** → **Connection Configuration**.

The **Connection Screen** dialog box appears.

6 From the **Connect Type** field, select **Ethernet**.

7 Set the IP address to the IP address of the site converter. Click **Connect**.

8 Choose **Tools** → **Set Date and Time**.

9 Enter the current date and time. Click **OK**.

The date and time is reset.

### 3.8.2.3
## Setting the Serial Security Services

The following procedure 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.

**Prerequisites:**
Ensure that you have the required credentials information (local service account password and elevated privileges password) to configure the site devices. 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.

**IMPORTANT:** Changing to the incorrect user credentials may lead to not being able to access the device through CSS or SSH. See Device Passwords and SNMPv3 Passphrases on page 107 for troubleshooting information.

**Procedure:**

1 Connect the CSS serial port to the SmartX Site Converter Serial port through an RJ-45 to female DB9 pin serial converter.

2 Launch the **CSS** application.

**NOTICE:** If Authentication Services are not enabled on a device, type any alphanumeric characters to populate the user name, Password, and Elevated Privileges Password fields, as they cannot be left blank.

The **Configuration/Service Software** main window appears.

3 To connect to the device using a Serial connection, choose **Tools** → **Connection Configuration**.

The **Connection Screen** dialog box appears.

4 Set the following serial connection parameters, then click **Connect**.

- Select **Serial** from the Connection Type field.
- Select a Baud rate of **19200**.
- Select the appropriate Com port (usually Com Port 1).

A confirmation dialog box appears telling you that CSS has connected with the device.

5 Click **OK**. If authentication on the device is enabled, a login screen appears. Provide all required credentials. Click **OK**.

6 Select **Security** → **Device Security Configuration** → **Security Services (Serial)**.

The Security Services Configuration dialog box opens.

7 Set the **Authentication Services** field to **Enabled**. This field enables local authentication services and must be enabled as a prerequisite for centralized authentication.

8 Click **Apply**.

9 Set the **Password Reset Mechanism** field. This field allows you to reset the passwords for two built-in device accounts to their default values.

10 To update the password for the device, select either **Service Account** or **Elevated Privilege** from the drop-down list. Click **Update password**.

A **Change Account Password** dialog box opens.

11 Enter the old password, then enter a new password and confirm the new password before clicking **Change Password**.

12 Click **OK** to save the new password.

The **Change Account Password** dialog box closes.

3.8.2.4

## Changing SNMPv3 Configuration and User Credentials on the SmartX Site Converter

The following procedure changes the SNMPv3 configuration and user credentials from Configuration/Service Software (CSS) on a selected device in the remote site. For more information on this feature, see the *SNMPv3* manual.

**NOTICE:** 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.

**Prerequisites:**
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).

**Procedure:**

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 Launch the **CSS** application.

**NOTICE:** If Authentication Services are not enabled on a device, type any alphanumeric characters to populate the user name, Password, and Elevated Privileges Password fields, as they cannot be left blank.

The **Configuration/Service Software** main window appears.

5 To connect to the device through an Ethernet connection, specifically for configuring the SNMPv3 User Credentials on the device, choose **Security → SNMPv3 Configuration → Configure SNMPv3 Users (Ethernet)**.

The **SNMPv3 Login/Connection** dialog box appears with MotoAdmin as the selected SNMPv3 user.

6 Enter the appropriate authentication and encryption passphrases/passwords in the fields.

**NOTICE:** 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 *CSS Online Help* section “Reset SNMPv3 Configuration (Serial)” to reset the passphrases to the current software release defaults.

7 Enter the IP address.

8 Click **OK**.

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.

9 To choose the SNMPv3 user whose credentials you want to update, select **user name** from the user name list in the User Information form of the Configure SNMPv3 Users dialog box.

**NOTICE:** 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.

The CSS retrieves the current credentials from the device for the selected user.

10 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:

- **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.

**NOTICE:** 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:

- **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.

The security level of the selected user is set.

11 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.

**NOTICE:** If you do not know the password, click the **I do not remember old password** check box.

12 Type the new password/passphrase into the **New Password** field.

**NOTICE:** Password must be between 8 and 64 characters in length and password must consist of upper or lowercase alphanumeric characters (excluding the @ # $ ^ or _ characters).

13 Type the same new password/passphrase into the **Confirm New Password** field.

14 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.

**NOTICE:** If you do not know the password, select the **I do not remember old password** check box.

15 Type the new password/passphrase into the **New Password** field, then type the same new password/passphrase into the **Confirm New Password** field.

16 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.

17 Type the new engine ID into the **New Engine ID** field.

**NOTICE:** The new engine ID must be between 1 and 27 characters and comply with the Engine ID Domain Name Syntax.

The authoritative engine ID is assigned.

**Postrequisites:** To create, update, or delete SNMPv3 users, continue on with “Adding or Modifying SNMPv3 Users.”

### 3.8.2.5
## Adding or Modifying SNMPv3 Users

The following procedure describes how to create, update, or delete an SNMPv3 user from the Configure SNMPv3 Users Screen dialog box.

**Procedure:**

1 Launch the Configuration/Service Software (CSS) application.

2 On the Security tab, select **SNMPv3 Configuration** → **Configure SNMPv3 Users**.

3 Log on to the device.

**NOTICE:** If Authentication Services are not enabled on a device, type any alphanumeric characters to populate the User Name, Password, and Elevated Privileges Password fields, as they cannot be left blank.

The **Configure SNMPv3 Users** dialog box appears.

4 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**. |

5 Click **Yes**.

The **Processing Requests** dialog box appears and processes the request. A green square indicates OK and a red square indicates failure.

6 After reviewing the processing status, click **OK**.

**NOTICE:** If you encounter any errors, go back to the appropriate step and correct the information entered.

7 Repeat these steps for any SNMPv3 users you wish to create, update, or delete.

8 Select **Cancel** to exit the **Configure SNMPv3 Users** dialog box.

9 On the main CSS window, select **File** → **Exit**. Click **OK**.

### 3.8.3
## Performing an SNMPv3 Connection Verification in the CSS

SNMPv3 credentials for the SmartX Site Controller can be verified in the Configuration/Service Software (CSS) application.

**Prerequisites:** 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.

**When and where to use:** Once the SNMPv3 user credentials have been created, modified, or deleted, you can perform a sanity check to ensure that the device is properly configured for SNMPv3. The following procedure describes how to verify the SNMPv3 connection.

**Procedure:**

1 Connect a service laptop or NM client with CSS to the SmartX Site Converter using an Ethernet cable, then launch the **CSS** application.

2 When the passphrase prompt screen opens, select the configured security level and enter the required passphrases.

**NOTICE:** If Authentication Services are not enabled on a device, type any alphanumeric characters to populate the user name, Password, and Elevated Privileges Password fields, as they cannot be left blank.

A confirmation dialog box appears indicating that the CSS has connected with the device.

3 Click **OK** if the connection was successful. This action indicates your SNMPv3 configuration is valid.

**NOTICE:** If you fail to connect or log on to the device in SNMPv3 mode, then the device is not properly configured for SNMPv3.

4 On the main CSS window, select **File** → **Exit**. Click **OK** to confirm that you want to exit.

### 3.8.4
## Network Services Configuration in the CSS

The Configuration/Service Software (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 Performing the Initial Configuration for the SmartX Site Converter on page 61 and the Password Configuration procedure is provided in Setting the SmartX Site Converter Local Password Configuration on page 65.

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 parameters. Each tab is its own procedure in this section; however, you do not need to launch Configuration/Service Software (CSS) and save the configuration on each tab if you are performing all of these steps at the same time. You 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 in 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 in the CSS. See the *Authentication Services* manual.
- Enabling RADIUS Authentication in the CSS. See the *Authentication Services* manual.
- Enabling Centralized Event Logging in the CSS (optional). See the *Centralized Event Logging* manual.

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

#### 3.8.4.1
### Customizing the Login Banner in the CSS

The following procedure describes how to edit the security notice in the login banner.

**Procedure:**

1. Connect to the device using Configuration/Service Software (CSS) through an Ethernet connection.
2. From the **Security** menu, select **Device Security Configuration → Remote Access/Login Banner (Ethernet)**.

   The **Remote Access/Login Banner** window appears displaying the Remote Access Configuration tab.
3. Click the **Login Banner** tab.
4. Edit the text of the banner.
5. Click one of the following options:
   - **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.

## 3.9
# Connecting the SmartX Site Converter to the Site Gateway

The site gateway provides the network connection for the SmartX Site Converter.

**When and where to use:** 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.

**Procedure:**

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.

   The SmartX Site Converter shares an Ethernet cable with the site gateway.
3. Verify the connection by accessing the site from the remote CSS.

3.10

# Installing the SmartX Site Converter Software

The Unified Network Configurator (UNC) is the primary network manager used to load Operating System software to the SmartX Site Converter devices. The following process lists the basic steps involved in the software installation on the device. You can also use the Software Download Manager (SWDL) program to load software on the SmartX Site Converter.

**When and where to use:** Use this process to install software on the Voice Processor Module (VPM) to use the hardware as a SmartX Site Converter.

**NOTICE:** You can use either the Unified Network Configurator (UNC) or the Software Download Manager (SWDL) application to load software on the SmartX Site Converter.

**Process:**

1. Discover the SmartX Site Converter device in the UNC. See Discovering the SmartX Devices with the UNC on page 73.
2. Log in to the UNC Server Application Using PuTTY. See “Logging in to the UNC Server Application with PuTTY” in the *Unified Network Configurator* manual for more information on this procedure.
3. Load the Operating System images to the UNC. See Loading the SmartX Site Converter OS Images to the UNC on page 75.
4. Enable FTP services in the UNC. See Loading OS Software to SmartX Site Converter Devices on page 76.
5. Transfer and install the OS image to the SmartX Site Converter. See Transferring and Installing the OS Image on page 76.
6. Inspect the SmartX Site Converter and bank device properties for the transferred and installed software. See Inspecting Device Properties for Transferred and Installed Software on page 77.
7. Disable FTP services for the UNC. See Disabling FTP Service on page 78.

3.10.1

## 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 Configuration/Service Software (CSS) application, and security parameters are enabled, use the following procedure to discover the device and then you can update configuration information using this configuration management application.

**NOTICE:** 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.

**Prerequisites:** The UNC Wizard and the EMC Smarts™ Network Configuration Manager applications.

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

**When and where to use:**
The UNC network management solution consists of two applications, and both the UNC Wizard and EMC Smarts™ Network Configuration Manager applications are used.

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.

**Procedure:**

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. Double-click the **Internet Explorer** on the desktop to log on to the UNC Wizard from the NM client.
3. Enter: `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).

   The **UNC Wizard** launches and a login dialog box appears.
4. Type the administrative user name and password. Click **OK**.

   The **UNC Wizard** appears.
5. From the list of available wizards on the left side, select **Subnet Discovery**.

   The right side of the window is updated with the Subnet Discovery form.
6. Select **RF Site** by clicking the **Discovery Type** drop-down list.
7. Type the ***<Zone ID>*** and ***<Site ID>***. Click **Submit**.

   An auto-discovery job is created in the **UNC Schedule Manager**. You are finished using the UNC Wizard.
8. To log on to the UNC from the NM client, enter: `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).

   After the UNC client launches, a login dialog box appears.
9. Type the administrative user name and password. Click **OK**.

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

   **EMC Smarts™ Network Configuration Manager** launches.
10. Press F7 (Schedule Manager).

    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) discovered.

    **NOTICE:** No sites should be in the Lost and Found folder. If there are, see the *Unified Network Configurator* 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.

    The SmartX sites are listed, which means they are available for channel configuration.

**Postrequisites:** 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.

### 3.10.2
## Logging on to the UNC Server Application with PuTTY

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

### 3.10.3
## Loading the SmartX Site Converter OS Images to the UNC

The following procedure 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).

**Prerequisites:** Obtain the *Transport*, *Motorola SmartX Site Converter*, and *Motorola VPM OS Image* media.

**Procedure:**

1. Launch an SSH terminal server session in PuTTY to access the **UNC Server Administration** menu.

   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**.

   The **OS Images Administration** menu appears.

4. Select **Load new OS images** from the menu. Press **Enter**.

   A message appears indicating there are two methods for loading OS Images.

5. Insert the *Transport*, *Motorola SmartX Site Converter*, and *Motorola VPM OS Image* media into the CD/DVD-ROM drive of the server.

   The drive light starts blinking on the server.

6. When the drive light stops blinking, press **Enter**.

   **NOTICE:** The *Transport*, *Motorola SmartX Site Converter*, and *Motorola VPM OS Image* media is packaged with the Network Management DVDs when an ASTRO® 25 system ships.

   The OS images load in the UNC.

7. Select **Eject CD** from the menu. Press **Enter**.

   The **User Configuration Server Administration** menu appears.

8. Remove the *Transport*, *Motorola SmartX Site Converter*, and *Motorola VPM OS Image* media from the CD/DVD-ROM drive of the server.
9. Select **quit**. Press **Enter**.

**Postrequisites:** Once OS images are distributed to the UNC, you can update the site converters configuration files to the UNC.

### 3.10.4
## 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.

**Prerequisites:** Enable FTP before you install this software.

**Procedure:**

1. Launch an SSH terminal server session in PuTTY to access the UNC Server Administration menu.
2. Select **Unix Administration** from the menu. Press **Enter**.
3. Select **FTP Services** from the menu. Press **Enter**.
4. Select **Enable FTP service** from the menu. Press **Enter**.

The FTP Services are enabled and available for software transfer and install operations.

### 3.10.5
## Transferring and Installing the OS Image

The following procedure describes how to download the OS from the UNC to the SmartX Site Converter.

**Procedure:**

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

2. In the left navigation pane, expand **Networks** → **Astro 25 Radio Network** → **Views**.

   The list of options expands.

3. Double-click **Motorola SmartX Site Converters** from the navigation pane.

   The view opens and all currently discovered SmartX Site Converter devices appear.

4. Select **Tools** → **OS Inventory**.

   **NOTICE:** You can also press the F9 key to select the OS Inventory.

   A list of the OS images appears.

5. Verify OS images loaded in the UNC server appear in the OS inventory.

   **NOTICE:** These images were automatically created during the “Loading the SmartX Site Converter OS Images to the UNC” procedure.

6. 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.

   The **Select OS Image** window appears.

7. Select **Software Image**. Click **Next**.

   The **Update OS Image** window appears.

8. Select each device that appears in the **Selected Devices** section.

**NOTICE:** In most cases, the “summary of device partitions” are already set up and you need to verify the values in step 8 to step 11.

This associates a version to a device instance.

9 Select **nvm partition** from the **Manage Partition for Device** section.

**NOTICE:** This is the only choice for SmartX Site Converter device.

This defines where the OS image is transferred.

10 Select the image for this device from the **Selected Image** section.

**NOTICE:** You can ignore the **Install** and **Copy** check boxes.

This populates the Image Info tab and informs the application which image to use.

11 Select **Device Options** → **Software Operations**.

12 Choose

- **transfer**
- **install**
- **both**

**NOTICE:** 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.

This indicates which operations occur when the job is executed.

13 Click **Schedule**.

14 Configure the schedule information and click **Approve and Submit**.

**NOTICE:** If you choose **Submit**, you are asked to approve the job later.

This approves the job and you can view it in the **Schedule Manager** window.

15 Press F7 (Schedule Manager) to verify the job status.

The **Schedule Manager** window appears in the UNC with the discovery jobs.

### 3.10.6
## Inspecting Device Properties for Transferred and Installed Software

Once the software has been transferred and installed, the following procedure guides you to inspect the device properties before assuming the installation was a success and disabling FTP service.

**Procedure:**

1 From the **Device** view, right-click the device, select **Pull** → **Pull Hardware Spec**.

**NOTICE:** You can skip this step if a **Pull All** or **Pull Hardware Spec** has already occurred.

The current software version information is updated in the UNC.

2 From the **Device** view, right-click on the device, then choose **Properties**.

**NOTICE:** If you select the Properties icon, you can view the device properties appear directly within the Device view.

3 Select the **Configuration** tab, then the **Hardware** tab.

4 Double-click the **Chassis** object from the **Physical Hardware** properties.

The **Chassis property tree** expands.

5 View the following properties and their values:

- **Bnk1:SmartX_Converter**: Transferred software in bank 1.
- **Bnk2:SmartX_Converter**: Transferred software in bank 2.
- **SmartX_Converter**: Installed and Running Software.

**NOTICE:** You can use the Table format (instead of the Diagram format) to view the Installed and Running Software in the Device view.

### 3.10.7
## Disabling FTP Service

**When and where to use:**
After the transfer and installation of the software, you must disable the FTP service. The following procedure describes how to disable FTP service.

**Procedure:**

1 Launch an SSH terminal server session in PuTTY to access the **UNC Server Administration** menu.

The **UNC Server Administration** menu appears.

2 Select **Application Administration** from the menu. Press **Enter**.

3 Select **FTP Services** from the menu. Press **Enter**.

4 Select Disable **FTP service** from the menu. Press **Enter**.

The FTP Services are disabled and unavailable for software transfer and install operations.

5 Press **q** three times to back out of the menus.

6 At the prompt, type `exit` to return to the previous menu.

7 Type `exit` again.

You have successfully logged out of the application.

8 Close the PuTTY connection.

Chapter 4

# SmartX Site Converter Configuration

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

## 4.1 Configuring the SmartX Site Converter

Once the SmartX Site Converter is installed in the system, perform these tasks to configure the device.

**When and where to use:** Perform this process after the SmartX Site Converter is installed in the ASTRO® 25 system.

**Process:**

1. Configure the SmartX Site Converter to transition the site to wide trunking in the UNC. See Configuring the SmartX Site Converter in the UNC on page 80.
2. Configure the channels in the UNC Wizard. See Configuring the SmartX Site Converter Channels in the UNC Wizard on page 84.
3. Configure the trunked 3600 sites and channels in the UNC Wizard. See Configuring the SMARTNET/SmartZone Devices in the Network Management Applications on page 85.
4. Monitor the SmartX Site Converter faults.
   a. Discover the SmartX Site Converter devices in the UEM. See Discovering the SmartX Site Converter Devices with the UEM on page 88.
   b. Verify SmartX Site Converter operation with the UEM. See Verifying System Installation with the UEM on page 89.
5. Connect the SmartX Site Converter and the channel bank. See Connecting the SmartX Site Converter and the Channel Bank on page 91.

## 4.2 SmartX Site Converter Network Management Configuration

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

### 4.2.1 Jitter Configuration for 3600 Sites

Jitter can introduce clicks or other undesired effects in audio signals, and loss of transmitted data between network devices. The amount of allowable jitter depends on the application. Motorola recommends combating jitter in the IMBE audio by configuring the IMBE Jitter Buffering Age (ms) parameter in the Unified Network Configurator.

The IMBE Jitter Buffer parameter is set based on measuring worst case jitter scenarios between a sourcing IP device and the destination SmartX Site Converter. Increasing this timer increases call delay. Setting the timer too low results in audio gaps in the transmit signaling. The recommended timer values for the IMBE Jitter Buffering Age (ms) parameter differ depending on whether the site is digital simulcast or not. The following tables map possible measured jitter values to corresponding

recommended timer values for this parameter. The 3600 simulcast sites that provide digital calls require a different timing value than the other RF site types and call combinations.

For any 3600 site other than digital simulcast, follow these recommendations.

Table 2: IMBE Jitter Buffering Age (ms) for 3600 Sites (Non-Digital Simulcast)

| IP Data Packet Variation Based on Y.1541 Standard in (ms) | Recommended Timer Value (ms) |
|---|---|
| 5 | 35 (default) |
| 10 | 45 |
| 15 | 55 |
| 20 | 65 |
| 25 | 75 |
| 30 | 85 |
| 35 | 95 |
| 39 | 100 |

For 3600 digital simulcast sites, follow these recommendations.

Table 3: IMBE Jitter Buffering Age (ms) for 3600 Digital Simulcast Sites

| IP Data Packet Variation Based on Y.1541 Standard in (ms) | Recommended Timer Value (ms) |
|---|---|
| 5 | 55 |
| 10 | 65 |
| 15 | 75 |
| 20 | 85 |
| 25 | 95 |
| 29 | 100 |

### 4.2.2
## Configuring the SmartX Site Converter in the UNC

**When and where to use:**
Once the SmartX Site Converter is discovered in the system and the OS and software are installed, follow this procedure 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. SeeConfiguring the SmartX Site Converter Channels in the UNC Wizard on page 84 to configure channels.

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 EMC Smarts™ Network Configuration Manager application.

**NOTICE:** 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:**

1. 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.

   After the UNC client launches, a login dialog box appears.

2. Type the administrative user name and password. Click **OK**.

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

   **EMC Smarts Network Configuration Manager** launches.

3. Select the **Network View** tab.

   The **UNC** window appears.

4. To open the list of available converter devices, select **Networks** → **Astro 25 Radio Network** → **Views** in the navigation pane.

   The list of options expands.

5. Double-click **Motorola SmartX Site Converters** from the navigation pane.

   The list of options expands.

6. Right-click the desired SmartX device or devices.
7. Select **Properties**, then select the **Communications** tab. If needed, use **Update Credentials** to:
   - Ensure that a Management Mechanism (protocol) appropriate for your organizations 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 EMC Smarts™ Network Configuration Manager Management Account credential for this device matches the local user name and password for this device. For information on adding and modifying EMC Smarts™ Network Configuration Manager credentials, search on “Credentials Manager” in the *Unified Network Configurator* manual.
8. Return to the **Motorola SmartX Site Converters** view and right-click the SmartX device or devices again.

   A pop-up menu appears.

9. Select **Editor** from the menu.

   A submenu appears.

10. Select **Configlet** from the menu.

    The **Configlet Editor** appears.

**CAUTION:** 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.

11 Click inside the **Common Configlet** section, then select the **Insert Template** icon from the menu bar.

A **Select Item** window appears.

12 Select **System** → **Motorola** → **SmartX**, then open the **Template - Motorola SmartX Site Converter - Update Site Parameters** template.

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**. If you do not set the ntp_active to **True**, the device fails the audit and is flagged as non-compliant.
- **Site Type**. 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**. 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 ulaw, both devices are configured the same.
- **Line Length**
- **Line Impedance**
- **Site ID**

**NOTICE:** This parameter is set based on measuring worst case jitter scenarios between a sourcing IP device and the destination SmartX Site Converter. Increasing this timer increases call delay. Setting the timer too low results in audio gaps in the transmit signaling. The recommended timer values for the IMBE Jitter Buffering Age (ms) parameter differ depending on whether the 3600 site is digital simulcast or not. See Jitter Configuration for 3600 Sites on page 79 for the recommended settings.

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

14 Click inside the **Common Configlet** section. Click **Insert Template** on the menu bar.

**15** Select **System** → **Motorola** → **SmartX**, then open the **Template - Motorola SmartX Site Converter - Add Line Interface** template.

The **Template Variable Substitution** window opens.

**16** Configure the **Line Interface_Index**. Click **OK**.

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

**17** Click **Insert Template** from the menu bar, then select **System** → **Motorola** → **SmartX**, then open the **Template - Motorola SmartX Site Converter - Add Site Controller Link** template.

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**.

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

**19** Click **Insert Template** from the menu bar, then select **System** → **Motorola** → **SmartX**, then open the **Template - Motorola SmartX Site Converter - Add ZC Site Link Path** template.

The **Template Variable Substitution** window opens.

**20** Configure the **ZC_Site_Link_Path_Index IP Address**. Click **OK**.

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

**21** Click **Schedule**.

The **Schedule Push Job** window appears.

**22** Configure the schedule information. Click **Approve and Submit**.

**NOTICE:** If you choose **Submit**, you are asked to approve the job later.

This approves the job and you can view it in the **Schedule Manager** window.

**23** Press **F7** (Schedule Manager).

The **Schedule Manager** window appears in the UNC with the discovery jobs.

**24** Verify that the **Zone** and **Site** containers include SmartX Site Converter device(s) discovered.

**NOTICE:** No sites should be in the **Lost and Found** folder. If there are, see the *Unified Network Configurator* manual for troubleshooting guidance.

**25** Refresh the **Network Device View** to get the most accurate results, verify that the site converter is compliant.

**NOTICE:** Non-compliant devices show a red circle with a line through it.

**26** If the site converter is not compliant, follow these steps:

**a** Right-click the device, the choose **Compliance Audit**.

**b** Select the appropriate **Zone** folder.

**c** Select the appropriate **Site** folder.

**d** Select the available **Site Standard**, and then the compliance results appear and contain any proposed remedies.

e Choose **Schedule** to push the recommended changes to the device, otherwise examine and make corrections to configuration as necessary.

### 4.2.3
## Configuring the SmartX Site Converter Channels in the UNC Wizard

The following procedure defines the channels in the ASTRO® 25 system.

**When and where to use:** The SmartX Site Converter channels are configured in the UNC Wizard. The following procedure describes how to define the channels.

**Procedure:**

1 Log on to the **UNC Wizard** from the NM client, by double-clicking the **Internet Explorer** icon on the desktop.

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**.

The **UNC Wizard** launches and a login dialog box appears.

3 Type the administrative user name and password. Click **OK**.

The **UNC Wizard** appears.

4 Select **Channel** located within **RF Site Level Configuration** section.

| If… | Then… |
|---|---|
| **If there are multiple zones,** | select a **Zone ID**. |
| **If there is a single zone,** | select a **Site**. |

**NOTICE:** A single zone automatically displays the available sites.

5 Select a **Site ID**.

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**.

**NOTICE:** If invalid data is entered, you must correct the problem and resubmit the configuration.

Channel audit is run behind the scenes and a remedy is scheduled in the Schedule Manager to match the Channel Wizard data.

9 Approve or deny any new remedies in the **Schedule Manager**.

| 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… | Then… |
|---|---|
| **If a remedy does not exist,** | indicate that the device configuration matches the Channel Wizard. |

**NOTICE:** You can run site level audits to confirm compliance. Channel audits are formed based on the Channel Wizard configuration.

10 Verify the channel configuration by refreshing the device view and ensure that the timestamp is accurate with the latest configuration.

4.3

# Configuring the SMARTNET/SmartZone Devices in the Network Management Applications

Configure the 3600 sites and channels in the Unified Network Configurator (UNC) and Provisioning Manager (PM) so that the zone controller can interface with these 3600 RF sites for call processing.

**Prerequisites:** Ensure you have the following information to complete this process.

- Access to the Unified Network Configurator and Provisioning Manager applications.
- A valid trespass protection ID number.
- Access to the 4.1 system database.

**When and where to use:** . Perform this process after the SmartX Site Converter is installed in the ASTRO® 25 system.

**Process:**

1 Add a 3600 site in the UNC. See Adding and Configuring 3600 Sites and Channels on page 85.

2 Add a 3600 channel in the UNC. See Adding a 3600 Channel on page 87.

3 Define a valid trespass protection ID list in the UNC. See Defining the Valid Trespass Protection ID List on page 88.

4 Configure modulation mapping in the PM. See “Subscriber Modulation Map” in the *Provisioning Manager* manual for the parameters required.

5 Migrate the security groups from the 4.1 database to 7.x. Contact the Motorola Solutions Support Center if you require assistance.

The 3600 sites and channels appear in the Unified Network Configurator (UNC) and Provisioning Manager (PM) and the ASTRO® 25 system zone controller can interface with the sites.

4.3.1

## Adding and Configuring 3600 Sites and Channels

**When and where to use:**
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. The following procedure describes how to add a 3600 site with 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.

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

**Procedure:**

1. Log on to the **Unified Network Configurator Wizard**.

   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**.

   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.

   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.

   The **Site Configuration Wizard** screen appears.

8. In the **Site Configuration Wizard**, edit the following parameters for a 3600 channel:
   - **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**

   **NOTICE:** Any changes made to site parameters cause an update to the business rules stored in EMC Smarts™ Network Configuration Manager.

9. Open the **Schedule Manager** and approve and submit any jobs that may have been created due to updates submitted here.
10. Configure the newly added 3600 site as an adjacent site in the **Unified Network Configurator System Wizard**.

    **IMPORTANT:** The 3600 sites can only be adjacent to other 3600 sites.

    **NOTICE:** 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.

11 Click **Publish Infrastructure Data** to synchronize the data between the UNC and the Provisioning Manager and transfer the new site information to the Provisioning Manager.

The site is fully operational on the system.

12 Add the 3600 site to the **Radio Site Access Profile** record. See “Radio Site Access Profile Parameters” in the *Provisioning Manager* manual.

13 Add the 3600 site to the **TG/MG Site Access Profile** record. See “TG/MG Site Access Profile Parameters” in the *Provisioning Manager* manual.

### 4.3.2
## Adding a 3600 Channel

The following procedure describes how to add a 3600 channel in the ASTRO® 25 7.x system in the UNC application.

**Procedure:**

1 Log on to the **Unified Network Configurator Wizard**.

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** → **RF Site Level Configuration**.

The right side of the window updates.

3 Select the **Zone ID** of the zone in which you want to add the channel.

The available channels at the site are listed.

4 Select the **Site ID** of the SmartX site.

The **Channel Configuration** form appears displaying the list of available channels.

5 Click **Add Row**.

A new row appears in the table.

6 Edit the following parameter for a 3600 channel:

- **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**

**NOTICE:** Any changes made to channel parameters cause an update to the business rules stored in EMC Smarts™ Network Configuration Manager.

7 Select **Tools** → **Schedule Manager** and approve and submit any jobs that may have been created due to updates submitted here.

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.

The channel is fully operational on the system.

### 4.3.3
## Defining the Valid Trespass Protection ID List

The following procedure 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, the additional sites can result in several system IDs appearing on the system. Since only one system ID is allowed in an ASTRO® 25 system, inform the system of other possible IDs that are allowed.

**Prerequisites:** See “Subscriber Modulation Map” in the *Provisioning Manager* manual for the parameters required to configure subscriber modulation mapping in the Provisioning Manager.

**When and where to use:** Perform the following procedure 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.

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

**Procedure:**

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.

3 Enter the valid system ID (hex) for the 3600 site.

4 Click **Submit** to save your additions or changes to the UNC Server.

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

### 4.4
# SmartX Site Converter Fault Monitoring

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.

### 4.4.1
## Discovering the SmartX Site Converter Devices with the UEM

The following procedure discovers the SmartX Site Converter and allows the Unified Event Manager to fault manage these devices.

**Procedure:**

1 To log on to the UEM from the NM client, double-click the **Internet Explorer** icon on the desktop.

2 Enter: `http://z<xxx>uem01:9090` in the **Address** field.

where **<*xxx*>** is where you need to identify the zone ID for the discovered devices.

3 Enter the appropriate admin user name and password. Click **OK**.

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**.

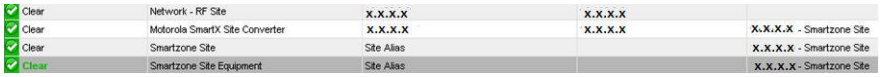
The **Discovery Status** dialog box appears with the job number for the discovery.

7 Click **View Job Status**.

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.

**Figure 22: SmartX Site Converter Discovery in the UEM**




You can view the log to verify that all devices were discovered.

### 4.4.2
## Verifying System Installation with the UEM

The following procedure describes how to use the Unified Event Managers 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:**

1 To log on to the **UEM** from the NM client, double-click the **Internet Explorer** icon on the desktop.

2 Enter: `http://z<xxx>uem01:9090` in the Address field.

where **<*xxx*>** is where you need to identify the zone ID for the discovered devices.

3 Enter the appropriate user name and password. Click **OK**.

The **UEM** main window appears.

4 Open the **Physical Detail View** map, and choose **SmartX Site Network**.

5 Choose **View Alarms**.

6 Verify the health of the system, including that

- 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.

8 Choose **SmartX Site ID**.

9 Choose **View Group Alarms**.

10 Verify the health of the system, including that

- wide trunking is enabled.
- site converters enabled.
- the site link up.
- the ZC link up.
- only clear, warning, and minor alarms appear.

## 4.5 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 three are additional remote site considerations:

1 ASTRO® 25 link specifications must be met if the SmartX Site Converter and site gateway are at the RF remote site.

2 Temperature range of SmartX Site Converter is 5 to 40 degree 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 not, 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.

4.5.1

## Connecting the SmartX Site Converter and the Channel Bank

The following procedure describes how to connect the site converter to the channel bank, which enables communication with the remote site.

**Prerequisites:** See the “SmartX Site Converter Reference” chapter for the E1/T1 pinout and cabling information.

**Procedure:**

1. Before connecting the SmartX Site Converter to the channel bank, verify the following:
   - 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 **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 as part of the RF Site object in the UNC. For ulaw, both devices are configured the same.
2. Connect the E1/T1 lines to appropriate channel bank.

   **NOTICE:** E1/T1 line 1 is the lower-right port and E1T1 line 2 is upper-right port.

3. To confirm the connection, log in to one of the following applications:
   - Unified Network Configurator (UNC) and perform a discovery of the SmartX Site Converter.
   - Unified Event Manager (UEM) and verify the following:
     - 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.

Chapter 5

# SmartX Site Converter Optimization

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

## 5.1 T1/E1 Optimization

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

## 5.2 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.

Chapter 6

# SmartX Site Converter Operation

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

6.1

## Turning On a SmartX Site Converter

The SmartX Site Converter does not have an on/off switch. The device is activated by supplying power. Perform the following procedure to apply power to the SmartX Site Converter and verify that it is working.

**Prerequisites:**

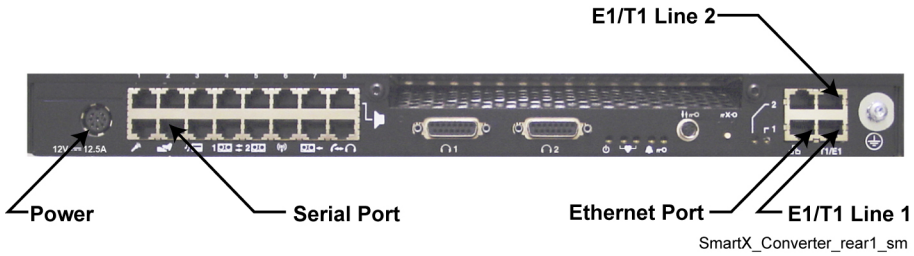
**WARNING:** Before performing this procedure, always make sure that power line cord is not connected to an AC source.

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

**Procedure:**

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

   **Figure 23: 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 “SmartX Site Converter Reference” chapter.

6.2

## Turning Off a SmartX Site Converter

Perform the following procedure to power down the SmartX Site Converter.

**Procedure:**

1. Disconnect the power line cord from the AC source.
2. Disconnect the power supply 12V output cable from the rear of the SmartX Site Converter chassis.

6.3
# SmartX Site Converter Reset

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

1 Rebooting the hardware.

2 Issuing a command from the Configuration/Service Software (CSS).

3 Issuing a command from the Unified Event Manager (UEM).

6.3.1
## Rebooting the SmartX Site Converter by Power Cycling the Hardware

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:**

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.

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 that the power LED is on.

The Power LED is green when the reboot completes.

6.3.2
## Rebooting the SmartX Site Converter in the CSS

The following procedure provides a method to reset the hardware is to reset the SmartX Site Converter in the Configuration/Service Software (CSS) application.

**Procedure:**

1 Launch the **CSS** application using a serial connection. See the “SmartX Site Converter Installation” chapter.

2 Select **Tools** → **Set IP Address and Box Number**.

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** to proceed with the reset.

The SmartX Site Converter restarts.

**Postrequisites:** Proceed to Changing SNMPv3 Configuration and User Credentials on the SmartX Site Converter on page 68 and reconfigure the SNMPv3 credentials.

6.3.3
## Rebooting the SmartX Site Converter in the UEM

The Unified Event Manager provides an option for resetting the SmartX Site Converter.

**Procedure:**

1. Launch the **Unified Event Manager**.
2. From the **Network Database** link, right-click on the **SmartX Site Converter** device.
3. Choose **Command**.
4. Select the entity associated with the device.
5. Choose **Reset**. Click **Apply**.

   The cursor changes into an hour glass when the process is initiated and it changes to normal when the process is completed.

## 6.4 SmartX Site Converter Log On

The SmartX Site Converter does have a default service account for the initial log on to the device, 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, log on, and password the first time you connect to the device. See the “SmartX Site Converter Installation” chapter.

## 6.5 Accounts Administration

You can set up a local password for the SmartX Site Converter in the Configuration/Service Software (CSS).

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 4: SmartX Site Converter Accounts on page 97 provides the user accounts and the network management application that can be used to set or change them.

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

Table 4: 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 (example, 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 Configuration/ Service Software (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. |

*Table continued…*

| Type of Account | Description and Network Management Application Used |
|---|---|
| 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 Configuration/Service Software. |
| 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. | |

6.6

## Restoring a SmartX Site Converter Configuration

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 this procedure. 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.

**NOTICE:** 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.

**When and where to use:** When you install and configure a SmartX Site Converter in 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.

**Procedure:**

1. Log on to the **EMC Smarts™ Network Configuration Manager** application.

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

   The **EMC Smarts™ Network Configuration Manager** main window appears.

2. From the **Devices View** menu bar, select **Device**.
3. Click **Config**.

   The **Configuration** window opens.

4. Change the configuration and click **Audit**.
5. Select one or more devices you want to audit.
6. Click **Audit**.

   The **Select the Items** window appears.

7. Select the following items:
   a. Select the **Zone** in which the device is located.
   b. Select the **Site ID** in which your device is located.
   c. Select the **Site Standard**.

8 Click **Select Item**.

The **Compliance Audit Results** window appears.

9 In the **Compliance Audit Results** window, perform one of the following actions:

| If… | Then… |
|---|---|
| **If the changes are valid,** | the device appears in the **Compliant** pane. Close the **Compliance Audit Results** window. |
| **If the changes are not valid,** | the device appears in the **Non-Compliant** pane. Perform the following actions:<br>**a** Select the device.<br>**b** Select **Preview**.<br>**c** In the Remedy Preview window, scroll the slider bar in the **Test Results** pane to find all red Xs.<br>**d** Select the red **X**.<br>**NOTICE:** The **Remedy Configlets** pane contains the lines of the configuration that must change to bring the device into compliance.<br>**e** Make the changes in the configuration window and rerun the audit. |

10 In the navigation pane, expand **Networks** and select **Astro 25 Radio Network**.

11 Double-click **Devices**.

The **Devices** (view) appears showing a list of devices in the contents pane.

12 Right-click the SmartX Site Converter whose configuration baseline you want to verify, then choose **Properties** from the pop-up menu.

13 Click the **History** tab.

The list of Baselines appears.

14 On the right side in the **History** tab, select the **Baseline** tab.

The name of the baseline displays.

15 Select the revision to be used instead of the current one.

**NOTICE:** See “Determining Which Version Is Currently the Baseline” in the *Unified Network Configurator* manual if you are not sure how to determine the devices baseline.

16 Click **Roll Back**.

The **Schedule Job** window appears.

17 Type the job name and schedule the job.

18 Click **Approve Submit** or click **Submit** , depending on your permissions.

**NOTICE:**

- 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 **EMC Smarts™ Network Configuration Manager** main window.
- If you clicked **Submit**, the status of the job is Pending. You can approve Pending jobs on the **Schedule Manager** window.

**19** Close the **Edit Network Properties** window.

**20** From the **Tools** menu, select **Schedule Manager** to view the pending rollback.

## 6.7 SmartX Site Converter Status in Network Managers

The operational status of the SmartX Site Converter is available within the network manager (UNC) and the fault manager (UEM).

### 6.7.1 SmartX Site Converter 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.

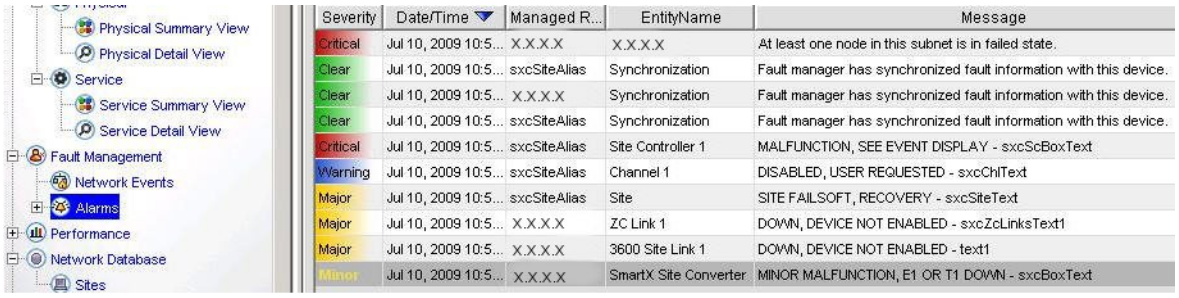
**SmartZone Site Equipment**
Site Controller equipment, communication, sub-site, and channel status.

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 on) and 3600 site faults are reported by the SmartX Site Converter. The following image depicts SmartX Site Converter alarms in the UEM.

**Figure 24: SmartX Site Converter Alarms in the UEM**

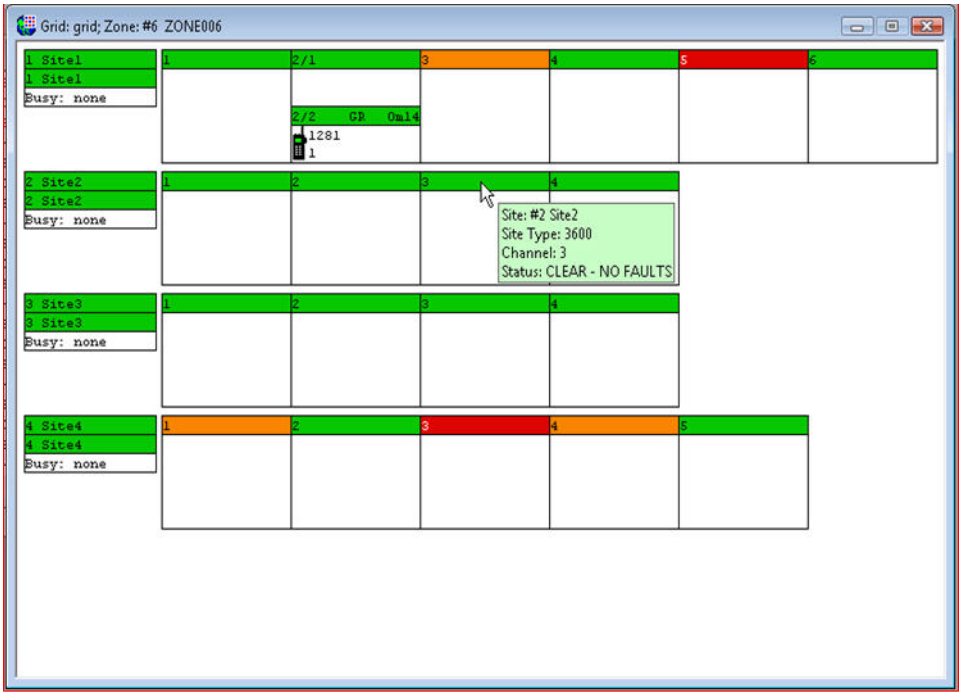



#### 6.7.1.1 3600 Site Status in ZoneWatch

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 this image.

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 used in the 9600 sites is due to differences in infrastructure management.

**Figure 25: 3600 Site Status in ZoneWatch**




### 6.7.2
## Viewing SmartX Site Converter Status in the UNC

The EMC Smarts™ Network Configuration Manager 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. You must schedule these remedy jobs manually.
The “UNC Operation” chapter of the *Unified Network Configurator* manual also describes how to generate an audit report and make devices compliant.

**Procedure:**

1 Log on to the **EMC Smarts Network Configuration Manager** application.

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

The **EMC Smarts Network Configuration Manager** main window appears.

2 In the navigation pane of the main **Unified Network Configurator** window, expand **Networks** and select the **Astro 25 Radio Network**.

3 Double-click **Devices**.

The diagram of devices appears in the right pane.

4 In the right pane upper menu, click **Table**.

The list of devices is populated in a table.

5 Click the **Status** column to sort devices by their status.

6 Scroll down to see SmartX Site Converters compliance status.

This page intentionally left blank.

Chapter 7

# SmartX Site Converter Maintenance

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

## 7.1 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.

## 7.2 SmartX Site Converter 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 hardware as a system upgrade.

This page intentionally left blank.

Chapter 8

# SmartX Site Converter Troubleshooting

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

## 8.1 SmartX Site Converter General Troubleshooting

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

### 8.1.1 Software Download Manager to the SmartX Site Converter Troubleshooting

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

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

The SNMPv3 user credentials can be reset to the default values at the remote site when necessary.

**Prerequisites:**
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 in, you use the defined Central Authentication credentials (user name and password).

**When and where to use:** 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 this procedure if you are at the site and have direct access to the device.

**CAUTION:** 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:**

1. Launch the **Configuration/Service Software** (CSS) application using a serial connection. See the “SmartX Site Converter Installation” chapter.
2. Log on with the local service account user name and password.
3. Type the **Elevated Privileges** password for administrative level access in the appropriate field.

   **NOTICE:**
   The device manages the Elevated Password Privileges password required for performing operations requiring administration level access. If you fail to elevate privileges, you cannot access or execute the mechanisms utilized to reset the SNMPv3 configuration and credentials.

4 Click **OK**.

A confirmation dialog box appears telling you that CSS has connected with the device.

5 Click **OK**.

**IMPORTANT:** If you have provided the wrong user credentials, go back to step 2 and try again. Per the security policies for your organization, the device may limit the number of login attempts. If you fail to log in and exceed the maximum number of attempts, you may be locked out of the device for some time. Your policy defines the lockout time duration (default is 15 minutes).

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.

6 To reset the SNMPv3 user credentials to the factory default, select **Security** → **SNMPv3 Configuration (serial)** → **Reset SNMPv3 Configuration (serial)**.

The **SNMPv3 Configuration** dialog box appears.

7 Click **Reset SNMPv3 Configuration** → **Exit**.

The **Reset SNMPv3 Configuration** dialog box closes.

8 To reboot the device, select **Tools** in the main CSS window.

9 Select **Set IP Address/Box Number**.

The **Set IP Address/Box Number** dialog box appears.

10 Click **Reset**.

The device reboots.

11 In the main CSS window, select **File** → **Exit**. Click **OK** to confirm that you want to exit.

12 Monitor the LEDs on the SmartX Site Converter to verify that the device reboots.

**Postrequisites:** 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.

### 8.1.3
## Resetting the SNMPv3 User Credentials to Defaults on Devices at a Remote Site through Telnet/SSH

The SNMPv3 user credentials can be reset to the default values at the remote site even when you do not have direct access to the device.

**Prerequisites:** Obtain the Fully Qualified Domain Name (FQDN) of the SmartX Site Converter 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 Configuration/Service Software (CSS), Telnet, and SSH to configure RF site devices.

**When and where to use:** Execute this procedure if you are not at the remote site and do not have direct access to the device.

**Procedure:**

1 To connect and log on to the device remotely over the network, use the PuTTY terminal services to connect to the device using SSH or Telnet.

**NOTICE:** Depending on the security policy of your system and site configuration, SSH or Telnet may be enabled or disabled. Try SSH first, since it is the preferred secure remote access service. Ensure that you know the IP address of the device before proceeding with these steps.

A log on warning banner appears prompting for a user name.

2 Type the local service user login and password.

**IMPORTANT:**
If the user name or password prompt appears again, you have entered the wrong credentials and must try again. If your security policy requires the use of Central Authentication rather than using the local service account to log on, use your defined Central Authentication user name and password.

Per the security policies of your organization, the device may limit the number of login attempts. If you fail to log in and exceed the maximum number of attempts, you may be locked out of the device for some time. Your policy determines the lockout duration (default is 15 minutes).

The device displays the CSS or `]-0` command prompt.

3 Enter: `enablepriv –E`

The `enablepriv` command prompt appears for the elevated privileges password.

4 Enter: ***<elevated privileges password>*** to gain the administration level access.

**IMPORTANT:**
If the user name or password prompt appears again, you have entered the wrong credentials and must try again.

If you fail to elevate privileges, you cannot view, access, or execute the commands utilized to reset the SNMPv3 configuration and credentials.

The CSS or `]-0` command prompt appears.

5 Enter: `redefault_usm` to reset the SNMPv3 user credentials to factory defaults.

The device displays a status message followed by the CSS or `]-0` command prompt.

6 Enter: `reset`

The device reboots.

7 Close the PuTTY connection.

8 Monitor the LEDs on the SmartX Site Converter to verify that the device reboots.

**NOTICE:** 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.

### 8.1.4
## Device Passwords and SNMPv3 Passphrases

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

**NOTICE:** 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. The default values are treated as sensitive information and are provided to you through secured communication.

Table 5: 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 the SNMPv3 passphrases. | ✓ | X | See the *CSS Online Helps* "SNMPv3 User Configuration." | See the *CSS Online Helps* "Resetting Device Passwords." |
| You know the local login, but not the SNMPv3 passphrases. | X | ✓ | See the *CSS Online Helps* "Reset SNMPv3 Configuration (Serial)." | See the *CSS Online Helps* "Device Security Configuration – Security Services (Serial)." |
| You know both passphrases and the local service password. | ✓ | ✓ | See the *CSS Online Helps* "SNMPv3 User Configuration." | See the *CSS Online Helps* "Device Security Configuration – Security Services (Serial)." |
| You do not know SNMPv3 passphrase nor service account password. | X | X | Contact Motorola Solutions Support Center. | Contact Motorola Solutions Support Center. |

## 8.2 Local Tools Troubleshooting

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

### 8.2.1 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**.

### 8.2.2 Troubleshooting the Ethernet Connection to the SmartX Site Converter

The first step in troubleshooting the SmartX Site Converter with the Configuration/Service Software (CSS) is to retrieve the logs and software version table. 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. The reports may indicate some minor cabling issues 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**
Contains time-stamped status and alarm messages that a service technician can use to troubleshoot the SmartX Site Converter.

**Engineering**
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 the device.

**Procedure:**

1. Connect the laptop with CSS to the SmartX Site Converter through the Ethernet cross-over cable.
2. Choose **File** → **Read Configuration From Device**.

   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 *CSS Online Help* for details. Provide the required credentials.

   **NOTICE:** If Authentication Services is enabled in the Security Services Configuration window, enter a user name 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 the user name, Password, and Elevated Privileges Password, as they cannot be left blank.
4. Click **OK**.

   The **Connection Screen** appears.
5. Choose **Service** → **Status Report Screen**.

   The **Service Report Screen** appears.
6. Click **Refresh** to see new messages that have occurred since the window was opened.

   **NOTICE:** 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.
7. Save the log to a text file, then review the information.

   **IMPORTANT:** 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.”

### 8.2.3
## Accessing the Software Version Information in the CSS

The Configuration/Service Software (CSS) provides the software version for use during troubleshooting.

**Procedure:**

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.

### 8.2.4
## SmartX Site Converter Configuration Troubleshooting

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, and you need to retrieve them from the archive file or re-configured 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#. Before 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 there is a disaster, see the appendix in the *Network Time Protocol 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 *Network Time Protocol Server* manual for more information.

### 8.3
## SmartX Site Converter 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, or channel. If a low battery alarm appears in the UEM, perform the battery replacement procedure in the “SmartX Site Converter Field Replaceable Entity” 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.

8.4

## SmartX Site Converter Software Installation Troubleshooting

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.

8.5

## Call Processing Troubleshooting from the SmartX Site Converter Perspective

Table 6: SmartX Site Converter Troubleshooting Scenarios on page 111 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 6: SmartX Site Converter Troubleshooting Scenarios

| Problem | Recovery Action |
|---|---|
| ZC link(s) are down | • Check connectivity between the site converter and network (for example, discoverable in UNC and UEM, connect with CSS).<br>• Check that ZC link IP addresses are configured correctly (UNC pull).<br>• Check that the site converter is configured with the correct site ID (UNC pull).<br>• Check that site converter requested state is “enabled” in the UEM. |
| Site converter minor malfunction (indicates a T1/E1 is down) | • Check that the E1/T1 configuration matches the cabling (UNC pull)<br>• Check that the E1/T1 parameters match those parameters programmed in the channel bank (UNC pull, channel bank configuration)<br>• Check the T1/E1 reports in the technician log (CSS).<br>**NOTICE:** If only one T1 line is connected to the site converter, then only one should be configured. |
| Site converter state is disabled | Check that the site requested state is enabled in the UEM. |
| Site link(s) are down or are periodically unstable | • Check that the site link configuration matches that in the channel bank (UNC pull)<br>• Check the E1/T1 configuration (including the site type) is correct and matches the site type in the ZDS (UNC pull)<br>• Check that the hardware cabling matches expected configuration (physical inspection)<br>• Check that site converter requested state is “enabled” (UEM)<br>• Check that the ZC link is functioning (UEM) |

*Table continued…*

| Problem | Recovery Action |
|---|---|
| | • Check the SmartX Site Converter state (UEM)<br>• Check the T1/E1 reports in the technician log (CSS)<br>• 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 | Check the following in the UEM:<br>• site requested state is “Wide Trunking”<br>• ZC and site links are functioning<br>• channel states are good<br>• Site reports on transient faults<br>• If the 3600 site is an IR Site, verify that the UNC Wizard Site Type parameter is set to IR. |
| Channel state not enabled | Check the following in the UEM:<br>• Check that channel requested state is “enabled”<br>• Check for transient faults indicating the issue<br>Check the following with a UNC Pull:<br>• Check that channel configuration matches that of the channel bank<br>• Check T1/E1 parameters match the values expected by the channel bank |
| Calls are failing | Check the following in the UEM:<br>• Check the site state<br>• 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 mode has been 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. |
| Site converter is not discovered in the UNC | See the “UNC Troubleshooting” in the *Unified Network Configurator* manual. This chapter provides scenarios and describes what to do if the site converter appears in the Lost and Found folder in the EMC Smarts™ Network Configuration Manager application. |
| Site converter is not discovered in the UEM | See “UEM Troubleshooting” chapter in the *Unified Event Manager* manual. |
| Site audio distortion (unintelligible) | Ensure that the Line Idle Pattern field for the RF Site object in the UNC conforms to the following guidelines: |

*Table continued…*

| Problem | Recovery Action |
|---|---|
| | • If the Line Idle Pattern field is set to **a-law**, then the connected channel bank must be set to **a-inv** (inverse a-law).<br>• 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 state 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.

Chapter 9

# SmartX Site Converter FRE

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

## 9.1 SmartX Site Converter Hardware Replacement

The SmartX Site Converter is a Field Replaceable Entity (FRE). There are no Field Replaceable Units (FRUs) associated with this hardware. If a failure occurs, replace the module.

## 9.2 FRE Parts List

The following table provides the Field Replaceable Entity (FRE) parts that are required for 3600 trunked sites to operate on an ASTRO® 25 radio system.

**NOTICE:** 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 plus two 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 7: Field Replaceable Entities

| Component | Part Number | Replacement Procedure |
|---|---|---|
| SmartX Site Converter Module | B1936A | See Replacing the SmartX Site Converter on page 116. |
| 3V coin cell Lithium battery | 52858500100 (CR2450HR) | See Replacing the SmartX Site Converter Battery on page 117. |
| 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 Replacing the SmartX Site Converter on page 116. |
| DC Cable (connects 12 VDC | 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/RJ45 VPM Programming Adapter | 58009256065 | Not applicable. |

*Table continued...*

| Component | Part Number | Replacement Procedure |
|---|---|---|
| S2500 Router | ST2500 | See the *S6000 and S2500 Routers* manual. |
| GGM 8000 | TYN4001A | See the *GGM 8000 System Gateway* manual. |

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

## 9.3 Replacing the SmartX Site Converter

In the event of a a hardware failure, you can replace the SmartX Site Converter.

**Prerequisites:**
Locate the following information before performing this procedure:

- IP address for the site converter
- Account user names and passwords for (types of accounts)

  Contact your system administrator to obtain this information.

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.

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

**When and where to use:** Replace the SmartX Site Converter when the Voice Processor Module hardware malfunctions.

**CAUTION:** 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.

**Procedure:**

1. Disconnect the SmartX Site Converter power supply line cord from an AC source.
2. Disconnect the power supply 12V cable from the rear of the SmartX Site Converter chassis.
3. Remove the existing site converter:
   a. Label and disconnect all communication cabling from the site converter.
   b. Disconnect the ground cable from the rear of the chassis.
   c. Remove the screws securing the site converter to the rack.
   d. Pull out the site converter through the front of the rack.

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:

   a Install the replacement site converter in the rack and secure it with the screws that were previously removed.

   b Secure the ground cable to the ground location on the rear of the chassis.

   c Attach all communication cabling to the site converter.

**Postrequisites:** Proceed to “Installing 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.

## 9.4 SmartX Site Converter Battery Replacement

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

The following table lists the recommended time table for replacing the MACEs coin cell battery.

Table 8: Battery Replacement Time

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

### 9.4.1 Replacing the SmartX Site Converter Battery

This procedure describes how to replace the battery.

**When and where to use:** Perform this procedure once a year on a stored Voice Processor Module and every two years on a functional SmartX Site Converter.

**Procedure:**

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.

6 Lift up an exposed edge of the battery until it “pops” out of the holder and put the old battery aside.

**NOTICE:** When replacing the battery, make sure that its wider side is at the top.

7 Place the new battery carefully on top of the holder and with a slight rocking action, push it downward into the holder.

The battery clicks into place.

8 Reinstall and secure the site converters 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.

**Postrequisites:** Properly dispose of the old (Lithium) battery.

## 9.5 SmartX Site Converter Component Disposal

The Motorola Solutions 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 Solutions Infrastructure Depot Operations (IDO) for further troubleshooting and repair. Return any failed units to the Motorola IDO at 2214 Galvin Dr, Elgin, IL 60123. The field shop contacts the Motorola Solutions 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.

Chapter 10

# SmartX Site Converter Reference

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

## 10.1 SmartX Site Converter Specifications

The following table provides the SmartX Site Converter/Voice Processor Module hardware specifications.

Table 9: SmartX Site Converter Hardware Specifications

| SmartX Site Converter | Specifications |
|---|---|
| Environmental Operating Range | • 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).<br>• Is capable of being continuously operated over an ambient temperature range of 5 °C to 40 °C.<br>• 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 temp at the vent openings cannot exceed 40 °C. Allow ventilation of 6 inches on the sides, front, and back, and 0 on top and bottom. Do not operate the hardware in a closed cabinet due to heat build up. |

## 10.2 SmartX Site Converter Connector Diagrams

Figure 26: SmartX Site Converter T1/E1 Port Connector Pinout Diagram on page 120 shows the pinout connections for the SmartX Site Converter.

**Figure 26: SmartX Site Converter T1/E1 Port Connector Pinout Diagram**

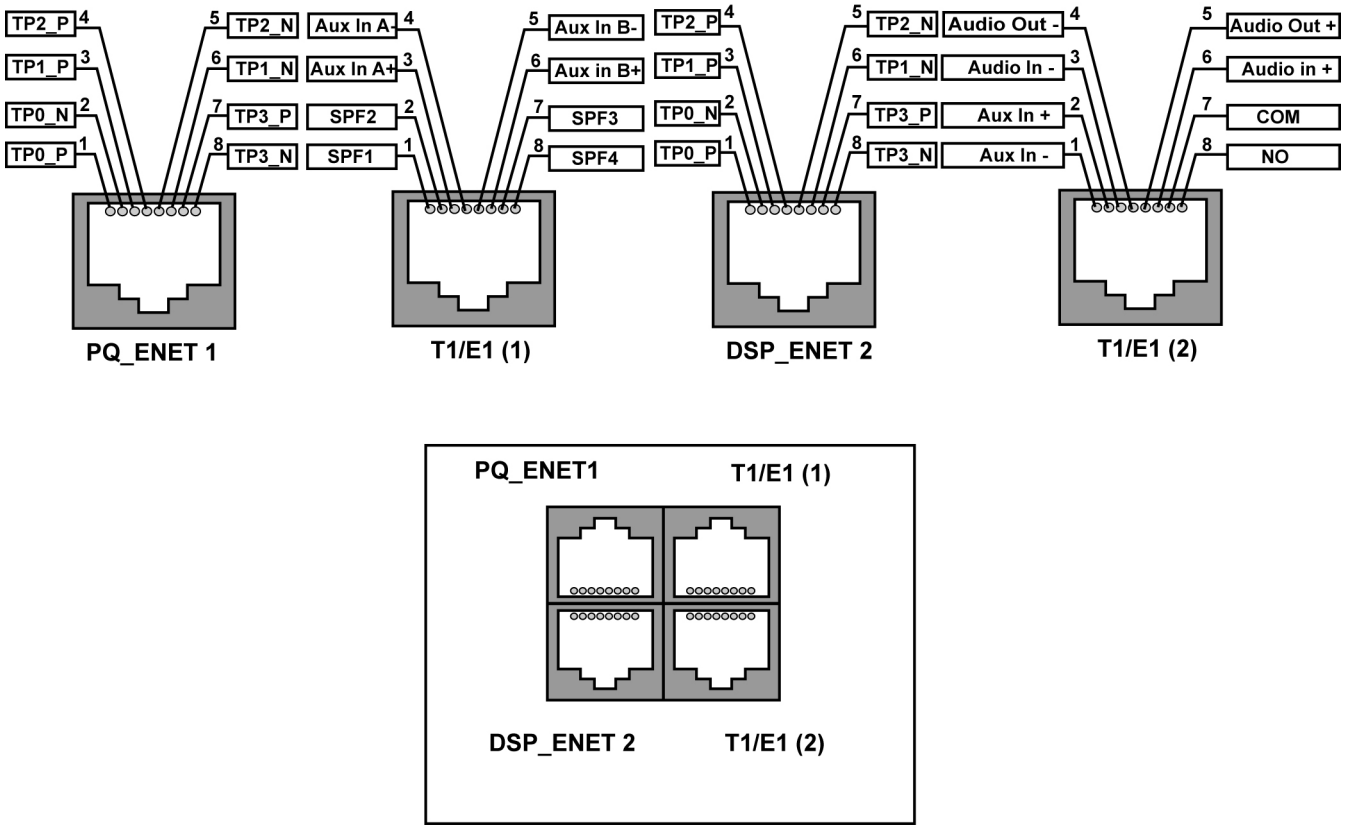



Table 10: E1/T1 Connections on page 120 shows the E1/T1 connections for the SmartX Site Converter.

Table 10: 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 11: SmartX Site Converter Serial Cable Connector Pinout on page 120 describes the serial cable connector used to configure the device in the Configuration/Service Software (CSS) application.

Table 11: SmartX Site Converter Serial Cable Connector Pinout

| DB9 | RJ-45 |
|---|---|
| 1 | |
| 2 | 8 |
| 3 | 1 |
| 4 | |

*Table continued…*

| DB9 | RJ-45 |
|---|---|
| 5 | 2 |
| 6 | |
| 7 | |
| 8 | |
| 9 | |

10.3
## SmartX Site Converter Ports to Function Map

The applicable ports include:

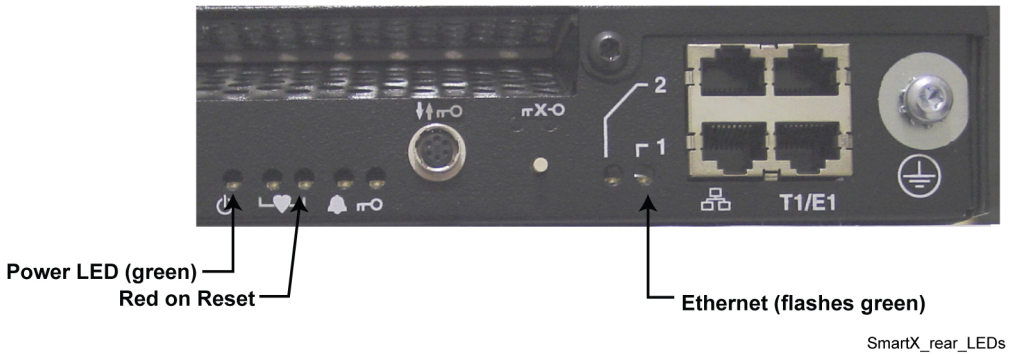
- AC power connection
- Serial port for connection to Configuration/Service Software
- Ethernet connector
- Two E1/T1 Line connectors

See Figure 2: Rear View of the SmartX Site Converter — Power Connection and Ports in Use on page 26 for location of these ports on the device.

10.4
## SmartX Site Converter LEDs

The SmartX Site Converter has five types of LEDs indicating the general conditions for the device and its Ethernet activities.

**Figure 27: SmartX Site Converter LEDs**




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

10.4.1
### Power LED

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

10.4.2
### Red on Reset LED

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

### 10.4.3
## Ethernet Activity LED

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

The following table explains the definitions for the SmartX Site Converter Ethernet Activity LED.

Table 12: 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 |

### 10.5
## SmartX Site Converter Cable Connections

The cross-over Ethernet cable connecting the SmartX Site Converter and site gateway and the TLine connections between SmartX Site Converter and the channel bank should comply with industry specifications. The lengths vary based on each organizations floor layout for their equipment.

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

Chapter 11

# 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.

## 11.1 Recovering the SmartX Site Converter

In event of a disaster or critical malfunction, follow this process to replace a SmartX Site Converter.

**When and where to use:** Use this process in the event of a disaster or critical malfunction of the hardware.

**Process:**

1. Remove the old SmartX Site Converter hardware. Install the new SmartX Site Converter hardware. See Installing the SmartX Site Converter Hardware on page 60.
2. Perform basic device configuration using the serial port. See Performing the Initial Configuration for the SmartX Site Converter on page 61.
3. Perform basic device configuration using the Ethernet port. See Configuring the SmartX Site Converter in the CSS (Ethernet Connection) on page 63.
4. Enable secure credentials.
   a. Set the SWDL transfer mode in the Configuration/Service Software. See Enabling Secure Software Download on page 64.
   b. Set the local password configuration. See Setting the SmartX Site Converter Local Password Configuration on page 65.
   c. Set the date and time in CSS. See Setting the Date and Time on the SmartX Site Converter on page 66.
   d. Set the serial security service. See Setting the Serial Security Services on page 67.
5. Complete the configuration of the Information Assurance features in the CSS, as follows:
   a. Create, update, or delete an SNMPv3 user. See Adding or Modifying SNMPv3 Users on page 70.
   b. Verify the SNMPv3 credentials. See Performing an SNMPv3 Connection Verification in the CSS on page 71.
   c. Configure DNS in the CSS. See Chapter 7 “Configuring DNS Using CSS” in the *Authentication Services* manual.
   d. Configure for SSH. See Chapter 4 “Configuring SSH for RF Site Devices and VPMs Using CSS – Overview” in the *Securing Protocols with SSH* manual.
   e. Configuring the local cache size for the SmartX Site Converter. See Chapter 7 “Setting the Local Cache Size for Centralized Authentication Using CSS” in the *Authentication Services* manual.
   f. Enable RADIUS authentication in the CSS. See Chapter 7 “Configuring RADIUS Sources and Parameters Using CSS” in the *Authentication Services* manual.

**g** Enable Centralized Authentication in the CSS. See Chapter 7 “Enabling/Disabling Centralized Authentication Using CSS” in the *Authentication Services* manual.

**h** Optionally, enable Centralized Event Logging in the CSS. See Chapter 6 “Enabling/Disabling Centralized Event Logging on Devices Using CSS” in the *Centralized Event Logging* manual.

**i** Customize the Login Banner in the CSS. See Customizing the Login Banner in the CSS on page 72.

**NOTICE:** 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 Connecting the SmartX Site Converter to the Site Gateway on page 72.

**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 Transferring and Installing the OS Image on page 76.

**9** Set up the SmartX Site Converter. See Configuring the SmartX Site Converter on page 79.